



2017

Cyber Security Solutions

Guneet Pahwa, B.Tech (IT)

Project Manager

CMAI TEMA

Prof N K GOYAL

President CMAI

Chairman Emeritus TEMA

www.cmai.asia

www.tematelecom.in

Contents

Acknowledgement	3
Digital India.....	4
Cashless India.....	5
Introduction	8
Major Cyber Attacks Past One Year.....	14
Cyber-Security Solutions	30
Antivirus & Mobile App Security.....	31
Authentication	41
Biometrics.....	50
Cryptography.....	57
Data Breach.....	63
Data Loss Prevention (DLP)	72
DDOS Attack Protection.....	84
Embedded System Security	94
Firewall.....	98
Fraud Detection and Prevention	105
IAM- Identity & Access Management	113
Incident Response	121
Intrusion Detection	128
Log Analysis & Management.....	135
Mainframe Security	140
Machine Learning Security- Adversarial Learning	142
Network Security Monitoring	147
Next Generation Firewall	154
Password Management	159
Patch Management	163
Penetration testing	167
Privileged Access Management (PAM)	178
Public Key Infrastructure (PKI)	186
Risk Analysis.....	193

SAP ERP Security.....	200
Software Development Security.....	205
Unified Threat Management.....	212
Web App & Website Security.....	215
WAF- Web Application Firewall	225
Wireless/Wi-Fi Security	230
Conclusion.....	241
Recommendations.....	242
References	244

Acknowledgement

"It is impossible to prepare a project report without the assistance & encouragement of other people. This one is certainly no exception."

We acknowledge information, data, and inputs from various sources of industry, government and media.

Cyber security is the need of the hour in India and this report is dedicated to the citizens of India.

Digital India

Digital India is a campaign launched by the Government of India to ensure that Government services are made available to citizens electronically by improved online infrastructure and by increasing Internet connectivity or by making the country digitally empowered in the field of technology.

It was launched on 2 July 2015 by Honorable Prime Minister Dr Narendra Modi. The initiative includes plans to connect rural areas with high-speed internet networks. Digital India consists of three core components. They are:

- The creation of digital infrastructure
- Delivery of services digitally
- Digital literacy

Digital Technologies which include Cloud Computing and Mobile Applications have emerged as catalysts for rapid economic growth and citizen empowerment across the globe. Digital technologies are being increasingly used by us in everyday lives from retail stores to government offices. They help us to connect with each other and also to share information on issues and concerns faced by us. In some cases they also enable resolution of those issues in near real time.

The objective of the Digital India Group is to come out with innovative ideas and practical solutions to realise Prime Minister Modi's vision of a digital India. Prime Minister Modi envisions transforming our nation and creating opportunities for all citizens by harnessing digital technologies. His vision is to empower every citizen with access to digital services, knowledge and information. This Group will come up with policies and best practices from around the world to make this vision of a digital India a reality.

Cashless India

The Digital India program is a flagship program of the Government of India with a vision to transform India into a digitally empowered society and knowledge economy.

“Faceless, Paperless, Cashless” is one of professed role of Digital India.

As part of promoting cashless transactions and converting India into less-cash society, various modes of digital payments are available.

These modes are:

Banking Cards (DEBIT / CREDIT / CASH / TRAVEL / OTHERS)

Banking cards offer consumers more security, convenience, and control than any other payment method. The wide variety of cards available – including credit, debit and prepaid – offers enormous flexibility, as well. These cards provide 2 factor authentication for secure payments e.g. secure PIN and OTP. RuPay, Visa, MasterCard are some of the example of card payment systems. Payment cards give people the power to purchase items in stores, on the Internet, through mail-order catalogues and over the telephone. They save both customers and merchants' time and money, and thus enable them for ease of transaction.

USSD

The innovative payment service *99# works on Unstructured Supplementary Service Data (USSD) channel. This service allows mobile banking transactions using basic feature mobile phone, there is no need to have mobile internet data facility for using USSD based mobile banking. It is envisioned to provide financial deepening and inclusion of underbanked society in the mainstream banking services.

*99# service has been launched to take the banking services to every common man across the country. Banking customers can avail this service by dialling *99#, a “Common number across all Telecom Service Providers (TSPs)” on their mobile phone and transact through an interactive menu displayed on the mobile screen. Key services offered under *99# service include, interbank account to account fund transfer, balance enquiry, mini statement besides host of other services. *99# service is currently offered by 51 leading banks & all GSM service providers and can be accessed in 12 different languages including Hindi & English as on 30.11.2016 (Source: NPCI). *99# service is a unique interoperable direct to consumer service that brings together the diverse ecosystem partners such as Banks & TSPs (Telecom Service Providers).

Aadhaar Enabled Payment System (AEPS)

AEPS is a bank led model which allows online interoperable financial transaction at PoS (Point of Sale / Micro ATM) through the Business Correspondent (BC)/Bank Mitra of any bank using the Aadhaar authentication.

UPI

Unified Payments Interface (UPI) is a system that powers multiple bank accounts into a single mobile application (of any participating bank), merging several banking features, seamless fund routing & merchant payments into one hood. It also caters to the "Peer to Peer" collect request which can be scheduled and paid as per requirement and convenience. Each Bank provides its own UPI App for Android, Windows and iOS mobile platform(s).

Mobile Wallets

A mobile wallet is a way to carry cash in digital format. You can link your credit card or debit card information in mobile device to mobile wallet application or you can transfer money online to mobile wallet. Instead of using your physical plastic card to make purchases, you can pay with your smartphone, tablet, or smart watch. An individual's account is required to be linked to the digital wallet to load money in it. Most banks have their e-wallets and some private companies. e.g. Paytm, Freecharge, Mobikwik, Oxigen, mRuppee, Airtel Money, Jio Money, SBI Buddy, itz Cash, Citrus Pay, Vodafone M-Pesa, Axis Bank Lime, ICICI Pockets, SpeedPay etc.

Banks pre-paid cards

A card issued by a financial institution that is preloaded with funds and is used like a normal credit card. A prepaid credit card works in the opposite way of a normal credit card, because instead of buying something with borrowed funds (through credit), you buy things with funds that have already been paid. This card functions like a gift card.

Point of sale

A point of sale (PoS) is the place where sales are made. On a macro level, a PoS may be a mall, a market or a city. On a micro level, retailers consider a PoS to be the area where a customer completes a transaction, such as a checkout counter. It is also known as a point of purchase.

Internet Banking

Internet banking, also known as online banking, e-banking or virtual banking, is an electronic payment system that enables customers of a bank or other financial institution to conduct a range of financial transactions through the financial institution's website.

Mobile Banking

Mobile banking is a service provided by a bank or other financial institution that allows its customers to conduct different types of financial transactions remotely using a mobile device such as a mobile phone or tablet. It uses software, usually called an app, provided by the banks or financial institution for the purpose. Each Bank provides its own mobile banking App for Android, Windows and iOS mobile platform(s).

Micro ATMs

Micro ATM meant to be a device that is used by a million Business Correspondents (BC) to deliver basic banking services. The platform will enable Business Correspondents (who could be a local kirana shop owner and will act as 'micro ATM') to conduct instant transactions.

The micro platform will enable function through low cost devices (micro ATMs) that will be connected to banks across the country. This would enable a person to instantly deposit or withdraw funds regardless of the bank associated with a particular BC. This device will be based on a mobile phone connection and would be made available at every BC. Customers would just have to get their identity authenticated and withdraw or put money into their bank accounts. This money will come from the cash drawer of the BC. Essentially, BCs will act as bank for the customers and all they need to do is verify the authenticity of customer using customers' UID. The basic transaction types, to be supported by micro ATM, are Deposit, Withdrawal, Fund transfer and Balance enquiry.

Introduction

This report is in continuation to the report titled "Cyber Business Security-Threats and Solutions", available at <http://cmai.asia/cybersecurity/docs/CyberBusinessSecurityTheatsSolutions.pdf>, published in November 2015.

Abstract from the above report:

"CYBER INSECURITY a major threat to businesses today:

Along with the world, which continues to embrace the ever evolving technology and its advantages, businesses have also started relying on technology extensively for storing great amount of sensitive data electronically. The ease in storing and accessing information has led to its increasing popularity. Along with the efficiencies the computer brings to the life of many, it has inadvertently created a new area of risk. The storage of sensitive information on computers opens business up to cyber-attacks, with hackers looking to acquire company or customer information such as passwords or credit card numbers. The hackers can then use or sell this information, harming businesses, consumers, and company reputations.

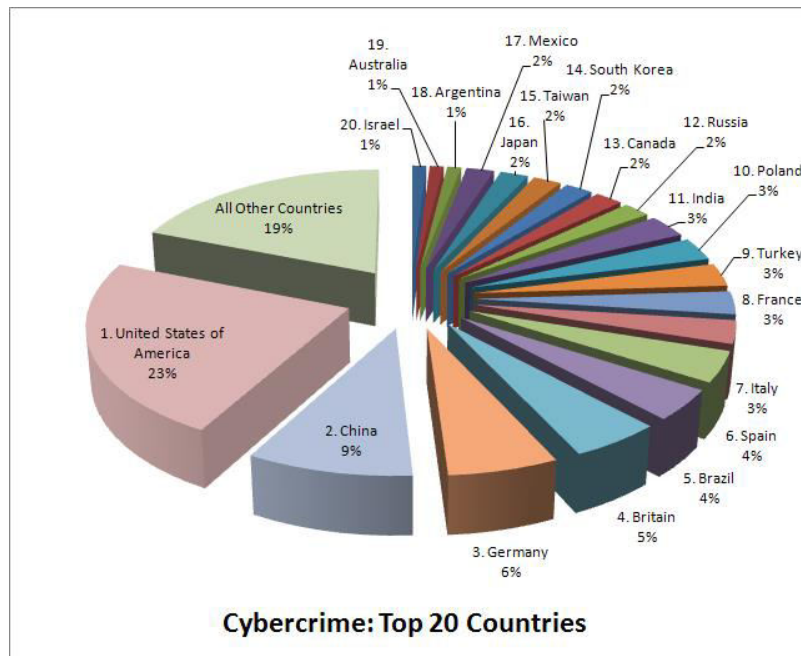
Many high profile security breaches have highlighted the issue of Cyber-Attacks. These attacks have left companies struggling to improvise on these issues, but what becomes an even major problem is regaining the trust of the customers and reassuring them that their sites and accounts are safe from any further attacks.

Cyber-crime today, has become a business, and the hackers are looking for real dollars, & this business is expanding day by day. Various businesses, big or small fall into this trap every day."

In this part of the report, the topic at hand is, all the solutions available in the market as of now to safeguard ourselves against cyber-attacks, the solutions individuals as well as organizations can use before, during and after the cyber-attacks to curb the effects of cyber-attacks since eliminating it all together is not possible.

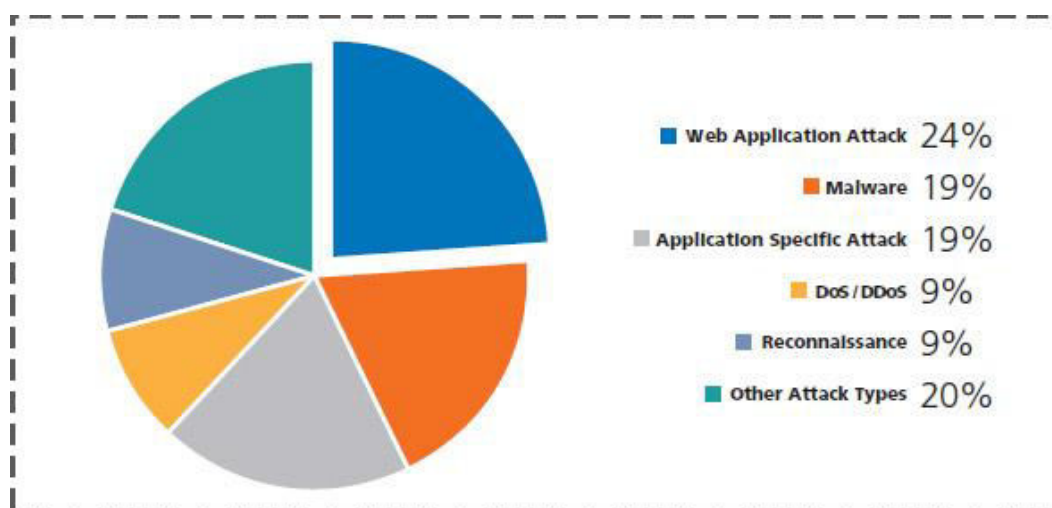
Spread of cyber-crime across nations

The popularity of internet has been growing day by day and today it is no more a luxury but a necessity. Agreeing to this fact, Internet brings along with it consequences, cyber-crime that affect everyone across the globe. Top 20 countries, worst affected by cyber-attacks are:



Most popular cyber attacks

2016 saw many cyber-attacks and the statistics go like:



Cyber-attack No. 1: Socially engineered Trojans

Socially engineered Trojans provide the No. 1 method of attack (not an exploit or a misconfiguration or a buffer overflow). An end-user browses to a website usually trusted -- which prompts him or her to run a Trojan. Most of the time the website is a legitimate, innocent victim that has been temporarily compromised by hackers.

Usually, the website tells users they are infected by viruses and need to run fake antivirus software. Also, they're nearly out of free disk space and need a fake disk defragger. Finally, they must install an otherwise unnecessary program, often a fake Adobe Reader or an equally well-known program. The user executes the malware, clicking past browser warnings that the program could possibly be harmful. Voilà, exploit accomplished! Socially engineered Trojans are responsible for hundreds of millions of successful hacks each year. Against those numbers, all other hacking types are just noise.

Countermeasure: Social engineered Trojans are best handled through end-user education that's informed by today's threats (such as trusted websites prompting users to run Trojans). Enterprises can further protect themselves by not allowing elevated users to surf the Web or answer email. An up-to-date antimalware program can't hurt, but strong end-user education provides better bang for the buck.

Cyber-attack No. 2: Unpatched software

Coming in a distant second is software with known, but unpatched exploits. The most common unpatched and exploited programs are Java, Adobe Reader, and Adobe Flash. It's been this way for a few years now. But strangely, not a single company I've ever audited has ever had these three programs perfectly patched. I just don't get it.

Countermeasure: Stop what you're doing right now and make sure your patching is perfect. If you can't, make sure it's perfect around the top most exploited products, including Java, Adobe, browser admins, OS patches, and more. Everyone knows that better patching is a great way to decrease risk. Become one of the few organizations that actually does it.

Cyber-attack No. 3: Phishing attacks

Approximately 70 percent of email is spam. Fortunately, antispam vendors have made great strides, so most of us have reasonably clean inboxes. Nonetheless, I get several spam emails each day, and at least a few of them each week are darned good phishing replicas of legitimate emails.

I think of an effective phishing email as a corrupted work of art: Everything looks great; it even warns the reader not to fall for fraudulent emails. The only thing that gives them away is the rogue link asking for confidential information.

Countermeasure: Decreasing risk from phishing attacks is mostly accomplished through better end-user education -- and with better antiphishing tools. Make sure your browser has antiphishing capabilities. I also love browsers that highlight the domain name of a host in a URL string.

Cyber-attack No. 4: Network-traveling worms

Computer viruses aren't much of a threat anymore, but their network-traveling worm cousins are. Most organizations have had to fight worms like Conficker and Zeus. We don't see the massive outbreaks of the past with email attachment worms, but the network-traveling variety is able to hide far better than its email relatives.

Countermeasure: Network-traveling worms can be defeated by blocking executables in email, better patching, disabling autorun capabilities, and strong password policies. Many network worms, like Conficker, will try to exploit network shares by logging on using a list of built-in, bad passwords: 12345, password2, qwerty, and the like. If any of your passwords are listed in the password manifest inside of a worm, you do not have a strong password policy.

Cyber attack No. 5: Advanced persistent threats

Lastly, I only know of one major corporation that has not suffered a major compromise due to an APT (advanced persistent threat) stealing intellectual property. APTs usually gain a foothold using socially engineered Trojans or phishing attacks.

A very popular method is for APT attackers to send a very specific phishing campaign -- known as spearphishing -- to multiple employee email addresses. The phishing email contains a Trojan attachment, which at least one employee is tricked into running. After the initial execution and first computer takeover, APT attackers can compromise an entire enterprise in a matter of hours. It's easy to accomplish, but a royal pain to clean up.

Countermeasure: Detecting and preventing an APT can be difficult, especially in the face of a determined adversary. All the previous advice applies, but you must also learn to understand the legitimate network traffic patterns in your network and alert on unexpected flows. An APT doesn't understand which computers normally talk to which other computers, but you do. Take the time now to start tracking your network flows and get a good handle of what traffic should be going from where to where. An APT will mess up and attempt to copy large amounts of data from a server to some other computer where that server does not normally communicate. When they do, you can catch them.

Types of attackers

Name: The Hacker Apprentice

PROFILE: The Hacker Apprentice is likely to be young, perhaps mid to late teens and male, perhaps an introvert. I am sure more females will enter this field as we see more females enter programming in general.

MOTIVATION: They will be interested in programming; probably learning to write code since their early childhood. Being a hacker seems glamorous and a way of 'showing off' their skills. Invariably, they aren't too technically savvy (yet) and their hacking expertise is low grade, only being able to hack weakly guarded systems. They'll use YouTube hacking videos to learn their trade. But don't be complacent. They can work their way up the cybercriminal ladder as they get older and more experienced if they are that way inclined. Most however, will mature out of this stage and move into working in computer or network focused professions.

Name: The Phisher

PROFILE: It seems that phishers are Chinese, Indonesian or American, according to Akamai research. But the profile is a mixed one. On the one hand you have phishers such as the Nigerian phishers who run bank phishing scams and have done so for years and then on the other hand, research by Verizon for their Data Breach Investigations Report 2015 has stated that 95% of incidents can be attributed to state sponsored actors. The reason for the wide profile of the Phisher is because of the success of this vector. It is used as both a general method of getting data like login credentials, but also a way directly into company resources using spear phishing methods.

MOTIVATION: Motivation is mixed too. General phishers are after financial gain. They want login credentials, or to get you to download malware that ultimately steals bank credentials. Spear phishers are after intellectual property, they can be part of the cyber espionage crew which are detailed below.

Name: My name is Bond, Hacker Bond

PROFILE: This cybercriminal is a spy. They may work alone or as a group which may be sponsored by a company or even a state. The general way into your organization is via spear phishing (see The Phisher above) and the use of APTs to persistently steal data. This cybercriminal is a very experienced programmer and architect. They should not be underestimated as they are at the top of their game. Often these types of cybercriminals work as part of a highly skilled group. A recent finding by security firm Kaspersky is of a group called the Equation Group. This group is one of the most highly sophisticated hacking groups of all time. Using highly specialized tools to perpetrate their crime, they are linked to malware infections across 30 countries and attack industries as diverse as government, mass media and aerospace.

MOTIVATION: This cybercriminal is after information and often also to create havoc, even potentially, warfare. Information on your business, such as company account details, manufacturing information, intellectual property, schematics and so on is all game for Mr. Bond. But this cybercriminal becomes most sinister when they are state sponsored and attack critical infrastructures, which can affect not only digital resources, but real world ones too. Probably the most famous cyberespionage attack is Stuxnet where Iranian nuclear facilities were targeted with the intention of taking them over. The cost of cyberespionage to the U.S. is massive. MacAfee in their 2013 report on The Economic Impact of Cybercrime and Cyberespionage has placed estimates of Intellectual Property losses of up to \$140 billion, so this must be one of the most successful and profitable cybercriminal personas.

Name: The Less Than Perfect Employee

PROFILE: An employee, ex-employee, contractor or even customer who has an axe to grind. Insider threats are the most prevalent cyber threats organizations face.

MOTIVATION: The motivations behind an insider doing damage to your organization is varied, but includes, revenge, cyberespionage (see above), for the fun of it, honest mistake, and for pure financial gain. We mentioned in a previous blog post about Insider Threats, that the costs incurred by these type of attacks far outweighs those incurred from phishing attacks, being on average, \$213,542 and \$45,959 respectively.

Name: The Hacktivist

PROFILE: An individual or group that wants to make a stand against something they think is wrong or for something they believe in. They have taken activism in the real world and placed it online. There are a number of groups that carry out attacks against targets that they have a grievance with. For example, the international group, Anonymous, carry out Denial of Service (DDOS) attacks against, mainly, government and religious websites.

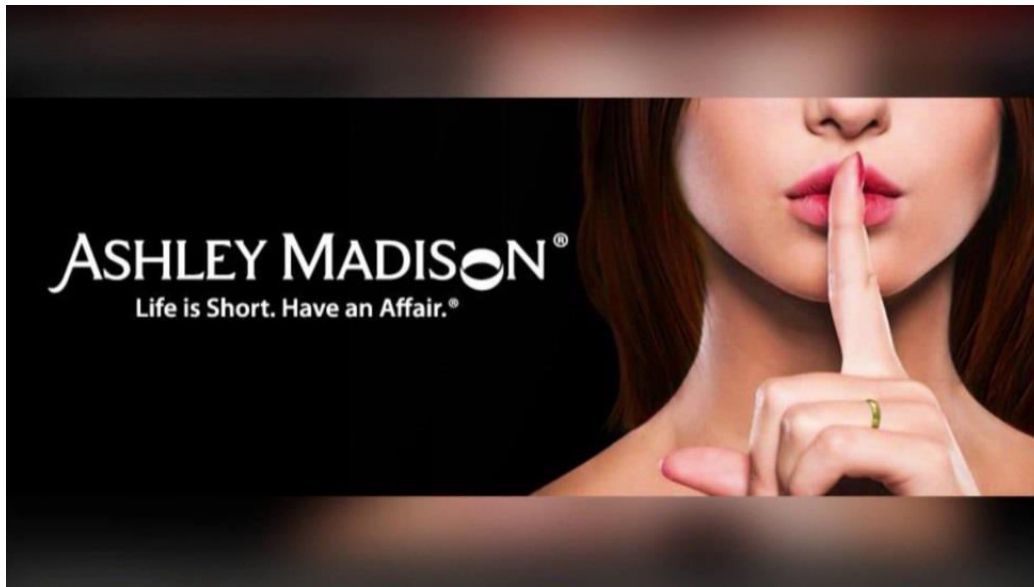
MOTIVATION: To carry out political acts of defiance. Just like real world activists take on issues that they believe need to be addressed, such as climate change, animal rights and so on. Hacktivists do the same thing, but using digital methods to spread their word and that often comes in the form of a cyber-attack. Motivation can be for good and bad. Sometimes hacktivism is used to attack foreign government policy. For example, Chinese hackers attacked U.S. government sites to protest against perceived U.S. Government wrongdoing against China (you can read more here in a previous blog post). Other times it is used to make a stand. Anonymous have recently targeted IS sympathisers by hijacking their Twitter accounts and either shutting them down, or flooding them with images of Japanese anime characters to alter search engine results for the word IS. Sometimes hacktivism is used as an excuse for hacking certain types of websites. For example, the recent attack on the customer accounts of the adultery website, Ashley Madison, was said to have been carried out to shame the users of the

site (rather than sell on their user account details – we shall wait and see how that pans out).

Major Cyber Attacks past One Year

1. Ashley Madison Data Breach
2. "Hacking Team" Hacked
3. John Brennan's Email ID Hacked
4. TalkTalk Hacked
5. Vodafone Hacked
6. Russian Hackers Spy in Germany
7. Air India's Loyalty Scheme Hacked
8. Social networking accounts hacked by OurMine (more on "OurMine's Unique way of selling its Security Products"), possibly 2012 LinkedIn breach lead to the compromised.
9. TATA assets management CEO's email account hacked

Ashley Madison Data Breach



Ashley Madison, or **The Ashley Madison Agency**, is a Canada-based online dating service and social networking service marketed to people who are married or in a committed relationship. It was founded in 2002 by Darren Morgenstern.

The company received attention on July 15, 2015, after hackers, "The Impact Group", stole all of its customer data and threatened to post all the data online if Ashley Madison and fellow Avid Life Media site EstablishedMen.com were not permanently closed.

How big was the breach?

The Ashley Madison breach included usernames, first and last names and hashed passwords for 33 million accounts, as well as partial credit card data, street names and phone numbers for a huge number of users. There were also records documenting 9.6 million transactions and 36 million email addresses.

The leak included PayPal accounts used by Ashley Madison executives, Windows domain credentials for employees and numerous proprietary internal documents.

Passwords were protected by the bcrypt hashing algorithm and were considered secure — but were they?

Lessons to be learnt:

- Storage is cheap and the data is very valuable. Since we have unlimited storage on the clouds, doesn't mean all of it is secure, even though it is encrypted. Thus if there is no privacy, there is no business.
- Putting all the data in one place is not a very good idea. That is exactly what happened here. If the data collected by the site would have been split and stored, the hacker would not have been able to access all storage points leading to exposure of large amount of data.
- As soon as a security related problem is found, it should immediately be sorted without any delay. The passwords of 11 million users were compromised days after the breach. The company did change its encryptions for the password but only for those who were signing up new. The encryption techniques for the old passwords were left as it is and they got compromised.
- When we know we are living in a not so secure cyber world, it is our prime duty to stay alert and aware of the new developments in the field so that we can safeguard ourselves.

“Hacking Team” Hacked

]HackingTeam[

Hacking Team is a Milan-based information technology company that sells offensive intrusion and surveillance capabilities to governments, law enforcement agencies and corporations. Hacking Team describes its lawful interception products as "offensive technology" and has been called into question over deliveries to Morocco and the United Arab Emirates. The company's "Remote Control System," called DaVinci, is able, it says, to break encryption on emails, files and Internet telephony protocols.

Phineas Fisher, the hacker who claimed responsibility for breaching Hacking Team last year published an explainer guide detailing his process in executing the attack. In July 2015, the hacker breached 400GB of Hacking Team's confidential documents, emails, and source code, which exposed the company's client list, which included the FBI and the U.S. Drug Enforcement Agency.

The leaked documents also demonstrated that the company sold its surveillance tools to several countries have been cited for human rights abuses, including Egypt, Bahrain, Morocco, Russia Uganda, among others.

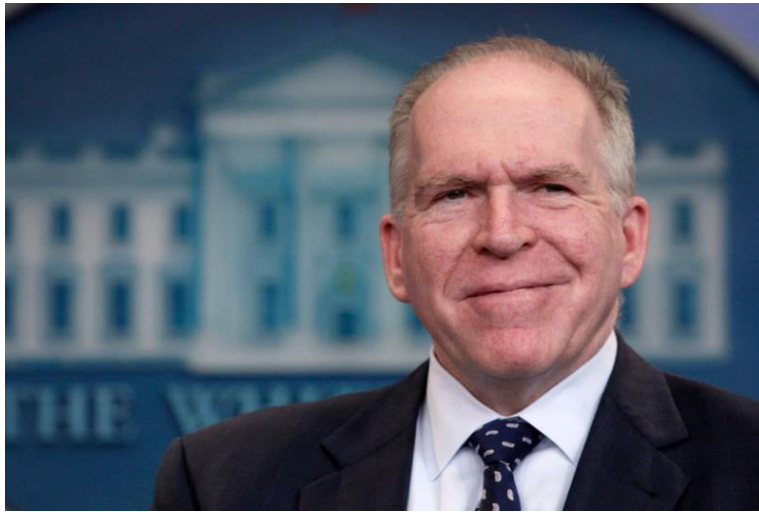
The hacker was also linked to hacking Gamma International, a U.K. company that sold a spyware product similar in functionally similar to the exploits used by Hacking Team.

Lessons to be learnt:

- Given the opportunity, the right amount of offence and the lack of the right amount of defence; anybody could be vulnerable. The hacker user zero day attack developed for the embedded systems of the server to get to the information, also the uninstalled updates for MangoDB, were a plus for the hacker.
- All the software updates should be timely installed to avoid any sort risks.
- Security shouldn't be taken lightly. When a company deals with high profile clients which for some purpose kept mysterious, the company should be very careful regarding the privacy they provide to their customers.
- One should be aware of the new developments and the activities on the server should be regularly monitored for any unauthorized or illegal accesses.

- The data was stored in decrypted form, which is not a legal way to store encrypted data, the poses a greater threat. Data stored in decrypted form, and encrypted using weak encryption techniques are equally bad for such an organisation.

John Brennan's Email ID Hacked



John Brennan became the **Director of the Central Intelligence Agency** in March 2013, replacing General David Petraeus who was forced to step down after becoming embroiled in a classified information mishandling scandal.

In July 2015, a self-proclaimed high school student employed social engineering as a tool to compromise the email ID. Emails contained sensitive information including Social Security Numbers and passport numbers of his family.

The teen, working with a group called "Crackas With Attitude," said he fooled Verizon into providing him with Brennan's personal data. The hacker said he used a reverse phone-number lookup to determine that Brennan has a Verizon Wireless account. He then called the company, posing as a technician whose "tools were down" to get details about the account, including Brennan's AOL email address. With that information, the teen called AOL and convinced a representative to reset the password, using Brennan's personal details provided by Verizon.

Lessons to be learnt:

- First, if one company is a weak link in the security chain, it can bring down other companies with it. In this case, it was Verizon failing to authenticate the attackers properly that eventually led to them being able to access the AOL email account.
- Do not send any sensitive information out over email if at all possible. With each document that John Brennan sent to his personal account, he effectively increased the odds that the document would be compromised. Corporate environment is very safe, secured with all the firewalls and latest technologies to avoid any data breach, by sending the sensitive data to a personal email id, takes the information outside the safe environment.
- When you set up an account and a company asks you to supply answers to those annoying questions, take an extra moment to make it hard on a hacker. Answers to easy questions can always be gained through some or the other ways, so the answers should be tricky, maybe a false answer.

TalkTalk Hacked



TalkTalk Telecom Group is a company which provides television, telecommunications, Internet access, and mobile network services to businesses and consumers in the United Kingdom. It was founded in 2003 as a subsidiary of Carphone Warehouse and was demerged as a standalone company in March 2010. Its headquarters are in London.

On 21st Oct, 2015 Wednesday morning TalkTalk customers experienced difficulty accessing its website. Fearing it was under attack, the company shut down its internal systems. The next day it revealed that customer details may have been accessed by intruders.

TalkTalk had come under a Distributed Denial of Service (DDOS) attack, where hackers flooded the company's site with internet traffic in an effort to overload digital systems and take them offline. But security analysts said that because customer information was taken it appears that a second attack may have been occurring at the same time, with intruders going after TalkTalk's customer database, which is a common tactic, with a DDOS attack used as a distraction to enact a more specific data breach.

Lessons to be learnt:

- One should periodically investigate and identify potential threats and then eliminate them time to time so that they do not become the reason for a big disaster in future. TalkTalk didn't correct security measures in place, such as firewalls that could detect the basic SQL vulnerabilities that lead to the attack. Companies need to ensure their Web applications are coded in a secure manner and that they are regularly tested for potential vulnerabilities.
- TalkTalk didn't have proper data storage methods in place too. They didn't tokenize the Credit Card details removing the initial 6 digits. The customer and bank account information were not encrypted and were stored in plaintext instead, which is considered as the worst practice when you have a lot of customers and you have to store their personally identifiable information. These mistakes often lead the company to come short of their goal to remain safe.
- More laws will not prevent criminals from attacking websites and systems. Nor will more laws make companies necessarily more secure, particularly if the focus in those companies is on being compliant with laws and regulations. What is required is a cultural change by consumers, regulators, and governments to ensure companies take a risk-based approach to security.
- A few companies fail to understand that data breaches can be expensive. The company cannot run on its name alone, every customer today demands security if they share their sensitive information with you.

Vodafone Hacked



Vodafone Group a British multinational telecommunications company has its headquarters in London and with its registered office in Newbury, Berkshire. Among mobile operator groups globally, Vodafone ranked fifth by revenue and second (behind China Mobile) in the number of connections (435.9 million) as of 2014.

The criminals got access to the user data from external sources, and the internal systems were not compromised, though after the incident. The company said that the banks of the affected customers were notified. The company also tried contacting the affected customers and helped them change the account details to regain control.

The only prevailing threat that remained was of phishing attacks.

Vodafone on its part was very alert and immediately came to the rescue, preventing a huge data breach. The users were warned well in time before any big incident could take place and all precautionary steps were taken.

Russian Hackers Spy in Germany



Germany's domestic secret service declared that it had evidence that Russia was behind a series of cyber-attacks, including one that targeted the German parliament in 2015.

The operations cited by the BfV intelligence agency ranged from an aggressive attack called Sofacy or APT 28 that hit NATO members and knocked French TV station TV5Monde off air, to a hacking campaign called Sandstorm that brought down part of Ukraine's power grid last year.

Cyberspace is a place for hybrid warfare. The campaigns BfV monitored, were generally about obtaining information i.e., spying, however, Russian secret services had also shown a readiness to carry out sabotage.

2015 attack on the German lower house of the parliament was when Germany itself fell victim to one of these rogue operations, with the Sofacy attack.

Chancellor Angela Merkel's CDU party confirmed it had been targeted in April, adding that "we have adapted our IT infrastructure as a result".

The BfV said that, the cyber-attacks carried out by Russian secret services are part of multi-year international operations that are aimed at obtaining strategic information.

Air India's Loyalty Scheme Hacked



A gang generated 20 email ids and diverted reward points earned by passengers, with possible help from some airline employees. The months-long investigation revealed that about 170 tickets were purchased by unfair means using driving licenses as ID, while many of them had the same signature, said Dhananjay Kumar, a senior manager with the national carrier. He said that as boarding passes were issued directly in these instances and driving licenses are not considered valid proof, the likelihood of insider involvement is strong.

Tickets worth almost Rs. 16 were sold on the basis of the stolen miles, say sources, adding that the probe may have merely scratched the surface as almost 20 lakh passengers are beneficiaries of AI's flying-returns program. The loot was first noticed in June '16 during the verification of "know your customer" documents uploaded by a member. The passenger submitted a driving license as identity proof, which is not legitimate, but the account was still approved.

On further investigation it was found out that these suspect user IDs had hacked various membership accounts and redeemed miles of genuine Flying Returns members. The details of the number of miles redeemed from each such account as well as the tickets issued along with ticket number, name has been retrieved.

Lessons to be learnt:

- Disgruntled employees can be a great threat to any company and past many years Air India has been unable to keep its employees happy. As claimed, this incident would not have been possible due to any insider involvement; it clearly indicates any company needs to take proper care of its employees. Keeping employees happy is one thing, but making sure they abide by the company regulations is another which is equally important.
- Moreover, regular audits are very important for timely reporting of any unwanted activities. The loss would not have been this large, if it would have been detected earlier. Moreover, this had been happening from a long time, indicating that Air India never aware that such a thing could happen.
- Learning from past and being alert for the future is very important. Air India and other airlines have faced such hacks earlier. This time the detection was just by chance during a Know you Customer Survey, leaving the possibility that if this would not have happened, the damage would have been bigger. If Air India would have been alert this incident would have been avoided.

OurMine's Unique way of selling its Security Products



Be whatever company, selling whichever product, to sell their product, they need to market it. Today every company is looking for an innovative idea to showcase their products and OurMine has outpaced them all.

OurMine as the Wired calls them are: hackers whose black hats are covered in the thinnest coat of white paint, or so patchwork that even they don't seem to remember which color they're wearing.

OurMine told Wired, "We don't need money, but we are selling security services because there is a lot [of] people [who] want to check their security...We are not black hat hackers, we are just a security group...we are just trying to tell people that nobody is safe."

They are right, no one as of today is safe be it online or offline.

The group has its own social networking accounts on which they are quite active, showcasing their work and polling for the next hack, though not many people follow them.

Also, many have come forward in protest of the group, describing the groups' activities to be unethical. Why? Because they hacked your Icon's Social Networking account?

OurMine is exploiting the database stolen in LinkedIn 2011 data breach which was sold to the dark web.

A lot said and done, why do we not blame the victims for such attacks. The Tech Heads of today, to which people look up to, are not being able to implement enough security. Using 4 year old data to hack their accounts today says enough about how seriously Cyber Crime is been taken today. Being famous, puts you on a greater risk of being attacked, because people want to overshadow you.

Cyber-crimes are not a joke, and it's high time that we pay close attention to the matter and be safe on the internet which is no longer a luxury.

Social networking accounts compromised by OurMine include:

- Google CEO Sundar Pichai's quora account
- UBER CEO, Travis Kalanick's twitter account
- Facebook founder, Mark Zuckerberg's twitter and pin-interest accounts
- The Twitter account of the microblogging site's co-founder and former CEO Evan Williams
- Spotify's Daniel Ek was also their target
- Amazon CTO Werner Vogels
- "Magic Mike" star Channing Tatum

But not to forget, marketing strategy developed by OurMine was undoubtedly eye-opening.

TATA assets management CEO's email account hacked



On June 14, the finance head of the firm received a mail from the 'CEO', asking him to transfer money to an account number. They had supposedly tried to reach the CEO to confirm, but he wasn't reachable as he was in the US, the company said.

Due to the pressure created by the hacker through subsequent mails, the finance official transferred Rs 7 lakh into the account without being aware that the sender was a hacker. The fraud came to fore when the firm sent the bank's settlement report of the wired money to the CEO's email ID and he claimed ignorance about having made any such request or receiving any money.

Then on June 15, another email reached the finance head from the same ID, this time demanding Rs 20 lakh be wired to another account with ICICI Bank, Allahabad. It was clear that the company had been conned.

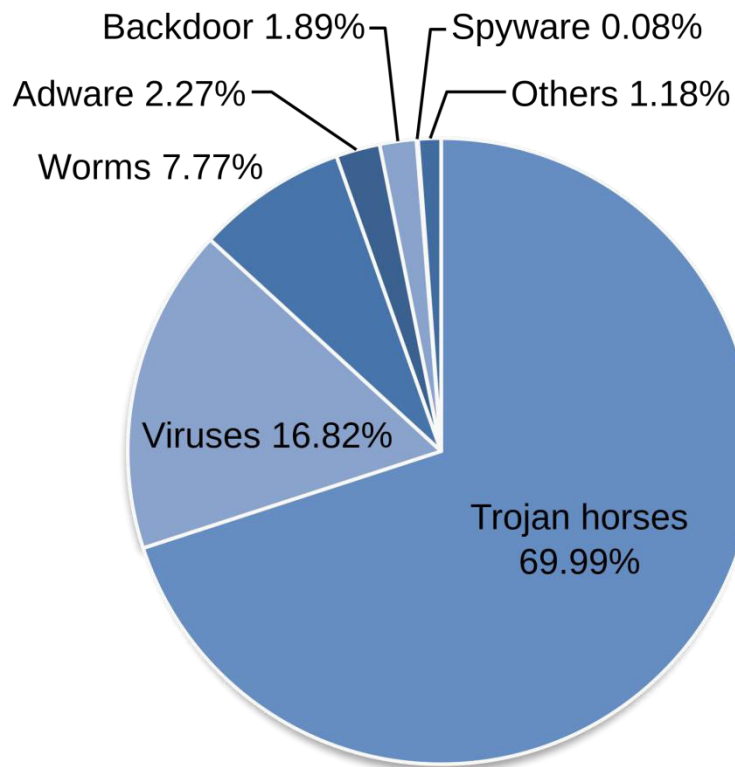
The fact that the mails first came in when the CEO was abroad indicates that the hacker was aware that he could be out of reach and the firm might wire the money if there was any distress communication.

Cyber-Security Solutions

The cyber space is increasing every day and so is the Dark web growing and imposing a greater threat to the development of Cyber Space. To protect the same, various technologies have been developed to detect the threats and safeguard systems against the evolving cyber-crimes. The technologies are:

1. Antivirus and Mobile app security
2. Authentication
3. Biometrics
4. Cryptography
5. Data Breach
6. DLP- Data Loss Prevention
7. DDoS attack protection
8. Embedded system security
9. Firewall
10. Fraud detection and prevention
11. IAM- Identity & Access Management
12. Incident Response
13. Intrusion Detection
14. Log Analysis & Management
15. Mainframe Security
16. Machine Learning Security
17. Network Security Monitoring
18. Next Generation Firewall
19. Password Management
20. Patch Management
21. Penetration Testing
22. Privileged Access Management
23. PKI-Public Key Infrastructure
24. Risk Analysis
25. SAP/ERP Security
26. Software Development Security
27. Unified Threat Management
28. Web App and Website Security
29. Web Application Firewall
30. Wireless/Wi-Fi Security

Antivirus & Mobile App Security



What are Malware?

