1. What is Security?

1. Security is “the quality or state of being secure—to be free from danger.” It means to be protected from adversaries, from those who would do harm, intentionally or otherwise.
2. A successful organization should have the following multiple layers of security in place for the protection of its operations:

- **Physical security** to protect the physical items, objects, or areas of an organization from unauthorized access and misuse
- **Personal security** to protect the individual or group of individuals who are authorized to access the organization and its operations
- **Operations security** to protect the details of a particular operation or series of activities
- **Communications security** to protect an organization’s communications media, technology, and content
- **Network security** to protect networking components, connections, and contents
- **Information security** to protect information assets

3. information security, therefore, is the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information. However, to protect the information and its related systems from danger, tools, such as policy, awareness, training, education, and technology, are necessary.

2. The Security Systems Development Life Cycle

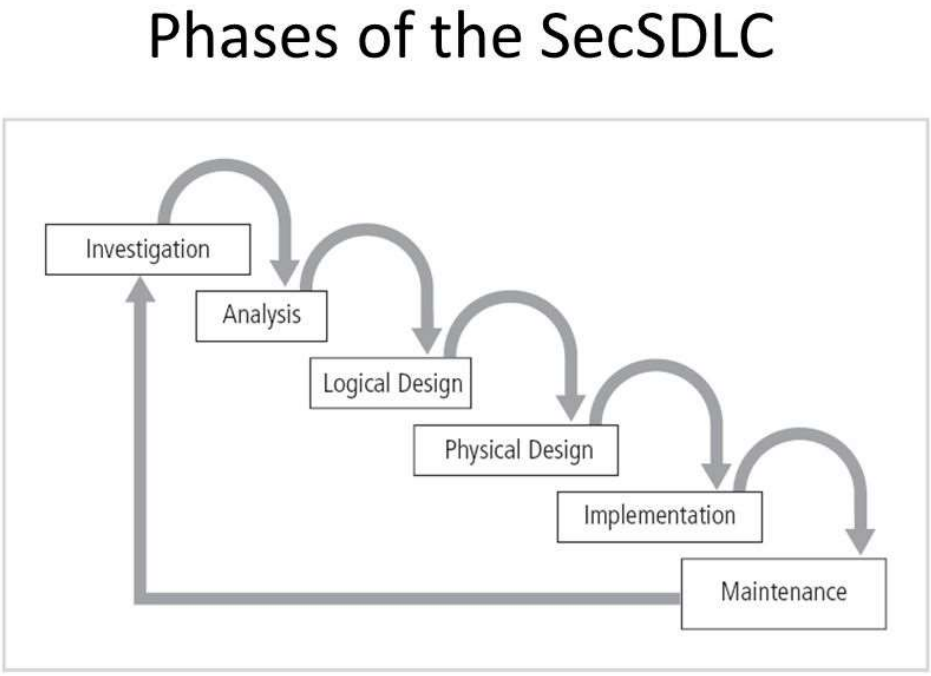


FIGURE 2-7 Phases of the SecSDLC

- **Security System Development Life Cycle (SecSDLC)** is defined as the set of procedures that are executed in a sequence in the software development cycle (SDLC). It is designed such that it can help developers to create software and applications in a way that reduces the security risks at later stages significantly from the start.
- The Security System Development Life Cycle (SecSDLC) is similar to Software Development Life Cycle (SDLC), but they differ in terms of the activities that are carried out in each phase of the cycle.
- SecSDLC eliminates security vulnerabilities. Its process involves identification of certain threats and the risks they impose on a system and the needed implementation of security controls to counter, remove and manage the risks involved. Whereas, in the SDLC process, the focus is mainly on the designs and implementations of an information system.

Phases involved in SecSDLC are:

- **System Investigation:** This process is started by the officials/directives working at the top-level management in the organization. The objectives and goals of the project are considered in order to execute this process. An Information Security Policy is defined which contains the descriptions of security applications and programs installed along with their implementations in organization's system.
- **System Analysis:** In this phase, detailed document analysis of the documents from the System Investigation phase are done. Already existing security policies, applications and software are analysed in order to check for different flaws and vulnerabilities in the system. Upcoming threat possibilities are also analyzed. Risk management comes under this process only.
- **Logical Design:** The Logical Design phase is concerned with the creation of tools and blueprints that are used in the implementation of different information security rules, as well as their applications and software. In order to avoid future losses, backup and recovery plans are also created. The procedures to take in the event of a calamity are also prepared. During this phase, the choice to outsource the firm project is made. It is determined if the project can be finished inside the organization or whether it must be outsourced to another company for completion.
- **Physical Design:** The technical teams get the tools and blueprints required for the software implementation and system security application. Various solutions are researched during this step for any unanticipated concerns that may arise in the future, and they are analyzed and written down to address the majority of the vulnerabilities that were overlooked during the analysis phase.
- **Implementation:** The solution decided in earlier phases is made final whether the project is in-house or outsourced. The proper documentation is provided of the product in order to meet the requirements specified for the project to be met. Implementation and integration process of the project are carried out with the help of various teams aggressively testing whether the product meets the system requirements specified in the system documentation.
- **Maintenance:** After the implementation of the security program, it must be ensured that it is functioning properly and is managed accordingly. The security program must be kept up to date accordingly in order to counter new threats that can be left unseen at the time of design.

3. Critical Characteristics of Information

The value of information comes from the characteristics it possesses.