"Malware" short for Malicious Software is a term for any software that gets installed on your machine and performs unwanted tasks, often for some third party's benefit. Malware programs can range from being simple annoyances (pop-up advertising) to causing serious computer invasion and damage (e.g., stealing passwords and data or infecting other machines on the network). Additionally, some malware programs are designed to transmit information about victim's web-browsing habits to advertisers or other third party interests without his knowledge.

Types of Malware:

- Virus –
Software that can replicate itself and spreads to other computers or are programmed to damage a computer by deleting files, reformatting the hard disk, or using up computer memory.
- Adware –
Software that is financially supported (or financially supports another program) by displaying ads when you're connected to the Internet.
- Spyware –
Spyware is software that surreptitiously gathers information and transmits it to interested parties. A type of information that is gathered includes the Websites visited, browser and system information, and your computer IP address.
- Browser hijacking software –
Advertising software that modifies the browser settings (e.g., default home page, search bars, toolbars), creates desktop shortcuts, and displays intermittent advertising pop-ups comes under this. Once a browser is hijacked, the software may also redirect links to other sites that advertise, or sites that collect Web usage information.
- Trojan Horses-
A Trojan horse or Trojan is a type of malware that is often disguised as legitimate software. Trojans can be employed by cyber-thieves and hackers trying to gain access to users' systems. Users are typically tricked by some form of social engineering into loading and executing Trojans on their systems. Once activated, Trojans can enable cyber-criminals to spy on you, steal your sensitive data, and gain backdoor access to your system. These actions can include deleting data, blocking data, modifying data, copying data, disrupting the performance of computers or computer networks.
- Rootkits-
Rootkits are designed to conceal certain objects or activities in your system. Often their main purpose is to prevent malicious programs being detected – in order to extend the period in which programs can run on an infected computer.
- Backdoors-
A backdoor Trojan gives malicious users remote control over the infected computer. They enable the author to do anything they wish on the infected computer – including sending, receiving, launching, and deleting files, displaying data, and rebooting the computer. Backdoor Trojans are often used to unite a group of victim computers to form a botnet or zombie network that can be used for criminal purposes.

- Ransomware-
This type of Trojan can modify data on your computer – so that your computer doesn't run correctly or you can no longer use specific data. The criminal will only restore your computer's performance or unblock your data, after you have paid them the ransom money that they demand.

How does Malware spread?

The ways in which malware attacks include:

- Email malware attacks which comes through infected email attachments
- Instant messaging attacks through IM attachments similar to email attachments
- File sharing is another way of malware attack, in which malware attacks through file sharing programs.
- Social networks: When you are surfing the internet, be cautious about third party software and applications. Even when you use social networking sites be careful to give consent to third-party applications for using your profile.
- Pirated software: malicious codes also spread in a system through pirated software. In majority cases, software seems to be legitimate when you download them, but they may be a big trouble for your system.
- E-mails: When you read emails malware spread through attachments, so it is always better to scan them prior to downloading.
- Removable media: USB sticks are another common way by which malware attack and spread in a system. Even systems in a computer lab might be infected with malware and when you transfer files from an infected system to your system with USB stick, the infection enters your system as well.
- Websites: There are many sites, which are infested with different malwares and these malwares enter your computer when you visit them.

Once malware makes its way into a system, they begin to damage a system's boot sector, data files; software installed in it and even the system BIOS. This further corrupts your files and your system might shut down as well. The main problem is that these malicious software programs are designed to spread in a system.

There is no end to the channels through which malware can attack your computer and once inside your system, these spread automatically and disrupts internet traffic as well. Some of these even give access to your computer. Malware like Trojan horses does not replicate themselves, but they can damage a system badly and these generally come in the form of screensavers or free games. Fortunately, there are ways through which you can protect your system from these malware attacks and you just need to be a little vigilant to avoid such attacks.

What is Antivirus?

Anti-virus software is a program or set of programs that are designed to prevent, search for, detect, and remove software viruses, and other malicious software like worms, trojans, adware, and more.

These tools are critical for users to have installed and up-to-date because a computer without anti-virus software installed will be infected within minutes of connecting to the internet. The bombardment is constant, with anti-virus companies update their detection tools constantly to deal with the more than 60,000 new pieces of malware created daily.

There are several different companies that build and offer anti-virus software and what each offers can vary but all perform some basic functions:

- Scan specific files or directories for any malware or known malicious patterns
- Allow you to schedule scans to automatically run for you
- Allow you to initiate a scan of a specific file or of your computer, or of a CD or flash drive at any time.
- Remove any malicious code detected –sometimes you will be notified of an infection and asked if you want to clean the file, other programs will automatically do this behind the scenes.
- Show you the 'health' of your computer

Always be sure you have the best, up-to-date security software installed to protect your computers, laptops, tablets and smartphones.

Features of Antivirus Software

- Background Scanning
- Full System Scans
- Virus Definitions

Background Scanning

Antivirus software scans all the files that you open from the back-end; this is also termed as on access scanning. It gives a real time protection safeguarding the computer from threats and other malicious attacks.

Full System Scans

Full system scans are essential when you install antivirus software for the first time or you have updated your antivirus software recently. This is done to make sure that there are no viruses present hidden on your system. Full system scans are also useful when you repair your infected computer.

Virus Definitions

Antivirus software depends on the virus definitions to identify malware. That is the reason it updates on the new viruses definitions. Malware definitions contain signatures for any new viruses and other malware that has been classified as wild. If the antivirus software scans any application or file and if it finds the file infected by a malware that is similar to the malware in the malware definition. Then antivirus software terminates the file from executing pushing it to the quarantine. The malware is processed accordingly corresponding to the type of antivirus software.

It is really essential for all the antivirus companies to update the definitions with the latest malware to ensure PC protection combating even the latest form of malicious threat.

Methods used to identify Malware

- Signature-based detection
- Heuristic-based detection
- Behavioral-based detection
- Sandbox detection
- Data mining techniques

Signature-based detection

This is most common in Traditional antivirus software that checks all the .EXE files and validates it with the known list of viruses and other types of malware. Or it checks if the unknown executable files shows any misbehavior as a sign of unknown viruses.

Files, programs and applications are basically scanned when they in use. Once an executable file is downloaded, it is scanned for any malware instantly. Antivirus software can also be used without the background on access scanning, but it is always advisable to use on access scanning because it is complex to remove malware once it infects your system

Heuristic-based detection

This type of detection is most commonly used in combination with signature-based detection. Heuristic technology is deployed in most of the antivirus programs. This helps the antivirus software to detect new or a variant or an altered version of malware, even in the absence of the latest virus definitions.

Antivirus programs use heuristics, by running susceptible programs or applications with suspicious code on it, within a runtime virtual environment. This keeps the vulnerable code from infecting the real world environment.

Behavioral-based detection

This type of detection is used in Intrusion Detection mechanism. This concentrates more in detecting the characteristics of the malware during execution. This mechanism detects malware only while the malware performs malware actions.

Sandbox detection

It functions most likely to that of behavioral based detection method. It executes any applications in the virtual environment to track what kind of actions it performs. Verifying the actions of the program that are logged in, the antivirus software can identify if the program is malicious or not.

Data mining techniques

This is of the latest trends in detecting a malware. With a set of program features, Data mining helps to find if the program is malicious or not.

Features of Antiviruses:

PROTECTION FROM VIRUSES

Malware Blocker

An industry first, the Malware Blocker feature blocks threats on Google Play before they can be installed and damage your device or data

App Virus Scanner

Scans every app you have installed and every one you download to filter out virus and malicious apps that can steal your information and cost you money

Unlimited Updates

Automatically updates virus protection files

Cloud Scanner

Features unlimited cloud scanning connections to ensure continuous protection

Malware Cleaner

Downloads a dedicated removal tool in accordance with the type of malware threat detected. Removes and restores the smartphone back to its normal settings

DATA THEFT PREVENTION

Privacy Scanner

Detects spyware by scanning all apps with Trend Micro Mobile App Reputation to identify ones that collect and potentially steal private information

NEW: Billing Security

Provides an extra layer of protection against fake monetary apps (banking, shopping, financial) that seek to steal your money or identity by deceiving you into believing

they are legitimate

SAFE SURFING

Malicious Website Blocker

Uses the Trend Micro Smart Protection Network to block malicious websites

Parental Controls

Filters inappropriate websites with age-based restrictions

CALL & TEXT BLOCKING

Call and Text Blocker

Filters unwanted calls and texts based on keywords, anonymous callers, whitelists, and blacklists

LOST DEVICE PROTECTION

Remote Locate

Helps you find your device on a Google map using GPS, Cell Towers, or Wi-Fi

Remote Scream

Enables you to trigger an alarm on your device - even if it is on silent

Remote Lock

Enables you to remotely lock your device (Accessing the phone again will require that you insert your Trend Micro password or a unique unlock code)

Remote Wipe

Allows you to perform a factory reset of the device from the web portal to wipe all your personal data

SIM Card Protection

Automatically locks if the SIM card is removed (Accessing the phone again will require that you insert your Trend Micro password or a unique unlock code)

Last Known Location

Automatically locates your device when the following actions take place: SIM removal, SIM replacement, Phone Restart

Low Power Location

The location of your device will be recorded just before it runs out of power

ONLINE STORAGE

Backup and Restore

Backup your contacts, photos, videos, calendar, call and text history, and music (5 GB of storage can be purchased separately)

Cross-Platform Contacts Backup and Restore

Copies and saves contact information between your iOS and Android devices

SOCIAL NETWORKING PRIVACY

Scan Facebook

Protects your privacy on Facebook by checking settings and recommending enhancements

SYSTEM OPTIMIZATION

NEW: App Manager

Allows you to recover space from unused or rarely used applications. Additionally, may increase performance due to fewer apps running in the background

Battery Optimizer and Status

Maximizes your battery life by killing non-essential background processes. It also shows how much time remains and how much time is needed to fully charge your battery

Smart Power Saver

Intelligently manages and disables the network connection when it is not in use to maximize your battery's life

Just-a-Phone

Turns off power draining features not required for phone and text message use, including 3G/4G, WiFi, Bluetooth, and running apps

Auto Just-a-Phone

Automatically turns on Just-a-Phone feature guided by a set schedule or a percentage of battery power remaining

Memory Status and Optimizer

Kills tasks to free up memory and CPU to maximize device performance. Also, shows the amount of free memory and the percentage remaining

SUPPORT & MORE

Online Technical Support

Offers support provided via online forums, knowledge base, and email

Uninstall Protection

Prevents unauthorized removal of the app (Uninstalling Mobile Security will require that you insert your Trend Micro password)

No Advertising

Does not allow third-party advertising to be displayed in the app

Authentication

Computer/network security hinges on two very simple goals:

- Keeping unauthorized persons from gaining access to resources
- Ensuring that authorized persons can access the resources they need

There are a number of components involved in accomplishing these objectives. One way is to assign access permissions to resources that specify which users can or cannot access those resources and under what circumstances. (For example, you may want a specific user or group of users to have access when logged on from a computer that is physically on-site but not from a remote dial-up connection.)

Access permissions, however, work only if you are able to verify the identity of the user who is attempting to access the resources. That's where authentication comes in. In this Daily Drill Down, we will look at the role played by authentication in a network security plan, popular types of authentication, how authentication works, and the most commonly used authentication methods and protocols.

Authentication and security

Authentication is an absolutely essential element of a typical security model. It is the process of confirming the identification of a user (or in some cases, a machine) that is trying to log on or access resources. There are a number of different authentication mechanisms, but all serve this same purpose.

Authentication vs. authorization

It is easy to confuse authentication with another element of the security plan: authorization. While authentication verifies the user's identity, authorization verifies that the user in question has the correct permissions and rights to access the requested resource. As you can see, the two work together. Authentication occurs first, then authorization.

For example, when a user who belongs to a Windows domain logs onto the network, his or her identity is verified via one of several authentication types. Then the user is issued an access token, which contains information about the security groups to which the user belongs. When the user tries to access a network resource (open a file, print to a

printer, etc.), the access control list (ACL) associated with that resource is checked against the access token. If the ACL shows that members of the Managers group have permission to access the resource, and the user's access token shows that he or she is a member of the Managers group, that user will be granted access (unless the user's account, or a group to which the user belongs, has been explicitly denied access to the resource).

Another example of authorization is the Dialed Number Identification Service (DNIS), which authorizes a dial-in connection based on the number called.

Logon authentication

Most network operating systems require that a user be authenticated in order to log onto the network. This can be done by entering a password, inserting a smart card and entering the associated PIN, providing a fingerprint, voice pattern sample, or retinal scan, or using some other means to prove to the system that you are who you claim to be.

Network access authentication

Network access authentication verifies the user's identity to each network service that the user attempts to access. It differs in that this authentication process is, in most cases, transparent to the user once he or she has logged on. Otherwise, the user would have to reenter the password or provide other credentials every time he or she wanted to access another network service or resource.

IPSec authentication

IP Security (IPSec) provides a means for users to encrypt and/or sign messages that are sent across the network to guarantee confidentiality, integrity, and authenticity. IPSec transmissions can use a variety of authentication methods, including the Kerberos protocol, public key certificates issued by a trusted certificate authority (CA), or a simple pre-shared secret key (a string of characters known to both the sender and the recipient).

An important consideration is that both the sending and receiving computers must be configured to use a common authentication method or they will not be able to engage in secured communications.

IPSec configuration

If IPSec policies have been configured to require that communications be secured, the sending and receiving computers will not be able to communicate at all if they do not support a common authentication method.

Remote authentication

There are a number of authentication methods that can be used to confirm the identity of users who connect to the network via a remote connection such as dial-up or VPN. These include:

- The Password Authentication Protocol (PAP)
- The Shiva PAP (SPAP)
- Challenge Handshake Authentication Protocol (CHAP)
- Microsoft CHAP (MS-CHAP)
- The Extensible Authentication Protocol (EAP)

Remote users can be authenticated via a Remote Authentication Dial-In User Service (RADIUS) or the Internet Authentication Service (IAS). Each of these will be discussed in more detail in the section titled Authentication Methods and Protocols.

It is especially important that remote users be properly authenticated, as they generally pose a greater security risk than on-site users.

Single Sign-On (SSO)

Single Sign-On (SSO) is a feature that allows a user to use one password (or smart card) to authenticate to multiple servers on a network without reentering credentials. This is an obvious convenience for users, who don't have to remember multiple passwords or keep going through the authentication process over and over to access different resources.

There are a number of SSO products on the market that allow for single sign-on in a mixed (hybrid) environment that incorporates, for example, Microsoft Windows servers, Novell NetWare, and UNIX.

Authentication types

There are several physical means by which you can provide your authentication credentials to the system. The most common—but not the most secure—is password authentication. Today's competitive business environment demands options that offer more protection when network resources include highly sensitive data. Smart cards and biometric authentication types provide this extra protection.

Password authentication

Most of us are familiar with password authentication. To log onto a computer or network, you enter a user account name and the password assigned to that account. This password is checked against a database that contains all authorized users and their passwords. In a Windows 2000 network, for example, this information is contained in Active Directory.

To preserve the security of the network, passwords must be “strong,” that is, they should contain a combination of alpha and numeric characters and symbols, they should not be words that are found in a dictionary, and they should be relatively long (eight characters or more). In short, they should not be easily guessed.

Password authentication is vulnerable to a password “cracker” who uses a brute force attack (trying every possible combination until hitting upon the right one) or who uses a protocol “sniffer” to capture packets if passwords are not encrypted when they are sent over the network.

Smart card authentication

Smart cards are credit card-sized devices that hold a small computer chip, which is used to store public and private keys and other personal information used to identify a person and authenticate him or her to the system. Logging onto the network with a smart card requires that you physically insert the card into (or slide it through) a reader and then enter a Personal Identification Number (PIN) in much the same way that you use an ATM card to access an automatic teller machine.

Smart cards use cryptography-based authentication and provide stronger security than a password because in order to gain access, the user must be in physical possession of the card and must know the PIN.

Biometric authentication

An even more secure type of authentication than smart cards, biometric authentication involves the use of biological statistics that show that the probability of two people having identical biological characteristics such as fingerprints is infinitesimally small; thus, these biological traits can be used to positively identify a person.

In addition to fingerprints, voice, retinal, and iris patterns are virtually unique to each individual and can be used for authentication purposes. This method of proving one's identity is very difficult to falsify, although it requires expensive equipment to input the fingerprint, voice sample, or eye scan. Another advantage over smart cards is that the user does not have to remember to carry a device; his or her biological credentials are never left at home.

How does authentication work?

In theory, authentication is relatively simple: A user provides some sort of credentials—a password, smart card, fingerprint, digital certificate—which identifies that user as the person who is authorized to access the system. There are, however, a multiplicity of methods and protocols that can be used to accomplish this. Regardless of the method, the basic authentication process remains the same.

The authentication process

In most instances, a user must have a valid user account configured by the network administrator that specifies the user's permissions and rights. User credentials must be associated with this account—a password is assigned, a smart card certificate is issued, or a biometric scan is entered into the database against which future readings will be compared.

When the user wants to log on, he or she provides the credentials and the system checks the database for the original entry and makes the comparison. If the credentials provided by the user match those in the database, access is granted.

Advantages of multilayered authentication

In a high-security environment, multilayered authentication adds extra protection. In other words, you can require that the user provide more than one type of credential, such as both a fingerprint and a logon password. This further decreases the chances of an unauthorized person circumventing the security system.

Authentication methods and protocols

There are a large number of authentication methods and protocols that can be used, depending on the application and security requirements. In the following sections, we will discuss:

- Kerberos
- SSL
- Microsoft NTLM
- PAP and SPAP
- CHAP and MS-CHAP
- EAP
- RADIUS
- Certificate services

These are by no means the only authentication methods in existence, but they are some of the most common.

Kerberos

Kerberos was developed at MIT to provide secure authentication for UNIX networks. It has become an Internet standard and is supported by Microsoft's latest network operating system, Windows 2000. Kerberos uses temporary certificates called tickets, which contain the credentials that identify the user to the servers on the network. In the current version of Kerberos, v5, the data contained in the tickets is encrypted, including the user's password.

A Key Distribution Center (KDC) is a service that runs on a network server, which issues a ticket called a Ticket Granting Ticket (TGT) to the clients that authenticates to the Ticket Granting Service (TGS). The client uses this TGT to access the TGS (which can run on the same computer as the KDC). The TGS issues a service or session ticket, which is used to access a network service or resource.

Secure Sockets Layer (SSL)

The SSL protocol is another Internet standard, often used to provide secure access to Web sites, using a combination of public key technology and secret key technology. Secret key encryption (also called symmetric encryption) is faster, but asymmetric public key encryption provides for better authentication, so SSL is designed to benefit from the advantages of both. It is supported by Microsoft, Netscape, and other major browsers, and by most Web server software, such as IIS and Apache.

SSL operates at the application layer of the DoD networking model. This means applications must be written to use it, unlike other security protocols (such as IPSec) that operate at lower layers. The Transport Layer Security (TLS) Internet standard is based on SSL.

SSL authentication is based on digital certificates that allow Web servers and clients to verify each other's identities before they establish a connection. (This is called mutual authentication.) Thus, two types of certificates are used: client certificates and server certificates.

Microsoft NTLM (NT LAN Manager)

NTLM authentication is used by Windows NT servers to authenticate clients to an NT domain. Windows 2000 uses Kerberos authentication by default but retains support for NTLM for authentication of pre-Windows 2000 Microsoft servers and clients on the network. UNIX machines connecting to Microsoft networks via an SMB client also use NTLM to authenticate.

Native mode

If you convert your Windows 2000 domain's status to native mode, NTLM support will be disabled.

NTLM uses a method called challenge/response, using the credentials that were provided when the user logged on each time that user tries to access a resource. This means the user's credentials do not get transferred across the network when resources are accessed, which increases security. The client and server must reside in the same domain or there must be a trust relationship established between their domains in order for authentication to succeed.

PAP

PAP is used for authenticating a user over a remote access control. An important characteristic of PAP is that it sends user passwords across the network to the authenticating server in plain text. This poses a significant security risk, as an unauthorized user could capture the data packets using a protocol analyzer (sniffer) and obtain the password.

The advantage of PAP is that it is compatible with many server types running different operating systems. PAP should be used only when necessary for compatibility purposes.

SPAP

SPAP is an improvement over PAP in terms of the security level, as it uses an encryption method (used by Shiva remote access servers, thus the name).

The client sends the user name along with the encrypted password, and the remote server decrypts the password. If the username and password match the information in the server's database, the remote server sends an Acknowledgment (ACK) message and allows the connection. If not, a Negative Acknowledgment (NAK) is sent, and the connection is refused.

CHAP and MS-CHAP

CHAP is another authentication protocol used for remote access security. It is an Internet standard that uses MD5, a one-way encryption method, which performs a hash operation on the password and transmits the hash result—instead of the password itself—over the network.

This has obvious security advantages over PAP/SPAP, as the password does not go across the network and cannot be captured.

The hash algorithm ensures that the operation cannot be reverse engineered to obtain the original password from the hash results. CHAP is, however, vulnerable to remote server impersonation.

MS-CHAP is Microsoft's version of CHAP. MS-CHAPv2 uses two-way authentication so that the identity of the server, as well as the client, is verified. This protects against server impersonation. MS-CHAP also increases security by using separate cryptographic keys for transmitted and received data.

EAP

EAP is a means of authenticating a Point-to-Point Protocol (PPP) connection that allows the communicating computers to negotiate a specific authentication scheme (called an EAP type).

A key characteristic of EAP is its extensibility, indicated by its name. Plug-in modules can be added at both client and server sides to support new EAP types.

EAP can be used with TLS (called EAP-TLS) to provide mutual authentication via the exchange of user and machine certificates.

EAP can also be used with RADIUS (see below).

RADIUS

RADIUS is often used by Internet service providers (ISPs) to authenticate and authorize dial-up or VPN users. The standards for RADIUS are defined in RFCs 2138 and 2139. A RADIUS server receives user credentials and connection information from dial-up clients and authenticates them to the network.

RADIUS can also perform accounting services, and EAP messages can be passed to a RADIUS server for authentication. EAP only needs to be installed on the RADIUS server; it's not required on the client machine.

Windows 2000 Server includes a RADIUS server service called Internet Authentication Services (IAS), which implements the RADIUS standards and allows the use of PAP, CHAP, or MS-CHAP, as well as EAP.

Certificate services

Digital certificates consist of data that is used for authentication and securing of communications, especially on unsecured networks (for example, the Internet). Certificates associate a public key to a user or other entity (a computer or service) that has the corresponding private key.

Certificates are issued by certification authorities (CAs), which are trusted entities that “vouch for” the identity of the user or computer. The CA digitally signs the certificates it issues, using its private key. The certificates are only valid for a specified time period; when a certificate expires, a new one must be issued. The issuing authority can also revoke certificates.

Certificate services are part of a network's Public Key Infrastructure (PKI). Standards for the most commonly used certificates are based on the X.509 specifications.

Biometrics

Biometrics is the measurement and statistical analysis of people's physical and behavioral characteristics. The technology is mainly used for identification and access control, or for identifying individuals that are under surveillance. The basic premise of biometric authentication is that everyone is unique and an individual can be identified by his or her intrinsic physical or behavioral traits.

There are two main types of biometric identifiers:

- Physiological characteristics: The shape or composition of the body.
- Behavioral characteristics: The behavior of a person.

Examples of physiological characteristics used for biometric authentication include fingerprints; DNA; face, hand, retina or ear features; and odor.

Behavioral characteristics are related to the pattern of the behavior of a person, such as typing rhythm, gait, gestures and voice. Certain biometric identifiers, such as monitoring keystrokes or gait in real time, can be used to provide continuous authentication instead of a single one-off authentication check.

Characteristics of Biometrics

A number of biometric characteristics may be captured in the first phase of processing. However, automated capturing and automated comparison with previously stored data requires that the biometric characteristics satisfy the following characteristics:

Universal

Every person must possess the characteristic/attribute. The attribute must be one that is universal and seldom lost to accident or disease.

Invariance of properties

They should be constant over a long period of time. The attribute should not be subject to significant differences based on age either episodic or chronic disease.

Measurability

The properties should be suitable for capture without waiting time and must be easy to gather the attribute data passively.

Singularity

Each expression of the attribute must be unique to the individual. The characteristics should have sufficient unique properties to distinguish one person from any other. Height, weight, hair and eye color are all attributes that are unique assuming a particularly precise measure, but do not offer enough points of differentiation to be useful for more than categorizing.

Acceptance

The capturing should be possible in a way acceptable to a large percentage of the population. Excluded are particularly invasive technologies, i.e. technologies which require a part of the human body to be taken or which (apparently) impair the human body.

Reducibility

The captured data should be capable of being reduced to a file which is easy to handle.

Reliability and tamper-resistance

The attribute should be impractical to mask or manipulate. The process should ensure high reliability and reproducibility.

Privacy

The process should not violate the privacy of the person.

Comparable

Should be able to reduce the attribute to a state that makes it digitally comparable to others. The less probabilistic the matching involved, the more authoritative the identification.

Inimitable

The attribute must be irreproducible by other means. The less reproducible the attribute, the more likely it will be authoritative.

Among the various biometric technologies being considered, the attributes which satisfy the above requirements are fingerprint, facial features, hand geometry, voice, iris, retina, vein patterns, palm print, DNA, keystroke dynamics, ear shape, odor, signature etc.

Biometric System Modules

Biometric systems are made up of five integrated modules.

- A **sensor** collects the raw biometric data and converts the information to a digital format. The quality of the data captured typically depends on the intuitiveness of the interface and the characteristics of the sensor itself.
- **Signal processing algorithms** perform quality control activities, extract features, and develop the biometric template. Quality control typically consists of three steps:
 - Quality assessment (determining the suitability of the sample),
 - Segmentation (separating the biometric data from “background noise”),
 - Enhancement (improving the quality of the sample and further reducing noise).
 - The outcome is a biometric template which contains only the discriminatory information necessary for recognizing the person.
- A **data storage component** (either centralized or decentralized) keeps information that new biometric templates will be compared to.
- A **matching algorithm** compares the new biometric template (the query) to one or more templates kept in data storage and creates a “match score.” A large match score indicates a greater similarity between the query and the stored template. In some cases, the goal is to measure the dissimilarity in which case the score is referred to as a “distance score.”
- Lastly, a **decision process** uses the results from the matching component to make a system-level decision. This can either be automated or human-assisted.

Multimodal Biometric Systems

Multimodal biometric systems are those that utilize more than one physiological or behavioral characteristic for enrollment, verification, or identification. In applications such as border entry/exit, access control, civil identification, and network security, multimodal biometric systems are looked to as a means of

- Reducing false non-match and false match rates,
- Providing a secondary means of enrollment, verification, and identification if sufficient data cannot be acquired from a given biometric sample, and
- Combating attempts to fool biometric systems through fraudulent data sources such as fake fingers.

A multimodal biometric verification system can be considered as a classical information fusion problem i.e. can be thought to combine evidence provided by different biometrics to improve the overall decision accuracy. Generally, multiple evidences can be integrated at one of the following three levels.

Abstract level

The output from each module is only a set of possible labels without any confidence value associated with the labels; in this case a simple majority rule may be used to reach a more reliable decision.

Rank level

The output from each module is a set of possible labels ranked by decreasing confidence values, but the confidence values themselves are not specified.

Measurement level

The output from each module is a set of possible labels with associated confidence values; in this case, more accurate decisions can be made by integrating different confidence values.

Biometric Authentication Systems

Looking at biometric systems in a more general way will reveal certain things all biometric-based authentication systems have in common. In general such systems work in two modes:

- **Enrollment mode**

In this mode biometric user data is acquired. This is mostly done with some type of biometric reader. Afterwards the gathered information is stored in a database where it is labeled with a user identity (e.g. name, identification number) to facilitate authentication.

- **Authentication mode**

Again biometric user data is acquired first and used by the system to either verify the users claimed identity or to identify who the user is. While identification involves the process of comparing the user's biometric data against all users in the database, the process of verification compares the biometric data against only those entries in the database which are corresponding to the users claimed identity.

Biometric verification becoming common

Authentication by biometric verification is becoming increasingly common in corporate and public security systems, consumer electronics, and point-of-sale applications. In addition to security, the driving force behind biometric verification has been convenience, as there are no passwords to remember or security tokens to carry. Measuring someone's gait doesn't even require a contact with the person.

Biometric devices, such as fingerprint readers, consist of:

- A reader or scanning device.
- Software that converts the scanned information into digital form and compares match points.
- A database that stores the biometric data for comparison.

Accuracy of biometrics

The accuracy and cost of readers has until recently been a limiting factor in the adoption of biometric authentication solutions but the presence of high quality cameras, microphones, and fingerprint readers in many of today's mobile devices means biometrics is likely to become a considerably more common method of authenticating users, particularly as the new FIDO specification means that two-factor authentication using biometrics is finally becoming cost effective and in a position to be rolled out to the consumer market.

The quality of biometric readers is improving all the time, but they can still produce false negatives and false positives. One problem with fingerprints is that people inadvertently leave their fingerprints on many surfaces they touch, and it's fairly easy to copy them and create a replica in silicone. People also leave DNA everywhere they go and someone's voice is also easily captured. Dynamic biometrics like gestures and facial expressions can change, but they can be captured by HD cameras and copied. Also, whatever biometric is being measured, if the measurement data is exposed at any point during the authentication process, there is always the possibility it can be intercepted. This is a big problem, as people can't change their physical attributes as they can a password. While limitations in biometric authentication schemes are real, biometrics is a great improvement over passwords as a means of authenticating an individual.

Cryptography

Cryptography is closely related to the disciplines of cryptology and cryptanalysis. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as clear text) into cipher text (a process called encryption), then back again (known as decryption). Individuals who practice this field are known as cryptographers.

Modern cryptography concerns itself with the following four objectives:

- 1) Confidentiality (the information cannot be understood by anyone for whom it was unintended)
- 2) Integrity (the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected)
- 3) Non-repudiation (the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information)
- 4) Authentication (the sender and receiver can confirm each other's identity and the origin/destination of the information)

Procedures and protocols that meet some or all of the above criteria are known as cryptosystems. Cryptosystems are often thought to refer only to mathematical procedures and computer programs; however, they also include the regulation of human behavior, such as choosing hard-to-guess passwords, logging off unused systems, and not discussing sensitive procedures with outsiders.

Types of Cryptosystems

Fundamentally, there are two types of cryptosystems based on the manner in which encryption-decryption is carried out in the system –

- Symmetric Key Encryption
- Asymmetric Key Encryption

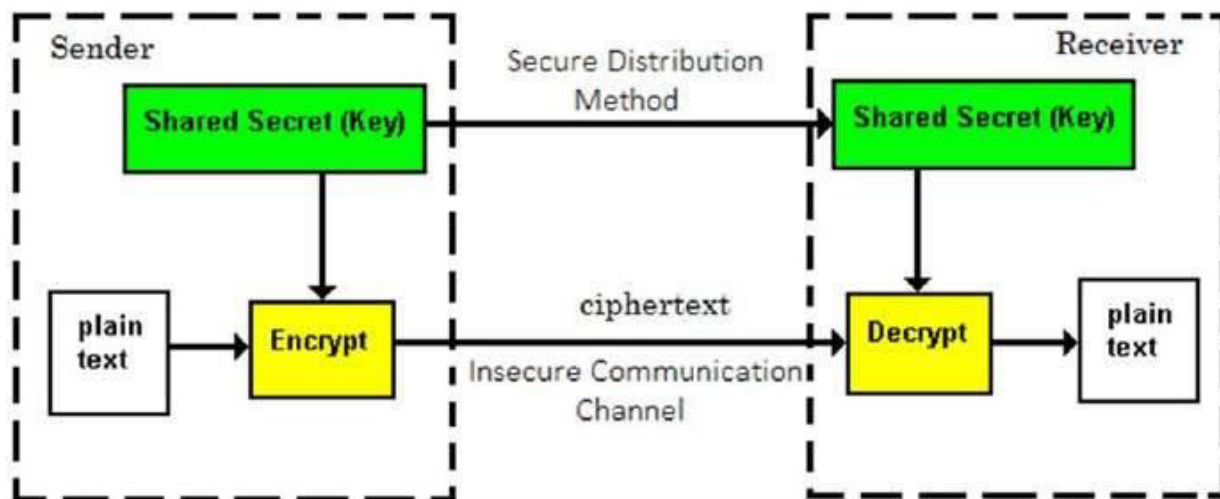
The main difference between these cryptosystems is the relationship between the encryption and the decryption key. Logically, in any cryptosystem, both the keys are closely associated. It is practically impossible to decrypt the cipher text with the key that is unrelated to the encryption key.

Symmetric Key Encryption

The encryption process where same keys are used for encrypting and decrypting the information is known as Symmetric Key Encryption.

The study of symmetric cryptosystems is referred to as symmetric cryptography. Symmetric cryptosystems are also sometimes referred to as secret key cryptosystems.

A few well-known examples of symmetric key encryption methods are – Digital Encryption Standard (DES), Triple-DES (3DES), IDEA, and BLOWFISH.



Prior to 1970, all cryptosystems employed symmetric key encryption. Even today, its relevance is very high and it is being used extensively in many cryptosystems. It is very unlikely that this encryption will fade away, as it has certain advantages over asymmetric key encryption.

The salient features of cryptosystem based on symmetric key encryption are –

- Persons using symmetric key encryption must share a common key prior to exchange of information.
- Keys are recommended to be changed regularly to prevent any attack on the system.
- A robust mechanism needs to exist to exchange the key between the communicating parties. As keys are required to be changed regularly, this mechanism becomes expensive and cumbersome.
- In a group of n people, to enable two-party communication between any two persons, the number of keys required for group is $n \times (n - 1)/2$.
- Length of Key (number of bits) in this encryption is smaller and hence, process of encryption-decryption is faster than asymmetric key encryption.
- Processing power of computer system required to run symmetric algorithm is less.

Challenge of Symmetric Key Cryptosystem

There are two restrictive challenges of employing symmetric key cryptography.

KEY ESTABLISHMENT

Before any communication, both the sender and the receiver need to agree on a secret symmetric key. It requires a secure key establishment mechanism in place.

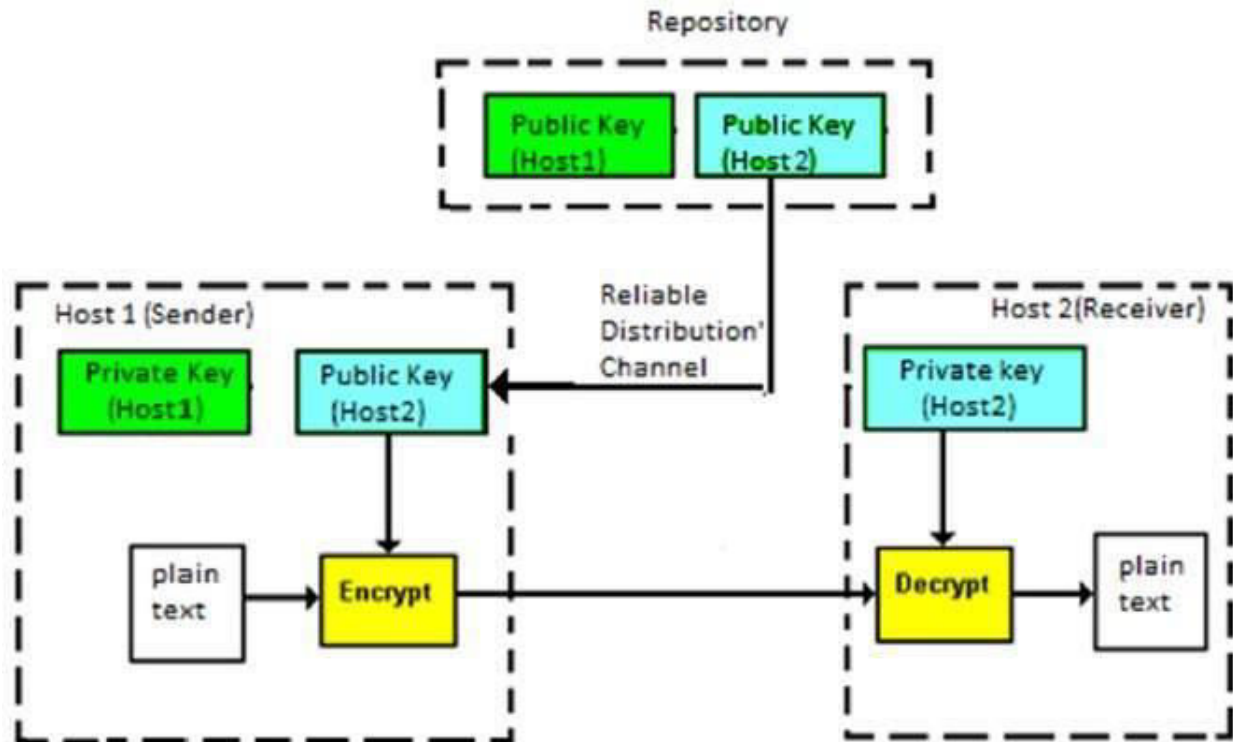
TRUST ISSUE

Since the sender and the receiver use the same symmetric key, there is an implicit requirement that the sender and the receiver 'trust' each other. For example, it may happen that the receiver has lost the key to an attacker and the sender is not informed.

These two challenges are highly restraining for modern day communication. Today, people need to exchange information with non-familiar and non-trusted parties. For example, a communication between online seller and customer. These limitations of symmetric key encryption gave rise to asymmetric key encryption schemes.

Asymmetric Key Encryption

The encryption process where different keys are used for encrypting and decrypting the information is known as Asymmetric Key Encryption. Though the keys are different, they are mathematically related and hence, retrieving the plaintext by decrypting cipher text is feasible. The process is depicted in the following illustration –



Asymmetric Key Encryption was invented in the 20th century to come over the necessity of pre-shared secret key between communicating persons. The salient features of this encryption scheme are as follows –

Every user in this system needs to have a pair of dissimilar keys, private key and public key. These keys are mathematically related – when one key is used for encryption, the other can decrypt the cipher text back to the original plaintext.

It requires to put the public key in public repository and the private key as a well-guarded secret. Hence, this scheme of encryption is also called Public Key Encryption.

Though public and private keys of the user are related, it is computationally not feasible to find one from another. This is a strength of this scheme.

When Host1 needs to send data to Host2, he obtains the public key of Host2 from repository, encrypts the data, and transmits.

Host2 uses his private key to extract the plaintext.

Length of Keys (number of bits) in this encryption is large and hence, the process of encryption-decryption is slower than symmetric key encryption.

Processing power of computer system required to run asymmetric algorithm is higher.

Symmetric cryptosystems are a natural concept. In contrast, public-key cryptosystems are quite difficult to comprehend.

You may think, how can the encryption key and the decryption key are 'related', and yet it is impossible to determine the decryption key from the encryption key? The answer lies in the mathematical concepts. It is possible to design a cryptosystem whose keys have this property. The concept of public-key cryptography is relatively new. There are fewer public-key algorithms known than symmetric algorithms.

Challenge of Public Key Cryptosystem

Public-key cryptosystems have one significant challenge – the user needs to trust that the public key that he is using in communications with a person really is the public key of that person and has not been spoofed by a malicious third party.

This is usually accomplished through a Public Key Infrastructure (PKI) consisting a trusted third party. The third party securely manages and attests to the authenticity of public keys. When the third party is requested to provide the public key for any communicating person X, they are trusted to provide the correct public key.

The third party satisfies itself about user identity by the process of attestation, notarization, or some other process – that X is the one and only, or globally unique, X. The most common method of making the verified public keys available is to embed them in a certificate which is digitally signed by the trusted third party.

Relation between Encryption Schemes

A summary of basic key properties of two types of cryptosystems is given below –

	Symmetric Cryptosystems	Public Key Cryptosystems
Relation between Keys	Same	Different, but mathematically related
Encryption Key	Symmetric	Public
Decryption Key	Symmetric	Private

Due to the advantages and disadvantage of both the systems, symmetric key and public-key cryptosystems are often used together in the practical information security systems.

Now, we get to the basic types of cryptography. While reading about these types of cryptography, it may be helpful to think of a key as a key to a door.

One Time Pad

A one time pad is considered the only perfect encryption in the world. The sender and receiver must each have a copy of the same pad (a bunch of completely random numbers), which must be transmitted over a secure line. The pad is used as a symmetric key; however, once the pad is used, it is destroyed. This makes it perfect for extremely high security situations (for example, national secrets), but virtually unusable for everyday use (such as email).

Steganography

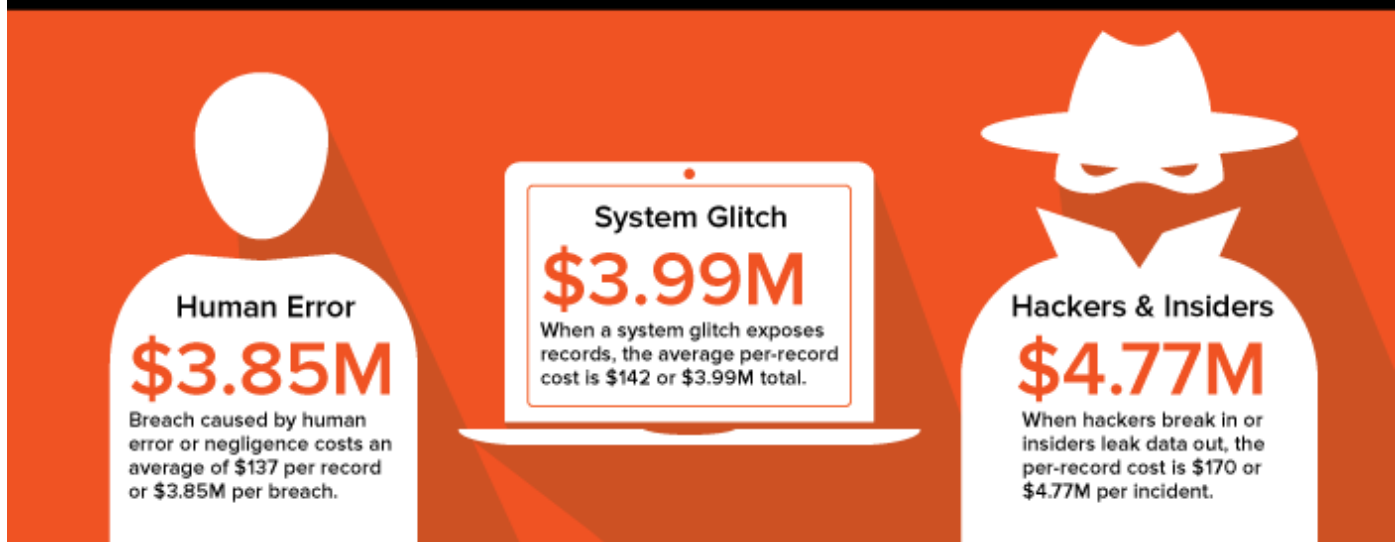
Steganography is actually the science of hiding information from people who would snoop on you. The difference between this and encryption is that the would-be snoopers may not be able to tell there's any hidden information in the first place. As an example, picture files typically have a lot of unused space in them. This space could be used to send hidden messages. If you do research on encryption, you may see the term steganography used on occasion. It is not, however, true encryption (though it can still be quite effective), and as such, we only mention it here for completeness.

Data Breach

A data breach is an incident where information is stolen or taken from a system without the knowledge or authorization of the system's owner. Victims of data breaches are usually large companies or organizations, and the data stolen may typically be sensitive, proprietary or confidential in nature (such as credit card numbers, customer data, trade secrets or matters of national security). Damage created by such incidents often presents itself as loss to the target company's reputation with their customer, due to a perceived 'betrayal of trust'. The damage may also involve the company's finances as well as that of their customers' should financial records be part of the information stolen.

The Cost of Data Breach

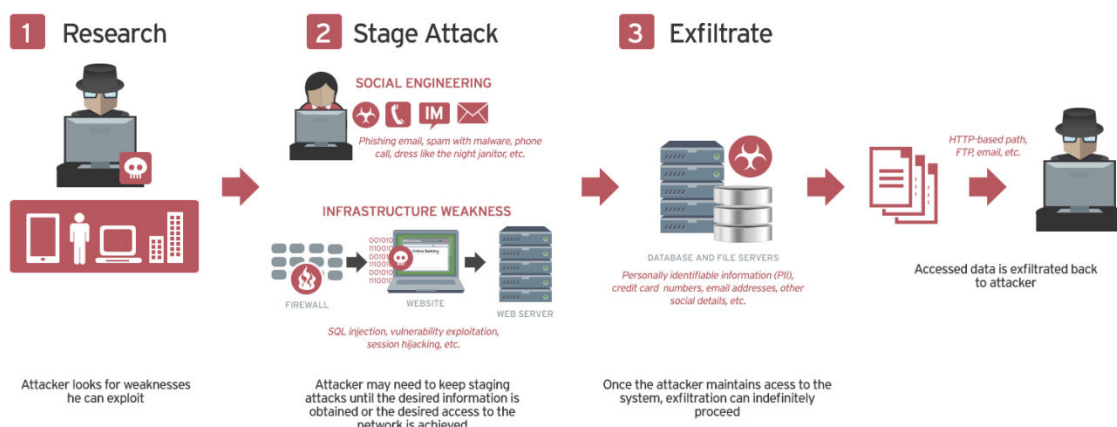
Data breach hits organizations squarely in the wallet. The average cost per record goes up depending on who or what caused the exposure.



Background

Data breaches may be a result of cybercriminal activity (targeted attacks) or by complete accident/human error (misplaced business laptop/smartphone).

How Data Breaches Occur



A typical data breach occurs in three phases:

- **Research.** The cybercriminal, having picked his target, looks for weaknesses that he can exploit: the target's employees, its systems, or its networks. This entails long hours of research on the cybercriminal's part, and may involve stalking employees' social networking profiles to finding what sort of infrastructure the company has.
- **Attack.** Having scoped out his target's weaknesses, the cybercriminal makes initial contact through either a network-based attack or through a social attacks
- In a **network** attack, the cybercriminal uses the weaknesses in the target's infrastructure to get into its network. These weaknesses may include (but are not limited to) SQL injection, vulnerability exploitation, and/or session hijacking.
- In a **social** attack, the cybercriminal uses social engineering in order to infiltrate the target's network. This may involve a maliciously-crafted email to one of the employees, tailor-made to catch that specific employee's attention. The mail could be a phishing mail, where the reader is fooled into supplying personal information to the sender, or one that comes with attached malware set to execute once accessed.

Either attack, if successful, allows the cybercriminal to:

- **Exfiltrate.** Once inside the network, the cybercriminal is free to extract the data he needs from the company's infrastructure and transmit it back to himself. This data may be used for either blackmail or black propaganda. It may also result in the cybercriminal having enough data for a more damaging attack on the infrastructure as well.

Other Causes of Data Breaches

- **Disgruntled employees.** Employees who mean to do harm to their employers by willingly stealing information from the company.
- **Lost or stolen devices.** Company devices that may be lost or stolen by employees who bring them home.
- **Malware-infected personal or network devices.** Company devices that may be infected with information-stealing malware.
- **Unintentional sharing.** Employees may accidentally share work-critical information, details and files with friends either through negligent file-handling practices or idle conversation.

Record Data Breaches

YEAR	ORGANIZATION	INDUSTRY	RECORDS STOLEN
2016	Myspace	Web	164000000
2016	VK	Web	100544934
2016	Turkish citizenship database	government	49611709
2016	Tumblr	Web	65,000,000
2016	LinkedIn	Web	117000000
2015	Voter Database	Web	191000000
2015	Anthem	Healthcare	80000000
2015	Securus Technologies	Web	70000000
2015	AshleyMadison.com	Web	37000000
2014	Ebay	Web	145000000
2014	JP Morgan Chase	Financial	76000000
2014	Home Depot	Retail	56000000
2013	Target	Retail	70000000
2013	Ubisoft	Gaming	58000000
2013	Evernote	Web	50000000
2013	Living Social	Web	50000000
2013	Adobe	Tech	36000000
2013	Court Ventures	Financial	200000000
2013	Massive American business hack	Financial	160000000

Best practices

For enterprises

Patch systems and networks accordingly.

IT administrators should make sure all systems in the network are patched and updated to prevent cybercriminals from exploiting vulnerabilities in unpatched/outdated software.

Educate and enforce.

Inform your employees about the threats, train them to watch out for social engineering tactics, and introduce and/or enforce guidelines on how to handle a threat situation if encountered.

Implement security measures.

Create a process to identify vulnerabilities and address threats in your network. Regularly perform security audits and make sure all of the systems connected to your company network are accounted for.

Create contingencies.

Put an effective disaster recovery plan in place. In the event of a data breach, minimize confusion by being ready with contact persons, disclosure strategies, actual mitigation steps, and the like. Make sure that your employees are made aware of this plan for proper mobilization once a breach is discovered.

For employees

Keep track of your banking receipts.

The first sign of being compromised by a cybercriminal is finding strange charges on your account that you did not make.

Don't believe everything you see.

Social engineering preys on the gullible. Be skeptical and vigilant.

Be careful of what you share on social media.

Don't get carried away by social media. If possible, don't list down too many details of yourself on your profile.

Secure all your devices.

Devices such as laptops, mobile devices, desktops should be secured. Ensure that they are protected by security software that is always updated.

Secure your accounts.

Use different email addresses and passwords for each account you have. You may opt to use a password manager to automate the process.

Do not open emails from unfamiliar senders.

If in doubt, delete them without opening it. Always try to verify who the sender is and the contents of the email first before opening any attachments.

The 8 Most Common Causes of Data Breach

It seems as though not a day goes by without a headline screaming that some organization has experienced a data breach, putting the business — and its customers and partners — at risk. To keep your own organization out of the news, it's important to understand the most common causes of data breaches and what you can do to mitigate the threats they present.

Weak and Stolen Credentials, a.k.a. Passwords

Hacking attacks may well be the most common cause of a data breach but it is often a weak or lost password that is the vulnerability that is being exploited by the opportunist hacker. Stats show that 4 in 5 breaches classified as a "hack" in 2012 were in-part caused by weak or lost (stolen) passwords!

Simple Solution: Use complex passwords and never share passwords.

Back Doors, Application Vulnerabilities

Why bother breaking the door down when the door is already open? Hackers love to exploit software applications which are poorly written or network systems which are poorly designed or implemented, they leave holes that they can crawl straight through to get directly at your data.

Simple Solution: Keep all software and hardware solutions fully patched and up to date.

Malware

The use of both direct and in-direct Malware is on the rise. Malware is by definition, malicious software; software loaded without intention that opens up access for a hacker to exploit a system and potentially other connected systems.

Simple Solution: Be wary of accessing web sites which are not what they seem or opening emails where you are suspicious of their origin, both of which are popular methods of spreading malware!

Social Engineering

As a hacker, why go to the hassle of creating your own access point to exploit when you can persuade others with a more legitimate claim to the much sought after data, to create it for you?

Simple Solution: If it looks too good to be true then it probably is too good to be true. Recognising which mail is genuine and which is not is very important.

Too Many Permissions

Overly complex access permissions are a gift to a hacker. Businesses that don't keep a tight rein on who has access to what within their organisation are likely to have either given the wrong permissions to the wrong people or have left out of date permissions around for a smiling hacker to exploit!

Simple Solution: Keep it Simple.

Insider Threats

The phrase "Keep your friends close and your enemies closer" could not be any more relevant. The rogue employee, the disgruntled contractor or simply those not bright enough to know better have already been given permission to access your data, what's stopping them copying, altering or stealing it?

Simple Solution: Know who you are dealing with, act swiftly when there is a hint of a problem and cover everything with process and procedure backed up with training.

Physical Attacks

Is your building safe and secure? Hackers don't just sit in back bedrooms in far off lands, they have high visibility jackets and a strong line in plausible patter to enable them to work their way into your building and onto your computer systems.

Simple Solution: Be vigilant, look out for anything suspicious and report it.

Improper Configuration, User Error

Mistakes happen and errors are made.

Simple Solution: With the correct professionals in charge of securing your data and the relevant and robust processes and procedures in place to prevent user error then mistakes and errors can be kept to a minimum and kept to those areas where they are less likely to lead to a major data breach.

Data Loss Prevention (DLP)

Data loss prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer.

DLP software products use business rules to classify and protect confidential and critical information so that unauthorized end users cannot accidentally or maliciously share data whose disclosure could put the organization at risk. For example, if an employee tried to forward a business email outside the corporate domain or upload a corporate file to a consumer cloud storage service like Dropbox, the employee would be denied permission.

Adoption of DLP is being driven by insider threats and by more rigorous state privacy laws, many of which have stringent data protection or access components. In addition to being able to monitor and control endpoint activities, some DLP tools can also be used to filter data streams on the corporate network and protect data in motion.

DLP products may also be referred to as data leak prevention, information loss prevention or extrusion prevention products.

Overview

Every organization fears losing its critical, confidential, highly restricted or restricted data. Fear of losing data amplifies for an organization if their critical data is hosted outside their premises, say onto a cloud model. To address this fear or issue that organizations face, a security concept known as "Data Loss Prevention" has evolved, and it comes in product flavors in the market. The most famous among them are Symantec, McAfee, Web-sense, etc. Each DLP product is designed to detect and prevent data from being leaked. These products are applied to prevent all channels through which data can be leaked.

Data is classified in the category of in-store, in-use and in-transit. We will learn about these classifications later in this article. Before starting the article, we have to keep in mind that the information is leaking from within the organization.

Types of Data to Protect

First of all we need to understand what type of data is needed to be protected. In DLP, data is classified in three categories:

- Data in motion: Data that needs to be protected when in transit i.e. data on the wire. This includes channels like HTTP/S, FTP, IM, P2P, SMTP.
- Data in use: Data that resides on the end user workstation and needs to be protected from being leaked through removable media devices like USB, DVD, CD's etc. will fall under this category.
- Data at rest: Data that resides on file servers and DBs and needs to be monitored from being getting leaked will fall under this category.

DLP Strategy

DLP products come with inbuilt policies that are already compliant with compliance standards like PCI, HIPPA, SOX, etc. Organizations just need to tune these policies with their organizational footprint. But the most important thing in DLP strategy is to identify the data to protect, because if an organization simply puts DLP across the whole organization, then a large number of false positives will result. The below section covers the data classification exercise.

Identify Sensitive Data

The first thing every organization should do is to identify all the confidential, restricted, and highly restricted data across the whole organization and across the three channels, i.e. for data in-transit, in-store and in-use. DLP products work with signatures to identify any restricted data when it is crossing boundaries. To identify the critical data and develop its signatures, there is a term in DLP products known as fingerprinting. Data is stored in various forms at various locations in an organization and it requires identifying and fingerprinting. Various products comes with a discovery engine which crawl all the data, index it and made it accessible though an intuitive interface which allows quick searching on data to find its sensitivity and ownership details.

Defining Policies

Once the sensitive data is discovered, an organization should build policies to protect the sensitive data. Every policy must consist of some rules, such as to protect credit card numbers, PII, and social security numbers. If there is a requirement for an organization to protect sensitive information and the DLP product does not support it out of the box, then organizations should create rules using regular expressions (regex). It should be noted that DLP policies at this stage should only be defined and not applied.

Determining Information Flow

It is very important for an organization to identify their business information flow. An organization should prepare a questionnaire to identify and extract all the useful information. A sample questionnaire is provided below:

- What should be the source and destination of the identified data?
- What are all the egress points present in the network?
- What processes are in place to govern the informational flow?

Identifying Business Owners of Data

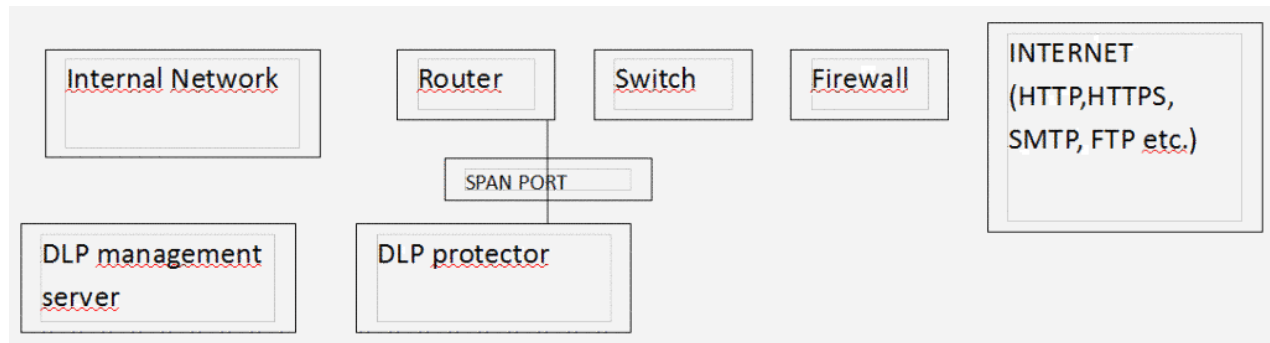
Identification of business owners of data is also an important step in the planning strategy of DLP, so a list should be prepared of whom to send the notifications to in case any sensitive data is lost.

Deployment Scenarios

As discussed earlier, sensitive data falls under three categories, i.e. data in motion, data at rest and data in use. After identifying the sensitive data and defining policies, the stage is then set up for the deployment of the DLP product. The below section covers the DLP deployment scenario of all three types:

- Data in motion: Data that needs to be protected when in transit, i.e. data on the wire. This includes channel like HTTP/S, FTP, IM, P2P, SMTP etc. The below diagram

shows the common implementation of DLP.



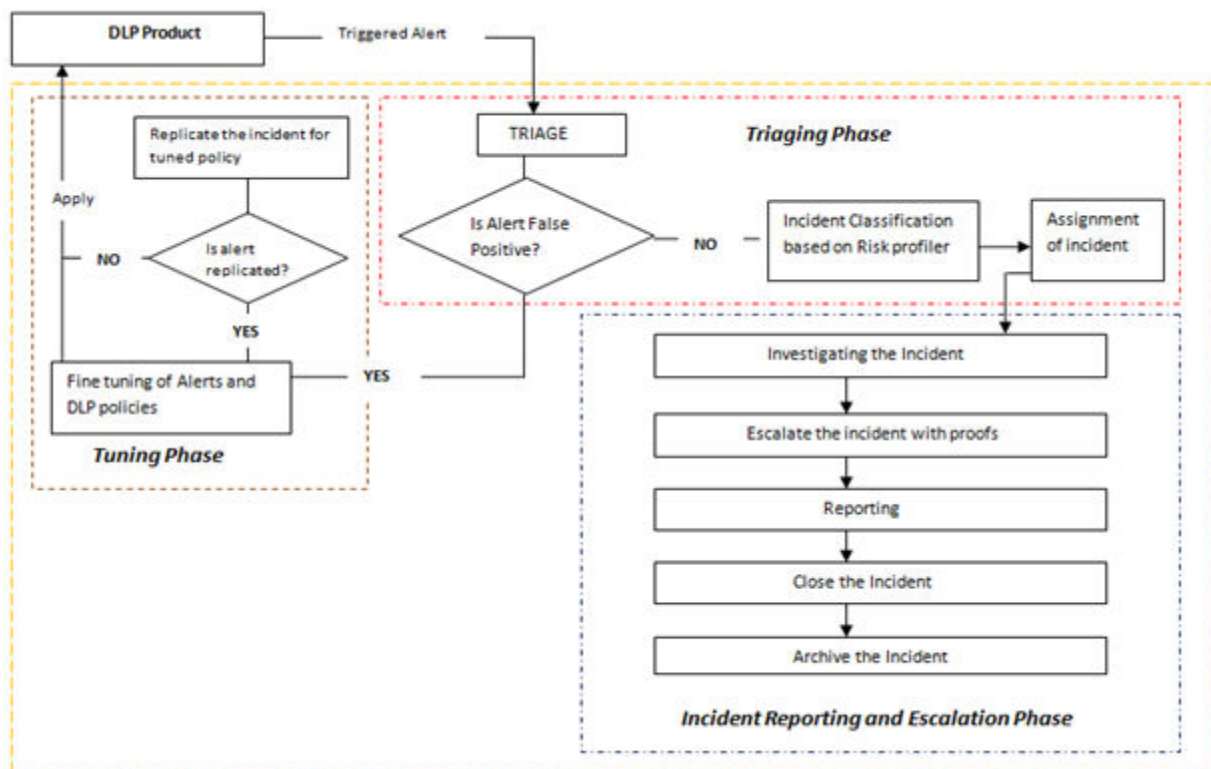
As in the above diagram, it is clear that DLP is not put in inline mode but rather put on a span port. It is very important to not put DLP protector appliance or software directly inline with the traffic, as every organization should start with a minimal basis and if put inline, it would result in huge number of false positives. In addition, if the DLP appliance is put in place, there is always a fear of network outage if the inline device fails. So the best approach is to deploy the DLP appliance in a span port first, and then after the DLP strategy is mature, then put into inline mode.

To mitigate the second risk, there can be two options. First, deploy DLP in High Availability mode, and second, configure the inline DLP product in bypass mode, which will enable the traffic to bypass the inline DLP product in case the DLP product is down.

- **Data in Use:** Data that resides on the end user workstation and needs to be protected from being leaked through removable media devices like USB, DVD, CDs, etc. will fall under this category. In Data in Use, an agent is installed in every endpoint device like laptop, desktop, etc. which is loaded with policies and is managed by the centralized DLP management server. Agents can be distributed on the endpoints via pushing strategies like SMS, GPO, etc. Since a DLP agent on the endpoint needs to interact with the centralized DLP management server in order to report incidents and get refreshed policies, the communication port must be added as an exception in the local firewall list.
- **Data in Store:** Data that resides on file servers and DBs and needs to be monitored from being getting leaked will fall under this category. All the data that resides in storage servers or devices are crawled using a DLP crawling agent. After crawling, data is fingerprinted to see any unstructured data is present or not.

DLP Operations

Deployment of security components is of no use if they cannot be monitored, and a DLP product is no exception. Below is an overview of what a DLP operation of an organization can be. First of all, the DLP product needs to be created with the right set of policies on the identified data among data at rest, in motion or in transit categories. I have tried to split the DLP operations into three phases, namely: triaging phase, reporting and escalation phase, and tuning phase. Let's understand these phases in detail.



- **Triaging phase:** In this phase, the security operation's team will monitor the alert fired or triggered by the policies set up in the DLP product. As mentioned earlier, DLP first should be put in observation mode to see and remove all the false positives. So when the security team receives the alert, the team will triage that event against various conditions like what type of data has been leaked, who has leaked it, through which channel it got leaked, any policy mis-configuration, etc. After performing this triaging, the team will declare the alert as an incident and start the incident classification phase where the team will process the incident with a risk profile. A risk profile is a text-based sheet which includes important information about the incident like type of policy, data type, channel type, severity type (low, medium, and high), etc. After processing and updating the risk profile, the security team will assign the incident to the respective team.
- **Incident Reporting and Escalation phase:** In this phase, the security team will assign the incident to the respective team. First, the security team will consult with the respective team to check whether the loss is a business acceptable risk or not. This can be due to reasons like change in policies at the backend, etc. If yes, the incident will be considered a false positive and moved to the tuning phase. If not, then the security team will escalate the incident along with proofs to the respective team. After escalating, security team will prepare the report as a part of monthly deliverable or for audit, and after this, the security team will close the incident and archive the incident. Archiving is important as some compliance requires it during a forensic investigation.
- **Tuning phase:** In this phase, all the incidents which are considered to be false positive are passed here. The security team's responsibility is to fine tune the policies as a result of some mis-configurations earlier or due to some business change and apply the changes to the DLP product as a draft version. To check whether the applied changes are fine, the incident is replicated and then checked whether the alert is generated or not. If not, then the changes are made final and applied, but if yes then fine tuning is required in the policies which are set up in the DLP product.

It should be noted that in DLP, there is no incident resolution phase, since any reported incident is a data loss (if it is not a false positive) and is thus escalated and then corresponding action is taken.

Best Practices for a Successful DLP Implementation

Below are some of the best practices that should be adopted in order to have a successful pre and post DLP deployment.

- Before choosing a DLP product, organizations should identify the business need for DLP.
- Organizations should identify sensitive data prior to DLP deployment.
- While choosing a DLP product, organizations should check whether the DLP product supports the data formats in which data is stored in their environment.
- After choosing a DLP product, DLP implementation should start with a minimal base to handle false positives and the base should be increasing with more identification of critical or sensitive data.
- DLP operations should be effective in triaging to eliminate false positives and fine tuning of DLP policies.
- A RACI matrix should be setup to draw out the responsibilities of DLP policies, implementation etc.
- A regular updating of risk profiles and a thorough documentation of the DLP incidents

Data Loss Prevention can provide some powerful protection for your sensitive information. It can be used to discover Personal Information (PI) within your environment, identify various forms of PI from names and phone numbers to government identifiers and credit card numbers, assemble multiple subsets of PI to accurately identify a whole record, and even do all of this in multiple languages.

It can also discover and identify Intellectual Property (IP), and even be trained to learn the difference between your IP and the IP of your business partners. It can alert you when someone tries to copy or share PI or IP. It can block or encrypt attempts to email, IM, blog, copy, or print this sensitive data. DLP can also "fingerprint" certain documents that you specifically want to protect or ignore.

DLP provides a strong set of capabilities, but it is primarily used to protect against unauthorized movements of sensitive data (e.g., the various ways you may transmit, copy or print sensitive data from one location to another). And, it is intended to provide this protection in one direction (inside-out). It is not intended to protect you from receiving sensitive data, but rather it is intended to protect the data you already have.

Pre-Installation Research

By implementing DLP you are about to invest a substantial amount of the company's money, time and resources. As a first step, research is important. Consult with research analysts such as Forrester or Gartner and gain a basic to intermediate understanding of the industry, the vendors and solutions available, and their particular strengths and weaknesses. Some DLP solutions offer robust features and support while others offer much less (i.e. "DLP Lite"). Understand company's environment and the ways in which sensitive data moves about before undertaking DLP.

Also, leverage your professional network. Ask what your peers are doing with DLP and what success or pains they've had. Talk to several vendors and narrow the field to a few. After narrowing the field, request preliminary pricing estimates — you will need this information for budgetary planning.

Note that far and away, most companies buy too much DLP. Plan to start small, pilot test in key areas, and grow into it. You will find that it will take you far longer to install, configure, optimize and find a way to effectively manage than you could have imagined. It does you, nor your company, no good to spend money on product or subscription licenses that go unused or are poorly deployed.

Give some thought to where DLP will be needed, and what it must accomplish to be successful.

Don't apply a shotgun approach unless it makes sense for your organization. Installing DLP on everything, everywhere can be very expensive and difficult to maintain. Think about the key applications and teams within your business that really need DLP technology due to the sensitivity of the data they have access to. You may find that you are able to apply an envelope of DLP protection around just your high-risk teams.

One way to think about this is to consider Pareto's "Law of the Vital Few" (or 80/20 rule). This principle states that 80% of your risks come from 20% of your sources. By focusing your DLP protections in your high-risk areas, you will make a significant positive impact on your company's risk profile and be able to share attractive ROI figures with senior management at the same time.

Identifying business requirements

Before diving into the technology and available vendor solutions, you should first build a good understanding of what your business requirements for DLP will be. Be sure that your business requirements include the following:

- **Transparency:** Requirements for transparency should be addressed so that it is clear what users may expect post installation. Think about how their use of data and information systems may change after the introduction of DLP into your environment. Will DLP complicate or simplify their lives?
- **Performance:** Consider the performance impact that your DLP solution may have on your environment. Performance of laptops and desktops may be impacted due to DLP endpoint client software, or large policies enforced at endpoints. The performance of your network and servers may also be impacted if DLP is used to aggressively discover the locations of sensitive data within your environment.
- **Compatibility:** Consider what operating systems and applications you will need DLP to support within your environment. Some DLP vendors provide support for Mac OS, but most don't for example.
- **Availability:** Consider whether your DLP solution will need to be highly available, or if best effort is good enough. If your DLP solution stops working for some reason, what will be the impact?

Define security requirements

After identifying your business requirements, next sketch out a set of security requirements to support them. You may decide you need to encrypt any PI when someone attempts to copy it to USB, or whenever someone attempts to move it off disk in any way. Perhaps you only care about large quantities of PI, so above a certain threshold you choose to block it from being moved. Or maybe you simply want DLP to alert support staff without blocking or encrypting anything. Each business has a different set of requirements. Define a set of security requirements that fit your specific business needs.

Communications

If you are pitching DLP to leadership, think "safety net" rather than "big brother." DLP should be considered a collaborative solution. Sell it in a positive light explaining how it can protect your sensitive data, keep your business out of the media (for the wrong reasons), and afford you a competitive advantage. Plan to involve key stakeholders from across the company early on. These key groups typically include IT, HR, Finance, Legal and Internal Audit. Later when you are ready to implement DLP, you will want and need support from these business leaders.

When you are ready to implement DLP, ensure that you apply good communications practices. Keep business leaders, stakeholders and users appropriately informed of your plans and timelines. The rule of thumb I follow for communications is:

- Tell them that you're going to tell them
- Tell them
- Then tell them that you told them

It seems redundant, but you will find this approach is highly effective in getting your message across. You will want to develop different communications for each segment of your business community; one for executive leadership; one for team leadership; and one for the end user population. Don't surprise anyone with DLP. Surprise in this case can quickly appear like "big brother" just moved in, and that is likely not the image you want.

Review architecture options

DLP solutions come in various forms including software, hardware or cloud-based solutions. Several DLP vendors offer a mixture of one or more of these. Depending on what sensitive data you wish to protect, where it resides, and how it is accessed, the DLP solution that is a best fit for your business may include any one or more of these.

Software-based DLP solutions include perpetual or subscription based licenses for endpoint clients and the management server. You will need to separately provide for the underlying computer hardware, operating system and virtualization software (if appropriate), a database server and management server.

Hardware based solutions include one or more DLP appliances. Minimally you will need to separately provide one or more Mail Transfer Agents (if you intend to encrypt or block emails), a database server and management server.

Cloud based DLP solutions typically represent a zero footprint subscription solution. Endpoint users are directed to your DLP cloud provider via either Web Cache Communication Protocol (WCCP) configurations on your routers, or a PAC file that is installed on each endpoint to redirect their outbound traffic to the DLP provider's cloud.

Roles & responsibilities

After you have a good idea which of the DLP architectures may best suit your needs, start to define the roles and responsibilities you will follow. Build a RACI chart which details who is responsible, who is accountable, who needs to be consulted and who is informed for each activity related to the care and feeding of your DLP solution. Doing so will clearly spell out who owns and does what. This will help you avoid conflicts with other support groups that manage DLP, or any of its underlying components, later on.

Each RACI entry is important, however, there are two particular items that you should include. First, ensure that you build in a segregation of duties to help prevent misuse. Do this by assigning rights to the security team allowing them to create DLP policies but not the ability to implement them. Then, assign rights to your support team (IT for example) allowing them to implement the DLP policies developed by the security team but not the ability to create policies. By applying this check and balance, we prevent a single team from subverting the solution or in causing harm by implementing something that should not have been implemented.

Secondly, it is very important to note that DLP will collect and report on the most sensitive information traversing your systems or networks. Think of all of the sensitive email discussions and documents shared between business leaders and board members, and HR for example. Allowing your support teams to be able to see this data is clearly inappropriate. You will therefore want to restrict access to the content of the DLP event (i.e., John Smith copied 1,000 names and social security numbers to a USB thumb drive and here are all of the social security numbers and names he copied).

On the other hand, the context of the DLP event should be available to support teams so they can address the event (i.e., John Smith copied 1,000 names and social security numbers to a USB thumb drive). Many DLP solutions provide for these distinctions. In fact,

it should be a showstopper if this capability does not exist in the solution you are considering.

Deploy cautiously & develop documentation

Deploy cautiously and consciously. Keep in mind that DLP is powerful technology, and if deployed improperly can impact key components of your communications. Keep your DLP deployments small at first. Then, as confidence with the solution grows expand into additional groups. Think about deploying to some of the highest risk areas of your business early on; you wouldn't want an otherwise preventable breach to have occurred while you were busy deploying to lower risk areas of the business, and you will learn more at the same time.

Begin by enabling monitoring only. Don't start out with blocking or auto-encrypting data until you are truly ready and understand the implications of getting any of this wrong. Expect help desk calls, and prepare your support teams so they are able to respond to them effectively. Determine what you will do when you learn of a given policy violation and gain alignment with stakeholders (Legal, HR, IT) for each scenario that is likely to occur.

Ensure that you document everything related to the architecture and deployment of DLP. If you were to burn it all to the ground, your documentation should be able to guide you through full re-deployment. If it cannot, then your documentation is insufficient. Lastly, share reports and metrics with leadership that illustrate the positive impact DLP is having on your ability to protect sensitive information. They will want to know how effectively their organization's money and resources have been spent.

DDoS Attack Protection

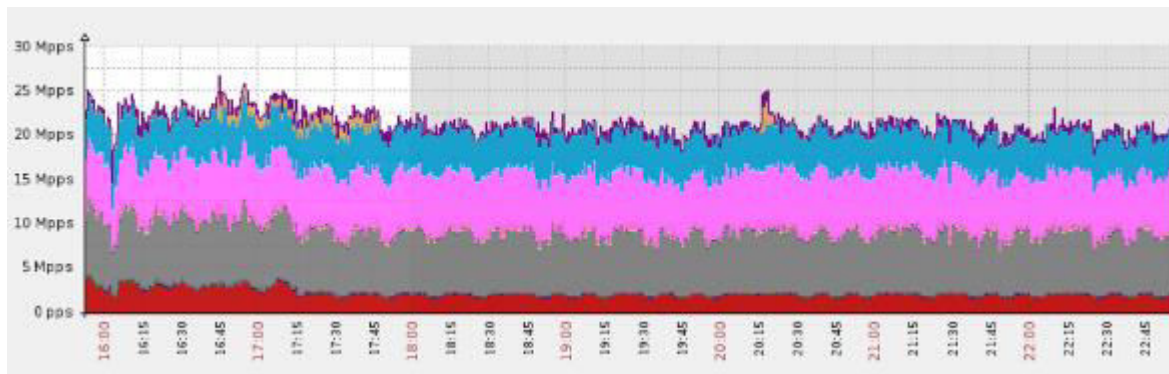
A distributed denial-of-service (DDoS) attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users.

In a typical DDoS attack, the assailant begins by exploiting a vulnerability in one computer system and making it the DDoS master. The attack master, also known as the botmaster, identifies and identifies and infects other vulnerable systems with malware. Eventually, the assailant instructs the controlled machines to launch an attack against a specified target.

Denial of Service Attack Types

DoS attacks can be divided into two general categories:

1. **Application layer attacks** (a.k.a., layer 7 attacks) can be either DoS or DDoS threats that seek to overload a server by sending a large number of requests requiring resource-intensive handling and processing. Among other attack vectors, this category includes HTTP floods, slow attacks (e.g., Slowloris or RUDY) and DNS query flood attacks.



Gaming website hit with a massive DNS flood, peaking at over 25 million packets per second

The size of application layer attacks is typically measured in requests per second (RPS), with no more than 50 to 100 RPS being required to cripple most mid-sized websites.

2. **Network layer attacks** (a.k.a., layer 3–4 attacks) are almost always DDoS assaults set up to clog the “pipelines” connecting your network. Attack vectors in this category include UDP flood, SYN flood, NTP amplification and DNS amplification attacks, and more.

Any of these can be used to prevent access to your servers, while also causing severe operational damages, such as account suspension and massive overage charges.

DDoS attacks are almost always high-traffic events, commonly measured in gigabits per second (Gbps) or packets per second (PPS). The largest network layer assaults can exceed 200 Gbps; however, 20 to 40 Gbps are enough to completely shut down most network infrastructures.

Attacker Motivations

DoS attacks are launched by individuals, businesses and even nation-states, each with their own particular motivation:

Hactivism – Hacktivists use DoS attacks as a means to express their criticism of everything from governments and politicians, including “big business” and current events. If they disagree with you, your site is going to go down (a.k.a., “tango down”).





Less technically-savvy than other types of attackers, hactivists tend to use premade tools to wage assaults against their targets. Anonymous is perhaps one of the best known hacktivist groups. They’re responsible for the cyberattack in February 2015 against ISIS, following the latter’s terrorist attack against the Paris offices of Charlie Hebdo, as well as the attack against the Brazilian government and World Cup sponsors in June 2014.

Typical assault method: DoS and DDoS

Cyber vandalism – Cyber vandals are often referred to as “script kiddies”—for their reliance on premade scripts and tools to cause grief to their fellow Internet citizens. These vandals are often bored teenagers looking for an adrenaline rush, or seeking to vent their anger or frustration against an institution (e.g., school) or person they feel has wronged them. Some are, of course, just looking for attention and the respect of their peers.

Alongside premade tools and scripts, cyber vandals will also result to using DDoS-for-hire services (a.k.a., booters or stressers), which can purchased online for as little as \$19 a pop.

Typical assault method: DoS and DDoS

\$23.99 1 month	\$34.99 1 month	\$44.99 10 years
1 Month Gold	1 Month Diamond	Lifetime Bronze
Time per boot	Time per boot	Time per boot
2400 sec	3600 sec	600 sec
Concurrents	Concurrents	Concurrents
1	2	2
Total network	Total network	Total network
220Gbps	220Gbps	220Gbps
Tools	Tools	Tools
Included	Included	Included
Support	Support	Support
24/7	24/7	24/7
Buy with Paypal   bitcoin	Buy with Paypal   bitcoin	Buy with Paypal   bitcoin

Example of booter advertised prices and capacities.

Extortion – An increasingly popular motivation for DDoS attacks is extortion, by which a cybercriminal demands money in exchange for stopping (or not carrying out) a crippling DDoS attack. Several prominent online software companies—including MeetUp, Bitly, Vimeo, and Basecamp—have been on the receiving end of these DDoS notes, some going offline after refusing to succumb to the extortionists' threats.

Similar to cyber vandalism, this type of attack is enabled by the existence of stresser and booter services.

Typical assault method: DDoS

Personal rivalry – DoS attacks can be used to settle personal scores or to disrupt online competitions. Such assaults often occur in the context of multiplayer online games, where players launch DDoS barrages against one another, and even against gaming servers, to gain an edge or to avoid imminent defeat by “flipping the table.”

Attacks against players are often DoS assaults, executed with widely available malicious software. Conversely, attacks against gaming servers are likely to be DDoS assaults, launched from stressers and booters .

Typical assault method: DoS, DDoS

Business competition – DDoS attacks are increasingly being used as a competitive business tool. Some of these assaults are designed to keep a competitor from participating in a significant event (e.g., Cyber Monday), while others are launched with a goal of completely shutting down online businesses for months.

One way or another, the idea is to cause disruption that will encourage your customers to flock to the competitor while also causing financial and reputational damage. An average cost of a DDoS attack to an organization can run \$40,000 per hour.

Business-feud attacks are often well-funded and executed by professional "hired guns," who conduct early reconnaissance and use proprietary tools and resources to sustain extremely aggressive and persistent DDoS attacks .

Typical assault method: DDoS

Cyberwarfare – State-sponsored DDoS attacks are being used to silence government critics and internal opposition, as well as a means to disrupt critical financial, health and infrastructure services in enemy countries.

Backed by nation-states, these well-funded and orchestrated campaigns are executed by tech-savvy professionals.

Typical assault method: DDoS

Preparing for DoS Attacks

The fact is that cybercrimes cannot be stooped, cybercriminals are going to attack. They will hit their targets, regardless of the defenses in place.

However, there are steps you can take to spot a brewing storm, including:

- Monitoring your traffic to look for abnormalities, including unexplained traffic spikes and visits from suspect IP address and geolocations. All of these could be signs of attackers performing "dry runs" to test your defenses before committing to a full-fledged attack. Recognizing these for what they are can help you prepare for the onslaught to follow.
- Keep an eye on social media (particularly Twitter) and public wastebins (e.g., Pastebin.com) for threats, conversations and boasts that may hint on an incoming attack.
- Consider using third-party DDoS testing (i.e., pen testing) to simulate an attack against your IT infrastructure so you can be prepared when the moment of truth arrives. When you undertake this, test against a wide variety of attacks, not just those with which you are familiar.
- Create a response plan and a rapid response team, whose job is to minimize the impact of an assault. When you plan, put in place procedures for your customer support and communication teams, not just for your IT professionals.

Four common categories of attacks



TCP Connection Attacks - Occupying connections

These attempt to use up all the available connections to infrastructure devices such as load-balancers, firewalls and application servers. Even devices capable of maintaining state on millions of connections can be taken down by these attacks.



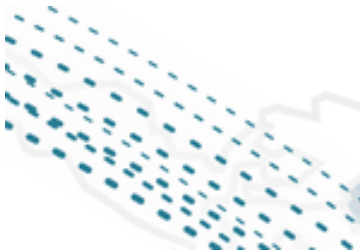
Volumetric Attacks - Using up bandwidth

These attempt to consume the bandwidth either within the target network/service, or between the target network/service and the rest of the Internet. These attacks are simply about causing congestion.



Fragmentation Attacks - Pieces of packets

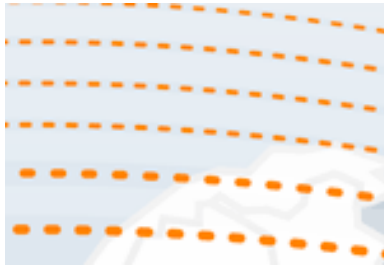
These send a flood of TCP or UDP fragments to a victim, overwhelming the victim's ability to re-assemble the streams and severely reducing performance.



Application Attacks - Targeting applications

These attempt to overwhelm a specific aspect of an application or service and can be effective even with very few attacking machines generating a low traffic rate (making them difficult to detect and mitigate).

Two ways attacks can multiply traffic they can send.



DNS Reflection - Small request, big reply.

By forging a victim's IP address, an attacker can send small requests to a DNS server and ask it to send the victim a large reply. This allows the attacker to have every request from its botnet amplified as much as 70x in size, making it much easier to overwhelm the target.



Chargen Reflection - Steady streams of text

Most computers and internet connected printers support an outdated testing service called Chargen, which allows someone to ask a device to reply with a stream of random characters. Chargen can be used as a means for amplifying attacks similar to DNS attacks above

Well-Known DDoS Attacks

This article would be incomplete without reference to some of the most well-known DDoS attacks. Some of the most famous documented DDoS attacks [12] [13] are summarized in the following:

- **Apache2**

This attack is mounted against an Apache Web server where the client asks for a service by sending a request with many HTTP headers. However, when an Apache Web server receives many such requests, it cannot confront the load and it crashes.

- **ARP Poison: Address Resolution Protocol (ARP)**

Poison attacks require the attacker to have access to the victim's LAN. The attacker deludes the hosts of a specific LAN by providing them with wrong MAC addresses for hosts with already-known IP addresses. This can be achieved by the attacker through the following process: The network is monitored for "arp who-has" requests. As soon as such a request is received, the malevolent attacker tries to respond as quickly as possible to the questioning host in order to mislead it for the requested address.

- [Back](#)

This attack is launched against an apache Web server, which is flooded with requests containing a large number of front-slash (/) characters in the URL description. As the server tries to process all these requests, it becomes unable to process other legitimate requests and hence it denies service to its customers.

- [CrashIIS](#)

The victim of a CrashIIS attack is commonly a Microsoft Windows NT IIS Web server. The attacker sends the victim a malformed GET request, which can crash the Web server.

- [DoSNuke](#)

In this kind of attack, the Microsoft Windows NT victim is inundated with "out-of-band" data (MSG_OOB). The packets being sent by the attacking machines are flagged "urg" because of the MSG_OOB flag. As a result, the target is weighed down, and the victim's machine could display a "blue screen of death."

- [Land](#)

In Land attacks, the attacker sends the victim a TCP SYN packet that contains the same IP address as the source and destination addresses. Such a packet completely locks the victim's system.

- [Mailbomb](#)

In a Mailbomb attack, the victim's mail queue is flooded by an abundance of messages, causing system failure.

- [SYN Flood](#)

A SYN flood attack occurs during the three-way handshake that marks the onset of a TCP connection. In the three-way handshake, a client requests a new connection by sending a TCP SYN packet to a server. After that, the server sends a SYN/ACK packet back to the client and places the connection request in a queue. Finally, the client acknowledges the SYN/ACK packet. If an attack occurs, however, the attacker sends an abundance of TCP SYN packets to the victim, obliging it both to open a lot of TCP connections and to respond to them. Then the attacker does not execute the third step of the three-way handshake that follows, rendering the victim unable to accept any new incoming connections, because its queue is full of half-open TCP

connections.

- **Ping of Death**

In Ping of Death attacks, the attacker creates a packet that contains more than 65,536 bytes, which is the limit that the IP protocol defines. This packet can cause different kinds of damage to the machine that receives it, such as crashing and rebooting.

- **Process Table**

This attack exploits the feature of some network services to generate a new process each time a new TCP/IP connection is set up. The attacker tries to make as many uncompleted connections to the victim as possible in order to force the victim's system to generate an abundance of processes. Hence, because the number of processes that are running on the system cannot be boundlessly large, the attack renders the victim unable to serve any other request.

- **Smurf Attack**

In a "smurf" attack, the victim is flooded with *Internet Control Message Protocol* (ICMP) "echo-reply" packets. The attacker sends numerous ICMP "echo-request" packets to the broadcast address of many subnets. These packets contain the victim's address as the source IP address. Every machine that belongs to any of these subnets responds by sending ICMP "echo-reply" packets to the victim. Smurf attacks are very dangerous, because they are strongly distributed attacks.

- **SSH Process Table**

Like the Process Table attack, this attack makes hundreds of connections to the victim with the *Secure Shell*(SSH) Protocol without completing the login process. In this way, the daemon contacted by the SSH on the victim's system is obliged to start so many SSH processes that it is exhausted.

- **Syslogd**

The Syslogd attack crashes the *syslogd* program on a Solaris 2.5 server by sending it a message with an invalid source IP address.

- **TCP Reset**

In TCP Reset attacks, the network is monitored for "tcpconnection" requests to the victim. As soon as such a request is found, the malevolent attacker sends a spoofed TCP RESET packet to the victim and obliges it to terminate the TCP connection.

- **Teardrop**

While a packet is traveling from the source machine to the destination machine, it may be broken up into smaller fragments, through the process of fragmentation. A Teardrop attack creates a stream of IP fragments with their offset field overloaded. The destination host that tries to reassemble these malformed fragments eventually crashes or reboots.

- **UDP Storm**

In a *User Datagram Protocol* (UDP) connection, a character generation ("chergen") service generates a series of characters each time it receives a UDP packet, while an echo service echoes any character it receives. Exploiting these two services, the attacker sends a packet with the source spoofed to be that of the victim to another machine. Then, the echo service of the former machine echoes the data of that packet back to the victim's machine and the victim's machine, in turn, responds in the same way. Hence, a constant stream of useless load is created that burdens the network.

Tools against DDoS Attack

Some of the best tools to help protect against DDoS attacks are:

1. Cloudflare

Cloudflare's layer 3 and 4 protection absorbs an attack before it reaches a server, which load balancers, firewalls, and routers do not.

Its layer 7 protection differentiates between beneficial and harmful traffic. Cloudflare clients include Cisco, Nasdaq, MIT and...the Eurovision song contest.

2. F5 Networks

F5 Networks Silverline has a huge traffic scrubbing capacity, and offers protection either onsite, in the cloud, or a combination of the two.

It offers protection across levels 3 to 7. Silverline can prevent high volume networks, stopping them reaching a company's network. 24/7 support is available.

3. Black Lotus

The firm's Protection for Networks service was designed with a focus on the hosting industry, and can be white labelled for their use.

Its protection for Services tool can be filtered and proxied at Layer 4, and requests are mitigated at layer 7. It also has a patent pending on Human Behaviour Analysis technology, to improve its service.

4. Arbor networks

From the security division of Netscout, Arbor Cloud offers both on site cloud protection for state-exhausting attacks against security infrastructure.

It also offers a multi-terabit, on-demand traffic scrubbing service, and 24/7 DDoS support via its Security Operations Center.

5. Incapsula

The Top Ten Reviews listing site gave Incapsula a gold award for its DDoS protection service this year. It has a global network of data centres, so can provide more scrubbing centres than many other providers.

It offers blanket protection against DDoS either as an always on service or on demand, and a 24/7 security team.

Embedded System Security

Embedded system security is the reduction of vulnerabilities and protection against threats in software running on embedded devices.

Like security in most IT fields, embedded system security involves a conscientious approach to hardware design and coding as well as added security software, an adherence to best practices and consultation with experts.

In the past, the large number of embedded operating systems and the fact that these systems did not typically have direct Internet communication provided some degree of security, both through obscurity and the fact that they were not convenient targets.

Traditionally, many of the hardware and hardware systems controlled by embedded software have not been easily interfaced with as they had little need to be exposed. Trends like machine-to-machine (M2M) communication, the Internet of Things and remotely-controlled industrial systems, however, have increased the number of connected devices and simultaneously made these devices targets.

The similarities between embedded OSes and live firmware updating in conjunction with the increased number of communication points create a large increase in the attack surface: Each communication point is a potential point of entry for hackers. A device's firmware may be hacked to spy on and take control of everything from Internet and wireless access points, USB accessories, IP cameras and security systems to pace makers, drones and industrial control systems.

Secure embedded system design challenges

Designers of a large and increasing number of embedded systems need to support various security solutions in order to deal with one or more of the security requirements described earlier. These requirements present significant bottlenecks during the embedded system design process, which are briefly described below:

1. Processing Gap

Existing embedded system architectures are not capable of keeping up with the computational demands of security processing, due to increasing data rates and complexity of security protocols. These shortcomings are most felt in systems that need to process very high data rates or a large number of transactions (e.g., network routers, firewalls, and web servers), and in systems with modest processing and memory

2. Battery Gap

The energy consumption overheads of supporting security on battery-constrained embedded systems are very high. Slow growth rates in battery capacities (5–8% per year) are easily outpaced by the increasing energy requirements of security processing, leading to a battery gap. Various studies [Carman et al. 2000; Perrig et al. 2002; Potlapally et al. 2003] show that the widening battery gap would require designers to make energy-aware design choices (such as optimized security protocols, custom security hardware, and so on) for security.

3. Flexibility

An embedded system is often required to execute multiple and diverse security protocols and standards in order to support (i) multiple security objectives (e.g., secure communications, DRM, and so on), (ii) interoperability in different environments (e.g., a handset that needs to work in both 3G cellular and wireless LAN environments), and (iii) security processing in different layers of the network protocol stack (e.g., a wireless LAN enabled PDA that needs to connect to a virtual private network, and support secure web browsing may need to execute WEP, IPSec, and SSL). Furthermore, with security protocols being constantly targeted by hackers, it is not surprising that they keep continuously evolving (see also Section 5.4). It is, therefore, desirable to allow the security architecture to be flexible (programmable) enough to adapt easily to changing requirements. However, flexibility may also make it more difficult to gain assurance of a design's security.

4. Tamper Resistance

Attacks due to malicious software such as viruses and trojan horses are the most common threats to any embedded system that is capable of executing downloaded applications [Howard and LeBlanc 2002; Hoglund and McGraw 2004; Ravi et al. 2004]. These attacks can exploit vulnerabilities in the operating system (OS) or application software, procure access to system internals, and disrupt its normal functioning. Because these attacks manipulate sensitive data or processes (integrity attacks), disclose confidential information (privacy attacks), and/or deny access to system resources (availability attacks), it is necessary to develop and deploy various HW/SW

countermeasures against these attacks. In many embedded systems such as smartcards, new and sophisticated attack techniques, such as bus probing, timing analysis, fault induction, power analysis, electromagnetic analysis, and so on, have been demonstrated to be successful in easily breaking their security [Ravi et al. 2004; Anderson and Kuhn 1996, 1997; Kommerling and Kuhn 1999; Rankl and Effing; Hess et al. 2000; Quisquater and Samyde 2002; Kelsey et al. 1998]. Tamper resistance measures must, therefore, secure the system implementation when it is subject to various physical and side-channel attacks. Later in this paper (see Section 6), we will discuss some examples of embedded system attacks and related countermeasures.

5. Assurance Gap

It is well known that truly reliable systems are much more difficult to build than those that merely work most of the time. Reliable ACM Transactions on Embedded Computing Systems, Vol. 3, No. 3, August 2004. 468 • S. Ravi et al. systems must be able to handle the wide range of situations that may occur by chance. Secure systems face an even greater challenge: they must continue to operate reliably despite attacks from intelligent adversaries who intentionally seek out undesirable failure modes. As systems become more complicated, there are inevitably more possible failure modes that need to be addressed. Increases in embedded system complexity are making it more and more difficult for embedded system designers to be confident that they have not overlooked a serious weakness.

6. Cost

One of the fundamental factors that influence the security architecture of an embedded system is cost. To understand the implications of a security-related design choice on the overall system cost, consider the decision of incorporating physical security mechanisms in a single-chip cryptographic module. The Federal Information Processing Standard (FIPS 140-2) [FIPS] specifies four increasing levels of physical (as well as other) security requirements that can be satisfied by a secure system. Security Level 1 requires minimum physical protection, Level 2 requires the addition of tamper-evident mechanisms such as a seal or enclosure, while Level 3 specifies stronger detection and response mechanisms. Finally, Level 4 mandates environmental failure protection and testing (EFP and EFT), as well as highly rigorous design processes. Thus, we can choose

to provide increasing levels of security using increasingly advanced measures, albeit at higher system costs, design effort, and design time. It is the designer's responsibility to balance the security requirements of an embedded system against the cost of implementing the corresponding security measures.

Use of Embedded Systems

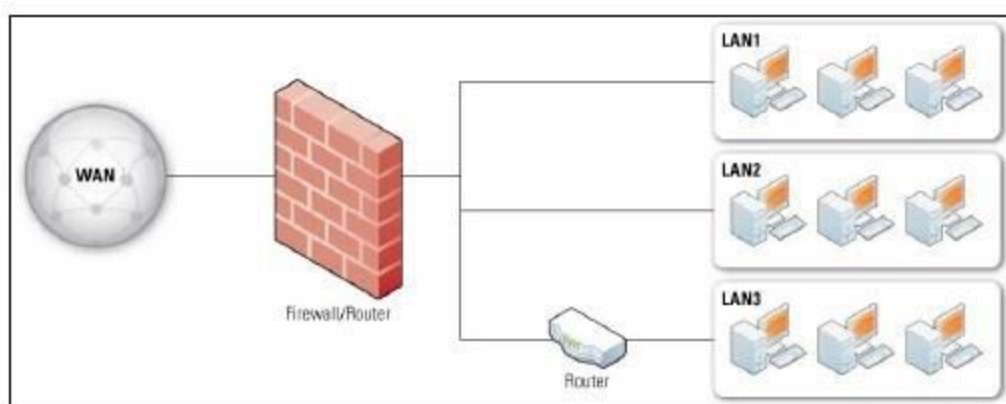
Home Applications	Dishwasher, Washing Machine, Microwave Oven, Top-set Box, Home Security Systems, HVAC system, DVD player, Answering Machine, Garden Sprinkler Systems, Lighting Systems, Remote Controls, Air Conditioners, Sprinklers.
Consumer Electronic Products	Cell phones, Cordless Phones, Digital Cameras, Video recorders, DVD players, TV set, Calculators, MP3 Players, Stereo Systems, Cable TV tuners, Digital watches, Personal PDA, iPhone.
Industrial applications	Personal Smart Phone, Fax Machines, Photo Copy Machines, Printers, Scanners, Assembly Line, Data Collection System, Monitoring Systems on Pressure, Voltage, Current, Temperature, Hazard Detecting System, Industrial Robot.
Business Equipment	ATM, Cash Registers, Alarm Systems, Card Readers, Finger Print Detectors, Automatic Toll Systems, Voice recognizers, Smart Vendor Machine, Cash Register, Bar Code Reader.
<u>Automobile</u>	GPS, Fuel Injection Controller, Anti-locking Brake System, Transmission Controller, Cruise Control, Active Suspension, Air- bag System, Air-Conditioner.
Communication Systems	Router, Hub, Cell Phone, Web Camera, Modem, Network Cards, Tele-conferencing System.
Aerospace	GPS system, Automatic Landing System, Flight Attitude Controller Inertial Guidance System, Space Robotics, RADAR.
Medical Technology	CT scanner, ECG, EEG, EMG, MRI, Glucose Monitor, Blood Pressure Monitor, Diagnostic Device, X-ray machines, Digital Pulse Monitor.
Security Systems	Face Recognition System, Finger Recognition, Irish Recognition, Building Security System, Airport Security System, Alarm System, Digital Access Card, Fingerprint based Smart Card.
Classroom applications	Smart Board, Smart Room, OCR, Calculator, Smart Cord, Stereo Systems, Projector.
Game and Entertainment	Video games, Robot, MP3, Mind Storm, Smart Toy.

Firewall

A firewall is a hardware or software system that prevents unauthorized access to or from a network. It can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet. All data entering or leaving the intranet pass through the firewall, which examines each packet and blocks those that do not meet the specified security criteria.

Generally, firewalls are configured to protect against unauthenticated interactive logins from the outside world. This helps prevent hackers from logging into machines on your network. More sophisticated firewalls block traffic from the outside to the inside, but permit users on the inside to communicate a little more freely with the outside.

Firewalls are essential since they provide a single block point, where security and auditing can be imposed. Firewalls provide an important logging and auditing function; often, they provide summaries to the administrator about what type/volume of traffic has been processed through it. This is an important benefit: Providing this block point can serve the same purpose on your network as an armed guard does for your physical premises.



Simple Routed Network with Firewall Device

Types of firewalls

The National Institute of Standards and Technology (NIST) 800-10 divides firewalls into three basic types:

Packet filters

Stateful inspection

Proxys

These three categories, however, are not mutually exclusive, as most modern firewalls have a mix of abilities that may place them in more than one of the three.

One way to compare firewalls is to look at the Transmission Control Protocol/Internet Protocol (TCP/IP) layers that each is able to examine. TCP/IP communications are composed of four layers; they work together to transfer data between hosts. When data transfers across networks, it travels from the highest layer through intermediate layers to the lowest layer; each layer adds more information. Then the lowest layer sends the accumulated data through the physical network; the data next moves upward, through the layers, to its destination. Simply put, the data a layer produces is encapsulated in a larger container by the layer below it. The four TCP/IP layers, from highest to lowest, are described further in the figure below.

Application Layer. This layer sends and receives data for particular applications, such as Domain Name System (DNS), Hypertext Transfer Protocol (HTTP), and Simple Mail Transfer Protocol (SMTP). The application layer itself has layers of protocols within it. For example, SMTP encapsulates the Request for Comments (RFC) 2822 message syntax, which encapsulates Multipurpose Internet Mail Extensions (MIME), which can encapsulate other formats such as Hypertext Markup Language (HTML).
Transport Layer. This layer provides connection-oriented or connectionless services for transporting application layer services between networks, and can optionally ensure communications reliability. Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are commonly used transport layer protocols. ²
IP Layer (also known as the Network Layer). This layer routes packets across networks. Internet Protocol version 4 (IPv4) is the fundamental network layer protocol for TCP/IP. Other commonly used protocols at the network layer are Internet Protocol version 6 (IPv6), ICMP, and Internet Group Management Protocol (IGMP).
Hardware Layer (also known as the Data Link Layer). This layer handles communications on the physical network components. The best known data link layer protocol is Ethernet.

TCP/IP Layers

Firewall implementation

The firewall remains a vital component in any network security architecture, and today's organizations have several types to choose from. It's essential that IT professionals identify the type of firewall that best suits the organization's network security needs.

Once selected, one of the key questions that shapes a protection strategy is "Where should the firewall be placed?" There are three common firewall topologies: the bastion host, screened subnet and dual-firewall architectures. Enterprise security depends on choosing the right firewall topology.

The next decision to be made, after the topology chosen, is where to place individual firewall systems in it. At this point, there are several types to consider, such as bastion host, screened subnet and multi-homed firewalls.

Remember that firewall configurations do change quickly and often, so it is difficult to keep on top of routine firewall maintenance tasks. Firewall activity, therefore, must be continuously audited to help keep the network secure from ever-evolving threats.

Network layer firewalls

Network layer firewalls generally make their decisions based on the source address, destination address and ports in individual IP packets. A simple router is the traditional network layer firewall, since it is not able to make particularly complicated decisions about what a packet is actually talking to or where it actually came from.

One important distinction many network layer firewalls possess is that they route traffic directly through them, which means in order to use one, you either need to have a validly assigned IP address block or a private Internet address block. Network layer firewalls tend to be very fast and almost transparent to their users.

Application layer firewalls

Application layer firewalls are hosts that run proxy servers, which permit no traffic directly between networks, and they perform elaborate logging and examination of traffic passing through them. Since proxy applications are simply software running on the firewall, it is a good place to do logging and access control. Application layer firewalls can be used as network address translators, since traffic goes in one side and out the other after having passed through an application that effectively masks the origin of the initiating connection.

In some cases, having an application in the way may impact performance and make the firewall less transparent. Older application layer firewalls that are still in use are not

particularly transparent to end users and may require some user training. However, more modern application layer firewalls are often totally transparent. Application layer firewalls tend to provide more detailed audit reports and tend to enforce more conservative security models than network layer firewalls.

Proxy firewalls

Proxy firewalls offer more security than other types of firewalls, but at the expense of speed and functionality, as they can limit which applications the network supports.

Unlike stateful firewalls or application layer firewalls, which allow or block network packets from passing to and from a protected network, traffic does not flow through a proxy. Instead, computers establish a connection to the proxy, which serves as an intermediary, and initiate a new network connection on behalf of the request. This prevents direct connections between systems on either side of the firewall and makes it harder for an attacker to discover where the network is, because they don't receive packets created directly by their target system.

Proxy firewalls also provide comprehensive, protocol-aware security analysis for the protocols they support. This allows them to make better security decisions than products that focus purely on packet header information.

Placement of a firewall

When developing a perimeter protection strategy for an organization, one of the most common questions is "Where should I place firewalls for maximum effectiveness?"

Security expert Mike Chapple breaks up firewall placement into three basic topology options: **bastion host**, **screened subnet** and **dual firewalls**.

The first, **bastion host** topology, is the most basic option, and is well suited for relatively simple networks. This topology would work well if you're merely using the firewall to protect a corporate network that is used mainly for surfing the Internet, but it is probably *not* sufficient if you host a website or email server.

The **screened subnet** option provides a solution that allows organizations to offer services securely to Internet users. Any servers that host public services are placed in the demilitarized zone (DMZ), which is separated from both the Internet and the trusted network by the firewall. Therefore, if a malicious user does manage to compromise the firewall, he or she does not have access to the Intranet (providing that the firewall is properly configured).

The most secure (and most expensive) option is to implement a **screened subnet** using two firewalls. The use of two firewalls still allows the organization to offer services to Internet users through the use of a DMZ, but provides an added layer of protection.

Are two firewalls better than one?

Most enterprises use a combination of firewalls, virtual private networks (VPNs) and intrusion detection/prevention systems (IDS/IPS) to limit access to internal networks.

Generally speaking, there isn't much work to do in these areas; it's about maintaining these controls and adapting them as dynamic infrastructures change. The maturity of the technology offers the opportunity to focus limited financial and human resources on more challenging problems, such as endpoint/server management and application security.

Two firewalls from different vendors may not cause processing delays, but if not used and arranged correctly, the devices can become a hassle for IT teams. If you're experiencing network latency by adding an additional firewall, consider the placement of the firewalls. Are they both directly connected to each other with nothing else in between? If that's the case, consider using a different firewall topology that will get the most out of the two firewalls.

Firewall implementation precautions

Many people think that as long as their SAN or NAS is behind a firewall then everything is protected. This is a myth of network security. Most storage environments span across multiple networks, both private and public.

Storage devices are serving up multiple network segments and creating a virtual bridge that basically negates any sort of firewall put in place. This can provide a conduit into the storage environment, especially when a system is attacked and taken control of in the DMZ or public segment. The storage back end can then be fully accessible to the attacker because there is a path for the attack.

Firewall management and maintenance

We can only dream that once you've made it through the challenging phases of firewall selection and architecture design, you're finished setting up a DMZ. In the real world of firewall management, we're faced with balancing a continuous stream of change requests and vendor patches against the operational management of our firewalls. Configurations change quickly and often, making it difficult to keep on top of routine maintenance tasks.

According to the Network security, expert Michael Chapple four practical areas where some basic log analysis can provide valuable firewall management data are:

Monitor rule activity

System administrators tend to be quick on the trigger to ask for new rules, but not quite so eager to let you know when a rule is no longer necessary. Monitoring rule activity can provide some valuable insight to assist you with managing the rulebase. If a rule that was once heavily used suddenly goes quiet, you should investigate whether the rule is still needed. If it's no longer necessary, trim it from your rulebase. Legacy rules have a way of piling up and adding unnecessary complexity.

Over the years, Chapple had a chance to analyze the rulebases of many production firewalls, and estimates that at least 20% of the average firewall's rulebase is unnecessary. There are systems where this ratio is as high as 60%.

Traffic flows

Monitor logs for abnormal traffic patterns. If servers that normally receive a low volume of traffic are suddenly responsible for a significant portion of traffic passing through the firewall (either in total connections or bytes passed), then you have a situation worthy of further investigation. While flash crowds are to be expected in some situations (such as a Web server during a period of unusual interest), they are also often signs of misconfigured systems or attacks in progress.

Rule violations

Looking at traffic denied by your firewall may lead to interesting findings. This is especially true for traffic that originates from inside your network. The most common cause of this activity is a misconfigured system or a user who isn't aware of traffic restrictions, but analysis of rule violations may also uncover attempts at passing malicious traffic through the device.

Denied probes

If you've ever analyzed the log of a firewall that's connected to the Internet, you know that it's futile to investigate probes directed at your network from the Internet. They're far too frequent and often represent dead ends. However, you may not have considered analyzing logs for probes originating from *inside* the trusted network. These are extremely interesting, as they most likely represent either a compromised internal system seeking to scan Internet hosts or an internal user running a scanning tool -- both scenarios that merit attention.

Firewall audit logs are a veritable goldmine of network security intelligence whose advantage the organization can take.

Fraud Detection and Prevention

Risk and Materiality are two concepts that are well known and understood by auditors. In the area of fraud these concepts apply to the risk of experiencing a fraud and the materiality of the losses to fraud. The assessment of the importance of these factors will, to some degree, determine how serious the company treats the prevention and detection of fraud. It will also affect the resources devoted to fraud related tasks by audit, so it is important for all auditors to give proper consideration to the risk and material of fraud in their organization.

What is Fraud?

There are many definitions for fraud and a number of possible criminal charges, including: fraud, theft, embezzlement, and larceny. The legal definition usually refers to a situation where:

- A person makes a material false statement
- The victim relies on that statement
- The criminal benefits

It should be noted that persons inside the organization or external to it could commit fraud. Further, it can be to the benefit of an individual; to part of an organization; or to the whole organization itself.

However, the most expensive and most difficult fraud for auditors to deal with is one that is committed by senior management - particularly if it is 'for' the benefit of the organization.

Why Does Fraud Happen?

Interviews with persons who committed fraud have shown that most people do not originally set out to commit fraud. Often they simply took advantage of an opportunity; many times the first fraudulent act was an accident – perhaps they mistakenly processed the same invoice twice. But when they realized that it wasn't noticed, the fraudulent acts became deliberate and more frequent. Fraud investigators talk about the 10 - 80 - 10 law which states that 10% of people will never commit fraud; 80% of people will commit fraud under the right circumstances; and 10% actively seek out opportunities for fraud. So we need to be vigilant for the 10% who are out to get us and we should try to protect the 80% from making a mistake that could ruin their lives.

Generally, fraud occurs because of a combination of opportunity, pressure and rationalization. An opportunity arises, the person feels that the act is not entirely wrong, and has pressure pushing them to commit the fraud.

Opportunity

An opportunity is likely to occur when there are weaknesses in the internal control framework or when a person abuses a position of trust. For example:

- Organizational expediency – 'it was a high profile rush project and we had to cut corners'
- Downsizing meant that there were fewer people and separation of duties no longer existed
- Business re-engineering brought in new application systems that changed the control framework, removing some of the key checks and balances

Pressure

The pressures are usually financial in nature, but this is not always true. For example, unrealistic corporate targets can encourage a salesperson or production manager to commit fraud. The desire for revenge – to get back at the organization for some perceived wrong; or poor self-esteem - the need to be seen as the top salesman, at any cost; are also examples of non-financial pressures that can lead to fraud.

Rationalization

In the criminal's mind rationalization usually includes the belief that the activity is not criminal. They often feel that everyone else is doing it; or that no one will get hurt; or it's just a temporary loan, I'll pay it back, and so on.

Interestingly, studies have shown that the removal of the pressure is not sufficient to stop an ongoing fraud. Also, the first act of fraud requires more rationalization than the second act, and so on. But, as it becomes easier to justify, the acts occur more often and the amounts involved increase in value. This means that, left alone, fraud will continue and the losses will only increase. I have heard it said that 'There is no such thing as a fraud that has reached maturity'. Fraud, ultimately, is fed by greed, and greed is never satisfied.

Who is responsible for the prevention and detection of fraud?

There are two main views - one states that management has the responsibility for the prevention and for the detection of fraud.

Management

- is responsible for the day to day business operations
- is responsible for developing and implementing controls
- has authority over the people, systems, and records
- has the knowledge, and authority to make changes

Therefore, fraud prevention and detection is their problem.

Audit

- has expertise in the evaluation and design of controls
- reviews and evaluates operations and controls
- has a requirement to exercise 'Due Diligence'

Therefore, fraud prevention and detection is audit's problem.

The reality is that both management and audit have roles to play in the prevention and detection of fraud. The best scenario is one where management, employees, and internal and external auditors work together to combat fraud. Furthermore, internal controls alone are not sufficient, corporate culture, the attitudes of senior management

and all employees, must be such that the company is fraud resistant. Unfortunately, many auditors feel that corporate culture is beyond their sphere of influence. However, audit can take steps to ensure that senior management is aware of the risk and materiality of fraud and that all instances of fraud are made known to all employees. Also audit can encourage management to develop Fraud Awareness Training and a Fraud Policy to help combat fraud. Finally, audit can review and comment on organizational goals and objectives to reduce the existence of unrealistic performance measures. So, there are a number of things auditors can do to help create a fraud resistant corporate culture.

FRAUD AWARENESS TRAINING

Fraud Awareness Training is a critical step in deterring fraud. It emphasizes the role that all employees have in preventing and detecting fraud - not just auditors. Often it is tied to a corporate ethics program, laying the foundation for all aspects of employee behavior.

CORPORATE FRAUD POLICY

A Corporate Fraud Policy sets out what employees are to do when fraud is suspected. It defines a consistent course of action and sets the tone for how the company will deal with fraud. In particular, it must clearly convey the message that no one has the authority to commit illegal acts - even to the benefit of the company.

Types of Fraud

Fraud comes in many forms but can be broken down into three categories: asset misappropriation, corruption and financial statement fraud. Asset misappropriation, although least costly, made up 90% of all fraud cases studied. These are schemes in which an employee steals or exploits its organization's resources. Examples of asset misappropriation are stealing cash before or after it's been recorded, making a fictitious expense reimbursement claim and/or stealing non-cash assets of the organization.

Financial statement fraud comprised less than five percent of cases but caused the most median loss. These are schemes that involve omitting or intentionally misstating information in the company's financial reports. This can be in the form of fictitious revenues, hidden liabilities or inflated assets.

Corruption fell in the middle and made up less than one-third of cases. Corruption schemes happen when employees use their influence in business transactions for their own benefit while violating their duty to the employer. Examples of corruption are bribery, extortion and conflict of interest.

Fraud Prevention

It is vital to an organization, large or small, to have a fraud prevention plan in place. The fraud cases studied in the ACFE 2014 Report revealed that the fraudulent activities studied lasted an average of 18 months before being detected. Imagine the type of loss your company could suffer with an employee committing fraud for a year and a half. Luckily, there are ways you can minimize fraud occurrences by implementing different procedures and controls.

Know Your Employees

Fraud perpetrators often display behavioral traits that can indicate the intention to commit fraud. Observing and listening to employees can help identify potential fraud risk. It is important for management to be involved with their employees and take time to get to know them. Often, an attitude change can clue you in to a risk. This can also reveal internal issues that need to be addressed. For example, if an employee feels a lack of appreciation from the business owner or anger at their boss, this could lead him or her to commit fraud as a way of revenge. Any attitude change should cause you to pay close attention to that employee. This may not only minimize a loss from fraud, but can make the organization a better, more efficient place with happier employees. Listening to employees may also reveal other clues.

Make Employees Aware/Set Up Reporting System

Awareness affects all employees. Everyone within the organization should be aware of the fraud risk policy including types of fraud and the consequences associated with them. Those who are planning to commit fraud will know that management is watching and will hopefully be deterred by this. Honest employees who are not tempted to commit fraud will also be made aware of possible signs of fraud or theft. These employees are assets in the fight against fraud. According to the ACFE 2014 Report, most occupational fraud (over 40%) is detected because of a tip. While most tips come from employees of the organization, other important sources of tips are customers, vendors, competitors and acquaintances of the fraudster. Since many employees are hesitant to report incidents to their employers, consider setting up an anonymous reporting system. Employees can report fraudulent activity through a website keeping their identity safe or by using a tip hotline.

Implement Internal Controls

Internal controls are the plans and/or programs implemented to safeguard your company's assets, ensure the integrity of its accounting records, and deter and detect fraud and theft. Segregation of duties is an important component of internal control that can reduce the risk of fraud from occurring. For example, a retail store has one

cash register employee, one salesperson, and one manager. The cash and check register receipts should be tallied by one employee while another prepares the deposit slip and the third brings the deposit to the bank. This can help reveal any discrepancies in the collections.

Documentation is another internal control that can help reduce fraud. Consider the example above; if sales receipts and preparation of the bank deposit are documented in the books, the business owner can look at the documentation daily or weekly to verify that the receipts were deposited into the bank. In addition, make sure all checks, purchase orders and invoices are numbered consecutively. Also, be alert to new vendors as billing-scheme embezzlers' setup and make payments to fictitious vendors, usually mailed to a P.O. Box.

Internal control programs should be monitored and revised on a consistent basis to ensure they are effective and current with technological and other advances. If you do not have an internal control process or fraud prevention program in place, then you should hire a professional with experience in this area. An expert will analyze the company's policies and procedures, recommend appropriate programs and assist with implementation.

Monitor Vacation Balances

You might be impressed by the employees who haven't missed a day of work in years. While these may sound like loyal employees, it could be a sign that these employees have something to hide and are worried that someone will detect their fraud if they were out of the office for a period of time. It is also a good idea to rotate employees to various jobs within a company. This may also reveal fraudulent activity as it allows a second employee to review the activities of the first.

Hire Experts

Certified Fraud Examiners (CFE), Certified Public Accountants (CPA) and CPAs who are certified in Financial Forensics (CFF) can help you in establishing antifraud policies and procedures. These professionals can provide a wide range of services from complete internal control audits and forensic analysis to general and basic consultations.

Live the Corporate Culture

A positive work environment can prevent employee fraud and theft. There should be a clear organizational structure, written policies and procedures and fair employment practices. An open-door policy can also provide a great fraud prevention system as it gives employees open lines of communication with management. Business owners and senior management should lead by example and hold every employee accountable for their actions, regardless of position.

Fraud Detection

In addition to prevention strategies, you should also have detection methods in place and make them visible to the employees. According to *Managing the Business Risk of Fraud: A Practical Guide*, published by Association of Certified Fraud Examiners (ACFE), the visibility of these controls acts as one of the best deterrents to fraudulent behavior. It is important to continuously monitor and update your fraud detection strategies to ensure they are effective. Detection plans usually occur during the regularly scheduled business day. These plans take external information into consideration to link with internal data. The results of your fraud detection plans should enhance your prevention controls. It is important to document your fraud detection strategies including the individuals or teams responsible for each task. Once the final fraud detection plan has been finalized, all employees should be made aware of the plan and how it will be implemented. Communicating this to employees is a prevention method in itself. Knowing the company is watching and will take disciplinary action can hinder employees' plans to commit fraud.

IAM- Identity & Access Management

An identity access management (IAM) system is a framework for business processes that facilitates the management of electronic identities. The framework includes the technology needed to support identity management.

An identity access management (IAM) system is a framework for business processes that facilitates the management of electronic identities. The framework includes the technology needed to support identity management.

IAM technology can be used to initiate, capture, record and manage user identities and their related access permissions in an automated fashion. This ensures that access privileges are granted according to one interpretation of policy and all individuals and services are properly authenticated, authorized and audited.

Poorly controlled IAM processes may lead to regulatory non-compliance because if the organization is audited, management will not be able to prove that company data is not at risk for being misused.

The list of technologies that fall under this category includes password-management tools, provisioning software, security-policy enforcement applications, reporting and monitoring apps, and identity repositories. Nowadays, these technologies tend to be grouped into software suites with assortments of additional capabilities, from enterprise-wide credential administration to automated smart-card and digital-certificates management.

The ID management buzz phrase of the moment is "identity lifecycle management." The concept encompasses the processes and technologies required for provisioning, de-provisioning, managing and synchronizing digital IDs, as well as features that support compliance with government regulations. Technologies that fall under the ID lifecycle-management rubric include tools for security principal creation, attribute management, identity synchronization, aggregation and deletion.

Identity Management Concepts

Authentication vs. Authorization

Authentication determines whether the user is who they claim to be. Authorization determines whether an authenticated user is allowed to access a specific resource or take a specific action. While these concepts are closely related, they are distinct.

Accounts, Identifiers, and Identities

An account is the representation of a user within a particular system. An identifier is how a user is labeled. In a system that uses UT EID-based single sign-on, the user account will be accessed using the UT EID as an identifier. An identity is the collection of accounts and identifiers associated with a particular person (or sometimes a non-person entity). An identity can be associated with multiple accounts and identifiers. For example, you may have multiple email accounts but all of those accounts belong to one identity (you).

Provisioning and Deprovisioning

The process of how user accounts are created when they are needed and how they are deleted, archived, or made inactive when no longer needed.

Identity Lifecycle

Like the real-world entities they represent, identities have a lifecycle. Their connection to the University will change over time and the accounts and authorizations they have will also change accordingly. However, the identity itself does not go away. When a user leaves the University (e.g. graduation, separation) their identity persists and they will continue to be able to authenticate using their UT EID. This allows individuals to later come back and apply for jobs, request transcripts, etc. Systems must take into account the current status of a user in their authorization schemes and change account authorizations when that status changes. So, for example, if a student or employee leaves the university, the wireless network will note the change in affiliation and remove authorizations for wireless access.

Need for IAM

It can be difficult to get funding for IAM projects because they don't directly increase either profitability or functionality. However, a lack of effective identity and access management poses significant risks not only to compliance but also an organization's overall security. These mismanagement issues increase the risk of greater damages from both external and inside threats.

Keeping the required flow of business data going while simultaneously managing its access has always required administrative attention. The business IT environment is ever evolving and the difficulties have only become greater with recent disruptive trends like bring-your-own-device (BYOD), cloud computing, mobile apps and an increasingly mobile workforce. There are more devices and services to be managed than ever before, with diverse requirements for associated access privileges.

With so much more to keep track of as employees migrate through different roles in an organization, it becomes more difficult to manage identity and access. A common problem is that privileges are granted as needed when employee duties change but the access level escalation is not revoked when it is no longer required.

This situation and request like having access like another employee rather than specific access needs leads to an accumulation of privileges known as privilege creep. Privilege creep creates security risk in two different ways. An employee with privileges beyond what is warranted may access applications and data in an unauthorized and potentially unsafe manner. Furthermore, if an intruder gains access to the account of a user with excessive privileges, he may automatically be able to do more harm. Data loss or theft can result from either scenario.

Typically, this accumulation of privilege is of little real use to the employee or the organization. At best, it might be a convenience in situations when the employee is asked to do unexpected tasks. On the other hand, it might make things much easier for an attacker who manages to compromise an over-privileged employee identity. Poor identity access management also often leads to individuals retaining privileges after they are no longer employees.

IAM Features

Double Down on Security: Two-Factor Authentication (2FA)

By now, it should go without saying that two-factor authentication is essential. Having one strong password to log into all of your accounts is convenient, but it's not enough, especially if that one password gets compromised. Two-factor authentication randomly generates and sends a unique verification code or a push notification to the user's phone, making the login process much more secure than one that uses passwords alone.

Set It and Forget It: Dynamic Password Management

People are notoriously bad at creating and then remembering multiple strong passwords, and as Intermedia's research shows, employees often take passwords with them – putting their previous employer at real risk. In light of that, IT teams should take the responsibility of creating passwords out of the employees' hands and in fact not even let employees know their corporate web application passwords, beyond their one master password.

Dynamic password management technology creates a unique, strong password for each of a user's corporate web applications and changes it on a pre-defined scheduled basis. Employees never know what those passwords are — they simply log into their SSO solution and the system logs them into all their web applications. This ensures that employees cannot log into those systems outside of work and take confidential information without the company's knowledge. And, most importantly, it means they can't take their passwords to corporate web applications with them when they leave the organization.

The Best of Both Worlds: App Shaping

Most IAM solutions give IT complete control over which corporate applications employees can access. However, it's growing increasingly important to have even more granular control than that.

Application shaping is new technology that gives IT complete control over what each employee or groups of employees can see and do within web applications. For example, you could redact certain data fields within these web applications for certain types of employees, disable certain features or even make web applications entirely read-only.

By removing high-risk features (e.g., exporting files, ability to mass delete, etc.), a company can increase its security, without limiting its workforce's flexibility.

See the Whole Picture: Capture Visuals for the Audit Trail

With compliance an ongoing concern for most businesses, any IAM solution should maintain an audit trail. However, just knowing who logged in and out and when they did it is no longer adequate. Advanced IAM solutions allow for IT teams to monitor the use of specific features within web applications, send alerts for unusual activity and even provide the option to capture screen shots when certain online behaviors occur. This provides visual evidence of exactly what the user was doing.

Get Smarter Restrictions: User-Empowered Identity

Digital identities need to be protected and who better than individual users to identify suspicious account activity? Premium IAM solutions now offer users with real-time notifications when suspicious events occur and empower users to perform immediate and appropriate responses.

For instance, if an attacker were to attempt to log in with a user's identity from a different country, the user would be presented with a security notification in the browser or via an SMS text message instead of an operations team being alerted, as they may not be aware of the individual's location. The user can then issue a response to disable the account or immediately change a password. This gives companies a higher level of assurance that their data and user accounts are protected.

The IAM Strategy

IAM is a combination of processes, technologies, and policies enabled by software to manage user identities throughout their life cycle. More specifically, the goal of IAM is to initiate, capture, record, and manage user identities and their related access permissions to proprietary information and other company resources. User identities can extend beyond corporate employees and include vendors, customers, floor machines, generic administrator accounts, and electronic access badges. As a result, improving access to network resources and managing an identity's life cycle can provide significant dividends for organizations, such as:

- A lower total cost of ownership through the increased efficiency and consolidation of identification and authorization procedures.
- Security improvements that reduce the risk of internal and external attacks.
- Greater access to information by partners, employees, and customers, thus leading to increased productivity, satisfaction, and revenue.
- Higher levels of regulatory compliance through the implementation of comprehensive security, audit, and access policies.
- Greater business agility during events such as mergers and acquisitions.

Here are some general strategies auditors can recommend for IT departments to consider when aligning the organization's IAM program to existing business strategies and regulatory compliance requirements:

- Obtain senior management support prior to designing and implementing an IAM program as the program will be an important part of companywide information security efforts.
- Understand the organization's IAM needs and define corresponding processes first.
- Automate the identity provisioning process to allow for the central administration of user identities.
- Consider the acquisition of directory servers, Meta directories (i.e., techniques for providing directory integration), virtual directory servers, and administration products (e.g., directory and public key infrastructure management tools and provisioning products).
- Build access layer and workflow processes. The access layer is used to mediate access to the shared media and other network resources, while workflow processes define and track the exchange of work among users.
- Lay out business requirements as much as possible before starting the integration of IAM processes.
- Before signing a contract with a vendor, check out references and foster a good partner relationship.

- Integrate the components and processes above, but realize that not all components might be needed at first based on the organization's strategic plan, business needs, and IAM project scope.

IAM Challenges

A chain is as strong as its weakest link, and when it comes to IT security, IAM is the weakest link in many organizations. For example, many IT departments store identity credentials as data objects in different data repositories. Because these organizations can have hundreds of discrete identity stores containing overlapping and conflicting data, synchronizing this information among multiple data repositories turns into a challenging, time consuming, and expensive ordeal, especially if the data is managed through the use of manual processes or custom scripts.

Another key challenge is related to cost. As a general rule, the costs of managing user identities should be as low as possible to ensure a reasonable return on investment in the IAM project. Too often, identity management projects become too large or cumbersome to finish on schedule; after all, there will always be more applications to integrate into the system. This can be accomplished by scaling identity life cycle management activities efficiently across various applications and network resources and employing as little staff as possible to manage IT applications.

Besides the challenges stemming from the use of manual processes to manage multiple data repositories, other identity synchronization issues include:

- Reducing the costs associated with managing large numbers of identity stores.
- Providing the ability to expand the organization's people and IT resources without a corresponding increase in IT staff.
- Increasing employee productivity by being able to find the right information about other users.
- Meeting regulatory requirements associated with privacy and access controls.
- Remembering to use more than one user ID.

Total Cost of Ownership of Identity and Access Management

IAM is an expensive investment. Besides the recommendations above, auditors can share the following tips with their IT department to help reduce the total cost of ownership of IAM activities:

Follow the rule of economy of scale

If more people use the same tool or application, its unit cost will decrease. Therefore, IT departments should search for and use the most popular off-the-shelf IAM solution first. Custom building an IAM application should be a last alternative (i.e., when no other commercial tool is available that can meet the organization's needs) due to the amount of time and resources required to create the tool.

Outsource IAM operations

If IT staff is based in North America or Europe, auditors can recommend that the organization consider outsourcing its tier 1 (i.e., help desk) or tier 2 (i.e., the person or company the employee calls when the help desk is not available) IAM support activities. The company also should consider outsourcing its tier 3 (i.e., the person or company that the tier 2 organization calls when they don't know the solution) IAM support activities and its architecture and integration work to a larger IT service company, such as Microsoft Corp., IBM, or Hewlett Packard, to reduce the amount of service down time.

Support costs are usually the largest portion of total ownership costs, followed by software and hardware costs.

Incident Response

Incident response is an organized approach to addressing and managing the aftermath of a security breach or attack (also known as an incident). The goal is to handle the situation in a way that limits damage and reduces recovery time and costs. An incident response plan includes a policy that defines, in specific terms, what constitutes an incident and provides a step-by-step process that should be followed when an incident occurs.

An organization's incident response is conducted by the computer incident response team, a carefully selected group that, in addition to security and general IT staff, may include representatives from legal, human resources, and public relations departments.

According to the SANS Institute, there are six steps to handling an incident most effectively:

1. **Preparation:** The organization educates users and IT staff of the importance of updated security measures and trains them to respond to computer and network security incidents quickly and correctly.
2. **Identification:** The response team is activated to decide whether a particular event is, in fact, a security incident. The team may contact the CERT Coordination Center, which tracks Internet security activity and has the most current information on viruses and worms.
3. **Containment:** The team determines how far the problem has spread and contains the problem by disconnecting all affected systems and devices to prevent further damage.
4. **Eradication:** The team investigates to discover the origin of the incident. The root cause of the problem and all traces of malicious code are removed.
5. **Recovery:** Data and software are restored from clean backup files, ensuring that no vulnerabilities remain. Systems are monitored for any sign of weakness or recurrence.
6. **Lessons learned:** The team analyzes the incident and how it was handled, making recommendations for better future response and for preventing a recurrence.

Incident Response Plan

An incident response plan (IRP) is a set of written instructions for detecting, responding to and limiting the effects of an information security event.

Incident response plans provide instructions for responding to a number of potential scenarios, including data breaches, denial of service/distributed denial of service attacks, firewall breaches, virus or malware outbreaks or insider threats. Without an incident response plan in place, organizations may either not detect the attack in the first place, or not follow proper protocol to contain the threat and recover from it when a breach is detected.

An incident response plan can benefit an enterprise by outlining how to minimize the duration of and damage from a security incident, identifying participating stakeholders, streamlining forensic analysis, hastening recovery time, reducing negative publicity and ultimately increasing the confidence of corporate executives, owners and shareholders. The plan should identify and describe the roles/responsibilities of the incident response team members who are responsible for testing the plan and putting it into action. The plan should also specify the tools, technologies and physical resources that must be in place to recover breached information.

Cyber Security Incident Response Team



A Computer Security Incident Response Team is an organization that receives reports of security breaches, conducts analyses of the reports and responds to the senders. A CSIRT may be an established group or an ad hoc assembly.

There are various types of CSIRTs. An internal CSIRTs is assembled as part of a parent organization, such as a government, a corporation, a university or a research network. National CSIRTs (one type of internal CSIRT), for example, oversee incident handling for an entire country. Typically, internal CSIRTs gather periodically throughout the year for proactive tasks such as DR testing, and on an as-needed basis in the event of a security breach. External CSIRTs provide paid services on either an on-going or as-needed basis.

CERT (Computer Emergency Readiness Team) lists the following among the roles of CSIRT members:

- Manager or team lead
- Assistant managers, supervisors, or group leaders
- Hotline, help desk, or triage staff
- Incident handlers
- Vulnerability handlers
- Artifact analysis staff
- Platform specialists
- Trainers
- Technology watch

As teams increased their capability and scope, they began to expand their activities to include more proactive efforts. These efforts included looking for ways to

- prevent incidents and attacks from happening in the first place by securing and hardening their infrastructure
- training and educating staff and users on security issues and response strategies
- actively monitoring and testing their infrastructure for weaknesses and vulnerabilities
- sharing data where and when appropriate with other teams

As organizations become more complex and incident management capabilities such as CSIRTs become more integrated into organizational business functions, it is clear that incident management is not just the application of technology to resolve computer security events. It is also the development of a plan of action, a set of processes that are consistent, repeatable, of high quality, measurable, and understood within the constituency. To be successful this plan should

- integrate into the existing processes and organizational structures so that it enables rather than hinders critical business functions
- strengthen and improve the capability of the constituency to effectively manage security events and thereby keep intact the availability, integrity, and confidentiality of an organization's systems and critical assets, where required
- support, complement, and link to any existing business continuity or disaster recovery plans where and when appropriate
- support, complement, and provide input into existing business and IT policies that impact the security of an organization's infrastructure
- implement a command and control structure, clearly defining responsibilities and accountability for decisions and actions
- be part of an overall strategy to protect and secure critical business functions and assets
- include the establishment of processes for
 - notification and communication
 - analysis and response
 - collaboration and coordination
 - maintenance and tracking of records

The OODA Loop

Developed by US Air Force military strategist John Boyd, the OODA loop stands for Observe, Orient, Decide, and Act.



Observe

Tools and Tactics – Vulnerability Analysis; SIEM Alerts; Application Performance Monitoring; IDS Alerts; Netflow Tools; Traffic Analysis; Log Analysis

Questions to Ask – What does normal activity look like on my network? How can I find and categorize events or user activity that aren't normal? And which require my attention now? Finally, how can I fine-tune my security monitoring infrastructure?

Key Takeaways – In this phase of incident response methodology, the more observations you can make, and document, around your business operations and network, the more successful you'll be at response and defense

Orient

Tools and Tactics – Security Research; Incident Triage; Situational Awareness; Security Research

Questions to Ask – Is your company preparing for a new software package or planning layoffs? Have you or anyone else in the wild seen attacks from this particular IP address before? Do you know what the root cause is? How large is the scope and impact?

Key Takeaways – In this phase of incident response methodology, it's important to try and think like the attacker so that you can orient your defense strategies against the latest attack tools and tactics. These are always changing so make sure you have the latest threat intelligence for your security monitoring tools. This will ensure that your tools are capturing the right information and providing accurate context.

Decide

Tools and Tactics – Hard copy documentation (pen, notebook and clock), your company's corporate security policy

Questions to Ask – Once you have all the facts, then it's time to ask yourself and your team how to act.

Key Takeaways – In this phase of incident response methodology, catalog all areas of your incident response process. Perhaps one of the most important areas to document here are communications around data collection and the decision-making process.

Act

Tools and Tactics – System backup and recovery tools; data capture and forensics analysis tools; patch management and other systems management, security awareness training tools and programs

Questions to Ask – How can I quickly remedy the affected systems and get them back online? How can this be prevented in the future? What are ways that we can educate users so these things don't happen again? Should we fine-tune our business process based on these lessons?

Key Takeaways – In this phase of incident response methodology, training, communication, and frequent improvement are important to success in reacting effectively during an incident. Everyone on your team should know their roles and what is expected of them also, it's recommended to keep up to date on security best practices and empower team members to speak up when they identify areas for improvement in your incident response methodology.

Intrusion Detection

Intrusion detection (ID) is a type of security management system for computers and networks. An ID system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). ID uses *vulnerability assessment* (sometimes referred to as *scanning*), which is a technology developed to assess the security of a computer system or network.

Intrusion detection functions include:

- Monitoring and analyzing both user and system activities
- Analyzing system configurations and vulnerabilities
- Assessing system and file integrity
- Ability to recognize patterns typical of attacks
- Analysis of abnormal activity patterns
- Tracking user policy violations

ID systems are being developed in response to the increasing number of attacks on major sites and networks, including those of the Pentagon, the White House, NATO, and the U.S. Defence Department. The safeguarding of security is becoming increasingly difficult, because the possible technologies of attack are becoming ever more sophisticated; at the same time, less technical ability is required for the novice attacker, because proven past methods are easily accessed through the Web.

Types of Intrusion Detection

Common types of Intrusion Detection:

Network Based IDS

Network based intrusion detection attempts to identify unauthorized, illicit, and anomalous behavior based solely on network traffic. A network IDS, using either a network tap, span port, or hub collects packets that traverse a given network. Using the captured data, the IDS system processes and flags any suspicious traffic. Unlike an intrusion prevention system, an intrusion detection system does not actively block network traffic. The role of a network IDS is passive, only gathering, identifying, logging and alerting. Example of Network IDS is SNORT.

Host Based IDS

Often referred to as HIDS, host based intrusion detection attempts to identify unauthorized, illicit, and anomalous behavior on a specific device. HIDS generally involves an agent installed on each system, monitoring and alerting on local OS and application activity. The installed agent uses a combination of signatures, rules, and heuristics to identify unauthorized activity. The role of a host IDS is passive, only gathering, identifying, logging, and alerting. Examples of HIDS are OSSEC - Open Source Host-based Intrusion Detection System; Tripwire; AIDE - Advanced Intrusion Detection Environment; Prelude Hybrid IDS

Physical IDS

Physical intrusion detection is the act of identifying threats to physical systems. Physical intrusion detection is most often seen as physical controls put in place to ensure CIA. In many cases physical intrusion detection systems act as prevention systems as well. Examples of Physical intrusion detections are Security Guards; Security Cameras; Access Control Systems (Card, Biometric); Firewalls; Man Traps; Motion Sensors

Signature Based IDS

A signature based IDS will monitor packets on the network and compare them against a database of signatures or attributes from known malicious threats.

This is similar to the way most antivirus software detects malware. The issue is that there will be a lag between a new threat being discovered in the wild and the signature for detecting that threat being applied to your IDS. During that lag time your IDS would be unable to detect the new threat.

Anomaly Based IDS

An IDS which is anomaly based will monitor network traffic and compare it against an established baseline. The baseline will identify what is "normal" for that network- what sort of bandwidth is generally used, what protocols are used, what ports and devices generally connect to each other- and alert the administrator or user when traffic is detected which is anomalous, or significantly different, than the baseline.

Passive IDS

A passive IDS simply detects and alerts. When suspicious or malicious traffic is detected an alert is generated and sent to the administrator or user and it is up to them to take action to block the activity or respond in some way.

Reactive IDS

A reactive IDS will not only detect suspicious or malicious traffic and alert the administrator, but will take pre-defined proactive actions to respond to the threat.

Typically this means blocking any further network traffic from the source IP address or user.

Intrusion Prevention System

Intrusion Prevention Systems (IPS) extended IDS solutions by adding the ability to block threats in addition to detecting them and has become the dominant deployment option for IDS/IPS technologies.

An Intrusion Prevention System (IPS) is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits. Vulnerability exploits usually come in the form of malicious inputs to a target application or service that attackers use to interrupt and gain control of an application or machine. Following a successful exploit, the attacker can disable the target application (resulting in a denial-of-service state), or can potentially access to all the rights and permissions available to the compromised application.

Unlike IDS, IPS performs two functions, first it tries to prevent an intrusion and if by chance it fails at it, IPS also detects the intrusion:

Prevention

The IPS often sits directly behind the firewall and it provides a complementary layer of analysis that negatively selects for dangerous content. Unlike its predecessor the Intrusion Detection System (IDS)—which is a passive system that scans traffic and reports back on threats—the IPS is placed inline (in the direct communication path between source and destination), actively analyzing and taking automated actions on all traffic flows that enter the network. Specifically, these actions include:

- Sending an alarm to the administrator (as would be seen in an IDS)
- Dropping the malicious packets
- Blocking traffic from the source address
- Resetting the connection

As an inline security component, the IPS must work efficiently to avoid degrading network performance. It must also work fast because exploits can happen in near real-time. The IPS must also detect and respond accurately, so as to eliminate threats and false positives (legitimate packets misread as threats).

Detection

The IPS has a number of detection methods for finding exploits, but signature-based detection and statistical anomaly-based detection are the two dominant mechanisms.

Signature-based detection is based on a dictionary of uniquely identifiable patterns (or signatures) in the code of each exploit. As an exploit is discovered, its signature is recorded and stored in a continuously growing dictionary of signatures. Signature detection for IPS breaks down into two types:

Exploit-facing signatures identify individual exploits by triggering on the unique patterns of a particular exploit attempt. The IPS can identify specific exploits by finding a match with an exploit-facing signature in the traffic stream

Vulnerability-facing signatures are broader signatures that target the underlying vulnerability in the system that is being targeted. These signatures allow networks to be protected from variants of an exploit that may not have been directly observed in the wild, but also raise the risk of false-positives.

Statistical anomaly detection takes samples of network traffic at random and compares them to a pre-calculated baseline performance level. When the sample of network traffic activity is outside the parameters of baseline performance, the IPS takes action to handle the situation.

IPS was originally built and released as a standalone device in the mid-2000s. This however, was in the advent of today's implementations, which are now commonly integrated into Unified Threat Management (UTM) solutions (for small and medium size companies) and next-generation firewalls (at the enterprise level).

	Intrusion Prevention System	IDS Deployment
Placement in network infrastructure	Part of the direct line of communication (inline)	Outside direct line of communication (out-of-band)
System type	Active (monitor & automatically defend) and/or passive	Passive (monitor & notify)
Detection Mechanisms	1. Statistical anomaly-based detection 2. Signature detection: -Exploit-facing signatures -Vulnerability-facing signatures	1. Signature detection: -Exploit-facing signatures

How IDS works

IDS systems can use different methods for detecting suspected intrusions. The two most common broad categories are by pattern matching and detection of statistical anomalies.

Pattern matching

Pattern matching is used to detect known attacks by their "signatures," or the specific actions that they perform. It is also known as signature-based IDS or misuse detection. The IDS looks for traffic and behavior that matches the patterns of known attacks. The effectiveness is dependent on the signature database, which must be kept up to date.

Pattern matching is analogous to identifying a criminal who committed a particular crime by finding his fingerprint at the scene. Fingerprint analysis is a type of pattern matching.

The biggest problem with pattern matching is that it fails to catch new attacks for which the software doesn't have a defined signature in its database.

Statistical anomaly

Anomaly-based detection watches for deviations from normal usage patterns. This requires first establishing a baseline profile to determine what the norm is, then monitoring for actions that are outside of those normal parameters. This allows you to catch new intrusions or attacks that don't yet have a known signature.

Anomaly detection is analogous to a police officer who walks or drives a particular beat every day and knows what is "normal" for that area. When he sees something that's out of the ordinary, it creates reasonable suspicion that criminal activity may be going on, even though he may not know exactly what crime is being committed or who is responsible.

There are several different anomaly detection methods, including:

- Metric model
- Neural network
- Machine learning classification

A problem with anomaly-based IDS is the higher incidence of false positives, because behavior that is unusual will be flagged as a possible attack even if it's not.

Where the IDS fits in your security plan

Edge or Front-end firewall is the first line of defense in protecting the network against intruders, and it will likely have its own intrusion detection capability, although it may detect and prevent only a limited number of known attacks/intrusions. A network-based IDS is often placed between the edge firewall and a back-end firewall that protects the internal network from the publicly accessible network in between.

Placing the IDS in this location allows it to do its job on all traffic that gets through the edge firewall and provides an extra layer of protection for the DMZ, which is the most vulnerable part of your network since it contains your public servers such as Internet-accessible Web servers, DNS servers, front-end mail servers, etc.

Putting the IDS in front of the edge firewall would result in a greater load on the IDS, since it would respond to many scans, probes and attack attempts that could otherwise be filtered out by the firewall. Also, the huge number of alerts might lead to an "IDS who cried wolf" situation in which administrators would start ignoring the alerts when many of them don't lead to real attacks.

IDS can also be placed behind the back-end firewall to detect intrusions on the internal LAN.

A multi-layered approach

The best security is afforded by using one than one IDS (for example, an IDS in the DMZ and another on the internal network) and by using both network and host-based IDS. Host-based IDS can **be installed on critical servers for multi-layered protection.**

Incident response

The detection of intrusions is only the first step in making an organization more secure and protecting against intruders. The real key is what happens after the intrusion is detected: your incident response plan.

To be effective, response must be as immediate as possible. That's why your IDS needs to include notification features and you need to set them up so that the alerts get to the proper people as quickly as possible after an intrusion is detected.

Incident response team should practice the following incident response procedures

- Preventing damage (or further damage)
- Tracking/identifying the intruder
- Preserving evidence in case the incident leads to criminal prosecution and/or civil litigation

Log Analysis & Management

Hackers are inventing new and increasingly sophisticated ways to break into corporate information systems, and companies must respond with more effective ways to protect their vital corporate information systems, networks, and data. Among the most reliable, accurate, and proactive tools in the security arsenal are the event and audit logs created by network devices.

Requirements for cyber security event logging:

- Management of event logging (eg. setting policy, defining roles and responsibilities, and reporting)
- Identification of business applications and technical infrastructure systems on which event logging should be enabled, including those that have been outsourced or are 'in the cloud'
- Configuration of information systems to generate the right cyber security-related events
- Regular 'tuning' and review to reduce the number of false positives to an acceptable level
- Storage of security-related events within event logs (eg. using local systems, central servers, SIEMs or by using storage provided by an external service provider)
- Analysis of security-related event logs (including normalization, aggregation and correlation)
- Synchronization of time stamps in event logs to a common, trusted source
- Protection of security-related event logs (eg. via encryption, access control and backup)
- Defined retention requirements and/or log rotation periods
- Taking necessary actions to remediate any issues identified and respond to cyber security incidents in a fast, effective manner

Advantages of Logging

- Logs provide clues about performance issues, application function problems, intrusion and attack attempts etc.
- The logs provide vital inputs for managing the computer security incidents, both for Incident Prevention and Incident Response Benefits
- When responding to computer security incident, logs provide leads to the activities performed over the system
- Facilitates cybercrime investigation
 - Determine the activity
 - Determine the origin of attack

Types of Event Logs

Event Log Type	Description
Application Log	Any event logged by an application. These are determined by the developers while developing the application. E.g.: An error while starting an application gets recorded in Application Log.
System Log	Any event logged by the Operating System. E.g.: Failure to start a drive during start-up is logged under System Logs
Security Log	Any event that matters about the security of the system. E.g. valid and invalid Logins and logoffs, any file deletion etc. are logged under this category.
Directory Service log	Records events of AD. This log is available only on domain controllers.
DNS Server log	Records events for DNS servers and name resolutions. This log is available only for DNS servers
File replication service log	Records events of domain controller replication This log is available only on domain controllers.

Key to a successful Log Analysis

Findings from project research revealed that effective logging can save time and money in case of a cyber security incident – and that it can also be very helpful as part of a defense (or prosecution) in a court case. Therefore key to a successful Log Analysis and maintenance is:

- Establish cyber security-related logging standards and procedures
- Configure systems to record the most important cyber-security related events and monitor these events for specified purposes
- Respond to alerts correctly (eg. to avoid overlooking indicative alerts or over-reacting to benign alerts)
- Aggregate what may seem like benign alerts into what is a coherent threat message
- Make appropriate event logs available to investigators in a suitable format
- Retain logs according to retention standards/procedures, storing them securely for possible forensic analysis at a later date.

Logging Challenges

- Struggling to understand the purpose, importance and effectiveness of the full range of data sources (putting them into some sort of 'pecking order' of importance)
- Suffering from the sheer volume of log management tasks such as:
 - o Turning on relevant logs, logging them correctly and keeping them long enough to
 - o Prioritization, storage, correlation and protection of logs
- Failing to examine alerts in an effective manner (eg. handling false positives, performing situational analysis and remediating issues)
- Being unsure as to which logs they need to pay most (and least) attention or the implications of the events that they record
- Not being able to find the right tools and people to help them easily, effectively and at the right price.

Mainframe Security

A mainframe is a computer that is capable of performing large-scale data processing in a self-contained structure, as opposed to having many individual (usually smaller) computers.

Mainframes typically have multiple processors. And they can be connected in a cluster and operate in a distributed computing system. However, the distinguishing feature of a mainframe is that it can run independently as a “centralized cluster” by dividing itself internally to work on problems in a parallel or multi-tasking way for extended periods of time, even years.

Mainframes offer virtualization. Virtualization allows you to create multiple logical computers within a single mainframe. Connecting several of those logical computers (also called logical partitions or LPARs) to work together is known as creating a cluster or sysplex. When multiple physical entities (mainframes) are physically connected, they are called sysplexes. Together, using virtualization, LPARS, and sysplexes offers enhanced horizontal scalability.

An important benefit offered by this design is that expensive reliability features are needed in only one server (as compared to being built in to many smaller servers). Also, the physical “footprint” of a mainframe is much smaller than that of a distributed server farm, and therefore is less expensive from an environmental perspective (that is, the amount of power, cooling, and floor space needed is much less). Mainframes can therefore be more cost-effective in solving the same business problems over the long term.

Mainframes are usually larger than most servers because of the necessary redundancy of design and components that allow the computer to deliver high availability as well as vertical and horizontal scalability (the ability to increase the capacity of the computer without replacing the entire unit). Also, mainframe components such as hot-pluggable processors, disks, interface adapters such as network cards or cryptographic engines, and even the power supply, can all be replaced or upgraded without taking the server offline.

Why mainframe security?

Barry Schrager, the founder of Mainframe Data Security, has written numerous pieces on the subject. He cites these statistics in a recent LinkedIn article:

- 71% of all Fortune 500 companies have their core business on the mainframe.
- 23 of the world's top 25 retailers use a mainframe.
- 92% of the top 100 banks use a mainframe.
- 10 out of 10 of the top insurers use a mainframe.
- More than 225 state and local governments worldwide rely on a mainframe.
- 9 of the top 10 global life and health insurance providers process their high-volume transactions on mainframe.

With the widespread use of mainframes today, it is absolutely necessary that they have excellent security. Everyday millions of transactions pass through mainframes; with poor security, this can lead to the loss of massive amounts of money and data. Mainframe security is a must for business continuity and has continuously evolved over the years to where it is today. When the mainframe became more networked with other devices and connected to end users on computers other than the original "dumb terminal," its security really broadened as the traditional physical security was no longer enough.

One rarely hears about a mainframe being involved in a major data security breach, but there was the infamous TJX Companies Inc. hacking case, the largest data security breach to date. In 2007, the retailer announced the discovery of a computer system's breach and the possible loss of millions of credit card records. As the world would learn later, the breach involved more than 45 million customer records and had gone undetected for a number of years.

Mainframes are so impenetrable that no one knows for sure what goes on inside them.

Since the advent of mainframes, security paradigms have changed dramatically. With the inclusion of privacy considerations in the information security discipline, the new paradigm forces us to deal with risks that apply to any and all computing platforms including mainframes.

Machine Learning Security- Adversarial Learning

Adversarial learning is a novel research field that lies at the intersection of machine learning and computer security. It aims at enabling the *safe* adoption of machine learning techniques in *adversarial settings* like spam filtering, computer security, and biometric recognition.

The problem is motivated by the fact that machine learning techniques have not been originally designed to cope with intelligent and adaptive adversaries, and, thus, in principle, the whole system security may be compromised by exploiting specific vulnerabilities of learning algorithms through a careful manipulation of the input data.

Accordingly, to improve the security of learning algorithms, the field of adversarial learning addresses the following main open issues:

- Identifying potential vulnerabilities of machine learning algorithms during learning and classification;
- Devising the corresponding attacks and evaluating their impact on the attacked system;
- Proposing countermeasures to improve the security of machine learning algorithms against the considered attacks.



Types of attacks:

- **Evasion attacks**

Evasion attacks are the most popular kind of attack that may be incurred in adversarial settings during system operation. For instance, spammers and hackers often attempt to evade detection by obfuscating the content of spam emails and malware code. In the evasion setting, malicious samples are modified at test time to evade detection, that is, to be misclassified as legitimate. No influence over the training data is possible.

- **Poisoning**

Machine learning algorithms are often re-trained on data collected during operation to adapt to changes in the underlying data distribution. For instance, an Intrusion Detection System (IDS) may be re-trained on a set of samples (TR) collected during network operation. Within this scenario, an attacker may poison the training data by injecting carefully designed samples to eventually compromise the whole learning process. Poisoning may thus be regarded as an adversarial contamination of the training data.

Machine Learning In Cyber Security

According to Matt Wolff, Chief Data Scientist at Cylance, when it comes to cyber security, there are two reasons why Machine Learning is a growing trend in this field:

- Lack of qualified, experienced individuals to successfully defend vital infrastructure and systems. The defensive game is complex and never ending; and one slip up by a security team can be enough to open the door for a security incident. In addition, the projected demand for excellent security professionals will continue to grow, compounding the current challenges around the dearth of talent.
- The collection and storage of large amounts of useful data points is already well underway in cyber security. It would be difficult to find a security analyst who is not currently overwhelmed by the vast amount of raw data that is collected every day in mature environments. There even exist a plethora of tools designed to help sort, slice, and mine this data in a somewhat automated fashion to help the analyst along in their day-to-day activities.

Advantages of machine learning

- With a machine learning approach, many of these tasks can be automated, and even deployed in real time to catch these activities before any damage is done. For example, a well-trained machine learning model will be able to identify unusual traffic on the network, and shut down these connections as they occur. A well-trained model would also be able to identify new samples of malware that can evade human generated signatures, and perhaps quarantine these samples before they can even execute. In addition, a machine learning model trained on the standard operating procedure of a given endpoint may be able to identify when the endpoint itself is engaging in odd behavior, perhaps at the request of a malicious insider attempting to steal or destroy sensitive information.
- In particular, applying machine learning to behavioral analytics is profoundly improving our ability to make sense of the volumes of data generated by security products in the average enterprise. When machine learning concepts like automated and iterative algorithms are used to learn patterns in data, we can probe data for structure, even if we do not know what that structure looks like.
- In the past, security products attempted to 'correlate' data to discern patterns and meaning. Instead, today we perform link analysis to evaluate relationships or connections between data nodes. Key relationships can be identified among various types of data nodes or objects, things we might think of as organizations, people, transactions, and so on.
- Machine learning is what enables us to bring together huge volumes of data that is generated by normal user activity from disparate, even obscure, sets of data -- to identify relationships that span time, place and actions. Since machine learning can be simultaneously applied to hundreds of thousands of discrete events from multiple data sets, "meaning" can be derived from behaviors and used an early warning detection or prevention system.
- The ultimate test for a machine-learning model is validation error on new data. In other words, machine learning is looking to match new data with what it's seen before, and not to test it to disprove, reject or nullify an expected outcome. Since machine learning uses an iterative, automated approach, it can reprocess data until a robust pattern is found. This allows it to go beyond looking for "known" or "common" patterns.
- Machine learning's ability to automatically detect changes over time that inform network behavioural profiles of what is and isn't normal traffic also makes it well-suited to helping the enterprise adapt to new forms of attacks without requiring human intervention. In conjunction with neural network machine learning models and their evolutionary programming adaptation process it is possible to iteratively create networks that become stronger at adapting to new problems, including aggressive automated invasions.

There is more value in using multistage machine-learning analysis and actual data in an effort to determine which machine learning model will work best for detecting real security events on any one particular network. Processing data streams from various subsystems (data transmission frequency measurements over time, for instance, or protocols in a network stream that identify affiliated applications and infrastructure devices) using a variety of machine learning models, and then comparing the learned data to the original raw data, lets an enterprise grade each data stream to reveal which models provide the highest predictability of anomaly detection for that distinct network. Machine learning models may run the gamut from associated rules learning, to sparse dictionary learning, to Bayesian fields and artificial neural networks.

Ideally, a data stream can be mastered using unsupervised learning techniques. This approach learns the features of a data set, and classifies it into a "cluster" of similar data—either normal or abnormal. This is in contrast to supervised learning, which requires that sample data for which the outcome already is known be used for training.

The industry really is just at the start of applying machine learning to the growing cybersecurity challenges of detecting and analysing increasingly sophisticated and targeted threats. The future will see neural networks trained in one data set become the input to others, thereby creating deep networks by extending the knowledge of high-level networks. The industry also will increase its use of hard AI—the simulation of biologic thinking in computers—in detection engines.

Network Security Monitoring

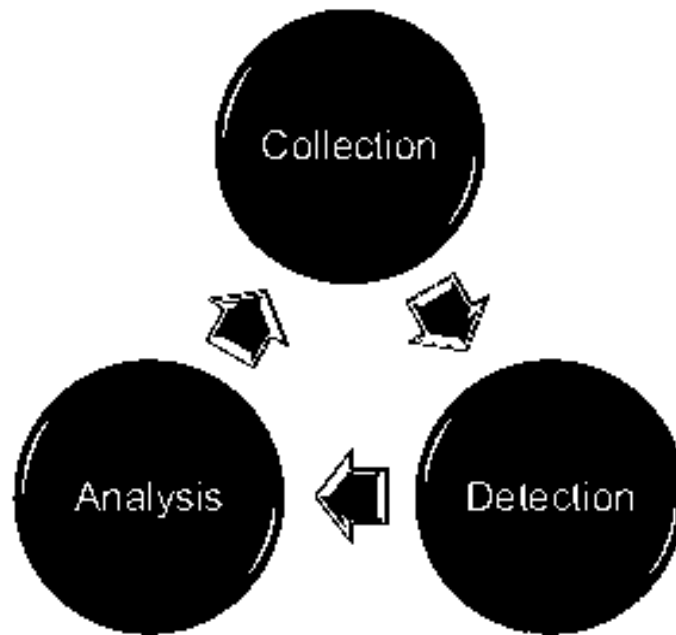
NMS (Network Security Monitoring) is the collection, analysis and escalation of indications and warnings to detect and respond to intrusions.

NMS is not an IDS, although it relies on IDS-like products as part of an integrated data collection and analysis suite. NMS involves collecting the full spectrum of data types (event, session, full content and statistical) needed to identify and validate intrusions.

The NSM model tries to give more control to the analyst by providing enough background to make independent decisions.

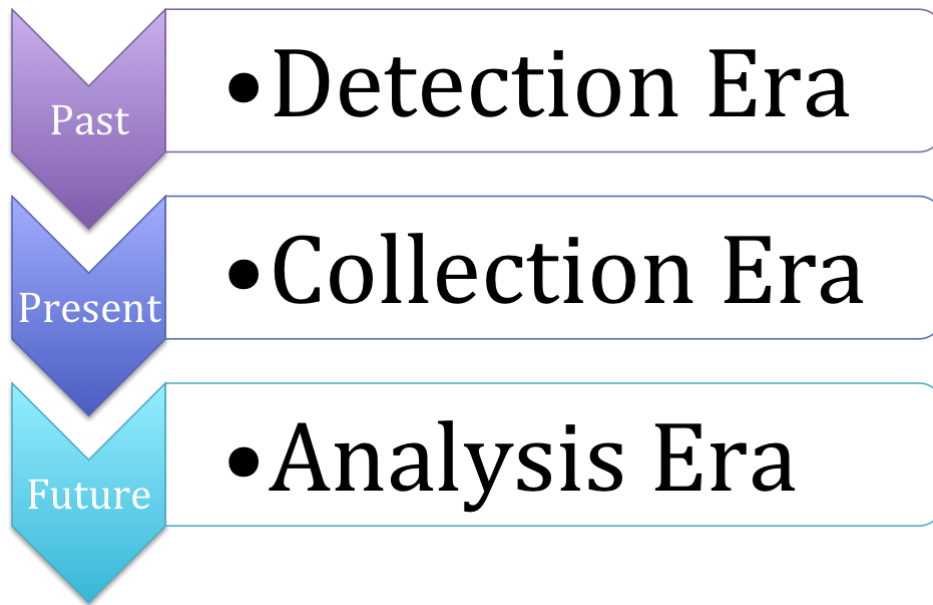
NSM is more concerned with network auditing than with real-time identification of intrusions. Although encryption denies the analyst the ability to see packet contents, it doesn't deny analysts the ability to see traffic patterns. Simply knowing who talked to whom, and when, is more information and that's how NSM handles encryption.

NSM Cycle



Collection is a function of hardware and software used to generate, organize, and store data to be used for detection and analysis. Detection is the process by which collected data is examined and alerts are generated based on observed events and data that are unexpected. This is typically accomplished through some form of signature, anomaly, or statistically based detection. Analysis occurs when a human interprets and investigates alert data to make a determination if malicious activity has occurred. Each of these processes feed into each other, with analysis feeding back into a collection strategy at the end of the cycle, which constantly repeats. This is what makes it a cycle. If that last part didn't happen, it would simply be a linear process.

While the NSM cycle flows from collection to detection and then analysis, this is not how the emphasis we as an industry has placed on these items has evolved. Looking back, the industry began its foray into what is now known as network security monitoring with a focus on detection. In this era came the rise of intrusion detection systems such as Snort that are still in use today. Organizations began to recognize that the ability to detect the presence of intruders on their network, and to quickly respond to the intrusions, was just as important as trying to prevent the intruder from breaching the network perimeter in the first place. These organizations believed that you should attempt to collect all of the data you can so that you could perform robust detection across the network. Thus, detection went forth and prospered, for a while.



As the size, speed, and function of computer networks grew, organizations on the leading edge began to recognize that it was no longer feasible to collect 100% of network data. Rather, effective detection relies on selectively gathering data relevant to your detection mission. This ushered in the era of collection, where organizations began to really assess the value received from ingesting certain types of data. For instance, while organizations had previously attempted to perform detection against full packet capture data for every network egress point, now these same organizations begin to selectively filter out traffic to and from specific protocols, ports, and services. In addition, these organizations are now assessing the value of data types that come with a decreased resource requirement, such as network flow data. This all worked towards performing more efficient detection through smarter collection. This brings us up to speed on where we stand in the modern day.

The goal of an analyst is to digest the alerts generated by various detection mechanisms and investigate multiple data sources to perform relevant tests and research to see if a network security breach has happened.

Best practices for successful NSM

- Perform network performance measurement before deploying the security monitoring solution. This is essential because security monitoring can have its own footprint on the network, especially if the monitoring solution is software-based, running on the servers.
- If possible and affordable, deploy more than one anti-virus solution. Many anti-virus software solutions don't offer spyware detection, or don't do it right; hence, a combination is always helpful.
- Deploy at least one FOSS packet-capturing software on the network. Though the IDS systems do this job partially, there can be situations where the IDS could be too busy to be used as a packet viewer, and a FOSS utility can come in handy for daily chores.
- Gather monitoring data at a secure place. It is often a mistake to gather security data on a desktop or a server which is easily accessible, making the network vulnerable at that point. Since security applies to the monitoring process too, the data captured must be stored in a secure manner.
- Monitor all layers; don't leave anything to chance. Usually, the data link layer is omitted from monitoring; however, since a new wave of attacks can exploit Ethernet frames too, it is important to take this layer into account. The same applies to the network layer, as most internal attacks can easily use it to exploit vulnerabilities.
- Deploy the IDS behind the firewall, since the firewall filters out everything that is not meant to enter the LAN. This improves the IDS' efficiency by keeping the clutter away.
- Capture VLANs separately. Since VLANs are separate TCP broadcast domains, separately gathering and analysing data for each can help detect internal and external security problems quickly.
- Consider all protocols. Many firms still use NetBIOS internally along with TCP/IP; such a situation demands monitoring all protocols on the wire. There are a few legacy types of attacks based on the NetBEUI protocol, which could be captured.
- Enable optimal auditing levels on the monitoring devices. Setting up too many audit event captures can easily confuse monitoring solutions while detecting an anomaly, whereas having very few audit logs can render security monitoring useless.

Types of monitoring

- Network tap – physical device which relays a copy of packets to an NSM server
- SPAN or mirrored ports – switch configuration which sends copies of packets to a separate port where NSM can connect
- Host NIC – configured to watch all network traffic flowing on its segment
- Serial port tap – physical device which relays serial traffic to another port, usually requires additional software to interpret data

Types of Data Collected

- Full content data – unfiltered collection of packets
- Extracted content – data streams, files, Web pages, etc.
- Session data – conversation between nodes
- Transaction data – requests and replies between nodes
- Statistical data – description of traffic, such as protocol and volume
- Metadata – aspects of data, e.g. who owns this IP address
- Alert/log data – triggers from IDS tools, tracking user logins, etc.

Challenges in Network Monitoring

- For starters, each of the seven layers of the OSI networking model has its own responsibilities, which call for separate methods of monitoring and security for each layer. Network monitoring is seemingly simple — but in reality, it's a very complex process. Mixing traditional network monitoring with security monitoring further complicates things from the design perspective, for network architects, network operations teams, and the systems administrators who manage it.
- The most important in network monitoring is the vast amount of data gathered by the monitoring tool, and the amount of time required to assimilate the information and apply intelligence to it, in order to achieve actionable decisions.
- Another challenge is caused by the unprecedented growth of a network, a result of the organisation's growth due to business expansion or company mergers. The bigger the network, the tougher it is to visualise the scale of network infrastructure. This can result in performance bottlenecks as well as security vulnerabilities. Finally, failure to incorporate proper monitoring tools is also a challenge to be addressed by senior IT management staff. It has been observed that relying purely on commercial products actually limits a firm's ability to bring diversification into the network monitoring process.

Challenges in Network Security

- From the infrastructure scaling point of view, irrespective of the size of an organisation, network security is often a complex area to deal with. Since network infrastructure contains components like firewalls, routers, managed switches, etc., the configurations and settings for each of these components further add to the complexity.
- Also, when faced with the choices of multiple devices offered by many vendors, it is easy for a network architect to get distracted from considering an appropriate solution customised to the network. As the network grows, it can be more prone to vulnerabilities and loopholes, needing tight security policies and careful designs, using cutting-edge technology devices and solutions.
- From the security point of view, a new breed of viruses and spyware has emerged recently, which exploits the operating system as well as the networking device's vulnerabilities, and can take control to cause enough damage. Though there are multiple security solutions available, hackers are often one step ahead of the cyber cops.
- It is often the case that an organisation is more prone to internal attacks than to attacks originating from outside the firm's network infrastructure. Preventing such attacks needs the latest techniques, such as the deployment of intrusion detection systems, unified threat management systems (UTMs), etc.

Next Generation Firewall

A next-generation firewall (NGFW) is a hardware- or software-based network security system that is able to detect and block sophisticated attacks by enforcing security policies at the application level, as well as at the port and protocol level.

Next-generation firewalls integrate three key assets: enterprise firewall capabilities, an intrusion prevention system (IPS) and application control. Like the introduction of stateful inspection in first-generation firewalls, NGFWs bring additional context to the firewall's decision-making process by providing it with the ability to understand the details of the Web application traffic passing through it and taking action to block traffic that might exploit vulnerabilities.

Next-generation firewalls combine the capabilities of traditional firewalls – including packet filtering, network address translation (NAT), URL blocking and virtual private networks (VPNs) -- with Quality of Service (QoS) functionality and features not traditionally found in firewall products. These include intrusion prevention, SSL and SSH inspection, deep-packet inspection and reputation-based malware detection as well as application awareness. The application-specific capabilities are meant to thwart the growing number of application attacks taking place on layers 4-7 of the OSI network stack.

NGFWs are integrated network security platforms that consist of in-line deep packet inspection (DPI) firewalls, IPS, application inspection and control, SSL/SSH inspection, website filtering and quality of service (QoS)/bandwidth management to protect networks against the latest in sophisticated network attacks and intrusion.

NGFWs are not traditional firewalls

Enterprises need to make an NGFW purchase decision based on need, risk and future growth. Don't buy a Cadillac if a Chevy pickup truck will do the job.

Unlike NGFWs, traditional packet-filtering firewalls only provide protection at Layer 3 (network) and Layer 4 (transport) of the OSI model. They include metrics to allow and deny packets by discriminating the source IP address of incoming packets, destination IP addresses, the type of Internet protocols the packet may contain -- e.g., normal data carrying IP packets, ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol), BOOTP (Bootstrap Protocol) and DHCP (Dynamic Host Configuration Protocol) -- and routing features.

Although firewalls are placed between the Internet and an internal network inside the DMZ, attackers have found ways to circumvent these controls and cause considerable damage before detection. Meanwhile, traditional firewalls often necessitate having to install separate IPS, Web application firewalls (WAFs), secure coding standards based on the Open Web Application Security Project's (OWASP) Top 10 vulnerabilities, strong encryption at the Web layer (SSL/TLS), and antivirus and malware prevention.

Having to deploy, manage and monitor this unwieldy number of network security products to mitigate multiple heterogeneous attack vectors is challenging, to say the least. In addition, this diverse array of security products can compromise each other's functionality at the expense of broadband resource usage, response times, and monitoring and maintenance requirements.

NGFWs address these issues by providing a single-vendor product with a common management process that includes multiple security services. It is, for the most part, a more cost-effective and pragmatic approach to network security.

NGFWs are not UTMs

Unified threat management systems (UTMs) are all-in-one network security platforms that are meant to provide simplicity, streamlined installation and use, as well as the ability to concurrently update all security functions. These systems, like NGFWs, clearly have a major advantage over acquiring a variety of network security technologies, as there's no need to maintain disparate security products and figure out how they all work together.

UTMs were originally designed for small to medium-sized businesses (SMBs), not large organizations, however. NGFWs, on the other hand, are generally more expansive and work to secure the networks of businesses from the size of an SMB to large enterprise environments. Unlike UTMs, most NGFWs, for example, offer threat intelligence, a degree of mobile device security, data loss prevention and an open architecture that allow clients to use regular expressions (regex) to tailor application control and even some firewall rule definitions.

Optimizing NGFW functionality

Optimal NGFW products must have three characteristics: be comprehensive, flexible and easy to use. Yes, this sounds oxymoronic, but achieving this trifecta is very doable for NGFW vendors.

First, NGFWs must be comprehensive, so that they include IPS, antivirus/malware prevention, application control, deep packet inspection and stateful firewalls (the former inspects incoming packets, the latter, outgoing), encryption, compression, QoS, and other capabilities. One drawback NGFWs need to overcome is the reluctance many enterprises have of relying on a single point of failure for network security.

Second, NGFWs must be flexible, which also means scalable, so that features can be modularized and activated based on need.

And third, NGFWs must be easy to use, with a fairly intuitive management interface that provides a clean and easy-to-read dashboard, feature activations, rule set definitions, configuration analysis, vulnerability assessments, activity reports and alerts.

Today's NGFWs make up a cadre of network security products that purport to offer these three characteristics. Although NGFW services are listed with commonly named features (e.g., DLP, application control and threat intelligence), a close look shows some variation between NGFW vendor products. For example, those NGFWs that offer mobile device security will admit this is not a mobile device management (MDM) product. They can identify mobile devices and operating systems, provide policy enforcement based on apps, users and content, and even extend a VPN tunnel to prevent malware, but they do not provide total device management as offered by MDM products.

Meanwhile, some NGFW features are more robust and advanced than others. So it is incumbent upon customers to carefully vet the features of individual NGFW products to determine the best fit for them. For example, not all NGFWs provide two-factor authentication or mobile device security, but then, not every customer needs those features. And while there are those NGFWs that say they support such features, some might require additional modules or products to make them work.

How NGFWs are sold

Most NGFWs are appliance-based, but some are available as virtual products (software) -- where enterprises can install them on their own servers -- and some delivered over the cloud as a software as a service. Most are modular, such that an enterprise can choose to purchase and activate features commensurate with their specific needs and risks.

Another important point about NGFWs: Never pay retail price. NGFW vendors want the business, and their job is to demonstrate the differentiators that set them apart from competitors.

Enterprises should also never buy the best or most technologically advanced product. They need to make an NGFW purchase decision based on need, risk and future growth. Don't buy a Cadillac if a Chevy pickup truck will do the job. Just make sure to know how long that pickup truck is needed, and ensure it'll be sufficient to maintain the organization's anticipated pace of growth.

The future of NGFWs

We live in exciting times. In speaking with top NGFW vendors, there are features under development that will make the IT department's life easier while further strengthening network security. These companies are also resolved to develop NGFW products that are better tailored to the network security requirements of SMBs, large enterprises and everything in between.

NGFW vendors are also spending a considerable amount of time and expense in R&D to keep pace with today's sophisticated attacks and meet the comprehensive, flexible and easy-to-use requirements outlined above. One of the major differentiators that, ironically, all of these major NGFW companies purport to be working on is threat intelligence that is current, open, continuous, adaptive and automatic.

In addition, all of today's NGFW vendors resolve to provide as comprehensive a coverage package to customers as possible without sacrificing performance.

Password Management

The majority of people use very weak passwords and reuse them on different websites. Passwords -- especially those not supported by two-step verification -- are last lines of defence against prying eyes.

A few ways in which account passwords can be compromised are:

- **Someone's out to get the password.**
There are many people who might want to take a peek into someone else's personal life. If these people know them well, they might be able to guess their e-mail password and use password recovery options to access the other accounts.
- **One can become the victim of a brute-force attack.**
Whether a hacker attempts to access a group of user accounts or just some specific person's, brute-force attacks are the go-to strategy for cracking passwords. These attacks work by systematically checking all possible passphrases until the correct one is found. If the hacker already has an idea of the guidelines used to create the password, this process becomes easier to execute.
- **There's a data breach.**
Every few months it seems another huge company reports a hacking resulting in millions of people's account information being compromised. And with the recent Heart bleed bug, many popular websites were affected directly.

Common ways of stealing Password

Applying passwords at various steps to access the data is not sufficient to safeguard the data today. Keeping default passwords or easy passwords result in creating a threat to the data. Many people realize that to avoid hacking, strong passwords are a must, but they fail to understand that the hackers/crackers are becoming sophisticated day by day.

Through social engineering or by guessing the passwords, they can easily break into the systems. One should therefore keep changing the passwords frequently and should be up to date with the latest techniques in use.

Methods to crack passwords:

- Guessing-

Various programs have been developed to guess a person's password, with any sort of personal information gained regarding him, from names, DOB, pet's name, license number etc. These programs are capable of searching a word spelled backwards. That is why it is advised to clear any personal information from one's password.

- Dictionary based attacks-

Certain programs have been developed, which run each and every word of the dictionary against a username in hope of finding a perfect match. Therefore it is advised to keep away from dictionary words of even the remotest language.

- Brute-Force attack-

By trying every conceivable combination of the keystrokes against a user name, Brute-Force attack is the most successful attack, and many programs can run this attack very quickly. Therefore it is advised to use a combination of upper and lower case words along with numbers and special characters and punctuation marks.

- Phishing-

Phishing scams are aimed to trick the person through IM or e-mails to provide their personal information. They might excite the recipient to respond. The best way to avoid being fooled is to not click on any such suspicious links.

- Shoulder surfing

Passwords are not always stolen online. The hacker may be standing behind you peeping in when you type your password. One should be careful and develop a habit of typing the password fast and by not looking at the keyboard.

Cyber security is based on the “weakest link”, and usually the password becomes that part of the chain which can be easily broken. Hence to create and maintain a strong password is very necessary.

What can be done with the stolen passwords?

- One can use charged services without victim's knowledge, resulting in them being charged for services which they have never used.
- Others can send spam mail using their name.
- Others can gain access to their email.

Strong Password is Necessary

While creating a password, a few points should be kept in the mind:

- Passwords are case sensitive, so a mixture of upper and lower case letters should be used
- The password should contain numerals & special characters randomly to make it strong. Put digits, symbols, and capital letters spread throughout the middle of your password, not at the beginning or end.
- A longer password is usually better than a more random password as long as the password is at least 12-15 characters long.
- Avoiding common sports and pop culture regardless of length is suggested. The more common a password is, the less secure it will be, so something no one else would be a better choice.
- Passwords are only as secure as the sites to which they are entrusted with. Limit the potential fallout by using a unique password everywhere. Or use a password manager.
- Admins who set password policies are better off requiring longer passwords and letting users keep them for longer, rather than requiring them to change passwords every one or two month. This encourages users to have stronger

passwords and avoids simple schemes like incrementing a number at the end of the password each time they have to reset it.

- Never give passwords to friends, even if they're really good friends. A friend can – maybe even accidentally – pass your password along to others or even become an ex-friend and abuse it.
- If password is in the dictionary, there is a chance someone will guess it. There's even software that criminals use that can guess words used in dictionaries.
- Programs or web services let you create a different very strong password for each of your sites. But you only have to remember the one password to access the program or secure site that stores your passwords for you.
- The best password in the world might not do you any good if someone is looking over your shoulder while you type or if you forget to log out on a cybercafé computer. Malicious software, including “keyboard loggers” that record all of your keystrokes, has been used to steal passwords and other information. To increase security, make sure you're using up-to-date anti-malware software and that your operating system is up-to-date.

In his guide to “mastering the art of passwords”, Dennis O'Reilly suggests creating a system that both allows you to create complex passwords and remember them.

For example, create a phrase like “I hope the Giants will win the World Series in 2016!” Then, take the initials of each word and all numbers and symbols to create your password. So, that phrase would result in this: IhtGwwtWSi2016!

Patch Management

The rise of widespread worms and malicious code targeting known vulnerabilities on unpatched systems, and the resultant downtime and expense they bring, is probably the biggest reason so many organizations are focusing on patch management. Along with these threats, increasing concern around governance and regulatory compliance has pushed enterprises to gain better control and oversight of their information assets. It's obvious that patch management is a critical issue. What is also clear is the main objective of a patch management program: to create a consistently configured environment that is secure against known vulnerabilities in operating system and application software.

The process used for patch management differs depending on the IT infrastructure of a company. In most cases, a large company with a large infrastructure typically automates patch management. This reduces the need for manual implementation. Small to mid-sized companies often choose to outsource their patch management to a managed IT services provider. A managed service provider can perform patches remotely.

There are a number of vulnerabilities that can endanger your network at any time. Patch management is a form of preventative maintenance that helps ensure your infrastructure's security. In some cases, there is a vulnerability in which a patch has not yet been released. A patch management system monitors your network and alerts technicians of exploits so that they can take action to prevent an attack even while a patch is in the process of being created.

Automated Patch Management

Patch management is very critical to business operations however it also tends to be considered a responsibility of the IT department. While this is partially true patch management within an organization's infrastructure cannot be successful without the understanding and support of the senior management.

Instead of waiting for the issue to be addressed when a problem occurs it is important to implement and plan for patch management in advance. The key concerns for many companies are in the number of patches and the manpower needed to deploy them. However, new technologies along with enterprises which offer patch management services have made patch management implementation and distribution easier and more cost effective.

Patch management services can help to keep your network secure while reducing costs.

An automated patch management solution involves the following processes:

Assess the vulnerability

Audit software in your production environment, evaluate potential security threats, vulnerabilities and non-compliances. This requires accurate inventory of IT assets to assess exposures.

Automated patch management relies on the Inventory component of Configuration Manager to perform scans that use the Windows® Update Agent (WUA) to scan endpoints and report information about found and missing patches.

Patch identification and download

Determine a reliable, timely source of information on software updates and a documented and secure download process.

Automated patch management uses Windows Server Update Services (WSUS) for downloading fixes for Windows operating systems and applications.

Patch testing

Validate a given patch in a test environment, provide the assurance that all necessary packages, pre-requisites, co-requisites, conflicts have been identified before deploying to production.

Patches can be deployed in a test environment to troubleshoot problems before patches are deployed in the enterprise.

Patch approval

Maintain strict control over what is being changed, which vulnerability the fix addresses, what services and applications are being impacted, and priority. Requires an approval process.

You use the WSUS interface to approve patches so that the automated patch management solution automatically creates software packages only for patches that have been approved.

Patch deployment

Prioritize the urgency of the patch deployment, schedule the deployment, build the installable unit, and deploy the patch.

An automated process generates software packages and activity plans, and then notifies the Administrator when they are ready to be submitted. The process relies on IBM Tivoli Configuration Manager Components and services, such as, Software Distribution and Activity Planner.

Patch verification

Validate that the patch was successfully applied on all eligible endpoints.

The automated patch management command line can be used to retrieve patch status information. Patch installations can also be monitored from the Activity Plan Monitor graphical user interface where activity plans are submitted.

Compliance management

Update the configuration baseline definitions to include the new patches, regularly analyse to assure that all endpoints remain in compliance, identify improvements and customize the patch management process accordingly.

Automated patch management is a dynamic process designed to identify any missing patches in your environment and to automatically create patches to cover the current vulnerabilities.

6 steps to an effective Patch Management System

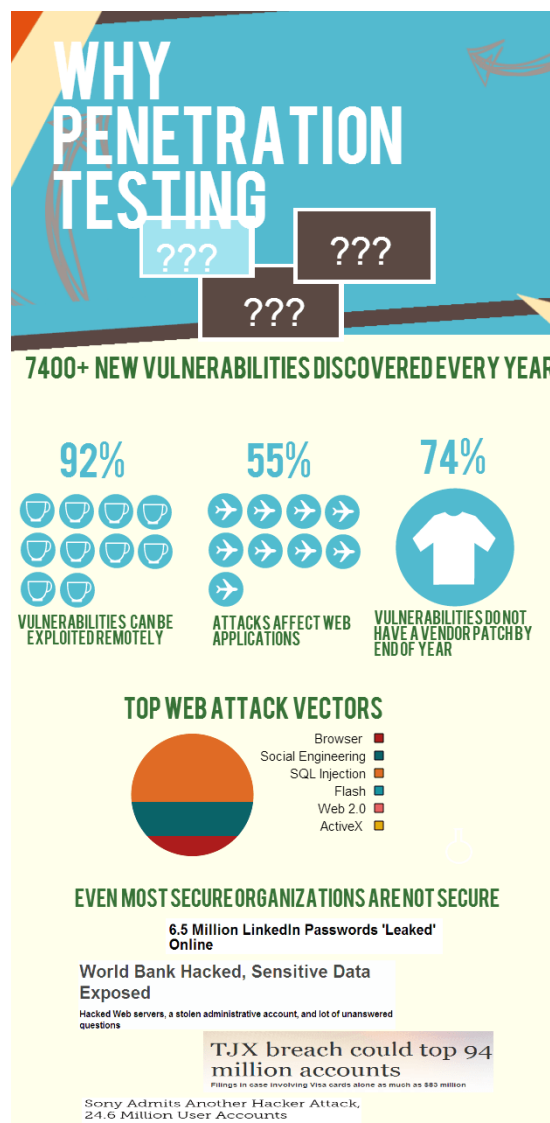
1. Develop an up-to-date inventory of all production systems, including OS types (and versions), IP addresses, physical location, custodian and function. Commercial tools ranging from general network scanners to automated discovery products can expedite the process (see Resources, below). You should inventory your network periodically.
2. Devise a plan for standardizing production systems to the same version of OS and application software. The smaller the number of versions you have running, the easier your job will be later.
3. Make a list of all the security controls you have in place--routers, firewalls, IDSes, AV, etc.--as well as their configurations. Don't forget to include system hardening or nonstandard configurations in your list of controls. This list will help you decide how to respond to a vulnerability alert (if at all).
4. Compare reported vulnerabilities against your inventory/control list. There are two key components to this. First, you need a reliable system for collecting vulnerability alerts. And second, you need to separate the vulnerabilities that affect your systems from those that don't.
5. Classify the risk. Assess the vulnerability and likelihood of an attack in your environment.
6. Apply the patch! You've determined which patches you need to install. Now comes the hard part: deploying them without disrupting uptime or production.

Information security is everybody's business and an effective patching process cannot be implemented without the cooperation and participation of end-users across the organization. Users should be made aware of the importance of IT security and patch management as part of their daily work process. If sufficient training is provided to end-users, they can often perform lightweight patching on their own workstations, which will reduce the workload on system administrators around basic patch management. User awareness is especially important in organizations that allow remote access to a corporate network, as a vulnerability exploited through a computer system in someone's home can threaten the security of the entire organization.

Penetration testing

Penetration testing is a type of security testing used to test the insecure areas of the system or application. The goal of this testing is to find all security vulnerabilities that are present in the system being tested. Vulnerability is the risk that an attacker can disrupt or gain authorized access to the system or any data contained within it. Vulnerabilities are usually introduced by accident during software development and implementation phase. Common vulnerabilities include design errors, configuration errors, software bugs etc.

Need of a Penetration testing:



Role and Responsibilities of Penetration Testers:

Penetration Testers job is to:

- Testers should collect required information from the Organization to enable penetration tests
- Find flaws that could allow hackers to attack a target machine
- Pen Testers should think & act like real hackers albeit ethically.
- Work done by Penetration testers should be reproducible so that it will be easy for developers to fix it
- Start date and End date of test execution should be defined in advance.
- Tester should be responsible for any loss in the system or information during the testing
- Tester should keep data and information confidential

Penetration is essential in an enterprise because -

- Financial sectors like Banks, Investment Banking , Stock Trading Exchanges want their data to be secured , and penetration testing is essential to ensure security
- In case if the software system is already hacked and organization wants to determine whether any threats are still present in the system to avoid future hacks.
- Proactive Penetration Testing is the best safeguard against hackers

Types of Penetration testing:

The type of penetration test selected usually depends on the scope and whether the organization wants to simulate an attack by an employee, Network Admin (Internal Sources) or by External Sources. There are three types of Penetration testing and they are

- Black Box Testing
- White Box Penetration testing
- Grey Box Penetration Testing

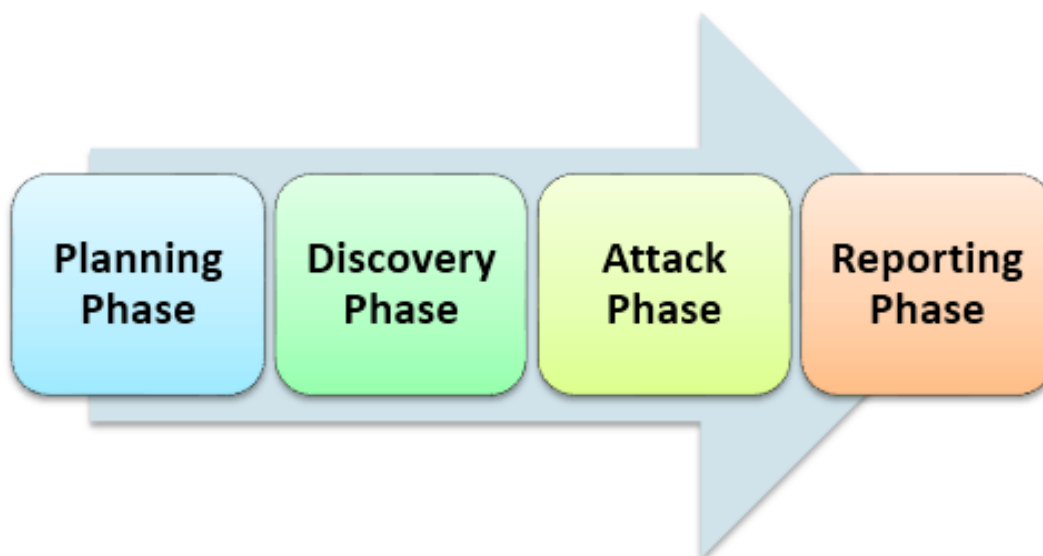
In black box penetration testing, tester has no knowledge about the systems to be tested. He is responsible to collect information about the target network or system.

In a white-box penetration testing, the tester is usually provided with a complete information about the network or systems to be tested including the IP address schema, source code, OS details, etc. This can be considered as a simulation of an attack by any Internal sources (Employees of an Organization).

In a grey box penetration testing, tester is provided with partial knowledge of the system. It can be considered as an attack by an external hacker who had gained illegitimate access to an organization's network infrastructure documents.

Steps in Penetration testing:

Following are activities needs to be performed to execute Penetration Test -



Planning phase

- Scope & Strategy of the assignment is determined
- Existing security policies, standards are used for defining the scope

Discovery phase

- Collect as much information as possible about the system including data in the system, user names and even passwords. This is also called as **FINGERPRINTING**
- Scan and Probe into the ports
- Check for vulnerabilities of the system

Attack Phase

- Find exploits for various vulnerabilities You need necessary security Privileges to exploit the system

Reporting Phase

- Report must contain detailed findings
- Risks of vulnerabilities found and their Impact on business
- Recommendations and solutions, if any

The prime task in penetration testing is to gather system information. There are two ways to gather information -

- 'One to one' or 'one to many' model with respect to host: A tester performs techniques in a linear way against either one target host or a logical grouping of target hosts (e.g. a subnet).
- 'Many to one' or 'many to many' model :The tester utilizes multiple hosts to execute information gathering techniques in a random, rate-limited, and in non-linear.

Manual Penetration vs. automated penetration testing

- Manual testing requires expert professionals to run the tests whereas Automated test tools provides clear reports with less experienced professionals
- Manual Testing requires excel and other tools to track it , but automation has centralized and standard tools
- In Manual testing, results vary from test to test but not in the case of Automated tests
- Memory Cleaning up should be remembered by users, but automated testing will have comprehensive clean ups.

Limitations of Penetration testing

Penetration Testing cannot find all vulnerabilities in the system .There are limitations of time, budget, scope, skills of Penetration Testers

Following will be side effects when we are doing penetration testing:

- Data Loss and Corruption
- Down Time
- Increase costs

Pen test strategies include

External testing strategy

External testing refers to attacks on the organization's network perimeter using procedures performed from outside the organization's systems, that is, from the Internet or Extranet. This test may be performed with non-or full disclosure of the environment in question. The test typically begins with publicly accessible information about the client, followed by network enumeration, targeting the company's externally visible servers or devices, such as the domain name server (DNS), e-mail server, Web server or firewall.

Internal testing strategy

Internal testing is performed from within the organization's technology environment. This test mimics an attack on the internal network by a disgruntled employee or an authorized visitor having standard access privileges. The focus is to understand what could happen if the network perimeter were successfully penetrated or what an authorized user could do to penetrate specific information resources within the organization's network. The techniques employed are similar in both types of testing although the results can vary greatly.

Blind testing strategy

A blind testing strategy aims at simulating the actions and procedures of a real hacker. Just like a real hacking attempt, the testing team is provided with only limited or no information concerning the organization, prior to conducting the test. The penetration testing team uses publicly available information (such as corporate Web site, domain name registry, Internet discussion board, USENET and other places of information) to gather information about the target and conduct its penetration tests. Though blind testing can provide a lot of information about the organization (so called inside information) that may have been otherwise unknown -- for example, a blind penetration may uncover such issues as additional Internet access points, directly connected networks, publicly available confidential/proprietary information, etc. But it is more time consuming and expensive because of the effort required by the testing team to research the target.

Double blind testing strategy

A double-blind test is an extension of the blind testing strategy. In this exercise, the organization's IT and security staff are not notified or informed beforehand and are "blind" to the planned testing activities. Double-blind testing is an important component of testing, as it can test the organization's security monitoring and incident identification, escalation and response procedures. As clear from the objective of this test, only a few people within the organization are made aware of the testing. Normally it's only the project manager who carefully watches the whole exercise to ensure that the testing procedures and the organization's incident response procedures can be terminated when the objectives of the test have been achieved.

Targeted testing strategy

Targeted testing or the lights-turned-on approach as it is often referred to, involves both the organization's IT team and the penetration testing team to carry out the test. There is a clear understanding of the testing activities and information concerning the target and the network design. A targeted testing approach may be more efficient and cost-effective when the objective of the test is focused more on the technical setting, or on the design of the network, than on the organization's incident response and other operational procedures. Unlike blind testing, a targeted test can be executed in less time and effort, the only difference being that it may not provide as complete a picture of an organization's security vulnerabilities and response capabilities.

Methods used in a penetration test

Passive research

As the name suggests, a passive research is a method used to gather as much information about an organization's systems configuration from public domain sources such as:

DNS (domain name service)

RIPE (Réseaux IP Européens)

USENET (newsgroups)

ARIN (American Registry for Internet Numbers)

*Passive research is generally performed at the beginning of an external penetration test.

Open source monitoring

This service is an associated technique that utilizes Internet meta-searches (multiple searches of Web sites, newswires, newsgroups and other sources) targeted on keyword that are important to the organization. The data is collected and discoveries are highlighted to the organization. This helps identify whether organization's confidential information has been leaked or whether an electronic conversation involving them has taken place. This enables an organization to take necessary measures to ensure confidentiality and integrity.

Network mapping and OS fingerprinting

Visualization of network configuration is an important part of penetration testing. Network mapping is used to create a picture of the configuration of the network being tested. A network diagram can be created which infers the logical locations and IP addresses of routers, firewalls, Web servers and other border devices.

Additionally, this examination can assist in identifying or "fingerprinting" operating systems. A combination of results from passive research and tools such as ping, traceroute and nmap, can help create a reasonably accurate network map.

An extension of network mapping is Port Scanning. This technique is aimed at identifying the type of services available on the target machine. The scan result reveals important

information such as function of a computer (whether it is a Web server, mail server etc) as well as revealing ports that may be serious security risks such as telnet. Port scans should include number of individual tests, including:

TCP (Transmission Control Protocol) scan

Connect scan

SYN (or half open) scan

RST (or Xmas-tree) scan

UDP (User Datagram Protocol) and ICMP (Internet Control Message Protocol) scans. Tools such as nmap can perform this type of scan.

Dynamic ports used by RPC (Remote Procedure Call) should be scanned using tool such as RPCinfo.

Spoofting

Spoofting involves creation of TCP/IP packets using somebody else's Internet addresses and then sending the same to the targeted computer making it believe that it came from a trusted source. It is the act of using one machine to impersonate another. Routers use the "destination IP" address in order to forward packets through the Internet, but ignore the "source IP" address. The destination machine only uses that source IP address when it responds back to the source. This technique is used in internal and external penetration testing to access computers that have been instructed to only reply to specific computers. This can result in sensitive information be released to unauthorised systems. IP spoofting is also an integral part of many network attacks that do not need to see responses (blind spoofting).

Network sniffing

Sniffing is technique used to capture data as it travels across a network. Sniffing is an important information gathering technique that enables capturing of specific information, such as passwords and also an entire conversation between specific computers, if required. To perform sniffing, the network card of computer needs to be put in promiscuous mode, so that it captures all data being sent across the network.

Sniffing is extensively used in internal testing where the sniffer or the computer in promiscuous mode is directly attached to the network enabling capturing of a great deal of information. Sniffing can be performed by a number of commercial tools such as Ethereal, Network Associates SnifferPro and Network Instruments Observer.

Trojan attack

Trojans are malicious programs that are typically sent into network as e-mail attachments or transferred via IM chat rooms. These programs run in stealth mode and get installed on the client computer without the users' knowledge. Once installed, they can open remote control channels to attackers or capture information. A penetration test aims at attempting to send specially prepared Trojans into a network.

Brute force attack

A brute force attack involves trying a huge number of alphanumeric combinations and exhaustive trial and error methods in order find legitimate authentication credentials. The objective behind this time consuming exercise is to gain access to the target system. Brute force attacks can overload a system and can possibly stop it from responding to legitimate requests. Additionally, if account lockout is being used, brute force attacks may close the account to legitimate users.

Vulnerability scanning/analysis

Vulnerability scanning/analysis is an exhaustive examination of targeted areas of an organization's network infrastructure aimed at determining their current state. The targets range from a single system or only critical systems to scanning the entire network. It is usually performed using automated tools that test for a multitude of potential weaknesses in a system against a database of known vulnerabilities and report potential security holes. And although they don't actively prevent attacks, many scanners provide additional tools to help fix found vulnerabilities. Some of the commonly used vulnerability scanners include: the open-source Nessus Project's Nessus, ISS Internet Scanner, GFI Software's GFI LANguard Network Security Scanner, eEye Digital Security's Retina Network Security Scanner, the BindView RMS vulnerability-management solutions and Network Associates CyberCop.

Scenario analysis

Once a vulnerability scanning has been done and weaknesses identified, the next step is to perform Scenario testing. This testing aims at exploiting identified security weaknesses to perform a system penetration that will produce a measurable result, such as stolen information, stolen usernames and passwords or system alteration. This level of testing assures that no false positives are reported and makes risk assessment of vulnerabilities much more accurate. Many tools exist to assist exploit testing, although the process is often highly manual. Exploit testing tends to be the final stage of penetration testing.

Privileged Access Management (PAM)

A privileged user is someone who has administrative access to critical systems. For instance, the individual who can set up and delete email accounts on Microsoft Exchange Server is a privileged user. The word is not accidental. Like any privilege, it should only be extended to trusted people. Only those seen as responsible can be trusted with “root” privileges like the ability to change system configurations, install software, change user accounts or access secure data. Of course, from a security perspective, it never makes sense to unconditionally trust anyone. That's why even trusted access needs to be controlled and monitored. And, of course, privileges can be revoked at any time.

Privileged accounts represent the largest security vulnerability an organization faces today. In the hands of an external attacker or malicious insider, privileged accounts allow attackers to take full control of an organization's IT infrastructure, disable security controls, steal confidential information, commit financial fraud and disrupt operations. Stolen, abused or misused privileged credentials are used in nearly all breaches. With this growing threat, organizations need controls put in place to proactively protect against, detect and respond to in-progress cyber-attacks before they strike vital systems and compromise sensitive data.

PAM makes it harder for attackers to penetrate a network and obtain privileged account access. PAM adds protection to privileged groups that control access across a range of domain-joined computers and applications on those computers. It also adds more monitoring, more visibility, and more fine-grained controls so that organizations can see who their privileged administrators are and what are they doing. PAM gives organizations more insight into how administrative accounts are used in the environment.

A PAM solution offers a secure, streamlined way to authorize and monitor all privileged users for all relevant systems. PAM lets you:

- Grant privileges to users only for systems on which they are authorized.
- Grant access only when it's needed and revoke access when the need expires.
- Avoid the need for privileged users to have or need local/direct system passwords.
- Centrally and quickly manage access over a disparate set of heterogeneous systems.
- Create an unalterable audit trail for any privileged operation.

Types of Privileged Accounts

Privileged accounts are broadly classified as:

- **Administrative accounts:** A non-generic personal (named) user account that is assigned to an administrative role or assumes elevated privileges in the process, and therefore has access to all standard user and privileged operations.
- **System accounts:** These are built into systems or applications, such as root on Unix/Linux systems or Administrator on Windows systems.
- **Operational accounts:** This type of account falls into two subcategories and may have elevated privileges:
 - **Shared accounts** set up to be used for administration and software installation. These accounts were not created for the exclusive use of a particular user, and may be shared by multiple users. They may also include emergency accounts, often known as "Firecall" or "break-glass" accounts, used in the event of an emergency that requires privileged access on a temporary basis.
 - **Service accounts or application accounts** that are used to allow remote (software-to-software) interactions with other systems, or to run system services.

Types of PAM Tools

Although it is theoretically possible to use manual processes to manage privileged access, in practice it is too cumbersome to do so, and virtually impossible to enforce such practices without specialized privileged access management (PAM) tools. PAM is a set of technologies designed to help organizations address the inherent problems related to privileged accounts. Gartner classifies the available PAM technologies in four main categories:

- **Shared-account password management (SAPM) tools:** Control use of (usually privileged) shared accounts
- **Application-to-application password management (AAPM) tools:** Control use of (usually privileged) application accounts for programmatic access
- **Super user privilege management (SUPM) tools:** Allow users granular, context-driven and/or time-limited use of super user privileges
- **Privileged session management (PSM) tools:** Manage privileged sessions to target systems and provide detailed privileged activity logging and monitoring

Components of PAM solutions

Privileged Access Management solutions vary in their architectures, but most offer the following components working in concert:

Access Manager

This PAM module governs access to privileged accounts. It is a single point of policy definition and policy enforcement for privileged access management. A privileged user requests access to a system through the Access Manager. The Access Manager knows which systems the user can access and at what level of privilege. A super admin can add/modify/delete privileged user accounts on the Access Manager. This approach reduces the risk that a former employee will retain access to a critical system.

Password Vault

The best PAM systems prevent privileged users from knowing the actual passwords to critical systems. This prevents a manual override on a physical device, for example. Instead, the PAM system keeps these password in a secure vault and opens access to a system for the privileged user once he has cleared the Access Manager.

Session Manager

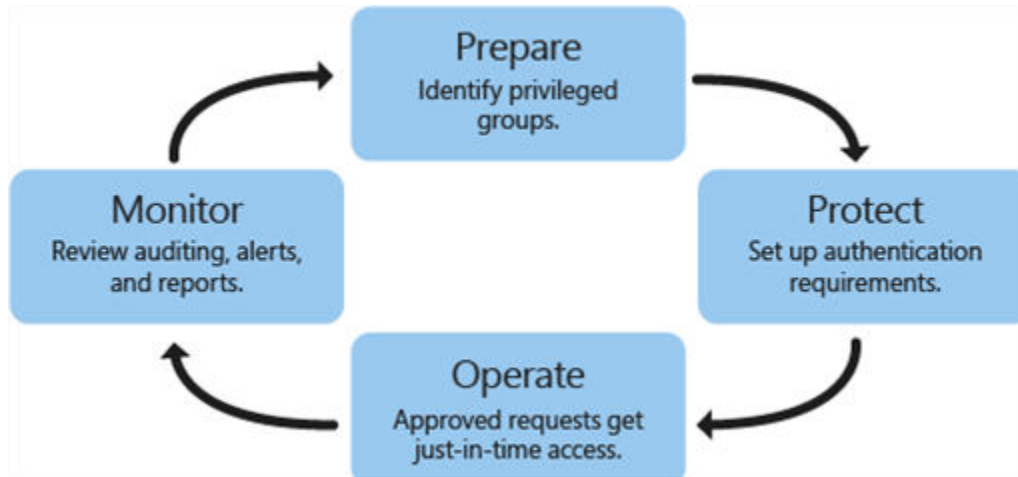
Access control is not enough. You need to know what a privileged user actually did during an administrative session. A Session Manager tracks actions taken during a privileged account session.

Challenges faced with Privileged Accounts

- Management of privileged access is a major challenge for most organizations. Regulators and auditors are increasingly aware of the need to control and monitor access to privileged accounts.
- Many organizations allow unrestricted and unmonitored use of privileged credentials that are shared among users, and thereby severely limiting the possibility of personal accountability.
- Many organizations assign full super user privileges to application developers, DBAs and others, which is an egregious violation of the principle of least privilege.
- Effective procedures around managing privileged access and shared accounts are cumbersome without specialized tools.
- A lack of access governance model for privileged accounts in most organizations leads to governance issues, such as accumulation of privileged access, orphaned accounts, ownership conflicts and others.

PAM Setup

PAM setup and operation has four steps:



Prepare:

Identify which groups in your existing forest have significant privileges. Recreate these groups without members in the bastion forest.

Protect:

Set up lifecycle and authentication protection, such as Multi-Factor Authentication (MFA), for when users request just-in-time administration. MFA helps prevent programmatic attacks from malicious software or following credential theft.

Operate:

After authentication requirements are met and a request is approved, a user account gets added temporarily to a privileged group in the bastion forest. For a pre-set amount of time, the administrator has all privileges and access permissions that are assigned to that group. After that time, the account is removed from the group.

Monitor:

PAM adds auditing, alerts, and reports of privileged access requests. You can review the history of privileged access, and see who performed an activity. You can decide whether the activity is valid or not and easily identify unauthorized activity, such as an attempt to add a user directly to a privileged group in the original forest. This step is important not only to identify malicious software but also for tracking "inside" attackers.

Advantages of PAM

PAM offers the following advantages:

- **Isolation/scoping of privileges:** Users do not hold privileges on accounts that are also used for non-privileged tasks like checking email or browsing the Internet. Users need to request privileges. Requests are approved or denied based on MIM policies defined by a PAM administrator. Until a request is approved, privileged access is not available.
- **Step-up and proof-up:** These are new authentication and authorization challenges to help manage the lifecycle of separate administrative accounts. The user can request the elevation of an administrative account and that request goes through MIM workflows.
- **Additional logging:** Along with the built-in MIM workflows, there is additional logging for PAM that identifies the request, how it was authorized, and any events that occur after approval.
- **Customizable workflow:** The MIM workflows can be configured for different scenarios, and multiple workflows can be used, based on the parameters of the requesting user or requested roles.

PAM Best Practices

- Identify all privileged accounts and their owners in your IT infrastructure. Review business, operational and regulatory requirements to classify these accounts based on the level of risk they present in your environment.
- Do not allow passwords for privileged accounts to be shared. Establish processes and controls for managing and monitoring the use of shared accounts and their passwords.
- Grant only the minimum level of privileges required to carry out a task, and limit the time when they can be used whenever possible.
- Evaluate and implement appropriate PAM tools and compensating controls, including risk-appropriate authentication methods for access to PAM tools.
- Establish privileged access governance by extending identity governance controls, such as automated provisioning, entitlements cataloguing and access certification, to privileged accounts and administrator access.

Public Key Infrastructure (PKI)

A public key infrastructure (PKI) supports the distribution and identification of public encryption keys, enabling users and computers to both securely exchange data over networks such as the Internet and verify the identity of the other party.

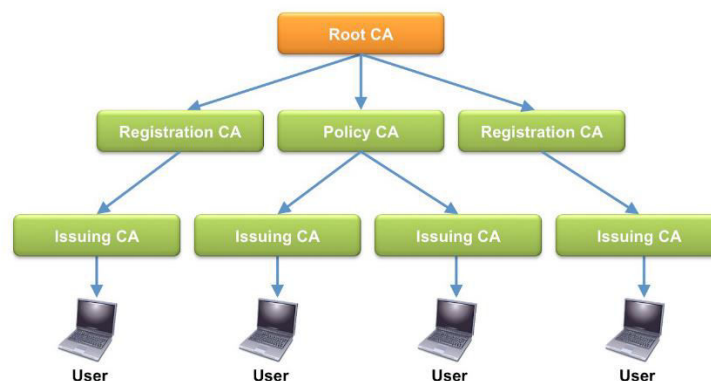
Without PKI, sensitive information can still be encrypted (ensuring confidentiality) and exchanged, but there would be no assurance of the identity (authentication) of the other party. Any form of sensitive data exchanged over the Internet is reliant on PKI for security.

Elements of PKI

A typical PKI consists of hardware, software, policies and standards to manage the creation, administration, distribution and revocation of keys and digital certificates. Digital certificates are at the heart of PKI as they affirm the identity of the certificate subject and bind that identity to the public key contained in the certificate.

A typical PKI includes the following key elements:

- A trusted party, called a certificate authority (CA), acts as the root of trust and provides services that authenticate the identity of individuals, computers and other entities
- A registration authority, often called a subordinate CA, certified by a root CA to issue certificates for specific uses permitted by the root
- A certificate database, which stores certificate requests and issues and revokes certificates
- A certificate store, which resides on a local computer as a place to store issued certificates and private keys



Certificates and Certification Authorities

For public-key cryptography to be valuable, users must be assured that the other parties with whom they communicate are “safe”—that is, their identities and keys are valid and trustworthy. To provide this assurance, all users of a PKI must have a registered identity. These identities are stored in a digital format known as a public key certificate. Certification Authorities (CAs) represent the people, processes, and tools to create digital certificates that securely bind the names of users to their public keys. In creating certificates, CAs act as agents of trust in a PKI. As long as users trust a CA and its business policies for issuing and managing certificates, they can trust certificates issued by the CA. This is known as third-party trust. CAs create certificates for users by digitally signing a set of data that includes the following information (and additional items):

- The user's name in the format of a distinguished name (DN). The DN specifies the user's name and any additional attributes required to uniquely identify the user (for example, the DN could contain the user's employee number).
- A public key of the user. The public key is required so that others can encrypt for the user or verify the user's digital signature.
- The validity period (or lifetime) of the certificate (a start date and an end date).
- The specific operations for which the public key is to be used (whether for encrypting data, verifying digital signatures, or both).

The CA's signature on a certificate allows any tampering with the contents of the certificate to be easily detected. (The CA's signature on a certificate is like a tamper-detection seal on a bottle of pills—any tampering with the contents of a certificate is easily detected) As long as the CA's signature on a certificate can be verified, the certificate has integrity. Since the integrity of a certificate can be determined by verifying the CA's signature, certificates are inherently secure and can be distributed in a completely public manner (for example, through publicly-accessible directory systems).

Users retrieving a public key from a certificate can be assured that the public key is valid. That is, users can trust that the certificate and its associated public key belong to the entity specified by the distinguished name. Users also trust that the public key is still within its defined validity period. In addition, users are assured that the public key may be used safely in the manner for which it was certified by the CA.

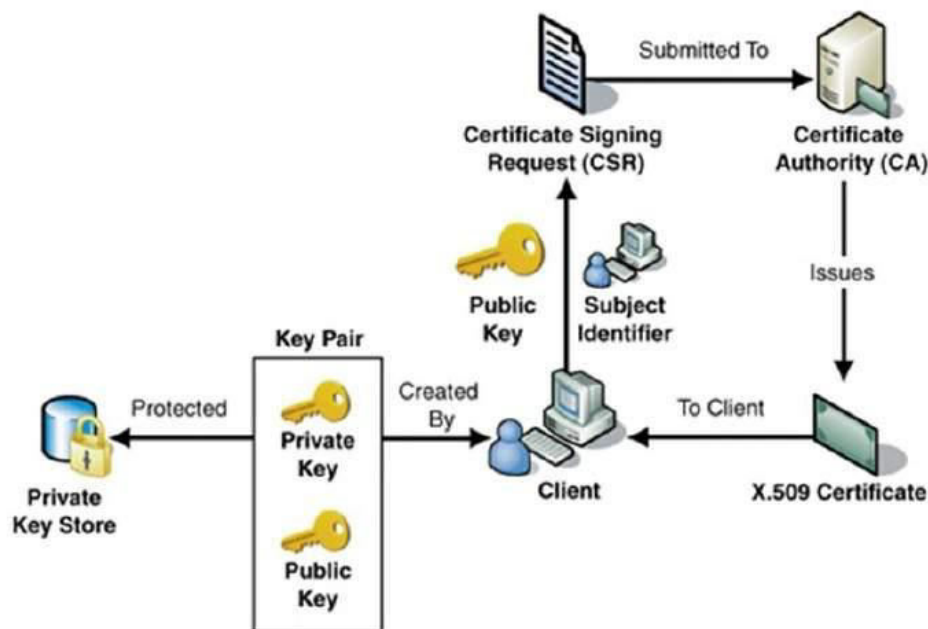
Digital Signature

For analogy, a certificate can be considered as the ID card issued to the person. People use ID cards such as a driver's license, passport to prove their identity. A digital certificate does the same basic thing in the electronic world, but with one difference.

Digital Certificates are not only issued to people but they can be issued to computers, software packages or anything else that need to prove the identity in the electronic world.

- Digital certificates are based on the ITU standard X.509 which defines a standard certificate format for public key certificates and certification validation. Hence digital certificates are sometimes also referred to as X.509 certificates.
- Public key pertaining to the user client is stored in digital certificates by The Certification Authority (CA) along with other relevant information such as client information, expiration date, usage, issuer etc.
- CA digitally signs this entire information and includes digital signature in the certificate.

Anyone who needs the assurance about the public key and associated information of client, he carries out the signature validation process using CA's public key. Successful validation assures that the public key given in the certificate belongs to the person whose details are given in the certificate.



Certificate repositories and certificate distribution

As mentioned earlier in this paper, the CA acts as a trusted third-party issuing certificates to users. Businesses also must distribute those certificates so they can be used by applications. Certificate repositories store certificates so that applications can retrieve them on behalf of users. The term repository refers to a network service that allows for distribution of certificates. Over the past few years, the consensus in the information technology industry is that the best technology for certificate repositories is provided by directory systems that are LDAP (Lightweight Directory Access Protocol)-compliant. LDAP defines the standard protocol to access directory systems. Several factors drive this consensus position:

- storing certificates in directories and having applications retrieve certificates on behalf of users provides the transparency required for use in most businesses
- many directory technologies supporting LDAP can be scaled to:
 - support a very large number of entries
 - respond efficiently to search requests due to their information storage and retrieval methods, and
 - be distributed throughout the network to meet the requirements of even the most highly-distributed organizations

In addition, the directories that support certificate distribution can store other organizational information. As discussed in the next section, the PKI can also use the directory to distribute certificate revocation information.

Support for Non-Repudiation

Repudiation occurs when an individual denies involvement in a transaction. (For instance, when someone claims a credit card is stolen, this means that he or she is repudiating liability for transactions that occur with that card any time after reporting the theft). Non-repudiation means that an individual cannot successfully deny involvement in a transaction. In the paper-world, individuals' signatures legally bind them to their transactions (for example, credit card charges, and business contracts). The signature prevents repudiation of those transactions. In the electronic world, the replacement for the pen-based signature is a digital signature. All types of electronic commerce require digital signatures because electronic commerce makes traditional pen-based signatures obsolete.

The signing private key

The most basic requirement for non-repudiation is that the key used to create digital signatures and signing be generated and securely stored in a manner under the sole control of the user at all times. It is not acceptable to back up the signing key. Unlike encryption key pairs, there is no technical or business requirement to backup or restore previous signing key pairs when users forget their passwords or lose, break, or corrupt their signing keys. In such cases, it is acceptable for users to generate new signing key pairs and continue using them from that time forward.

The need for two key pairs

It is difficult to simultaneously support key backup and recovery and non-repudiation. To support key backup and recovery the decryption keys must be backed up securely. To support non-repudiation, the keys used for digital signature cannot be backed up and must be under the sole control of the user at all times. To meet these requirements, a PKI must support two key pairs for each user. At any point in time, a user must have one current key pair for encryption and decryption, and a second key pair for digital signature and signature verification. Over time, users will have numerous key pairs that must be managed appropriately.

Client-side softwares

When discussing requirements for PKIs, businesses often neglect the requirement for client-side software. (For instance, many people only focus on the CA component when discussing PKIs). Ultimately, however, the value of a PKI is tied to the ability of users to use encryption and digital signatures. For this reason, the PKI must include client-side software that operates consistently and transparently across applications on the desktop (for example, email, Web browsing, e-forms, file/folder encryption). A consistent, easy-to-use PKI implementation within client-side software lowers PKI operating costs. In addition, client-side software must be technologically enabled to support all of the elements of a PKI discussed earlier in this paper. The following list summarizes the requirements client-side software must meet to ensure that users in a business receive a usable, transparent (and thus, acceptable) PKI.

Public key certificates

To provide third-party trust, all PKI-enabled applications must use certificates in a consistent, trustworthy manner. The client-side software must validate the CA's signature on certificates and ensure that the certificates are within their validity periods

Key backup and recovery

To ensure users are protected against loss of data, the PKI must support a system for backup and recovery of decryption keys. With respect to administrative costs, it is unacceptable for each application to provide its own key backup and recovery. Instead, all PKI-enabled client applications should interact with a single key backup and recovery system. The interactions between the client-side software and the key backup and recovery system must be secure, and the interaction method must be consistent across all PKI-enabled applications.

Support for non-repudiation

To provide basic support for non-repudiation, the client-side software must generate the key pairs used for digital signature. In addition, the client-side software must ensure that the signing keys are never backed up and remain under the users' control at all times. This type of support must be consistent across all PKI-enabled applications.

Automatic update of key pairs

To enable transparency, client-side applications must automatically initiate updating of users' key pairs. This activity must be done in accordance with the security policies of

the organization. It is unacceptable for users to have to know that their key pairs require updating. To meet this requirement across all PKI-enabled applications, the client-side software must update key pairs transparently and consistently.

Management of key histories

To enable users to easily access all data encrypted for them (regardless of when it was encrypted), PKI-enabled applications must have access to users' key histories. The client-side software must be able to securely recover users' key histories.

A scalable certificate repository

To minimize the costs of distributing certificates, all PKI-enabled applications must use a common, scalable certificate repository.

Risk Analysis

Risk analysis is the process of defining and analyzing the dangers to individuals, businesses and government agencies posed by potential natural and human-caused adverse events. In IT, a risk analysis report can be used to align technology-related objectives with a company's business objectives. A risk analysis report can be either quantitative or qualitative.

In quantitative risk analysis, an attempt is made to numerically determine the probabilities of various adverse events and the likely extent of the losses if a particular event takes place.

Qualitative risk analysis, which is used more often, does not involve numerical probabilities or predictions of loss. Instead, the qualitative method involves defining the various threats, determining the extent of vulnerabilities and devising countermeasures should an attack occur.

Risk analysis, which is a tool for risk management, is a method of identifying vulnerabilities and threats, and assessing the possible damage to determine where to implement security safeguards. Risk analysis is used to ensure that security is cost effective, relevant, timely and responsive to threats. Security can be quite complex, even for well-versed security professionals, and it is easy to apply too much security, not enough security or the wrong security components, and spend too much money in the process without attaining the necessary objectives. Risk analysis helps companies prioritize their risks and shows management the amount of money that should be applied to protecting against those risks in a sensible manner.

A risk analysis has four main goals:

- Identify assets and their values
- Identify vulnerabilities and threats
- Quantify the probability and business impact of these potential threats
- Provide an economic balance between the impact of the threat and the cost of the countermeasure

The process of conducting a risk analysis is very similar to identifying an acceptable risk level. Essentially, you do a risk analysis on the organization as a whole to determine the acceptable risk level. This is then your baseline to compare all other identified risks to determine whether the risk is too high or if it is under the established acceptable risk level.

Why Risk Analytics?

Today, risk analytics techniques make it possible to measure, quantify, and even predict risk with more certainty than ever before. That's a big deal for organizations that have relied heavily on the opinions of leaders at the business unit level to monitor, assess, and report risk. Even for executives with sound intuition, it was virtually impossible to construct an enterprise level view of risk spanning many different parts of the business.

This is where analytics excels. It helps establish a baseline for measuring risk across the organization by pulling together many strands of risk into one unified system and offering executive's clarity in identifying, viewing, understanding, and managing risk.

Taking a unified approach to risk management is a key component of becoming what we call a Risk Intelligent Enterprise™—one in which boards and executives integrate risk considerations into strategic decision making, and where business units and functions incorporate risk intelligence into the many actions they take.

Steps to conduct Risk Analysis

Step one: Identify assets and their values

Risk analysis provides a cost/benefit comparison, which compares the annualized cost of safeguards to protect against threats with the potential cost of loss. A safeguard, in most cases, should not be implemented unless the annualized cost of loss exceeds the annualized cost of the safeguard itself. This means that if a facility is worth \$100,000, it does not make sense to spend \$150,000 trying to protect it.

The value placed on assets (including information) is relative to the parties involved, what work was required to develop it, how much it costs to maintain, what damage would result if it were lost or destroyed, and what benefit another party would gain if it were to obtain it. If a company does not know the value of the information and the other assets it is trying to protect, it does not know how much money and time it should spend on protecting them.

The value of an asset should reflect all identifiable costs that would arise if there were an actual impairment of the asset. If a server costs \$4,000 to purchase, this value should not be input as the value of the asset in a business risk assessment. Rather, the cost of replacing or repairing it, the loss of productivity and the value of any data that may be corrupted or lost, need to be accounted for to properly capture the amount the company would lose if the server were to fail for one reason or another.

The following issues should be considered when assigning values to assets:

- Cost to acquire or develop the asset
- Cost to maintain and protect the asset
- Value of the asset to owners and users
- Value of the asset to adversaries
- Value of intellectual property that went into developing the information
- Price others are willing to pay for the asset
- Cost to replace the asset if lost
- Operational and production activities that are affected if the asset is unavailable
- Liability issues if the asset is compromised
- Usefulness and role of the asset in the organization

Understanding the value of an asset is the first step to understanding what security mechanisms should be put in place and what funds should go toward protecting it. A very important question is how much it could cost the company to not protect the asset.

Step two: Identify vulnerabilities and threats

Once the assets have been identified and assigned values, all of the vulnerabilities and associated threats need to be identified for each asset or group of assets. The IRM team needs to identify the vulnerabilities that could affect each asset's integrity, availability or confidentiality requirements. All of the relevant vulnerabilities need to be identified and documented so that the necessary countermeasures can be implemented.

Since there is a large amount of vulnerabilities and threats that can affect the different assets, it is important to be able to properly categorize them. The goal is to determine which threats and vulnerabilities could cause the most damage so that the most critical items can be taken care of first.

Step three: Quantify the probability and business impact of these potential threats

The team carrying out the risk assessment needs to figure out the business impact for the identified threats.

To estimate potential losses posed by threats, answer the following questions:

What physical damage could the threat cause, and how much would that cost?

How much productivity loss could the threat cause, and how much would that cost?

What is the value lost if confidential information is disclosed?

What is the cost of recovering from a virus attack?

What is the cost of recovering from a hacker attack?

What is the value lost if critical devices were to fail?

What is the single loss expectancy (SLE) for each asset and each threat?

This is just a small list of questions that should be answered. The specific questions will depend upon the types of threats the team uncovers.

The team then needs to calculate the probability and frequency of the identified vulnerabilities being exploited. The team will need to gather information about the likelihood of each threat taking place from people in each department, past records and official security resources. If the team is using a quantitative approach, then they will calculate the annualized rate of occurrence (ARO), which is how many times the threat can take place in a 12-month period.

Step four: Identify countermeasures and determine cost/benefit

The team then needs to identify countermeasures and solutions to reduce the potential damages from the identified threats.

A security countermeasure must make good business sense, meaning that it is cost-effective and that its benefit outweighs its cost. This requires another type of analysis: a cost/benefit analysis.

A commonly used cost/benefit calculation for a given safeguard is:

$$(\text{ALE before implementing safeguard}) - (\text{ALE after implementing safeguard}) - (\text{annual cost of safeguard}) = \text{value of safeguard to the company}$$

For example, if the ALE of the threat of a hacker bringing down a Web server is \$12,000 prior to implementing the suggested safeguard, \$3,000 after implementing the safeguard, and the annual cost of maintenance and operation of the safeguard is \$650, then the value of this safeguard to the company is \$8,350 each year.

The cost of a countermeasure is more than just the amount that is filled out on the purchase order. The following items need to be considered and evaluated when deriving the full cost of a countermeasure:

- Product costs
- Design/planning costs
- Implementation costs
- Environment modifications
- Compatibility with other countermeasures
- Maintenance requirements
- Testing requirements
- Repair, replacement or update costs
- Operating and support costs
- Effects on productivity

So, for example, the cost of this countermeasure could be:

\$5,500 for the product

\$2,500 for training

\$3,400 for the lab and testing time

\$2,600 for the loss in user productivity once the product was introduced into production

\$4,000 in labor for router reconfiguration, product installation, troubleshooting, and installation of the two service patches.

The real cost of this countermeasure is \$18,000. If our total potential loss was calculated at \$9,000, we went over budget by 100% when applying this countermeasure for the identified risk. Some of these costs may be hard or impossible to identify before they are acquired, but an experienced risk analyst would account for many of these possibilities.

It is important that the team knows how to calculate the actual cost of a countermeasure to properly weigh it against the benefit and savings the countermeasure is supposed to provide.

Goals of risk analysis

The risk analysis team should have clearly defined goals that it is seeking. The following is a short list of what generally is expected from the results of a risk analysis:

- Monetary values assigned to assets
- Comprehensive list of all possible and significant threats
- Probability of the occurrence rate of each threat
- Loss potential the company can endure per threat in a 12-month time span
- Recommended safeguards, countermeasures and actions

Although this list looks short, there is usually an incredible amount of detail under each bullet item. This report is presented to senior management, which will be concerned with possible monetary losses and the necessary costs to mitigate these risks. Although the reports should be as detailed as possible, there should be executive abstracts so that senior management may quickly understand the overall findings of the analysis.

Benefits of Risk Analytics

Get the details

Risk analytics helps take the guesswork out of managing risk-related issues by using a range of techniques and technologies to extrapolate insights, calculate likely scenarios, and predict future events.

Understand the complexity

An organization's exposure to risk is influenced by increasing volumes of structured data—such as databases—and unstructured data—such as websites, social media, and blogs—that are available to an organization internally and externally. Risk analytics can be leveraged to integrate this data into a single, unified view, gather valuable information, and enable actionable insights.

Cross the divide

In their scramble to build effective risk strategies, teams often fail to consider the overall impact to the organization. Risk analytics pulls data across the organization into one central platform, helping create a truly enterprise-wide approach.

Lay the groundwork

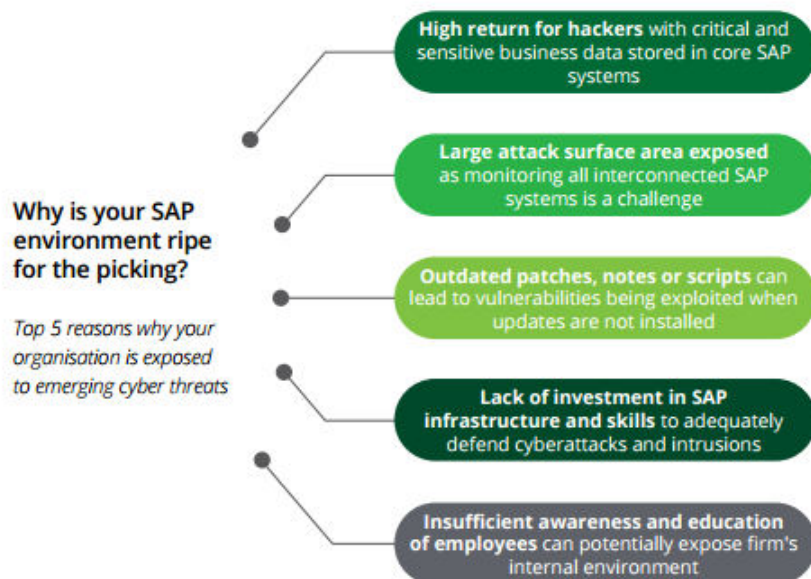
Risk is such a wide-ranging issue, spilling across organizational barriers, that it can be hard to know exactly what to do with risk-related insights. Risk analytics is instrumental in this scenario, allowing organizations to develop foresight with respect to potential risks and zero in on “crunchy” questions that lay the groundwork for action.

SAP ERP Security

SAP Enterprise Central Component (also known as SAP ERP, earlier – as SAP R/3) is a heart of Enterprise Resource Management. It is undoubtedly one of the major elements of any business as it enables effective management, storage and processing of such critical information as personal data of employees, financial and tax reports information about material resources and more, depending on the modules enabled. Unauthorized access to this system can result in disruption of key business processes and data corruption.

Enterprise resource planning (ERP) systems are the backbone of many large organizations and are critical to successfully running business operations.

However, many ERP systems are very complex with a diverse set of stakeholders throughout the enterprise. They have also been in place for decades in some enterprises and may have accumulated many years of technical debt -- making ERP security difficult and costly to maintain.



SAP ERP Security Risks

There are multiple risks related to SAP ERP systems. Some of them are:

Misappropriation of material resources (Fraud)

Having access to the Material Management (MM) module enables an attacker to modify material resources data in any way that's beneficial, for example one can manipulate any data that has to do with the quantity of material resources in stock or being delivered; or pilfer from warehouses in collusion with organization's employees.

Embezzlement of funds (Fraud)

By means of VD01 transaction in Sales and Distribution (SD) module an attacker can create fake vendor to generate sales orders on behalf of this vendor via VA01 transaction. The outcome would most probably be money embezzlement.

Manipulation of credit limits (Sabotage)

Access to Sales and Distribution module would give an attacker the opportunity to change limits for credit operations by using FD32 or F.34 transactions. Thus, when there would be no limits for purchasing on credit it could cause an organization to fall into a money pit.

Product cost manipulation (Sabotage, Fraud)

Using access to Sales and Distribution module an attacker can also substitute the data used for product cost assignment. Products pricing in SAP is processed automatically by measuring multiple criteria: monetary value of the transaction, customer type, season, discount availability, markups, etc. These actions are managed by VK11, VK12 and VK14 transactions. Due to the fact that the price is calculated automatically, pricing determination processes may be incomprehensible to an executor. Thus, actions of product cost manipulation may even remain unnoticed.

Credit card data theft (espionage)

There are many tables in Sales and Distribution module that store credit card data: VCKUN, VCNUM, CCARDEC and more than 50 others. Besides material losses to your organization, stealing credit card data would jeopardize business credibility.

SAP vulnerabilities

In its report, Onapsis researchers found more than 95% of SAP systems are exposed to vulnerabilities that could lead to a detrimental compromise of enterprise data and processes.

These issues were identified through hundreds of security assessments of SAP systems.

Researchers stated there appears to be a disconnect between enterprise information security teams and SAP operations teams; the SAP vulnerabilities identified support this assertion given the vulnerabilities are basic information security issues that have likely been addressed in other parts of an enterprise's information security program.

According to the Onapsis report, the top three most common attack vectors on SAP systems that threaten ERP security are:

- A low-security customer Web portal;
- Malicious accounts being used in customer or supplier portals; and
- Vulnerabilities in the underlying database protocols.

All three of these issues contribute to the technical debt in securing an SAP system.

In the first vector, for example, a lower-security customer Web portal that is exposed to the Internet could be set up to allow customers to connect from anywhere to place orders. However, this customer Web portal can be used as part of an attack, with the attacker pivoting from the lower-security system to other more critical systems, and eventually the entire SAP system.

In the second attack vector, customer and supplier portals could potentially be infiltrated; backdoor users could pivot the SAP portals and other platforms to continue on and attack the internal network.

In the third attack vector, an attacker can exploit insecure database protocol configurations that would allow them to execute commands on the operating system. At this point, the attacker has complete access to the operating system and can potentially modify or disrupt any information stored in the database.

Note that these are all common attack methods and should not be surprising to any information security professional.

SAP Security audit checklist

Checks conducted during security assessment:

- Security assessment of network, OS, DBMS related to SAP
- SAP vulnerability assessment
- Whitebox security configuration checks
- Critical access control checks
- SAP custom code security review
- SAP segregation of duties analysis

Best practices for SAP and ERP security

While enterprises need to include all systems in an information security program, the specific resources devoted to securing a particular asset should correspond to the system's value to the organization. These value assets should be established through a business impact analysis.

In addition, though enterprises might be hesitant to make any changes to production systems, all systems must have basic information security hygiene in place to prevent security incidents. These basic steps are necessary to prevent, mitigate, defend and monitor for security incidents. SAP has a security guide and SearchSAP has many resources on the basic security controls necessary for a SAP system -- including vulnerability management, patch management and role-based access control. Vulnerability management can be implemented in an SAP system by periodically scanning application, Web, database and other associated servers, and then feeding that data into a patch management program for testing and deployment. And while role-based access control is critical for application security, it should also extend to other aspects of the system so proper separation of duties is upheld to limit the risk of rogue use.

Given the critical nature of SAP systems, one major concern for ongoing security controls has been the potential for downtime from security. If an SAP system can't be "down" for business reasons, plans should be in place on how to apply patches or make other security changes without disrupting operations. This might include ensuring a high-availability system is in place, such as a backup system that automatically takes over when the primary system is being patched or is having changes made.

Another consideration to keep in mind is that other security technologies -- such as an intrusion detection system, monitoring tools, among others -- which should be in place, can be specifically tuned to monitor an SAP system.

Additionally, monitoring SAP application logs is necessary to identify compromised accounts or other malicious activity at the application level. Using the concept of least privilege -- including restricted network access throughout -- will make it more difficult for an attacker to find an exploitable vulnerability to gain complete access or to easily identify other systems to attack.

Again, enterprises need to ensure all systems are part of their information security program -- including SAP systems. Excluding SAP systems in the past is what has allowed for these basic security vulnerabilities to still be present in SAP systems today.

Some of these vulnerabilities have been well known in the information security community for decades, so applying the processes and fixes found outside SAP systems can significantly improve SAP security and prevent more severe incidents from affecting critical business operations.

Software Development Security

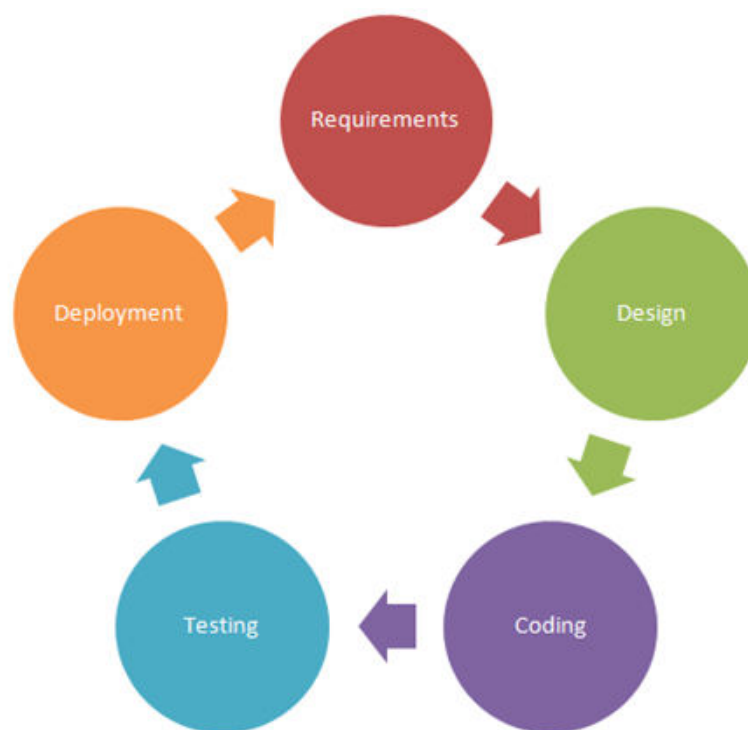
The software development life cycle

The software development life cycle, or SDLC, encompasses all of the steps that an organization follows when it develops software tools or applications. Organizations that incorporate security in the SDLC benefit from products and applications that are secure by design.

In an organization that's been around for several years or more, the SDLC is well-documented and usually includes the steps that are followed and in what order, the business functions and/or individuals responsible for carrying out the steps and information about where records are kept.

A typical SDLC model contains the following main functions:

- Conceptual definition. This is a basic description of the new product or program being developed, so that anyone reading it can understand the proposed project.
- Functional requirements and specifications. This is a list of requirements and specifications from a business function perspective.
- Technical requirements and specifications. This is a detailed description of technical requirements and specifications in technical terms.
- Design. This is where the formal detailed design of the product or program is developed.
- Coding. The actual development of software.
- Test. This is the formal testing phase.
- Deployment. This is where the software or product is installed in production.



Getting the right security information to the right people

Many people in the entire development process need all kinds of information, including security information, in a form that is useful to them. Here is the type of information that is required during each phase of the SDLC.

- Conceptual -- Organization information security principles and strategies
- Functional requirements and specifications -- Information security requirements
- Technical requirements and specifications -- Information security requirements
- Design -- Enterprise security architecture and security product standards
- Coding -- Development standards, practices, libraries and coding examples
- Testing -- Test plans that show how to verify each security requirement
- Deployment -- Procedures for integrating existing authentication, access controls, encryption, backup, etc.

If you are wondering why maintenance is omitted from the life cycle example here, it is because maintenance is just an iteration of the life cycle: when a change is needed, the entire process starts all over again. All of the validations that are present the first time through the life cycle are needed every time thereafter.

Finally, one may say that these changes represent a lot of extra work in a development project. This is not the case – these additions do not present that much extra time. These are but small additions that reap large benefits later on.

Fix it now or pay the price later

Organizations that fail to involve information security in the life cycle will pay the price in the form of costly and disruptive events. Many bad things can happen to information systems that lack the required security interfaces and characteristics. Some examples include:

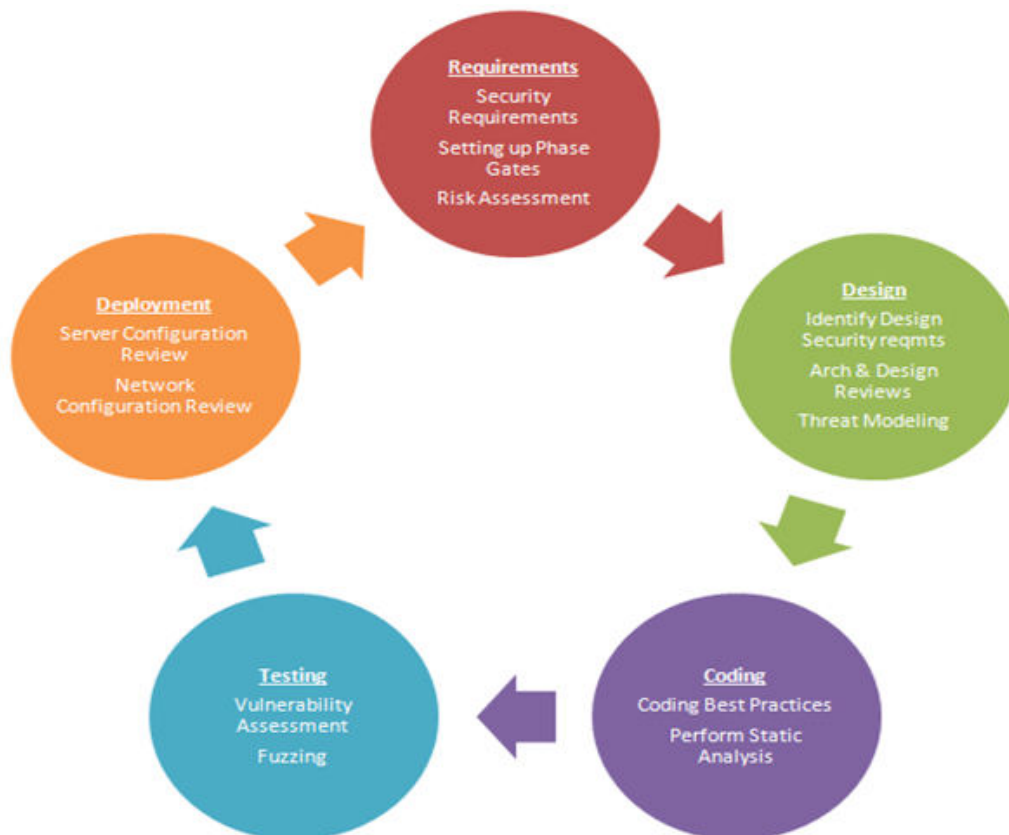
- Orphan user accounts (still-active accounts that belong to employees or contractors who have left the organization) that exist because the information system does not integrate with an organization's identity management or single sign-on solution.
- Defaced Web sites as a result of systems that were not built to security standards and, therefore, include easily exploited weaknesses.
- Fraudulent transactions that occur because an application lacked adequate audit trails and/or the processes required to ensure they are examined and issues dealt with.

Secure SDLC

A Secure SDLC process ensures that security assurance activities such as penetration testing, code review, and architecture analysis are an integral part of the development effort. The primary advantages of pursuing a Secure SDLC approach are:

- More secure software as security is a continuous concern
- Awareness of security considerations by stakeholders
- Early detection of flaws in the system
- Cost reduction as a result of early detection and resolution of issues
- Overall reduction of intrinsic business risks for the organization

A Secure SDLC is set up by adding security-related activities to an existing development process. For example, writing security requirements alongside the collection of functional requirements, or performing an architecture risk analysis during the design phase of the SDLC.



Many Secure SDLC models have been proposed, for example:

- **MS Security Development Lifecycle (MS SDL):** One of the first of its kind, the MS SDL was proposed by Microsoft in association with the phases of a classic SDLC.
- **NIST 800-64:** Provides security considerations within the SDLC. Standards were developed by the National Institute of Standards and Technology to be observed by US federal agencies.
- **OWASP CLASP (Comprehensive, Lightweight Application Security Process):** Simple to implement and based on the MS SDL. It also maps the security activities to roles in an organization.

Implementing Security at each level

The idea is to have security built in rather than bolted on, maintaining the security paradigm during every phase, to ensure a secure SDLC.

Phase 1: Requirements gathering and analysis

The software development process typically starts with requirements gathering and systems analysis, the results of which are then used to create the design. The business analysts and other personnel putting together requirements and functional specifications need to be clued in to security needs, or better still, someone who understands security from a product life cycle perspective should be on the team.

During requirements gathering for a secure SDLC, the first step is to identify applicable policies and standards and the mandates that the software will need to follow; compliance is an important factor to incorporate a standard framework, as well as to ensure audit requirements are met. Next, the compliance requirements can be mapped to the security controls.

This is followed up by developing a confidentiality, integrity and availability (CIA) matrix that helps define the foundation of security controls, and is instrumental in creating a secure software design. At this point security 'toll gates' are set, which are essentially criteria that need to be met for the project to move on to the coding phase.

Phase 2: Design

An architectural blueprint is now created, taking all the security requirements into consideration. This defines the entry and exit points in addition to defining how the business logic would interact with the different layers of the software.

In keeping with the secure SDLC paradigm, threat modeling is performed, which puts the software through various scenarios of misuse to assess the security robustness. In the process, various avenues to tackle potential problems emerge. One must keep in mind that the application communicates in a distributed environment rather than just a single system.

Phase 3: Coding

The best practices in the coding phase of a secure SDLC revolve around educating the developers. Instead of focusing only on language- or platform-specific problems, developers need an insight into how security vulnerabilities are created. These include not just technical vulnerabilities, but also problems from a business logic perspective.

It is necessary to establish secure coding practices among developers through guidelines and awareness campaigns. A source code review helps in making sure the coding quality is maintained, in addition to meeting secure coding standards. Organizations can also procure automatic code review tools to ensure security.

Phase 4: Quality assurance

The three pillars of quality are performance, functionality and security. Without embedded security, the quality of the software is questionable, thus making security a *de facto* quality vector. Tools to measure technical vulnerabilities are all very well, but the human factor cannot be underestimated, especially when it comes to business logic.

For a secure SDLC, outsourcing of software testing is a good idea, for cost savings definitely, but more so to leverage the specialized testing knowledge, skills and experience of the experts in the company being outsourced to.

When outsourcing, legalities like data sensitivity must be considered, and access to production databases should be avoided. Data should be masked or sanitized and the scope of the testing pre-defined.

Phase 5: Deployment

In the final deployment phase of a secure SDLC, the different components of the platform interact with each other. Platform security cannot be ignored, for while the application itself might be secure, the platform it operates on might have exploitable flaws. Platforms thus need to be made secure by turning off unwanted services, running the machines on the least privilege principle, and making sure there are security safeguards such as IDS, firewalls, and so on.

Development, as the very name suggests, is an on-going process. Updates, patches and enhancements to the application code are constantly required. It is a cycle that repeats itself, but security, even at the time of these modifications, must always be in focus to ensure a robust and secure SDLC.

Unified Threat Management

A new category of network security products -- called unified threat management (UTM) -- promises integration, convenience and protection from pretty much every threat out there; these are especially valuable for enterprise use. As Mike Rothman explains, the evolution of UTM technology and vendor offerings make these products even more valuable to enterprises.

Security expert Karen Scarfone defines UTM products as firewall appliances that not only guard against intrusion but also perform content filtering, spam filtering, application control, Web content filtering, intrusion detection and antivirus duties; in other words, a UTM device combines functions traditionally handled by multiple systems. These devices are designed to combat all levels of malicious activity on the computer network.

An effective UTM solution delivers a network security platform comprised of robust and fully integrated security and networking functions along with other features, such as security management and policy management by a group or user. It is designed to protect against next generation application layer threats and offers a centralized management through a single console, all without impairing the performance of the network.

Advantages of using UTM

Convenience and ease of installation are the two key advantages of unified threat management security appliances. There is also much less human intervention required to install and configure them appliances. Other advantages of UTM are listed below:

Reduced complexity

The integrated all-in-one approach simplifies not only product selection but also product integration, and ongoing support as well.

Ease of deployment

Since there is much less human intervention required, either vendors or the customers themselves can easily install and maintain these products.

Integration capabilities

UTM appliances can easily be deployed at remote locations without the on-site help of any security professional. In this scenario a plug-and-play appliance can be installed and managed remotely. This kind of management is synergistic with large, centralized software-based firewalls.

Black box character

Users have a tendency to play with things, and the black box nature of a UTM limits the damage users can do and, thus, reduces help desk calls and improves security.

Troubleshooting ease

When a box fails, it is easier to swap out than troubleshoot. This process gets the node back online quicker, and a non-technical person can do it, too. This feature is especially important for remote offices without dedicated technical staff on site.

Some of the leading UTM solution providers are Check Point, Cisco, Dell, Fortinet, HP, IBM and Juniper Networks.

Challenges of using UTM

UTM products are not the right solution for every environment. Many organizations already have a set of point solutions installed that, combined, provide network security capabilities similar to what UTM's offer, and there can be substantial costs involved in ripping and replacing the existing technology to install a UTM replacement. There are also advantages to using the individual products together, rather than a UTM. For instance, when individual point products are combined, the IT staff is able to select the best product available for each network security capability; a UTM can mean having to compromise and acquire a single product that has stronger capabilities in some areas and weaker ones in others.

Another important consideration when evaluating UTM solutions is the size of the organization in which it would be installed. Smallest organizations might not need all the network security features of a UTM. There is no need for a smaller firm to tax its budget with a UTM if many of its functions aren't needed. On the other hand, a UTM may not be right for larger, more cyber-dependent organizations either, since these often need a level of scalability and reliability in their network security that UTM products might not support (or at least not support as well as a set of point solutions). Also a UTM system creates a single point of failure for most or all network security capabilities; UTM failure could conceivably shut down an enterprise, with a catastrophic effect on company security. How much an enterprise is willing to rely on a UTM is a question that must be asked, and answered.

Web App & Website Security

As most businesses rely on web sites to deliver content to their customers, interact with customers, and sell products certain technologies are often deployed to handle the different tasks of a web site. A content management system like Joomla! or Drupal may be the solution used to build a robust web site filled with product, or service, related content. Businesses often turn to blogs using applications like WordPress or forums running on phpBB that rely on user generated content from the community to give customers a voice through comments and discussions. ZenCart and Magento are often the solutions to the e-commerce needs of both small and large businesses who sell directly on the web. Add in the thousands of proprietary applications that web sites rely and the reason securing web applications should be a top priority for any web site owner, no matter how big or small.

The Foundations of Security

Security relies on the following elements:

AUTHENTICATION

Authentication addresses the question: who are you? It is the process of uniquely identifying the clients of your applications and services. These might be end users, other services, processes, or computers. In security parlance, authenticated clients are referred to as *principals*.

AUTHORIZATION

Authorization addresses the question: what can you do? It is the process that governs the resources and operations that the authenticated client is permitted to access. Resources include files, databases, tables, rows, and so on, together with system-level resources such as registry keys and configuration data. Operations include performing transactions such as purchasing a product, transferring money from one account to another, or increasing a customer's credit rating.

AUDITING

Effective auditing and logging is the key to non-repudiation. Non-repudiation guarantees that a user cannot deny performing an operation or initiating a transaction. For example, in an e-commerce system, non-repudiation mechanisms are required to make sure that a consumer cannot deny ordering 100 copies of a particular book.

CONFIDENTIALITY

Confidentiality, also referred to as *privacy*, is the process of making sure that data remains private and confidential, and that it cannot be viewed by unauthorized users or eavesdroppers who monitor the flow of traffic across a network. Encryption is frequently used to enforce confidentiality. Access control lists (ACLs) are another means of enforcing confidentiality.

INTEGRITY

Integrity is the guarantee that data is protected from accidental or deliberate (malicious) modification. Like privacy, integrity is a key concern, particularly for data passed across networks. Integrity for data in transit is typically provided by using hashing techniques and message authentication codes.

AVAILABILITY

From a security perspective, availability means that systems remain available for legitimate users. The goal for many attackers with denial of service attacks is to crash an application or to make sure that it is sufficiently overwhelmed so that other users cannot access the application.

Risks Associated with Web Applications

Web applications allow visitors access to the most critical resources of a web site, the web server and the database server. Like any software, developers of web applications spend a great deal of time on features and functionality and dedicate very little time to security. Its not that developers don't care about security, nothing could be further from the truth. The reason so little time is spent on security is often due to a lack of understanding of security on the part of the developer or a lack of time dedicated to security on the part of the project manager.

For whatever reason, applications are often riddled with vulnerabilities that are used by attackers to gain access to either the web server or the database server. From there any number of things can happen. They can:

- Deface a web site
- Insert spam links directing visitors to another site
- Insert malicious code that installs itself onto a visitor's computer
- Insert malicious code that steals session IDs (cookies)
- Steal visitor information and browsing habits
- Steal account information
- Steal information stored in the database
- Access restricted content

Attacks on Web Application

- Code injection: hackers find ways to insert malicious executable code into legitimate traffic sent to an endpoint
- Broken authentication and session management: compromising user identities in a variety of ways
- Cross-site scripting: similar to code injection, but involving scripts instead, drawn from inappropriate sources
- Insecure direct object references: obtaining file access when it's not actually authorized
- Security misconfiguration: a failure of the admin, sometimes as simple as leaving passwords as defaults
- Sensitive data exposure: failure to shield data in proportion to its business value or customer sensitivity
- Missing function level access control: failure to verify functions are actually limited by access rights
- Cross-site request forgery: compromising an unexpected web application by leveraging validated authentication information
- Components with known vulnerabilities: a vulnerable element, such as a Java class, hasn't been patched
- Invalidated redirects and forwards: sending web users to unexpected sites that serve hacker interests

Web application security testing

There are also many commercial solutions designed to automate some of the testing. “Black box” solutions don’t try to assess application code per se, but instead just treat the application in a monolithic way. These are typically known as “web application security scanners,” “vulnerability scanners,” “penetration testing tools,” etc., and work by simulating a running, active, environment. Once installed, they then stress-test an application for flaws in ways that real-world users presumably would. These flaws, once exposed in the reports the solution generates, can then be addressed by the development team.

“White box” solutions, on the other hand, do look into the structure and code of the application itself — evaluating to some extent how well implemented the secure coding best practices were by the engineers who built the application. For instance, static analysis (as described above) can be performed to automatically trace process execution and predict what should happen in an up-and-running application (that isn’t actually up and running), thus spotting clear application security issues.

Another good testing idea is “fuzzing,” which basically just means hammering an application with many different kinds of data. That includes data of a completely inappropriate format for which the application was never designed, as well as random data that doesn’t make sense because it hasn’t got a format. This is a good way of revealing web application security flaws in an application via input that a normal human being (whether working in quality assessment or a typical user) might never even imagine, let alone carry out — but a hacker might.

In the case of applications that require a secure log-in process, let’s not forget web application security basics - it’s wise to try password crackers. These can train a spotlight on predictable issues, such as the strength of the password the application requires, whether it’s possible to break the authentication code in any of several commonplace ways, the minimum time interval between password entry attempts, or how many failed passwords can be entered before a user is locked out.

The Need to Avoid Attacks

With so many web sites running applications, attackers have taken to creating automated tools that can launch well-coordinated attacks against a number of vulnerable web sites at once. With this capability, the targets of these malicious hackers are no longer limited to large corporate web sites. Smaller web sites are just as easily caught up in the net cast by these automated attacks.

The repercussion of having your web site compromised can be devastating to any business, no matter what the industry or size of the company. The after-effects of these attacks include:

- Stolen data
- Compromised user accounts
- Loss of trust with customers and/or visitors
- Damaged brand reputation
- Lost sales revenue
- Your site labeled as a malicious site
- Loss of search engine rankings

Ways to Strengthen Web App Security

Building Secure Web Services and AJAX Topics

Web Services

This section deals with the common issues facing web developers as they work to build secure web apps, whether that includes Java, pHp, AJAX or other web languages and/or technologies.

Secure Web Application and Secure Coding Topics

Authentication

This section deals with authentication issues associated with secure web apps, such as basic/digest authentication, form-based authentication, integrated (SSO) authentication, etc.

Authorization

This section addresses authentication issues, ensuring a user has the appropriate privileges to view a resource. Topics such as principle of least privilege, client-side authorization tokens, etc. are addressed here.

Session Management

This section addresses topics such as authenticated users having a robust and cryptographically secure association with their session, applications enforcing authorization checks and applications avoiding or preventing common web attacks, such as replay, request forging and man-in-the-middle.

Data Validation

This section deals with applications being robust against all forms of input data, whether obtained from the user, infrastructure, external entities or databases.

Interpreter Injection

This section addresses application issues so they are secure from well-known parameter manipulation attacks against common interpreters.

Canonicalization, Locale and Unicode

This section addresses issues that help to ensure the application is robust when subjected to encoded, internationalized and Unicode input.

Error Handling, Auditing and Logging

This section deals with designing well-written applications that have dual-purpose logs and activity traces for audit and monitoring. This makes it easy to track a transaction without excessive effort or access to the system. They should possess the ability to easily track or identify potential fraud or anomalies end-to-end.

Distributed Computing

This section deals with synchronization and remote services to web applications, by hardening applications against:

- time of check, time of use race conditions
- distributed synchronization issues
- common multi-programming, multi-threaded and distributed security issues

Buffer Overflow

This section addresses issues such as:

- Applications do not expose themselves to faulty components
- Applications create as few buffer overflows as possible
- Developers are encouraged to use languages and frameworks that are relatively immune to buffer overflows.

Administrative Interfaces

This section addresses issues such that:

- Administrator level functions are appropriately segregated from user activity
- Users cannot access or utilize administrator functionality
- Provide necessary audit and traceability of administrative functionality

Cryptography

This section helps to ensure that cryptography is safely used to protect the confidentiality and integrity of sensitive user data.

Configuration

This section is focused on creating secure web applications which are as well-built and secure out-of-the-box as possible.

Software Quality Assurance (QA)

According to the OWASP guide, "The software quality assurance goal is to confirm the confidentiality and integrity of private user data is protected as the data is handled, stored, and transmitted. The QA testing should also confirm the application cannot be hacked, broken, commandeered, overloaded, or blocked by denial of service attacks, within acceptable risk levels. This implies that the acceptable risk levels and threat

modeling scenarios are established up front, so the developers and QA engineers know what to expect and what to work towards."

Deployment

This section deals with the issues surrounding secure deployment of web applications.

Maintenance

This section addresses issues such as:

- Products are properly maintained post deployment
- Minimize the attack surface area throughout the production lifecycle
- Security defects are fixed properly and in a timely fashion

WAF- Web Application Firewall

Over the past few years, a clear trend has emerged within the information security landscape; web applications are under attack. "Web applications continue to be a prime vector of attack for criminals, and the trend shows no sign of abating; attackers increasingly shun network attacks for cross-site scripting, SQL injection, and many other infiltration techniques aimed at the application layer." (Sarwate, 2008) Web application vulnerabilities can be attributed to many things including poor input validation, insecure session management, improperly configured system settings and flaws in operating systems and web server software. Certainly writing secure code is the most effective method for minimizing web application vulnerabilities. However, writing secure code is much easier said than done and involves several key issues. First of all, many organizations do not have the staff or budget required to do full code reviews in order to catch errors. Second, pressure to deliver web applications quickly can cause errors and encourage less secure development practices. Third, while products used to analyze web applications are getting better, there is still a large portion of the job that must be done manually and is susceptible to human error. Securing an organization's web infrastructure takes a defense in depth approach and must include input from various areas of IT including the web development, operations, infrastructure, and security teams.

One technology that can help in the security of a web application infrastructure is a web application firewall. A web application firewall (WAF) is an appliance or server application that watches http/https conversations between a client browser and web server at layer 7. The WAF then has the ability to enforce security policies based upon a variety of criteria including signatures of known attacks, protocol standards and anomalous application traffic.

WAF Placement

Appliance-based WAF deployments typically sit directly behind an enterprise firewall and in front of organizational web servers. Deployments are often done in-line with all traffic flowing through the web application firewall. However, some solutions can be "out of band" with the use of a network monitoring port. If network based deployments are not preferred, organizations have another option. Host or server based WAF applications are installed directly onto corporate web servers and provide similar feature sets by processing traffic before it reaches the web server or application.

Security Model

A WAF typically follows either a positive or negative security model when it comes to developing security policies for your applications. A positive security model only allows traffic to pass which is known to be good, all other traffic is blocked. A negative security model allows all traffic and attempts to block that which is malicious. Some WAF implementations attempt to use both models, but generally products use one or the other. "A WAF using a positive security model typically requires more configuration and tuning, while a WAF with a negative security model will rely more on behavioral learning capabilities." (Young, 2008)

Operating Modes

Web Application Firewalls can operate in several distinct modes. Vendor names and support for different modes vary, so check each product for specific details if a particular mode is desired. Each mode offers various pros and cons which require organizations to evaluate the correct fit for their organization.

Reverse Proxy

The full reverse proxy mode is the most common and feature rich deployment in the web application firewall space. While in reverse proxy mode a device sits in line and all network traffic passes through the WAF. The WAF has published IP addresses and all incoming connections terminate at these addresses. The WAF then makes requests to back end web servers on behalf of the originating browser. This mode is often required for many of the additional features that a WAF may provide due to the requirement for connection termination. The downside of a reverse proxy mode is that it can increase latency which could create problems for less forgiving applications.

Transparent Proxy

When used as a transparent proxy, the WAF sits in line between the firewall and web server and acts similar to a reverse proxy but does not have an IP address. This mode does not require any changes to the existing infrastructure, but cannot provide some of the additional services a reverse proxy can.

Layer 2 Bridge

The WAF sits in line between the firewall and web servers and acts just like a layer 2 switch. This mode provides high performance and no significant network changes, however does not provide the advanced services other WAF modes may provide.

Network Monitor/Out of Band

In this mode, the WAF is not in line and watches network traffic by sniffing from a monitoring port. This mode is ideal for testing a WAF in your environment without impacting traffic. If desired, the WAF can still block traffic in this mode by sending TCP resets to interrupt unwanted traffic.

Host/Server Based

Host or server based WAFs are software applications which are installed on web servers themselves. Host based WAFs do not provide the additional features which their network based counterparts may provide. They do, however, have the advantage of removing a possible point of failure which network based WAFs introduce. Host based WAFs do increase load on web servers so organizations should be careful when introducing these applications on heavily used servers.

WAF Features

WAF appliances are often either add-on components of existing application delivery controllers or include additional features to improve the reliability and performance of web applications. These additional features can help make the case for implementing a WAF for organizations not already taking advantage of such features. Not all WAF solutions have these features and many are dependent upon the deployment mode chosen. Typically a reverse-proxy deployment will support each of these features.

Caching

Reducing load on web servers and increasing performance by caching copies of regularly requested web content on the WAF thus reducing repeated requests to back end servers.

Compression

In order to provide for more efficient network transport, certain web content can be automatically compressed by the WAF and then decompressed by the browser.

SSL Acceleration

Use of hardware based SSL decryption in a WAF to speed SSL processing and reduce the burden on back-end web servers.

Load Balancing

Spreading incoming web requests across multiple back end web servers to improve performance and reliability.

Connection Pooling

Reduces back end server TCP overhead by allowing multiple requests to use the same back end connection.

Implementation, Tuning and Maintenance

Web application firewalls are certainly not a plug and play solution. They require rigorous testing prior to implementation and regular tuning thereafter.

During the implantation phase, most vendors will have either a learning or passive mode so that the WAF can be properly tuned before blocking any traffic. A solution based upon a positive security model will need to learn what “normal” traffic looks like for your applications. Negative security model solutions will typically be deployed in a non-blocking mode so that any false positives can be tuned prior to turning on blocking capabilities. Similarly to intrusion prevention systems, a WAF requires regular monitoring of log files to detect attacks and tune false positives.

Organizations also need to consider how to incorporate WAF testing and tuning into their standard development practices so that the impact of new applications can be evaluated prior to deployment.

PCI Compliance

One of the major reasons organizations have an interest in web application firewalls is PCI DSS version 1.1. Requirement 6.6 states that organizations need to protect web applications by either reviewing all custom code for vulnerabilities or installing a web application firewall. This choice sparked a bit of controversy in the industry over which was the best practice. There are a myriad of arguments on both sides, but most agree that the best approach is to implement both methods rather than choosing one over the other. This requirement, however, has certainly shown a bright spotlight on WAF technology and, if anything, given vendors fuel to sell their products.

Wireless/Wi-Fi Security

Wireless networks are forcing organizations to completely rethink how they secure their networks and devices to prevent attacks and misuse that expose critical assets and confidential data. By their very nature, wireless networks are difficult to roll out, secure and manage, even for the most savvy network administrators.

Wireless networks offer great potential for exploitation for two reasons; they use the airwaves for communication, and wireless-enabled laptops are ubiquitous. To make the most of their security planning, enterprises need to focus on threats that pose the greatest risk. Wireless networks are vulnerable in a myriad of ways, some of the most likely problems being rogue access points (APs) and employee use of mobile devices without appropriate security precautions, but malicious hacking attempts and denial-of-service (DoS) attacks are certainly possible as well.

Unlike traditional wired networks in which communications travel along a shielded copper wire pair or optical cable, wireless radio frequency (RF) signals literally traverse the open air. As a result, RF signals are completely exposed to anybody within range and subject to fluctuating environmental factors that can degrade performance and make management an administrative nightmare. Whether authorized or not, wireless access points and their users are subject to malicious activity and employee misuse.

Additional wireless access security challenges come through the use of wireless-enabled devices by employees, the growing amount of confidential data residing on those devices, and the ease with which end users can engage in risky wireless behavior. The value of connectivity typically outweighs concerns about security, as users need to get work done while at home or while traveling. Survey data from the leading research group, Gartner, shows that at least 25 percent of business travelers connect to hotspots, many of which are unsecure, while traveling. Furthermore, about two-thirds of those who use hotspots connect to online services via Wi-Fi at least once a day highlighting the need for extending wireless security outside of the enterprise.

To ensure effective, automated wireless threat protection, companies and government organizations should implement a complete wireless security solution covering assets across the enterprise that enables them to discover vulnerabilities, assess threats, prevent attacks, and ensure ongoing compliance - in the most secure, easy-to-use and cost-effective manner available.

IT departments must have a pre-emptive plan of action to prevent malicious attacks and employee misuse which compromise an organization's data privacy and enforce security policies for wireless use - both inside and outside their facilities. Whether or not a

company has authorized the use of wireless or has a 'no wireless' policy, their networks, data, devices and users are exposed and at risk.

Wi-Fi Standards

- 802.11a
 - Frequency: 5.0 GHz
 - Typical Maximum Speed: 54 Mbps
- 802.11b
 - Frequency: 2.4 GHz
 - Typical Maximum Speed: 11 Mbps
- 802.11g
 - Frequency: 2.4 GHz
 - Typical Maximum Speed: 54 Mbps
- 802.11n
 - Frequency: 2.4 GHz or 5.0 GHz
 - Typical Maximum Speed: 600 Mbps
- 802.11ac
 - Frequency: 5.0 GHz
 - Typical Maximum Speed: 6 Gbps

Common Wi-Fi Security Standards

Most Wi-Fi devices including computers, routers, and phones support several security standards. The available security types and even their names vary depending on a device's capabilities.

WEP: WEP stands for Wired Equivalent Privacy. It is the original wireless security standard for Wi-Fi and is still commonly used on home computer networks. Some devices support multiple versions of WEP security

- WEP-64-bit key (sometimes called WEP-40)
- WEP 128-bit key (sometimes called WEP-104)
- WEP 256-bit key

and allow an administrator to choose one, while other devices only support a single WEP option. WEP should not be used except as a last resort, as it provides very limited security protection.

WPA: WAP stands for Wi-Fi Protected Access. This standard was developed to replace WEP. Wi-Fi devices typically support multiple variations of WPA technology. Traditional WPA, also known as WPA-Personal and sometimes also called WPA-PSK (for pre-shared key), is designed for home networking while another version, WPA-Enterprise, is designed for corporate networks.

WAP2: WAP2 is an improved version of Wi-Fi Protected Access supported by all newer Wi-Fi equipment. Like WPA, WPA2 also exists in Personal/PSK and Enterprise forms.

802.1X: 802.1X provides network authentication to both Wi-Fi and other types of networks. It tends to be used by larger businesses as this technology requires additional expertise to set up and maintain.

802.1X works with both Wi-Fi and other types of networks. In a Wi-Fi configuration, administrators normally configure 802.1X authentication to work together with WPA/WPA2-Enterprise encryption. 802.1X is also known as **RADIUS**.

Wi-Fi Attacks

War Driving

This is the act of driving around neighborhoods and areas to enumerate what wireless networks exist, what type of encryption (if any) is used, password (if known), and any other pertinent information. This information may be chalked or painted to the street or sidewalk or posted to various websites. Some websites, like SkyHook ask their users for this. Be cautious when you see various cars sitting outside your house for long periods of time (unless you live near a Pokemon Gym or a Pokestop).

Cracking Attacks

Just like anything else using Passwords, there are desires and ways to crack those passwords to gain access. Without password attacks, there would be no [Have I Been Pwned](#) and other similar sites. Very much like other password attacks, there are the simplistic attacks (brute force) and the complex attacks. While brute force will eventually work, there are methods to minimize the impact if compromised. These mitigating factors are mentioned below in the Wi-Fi Security Tips. One tool, or rather a suite of tools, used to crack Wi-Fi (WEP, WPA1, and WPA2) passwords is Aircrack-ng. It is the replacement for Aircrack-ng. You will also need the aircrack-ng, airodump-ng, and aireplay-ng tools (hence the suite) as well as a wireless card set to "Monitor Mode" (like promiscuous mode) to steal the handshake file and replay handshake to get the file to crack. Once you have the file, you can use your favorite password list (mine is a custom list with rockyou.txt as a base) to attempt to crack the key.

Denial of Service

A Denial of Service (DoS) attack is more of a nuisance than a true technical attack. Think of it as an extreme brute force attack that overwhelms something, in this case, a Wi-Fi network or assets/nodes on it. My broad over generalization of it being a nuisance vice technical is an exaggeration; sometimes the vectors of attack for a DoS are very technical. Many technologies, namely web servers and websites, have DoS protective measures, as the internet can connect to them if they are public facing.

Karma Attacks

Karma was a tool that was used to sniff, probe, and attack wi-fi networks using Man-in-the-Middle (MITM) methods. It has since fell from support as Karma but now exists as several other products. For the scope of this blog post, I will be focusing on the current incarnation known as Karmetasploit a portmanteau of Karma and Metasploit. Once the run control file is obtained and everything properly configured, the attacker will use airon-ng and airbase-ng (relative of all the other airX-ng tools) to establish itself as a wireless access point (AP). This is what perpetrates the Wi-Fi version of the Evil Twin attack. In perpetrating the actual attack, the attacker will open metasploit and input the Karma run control file then wait for users to connect. Once they connect, the attacker has visibility into what the victim is doing and browsing as well as the capability to interrogate the victim machine and extract cookies, passwords, and hashes. This could be combined with password attacks like Mimikatz or replay attacks. The attacker can also establish a meterpreter session with the victim for further exploitation.

Ways to secure Wi-Fi Network

Change the Network Name

The service set identifier (SSID) is the name that's broadcast from your Wi-Fi to the outside world so people can find the network. While you probably want to make the SSID public, using the generic network name/SSID generally gives it away. For example, routers from Linksys usually say "Linksys" in the name; some list the make and model number ("NetgearR6700"). That makes it easier for others to ID your router type. Give your network a more personalized moniker.

It's annoying, but rotating the SSID(s) on the network means that even if someone had previous access—like a noisy neighbor—you can boot them off with regular changes. It's usually a moot point if you have encryption in place, but just because you're paranoid doesn't mean they're not out to use your bandwidth. (Just remember, if you change the SSID and don't broadcast the SSID, it's on you to remember the new name all the time and reconnect ALL your devices—computers, phones, tablets, game consoles, talking robots, cameras, smart home devices, etc.

Activate Encryption

This is the ultimate Wi-Fi no-brainer; no router in the last 10 years has come without encryption. It's the single most important thing you must do to lock down your wireless network. Navigate to your router's settings and look for security options. Each router brand will likely differ; if you're stumped, head to your router maker's support site.

Once there, turn on WPA2 Personal (it may show as WPA2-PSK); if that's not an option use WPA Personal (but if you can't get WPA2, be smart: go get a modern router). Set the encryption type to AES (avoid TKIP if that's an option). You'll need to enter a password, also known as a network key, for the encrypted Wi-Fi.

This is NOT the same password you used for the router—this is what you enter on every single device when you connect via Wi-Fi. So make it a long nonsense word or phrase no one can guess, yet something easy enough to type into every weird device you've got that uses wireless. Using a mix of upper- and lowercase letters, numbers, and special characters to make it truly strong, but you have to balance that with ease and memorability.

Double Up on Firewalls

The router has a firewall built in that should protect your internal network against outside attacks. Activate it if it's not automatic. It might say SPI (stateful packet inspection) or NAT (network address translation), but either way, turn it on as an extra layer of protection.

For full-bore protection—like making sure your own software doesn't send stuff out over the network or Internet without your permission—install a firewall software on your PC as well.

Turn Off Guest Networks

It's nice and convenient to provide guests with a network that doesn't have an encryption password, but what if you can't trust them? Or the neighbors? Or the people parked out front? If they're close enough to be on your Wi-Fi, they should be close enough to you that you'd give them the password. (Remember—you can always change your Wi-Fi encryption password later.)

Use a VPN

A virtual private network (VPN) connection makes a tunnel between your device and the Internet through a third-party server—it can help mask your identity or make it look like you're in another country, preventing snoops from seeing your Internet traffic. Some even block ads. A VPN is a smart bet for all Internet users, even if you're not on Wi-Fi.

Update Router Firmware

Just like with your operating system and browsers and other software, people find security holes in routers all the time to exploit. When the router manufacturers know about these exploits, they plug the holes by issuing new software for the router, called firmware. Go into your router settings every month or so and do a quick check to see if you need an update, then run their upgrade. New firmware may also come with new features for the router, so it's a win-win.

Turn Off WPS

Wi-Fi Protected Setup, or WPS, is the function by which devices can be easily paired with the router even when encryption is turned on, because you push a button on the router and the device in question. Voila, they're talking. It's not that hard to crack, however, and means anyone with quick physical access to your router can instantly pair their equipment with it. Unless your router is locked away tight, this is a potential opening to the network you may not have considered.

Don't Broadcast the Network Name

This makes it harder, but not impossible, for friends and family to get on the Wi-Fi; that means it makes it a lot harder for non-friends to get online. In the router settings for the SSID, check for a "visibility status" or "enable SSID broadcast" and turn it off. In the future, when someone wants to get on the Wi-Fi, you'll have to tell them the SSID to type in—so make that network name something simple enough to remember and type. (Anyone with a wireless sniffer, however, can pick the SSID out of the air in very little time. The SSID is not so much as invisible as it is camouflaged.)

Disable DHCP

The Dynamic Host Control Protocol (DHCP) server in your router is what IP addresses are assigned to each device on the network. For example, if the router has an IP of 192.168.0.1, your router may have a DHCP range of 192.168.0.100 to 192.168.0.125—that's 26 possible IP addresses it would allow on the network. You can limit the range so (in theory) the DHCP wouldn't allow more than a certain number of devices—but with everything from appliances to watches using Wi-Fi, that's hard to justify.

For security you could also just disable DHCP entirely. That means you have to go into each device—even the appliances and watches—and assign it an IP address that fits with your router. (And all this on top of just signing into the encrypted Wi-Fi as it is.) If that sounds daunting, it can be for the layman. Again, keep in mind, anyone one with the right Wi-Fi hacking tools and a good guess on your router's IP address range can probably get on the network even if you do disable the DHCP server.

Filter on MAC Addresses

Every single device that connects to a network has a media access control (MAC) address that serves as a unique ID. Some with multiple network options—say 2.4GHz Wi-Fi, and 5GHz Wi-Fi, and Ethernet—will have a MAC address for each type. You can go into your router settings and physically type in the MAC address of only the devices you want to allow on the network. You can also find the "Access Control" section of your router to see a list of devices already connected, then select only those you want to allow or block. If you see items without a name, check its listed MAC addresses against your known products—MAC addresses are typically printed right on the device. Anything that doesn't match up may be an interloper. Or it might just be something you forgot about—there is a lot of Wi-Fi out there.

Offer Separate Wi-Fi for Guests

Never allow an untrusted or unfamiliar person have access to your private Wi-Fi network. If you want to offer visitors or guests wireless Internet access, make sure that such access is segregated from your company's main network so they can't possibly get into your computers and files, and eavesdrop on your traffic.

Consider purchasing a separate Internet connection for guests and setting up an additional wireless router or APs. Some wireless routers, such as D-Link's Xtreme N Gigabit Router (DIR-655), offer guest access on another SSID, or network name, that's separate from your private network and requires only a single Internet connection. To see if your router offers this option, check the user manual or log in to the router's Web-based control panel by typing its IP address into a browser and look for a guest feature. Additionally, most business-class APs offer the same functionality by creating Virtual LANs (VLANs) and multiple SSIDs.

When configuring guest access, you could even enable separate encryption so you can still try to control who connects and uses your Internet access. With a wireless router, you should use the guest access settings.

Physically Secure Your Network Gear

Besides enabling encryption to secure your private wireless network, you need to think about the physical security of your network. Make sure that your wireless router or APs are all secured from visitors. An intruder could easily plug into the network if it's in reach or reset it to factory defaults to clear the security. To prevent this, you could, for instance, mount the hardware high on walls or above a false ceiling. Also, if your office has Ethernet network ports on the walls, make sure that they aren't within the reach of visitors, or disconnect them from the network. If you have a larger network with a wiring closet, make sure it stays locked and secure.

Ensure Websites Are Encrypted Outside the Office

If you don't use a VPN connection to secure all your traffic when out of the office, at least ensure that any websites you log in to are encrypted. Highly sensitive websites, such as banks, use encryption by default, but others, such as social networking sites and email providers, don't always do so.

To ensure that a website is using encryption, access it via a Web browser and try to use SSL/HTTPS encryption. You can see if the site supports SSL encryption by adding the letter **s** to its address: **https://** instead of **http://**. If it's encrypted, you'll also see some sort of notification in the browser about the security, such as a padlock or green-colored address bar. If you don't see any notification or it shows an error, it may not be secure; you should therefore consider waiting to access the site until you're on a private network at home or in the office.

If you check your email with a client program such as Microsoft Outlook, you should try enabling SSL encryption for your email server in your account settings (see Figure 6). However, many email providers don't support encrypted connections via client programs. If that's the case, check your email via the Web browser--using SSL/HTTPS--if possible.

Shop for Secure Wi-Fi Gear

When shopping for a Wi-Fi router or access points, keep security in mind. As mentioned, some consumer-level wireless routers, such as the D-Link Xtreme N Gigabit Router, offer a wireless guest feature, so you can keep visitors off your private network. And business-class routers and APs usually offer VLAN and multiple SSID support, which you can configure to do the same.

Additionally, some business-level routers offer integrated VPN servers. You can use VPN connections to secure your Wi-Fi hotspot sessions, remotely access your network, or link multiple offices together. Some, such as the ZyXEL 802.11a/b/g/n Business Access Point, even have an embedded RADIUS server, so you can use the Enterprise mode of WPA2 security.

When shopping the big-box stores, you'll find mostly consumer-level wireless routers. You can check the box for features, but I suggest investigating online before purchasing. Check the manufacturer's site and read through the model's product description pages to get a better idea of what features it supports.

When shopping online for consumer or business gear, some Web stores include a lengthy description, but again, check the manufacturer's site for a full feature list.

Conclusion

A few years ago cyber-attacks were on the margins of news stories. But after a series of high-profile attacks against major financial institutions, retailers and health care providers, people realize that cyber-attacks aren't going away.

The need to address increasingly sophisticated threats has rapidly gone from an IT issue to a top priority, and laid back attitude towards cyber security will make the respective organization pay not only in terms of cash and kind but also in terms of reputation.

There are thousands of cyber security products present in the market today, and each day hundreds of new products are released. So, it is the responsibility of an individual and the organizations to employ the solution that best suits its needs and stay safe in the world of never stopping cyber attacks.

Recommendations

Government of India is focused on Digital India, make in India, which are being used to empower the citizens of India. It is expected to result in one trillion economy in next seven years. Digital Payments is another focus area. It is felt that cyber security needs to be given priority to secure the digital payments and IT infrastructure of India.

Digital India is the growth engine that has the potential to transform India into knowledge led economy and society. The digital revolution now stands at the cusp of a transformation, with the government having laid out its vision of a digitally enabled India.

The transformation of the cash to cash less society is getting limited because of the love of cash and currency. We believe that massive efforts are needed to bring about that change. It is also a fact that the people of India despite the handicap of cyber education are quick to adopt technology when it affects their living. This was amply proven by the speed with which the society took to mobile phone and its applications.

CMAI, is Asia's largest ICT Association with 48,500 members and 54 MOU Partners worldwide. CMAI is actively engaged in promotion of Digital India and Digital Payments.

CMAI is dealing with more than one lack Educational institutions and academic professionals consisting of Universities and technical/engineering colleges/schools etc. CMAI has initiated free online training programs and large scale education for the use of e-transaction and transformation of India to a digital economy.

Cyber security is need of the hour to protect digital payments and ICT infrastructure of India. The report is an attempt to put together various aspects of cyber security solutions. The report interlaid suggests:

- Focus on cyber security aspects
- Initiate large scale on line programs for the education of e-transactions and digital economy.
- CMAI also recommends that specialized skill/vocational courses be immediately started for cyber security and digital payments.
- Provide volunteers to help in educating people at the grass root level especially rural population for the use of ICT and safe e payments over currency.
- Involve students from the University network and senior citizens for educating the rural and low income urban population for the use of IT, safe e payments and cyber security aspects.
- Support Govt. initiative to enhance cyber security and to provide a watch dog mechanism to control cyber security breach and cyber frauds.
- CMAI also recommends that all available options for increasing the connectivity should be explored including satellite, optical fibre and new technologies such as White Space etc.

References

- www.google.co.in
- <https://www.mygov.in/group/digital-india/>
- <https://www.mygov.in/group/digital-india/>
- <https://securityintelligence.com/two-important-lessons-from-the-ashley-madison-breach/>
- <http://www.cio.com/article/2987830/online-security/ashley-madison-breach-shows-hackers-may-be-getting-personal.html>
- <http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-ashley-madison-hack-a-timeline/>
- <http://surveillance.rsf.org/en/hacking-team/>
- https://en.wikipedia.org/wiki/Hacking_Team
- <https://nakedsecurity.sophos.com/2016/04/19/how-hacking-team-got-hacked/>
- <http://www.scmagazine.com/hacker-behind-hacking-team-breach-publishes-how-to-guide/article/490541/>
- <http://malwarejake.blogspot.in/2016/04/lessons-learned-from-hacking-team.html>
- <http://edition.cnn.com/2015/10/27/politics/john-brennan-email-hack-outrage/>
- <http://nypost.com/2015/10/27/cia-director-outraged-with-teenager-who-hacked-him/>
- <http://www.mirror.co.uk/news/uk-news/vodafone-hacked-cyber-thieves-steal-6742472>
- <http://www.ibtimes.co.uk/vodpahone-hack-almost-2000-customer-accounts-have-been-accessed-by-hackers-1526638>
- <https://next.ft.com/content/9bfb4e72-7965-11e5-a95a-27d368e1ddf7>
- <http://www.itpro.co.uk/security/24136/talktalk-hack-what-to-do-if-hackers-have-your-data-20>
- <https://pdfs.semanticscholar.org/3ba9/52ee1b042b224109d6a586a18830cef1068a.pdf>
- <http://www.bbc.com/news/business-34743185>
- <http://www.bankinfosecurity.in/blogs/5-lessons-from-talktalk-hack-p-1967>
- <http://www.cyberwar.news/2016-05-16-germany-says-russian-government-was-behind-aggressive-hack-of-its-government-systems.html>
- <http://www.wsj.com/articles/germany-points-finger-at-russia-over-parliament-hacking-attack-1463151250>
- <http://www.securityweek.com/evidence-russia-behind-cyber-attacks-germany-secret-service>
- <https://ist.mit.edu/security/malware>
- <https://antivirus.comodo.com/how-antivirus-software-works.php>
- <https://www.lookout.com/know-your-mobile/what-is-a-mobile-threat>
- <http://www.webroot.com/in/en/home/resources/tips/pc-security/security-what-is-anti-virus-software>
- <https://pralab.diee.unica.it/en/AdversarialMachineLearning>
- <https://www.datanami.com/2016/04/21/machine-learning-can-applied-cyber-security/>

- <http://www.csoonline.com/article/3046543/security/machine-learning-is-reshaping-security.html>
- <https://www.cnet.com/how-to/the-guide-to-password-security-and-why-you-should-care/>
- <http://searchsecurity.techtarget.com/Six-steps-for-security-patch-management-best-practices>
- <http://securityaffairs.co/wordpress/6370/security/5-reasons-why-you-need-good-patch-management.html>
- <http://www.itpro.co.uk/security/27713/the-importance-and-benefits-of-effective-patch-management>
- http://www.ibm.com/support/knowledgecenter/SSTFWG_4.3.1/com.ibm.tivoli.itcm.doc/CMPMmst20.htm
- <http://www.infoworld.com/article/2616316/security/the-5-cyber-attacks-you-re-most-likely-to-face.html?page=2>
- <http://www.redbooks.ibm.com/redbooks/pdfs/sg246776.pdf>
- <http://searchsecurity.techtarget.com/definition/biometrics>
- <http://www.itbusinessedge.com/slideshows/top-iam-features-to-help-protect-your-vital-enterprise-data-07.html>
- <http://searchmidmarketsecurity.techtarget.com/definition/intrusion-detection>
- <https://www.sans.org/security-resources/idfaq/what-is-intrusion-detection/1/1>
- <https://www.sagedatasecurity.com/blog/cyber-threat-detection-5-keys-to-log-analysis-success-infographic>
- <http://opensourceforu.com/2011/06/best-practices-network-security-monitoring/>
- <https://www.slideshare.net/dgpeters/ics-network-security-monitoring-nsm>
- <https://www.beyondtrust.com/products/powerbroker/>
- <https://docs.microsoft.com/en-us/microsoft-identity-manager/pam/privileged-identity-management-for-active-directory-domain-services>
- <http://blog.wallix.com/what-is-privileged-access-management-pam>
- <http://searchsecurity.techtarget.com/definition/PKI>
- <http://searchsecurity.techtarget.com/tip/ERP-security-How-to-defend-against-SAP-vulnerabilities>
- <http://searchsecurity.techtarget.com/tip/Security-in-the-software-development-life-cycle>
- <https://www.synopsys.com/blogs/software-security/secure-sdlc/>
- <http://resources.infosecinstitute.com/intro-secure-software-development-life-cycle/#gref>
- <http://in.pcmag.com/networking/81330/feature/12-ways-to-secure-your-wi-fi-network>
- <https://www.alienvault.com/blogs/security-essentials/security-issues-of-wifi-how-it-works>