Availability - enable users who need to access information to do so without interference or obstruction and in the required format. The information is said to be available to an authorized user when and where needed and in the correct format.
Accuracy - free from mistake or error and having the value that the end-user expects. If information contains a value different from the user's expectations due to the intentional or unintentional modification of its content, it is no longer accurate.
Authenticity - the quality or state of being genuine or original, rather than a reproduction or fabrication. Information is authentic when it is the information that was originally created, placed, stored, or transferred.
Confidentiality - the quality or state of preventing disclosure or exposure to unauthorized individuals or systems.
Integrity - the quality or state of being whole, complete, and uncorrupted. The integrity of information is threatened when the information is exposed to corruption, damage, destruction, or other disruption of its authentic state.
Utility - the quality or state of having value for some purpose or end. Information has value when it serves a particular purpose. This means that if information is available, but not in a format meaningful to the end-user, it is not useful.
Possession - the quality or state of having ownership or control of some object or item. Information is said to be in possession if one obtains it, independent of format or another characteristic. While a breach of confidentiality always results in a breach of possession, a breach of possession does not always result in a breach of confidentiality.

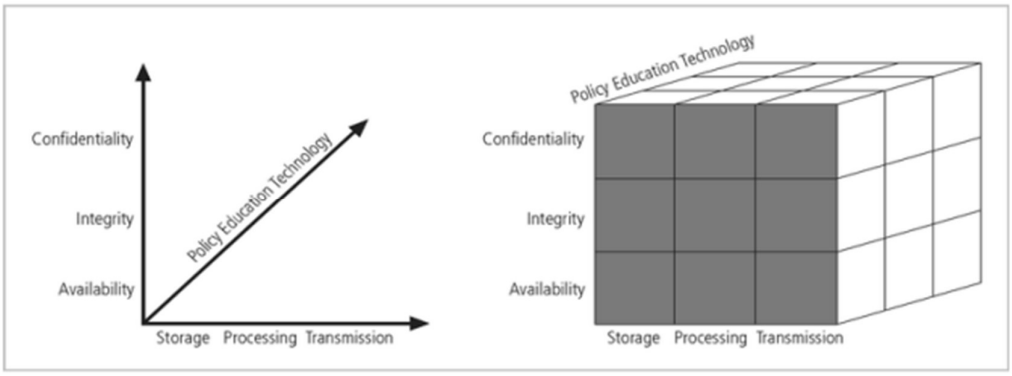


FIGURE 1-3 NSTISSC Security Model

4. Threat

Threat is an object, person, or other entity that represents a constant danger to an asset.

To better understand the numerous threats facing the organization, a categorization scheme has been developed, allowing us to group threats by their respective activities. By examining each threat category in turn, management can most effectively protect its information through policy, education and training, and

technology controls.

TABLE 2-1 Threats to Information Security[4]

Categories of threat	Examples
1. Acts of human error or failure	Accidents, employee mistakes
2. Compromises to intellectual property	Piracy, copyright infringement
3. Deliberate acts of espionage or trespass	Unauthorized access and/or data collection
4. Deliberate acts of information extortion	Blackmail of information disclosure
5. Deliberate acts of sabotage or vandalism	Destruction of systems or information
6. Deliberate acts of theft	Illegal confiscation of equipment or information
7. Deliberate software attacks	Viruses, worms, macros, denial-of-service
8. Forces of nature	Fire, flood, earthquake, lightning
9. Deviations in quality of service from service providers	Power and WAN service issues
10. Technical hardware failures or errors	Equipment failure
11. Technical software failures or errors	Bugs, code problems, unknown loopholes
12. Technological obsolescence	Antiquated or outdated technologies

Potential Acts of Human Error or Failure

This category includes the possibility of acts performed without intent or malicious purpose by an individual who is an employee of an organization.

Inexperience, improper training, the making of incorrect assumptions, and other circumstances can cause problems.

Employees constitute one of the greatest threats to information security, as the individuals closest to the organizational data.

Employee mistakes can easily lead to the following: revelation of classified data, entry of erroneous data, accidental deletion or modification of data, storage of data in unprotected areas, and failure to protect information.

Many threats can be prevented with controls, ranging from simple procedures, such as requiring the user to type a critical command twice, to more complex procedures, such as the verification of commands by a second party.

Deliberate Acts of Espionage or Trespass

This threat represents a well-known and broad category of electronic and human activities that breach the confidentiality of information.

When an unauthorized individual gains access to the information an organization is trying to protect, that act is categorized as a deliberate act of espionage or trespass.

The threat of Trespass can lead to unauthorized, real or virtual actions that enable information gatherers to enter premises or systems they have not been authorized to enter.

Controls are sometimes implemented to mark the boundaries of an organization's virtual territory.

These boundaries give notice to trespassers that they are encroaching on the organization's cyberspace.

Deliberate Acts of Information Extortion

The threat of information extortion is the possibility of an attacker or formerly trusted insider stealing information from a computer system and demanding compensation for its return or for an agreement to not disclose the information.

Extortion is common in credit card number theft.

Deliberate Acts of Sabotage or Vandalism

This category of threat addresses the individual or group of individuals who want to deliberately sabotage the operations of a computer system or business, or perform acts of vandalism to either destroy an asset or damage the image of the organization.

Deliberate Acts of Theft

Theft is the illegal taking of another's property. Within an organization, that property can be physical, electronic, or intellectual.

The value of information suffers when it is copied and taken away without the owner's knowledge.

Physical theft can be controlled quite easily. A wide variety of measures can be used from simple locked doors, to trained security personnel, and the installation of alarm systems.

Electronic theft, however, is a more complex problem to manage and control. Organizations may not even know it has occurred.

Deliberate Software Attacks

Deliberate software attacks occur when an individual or group designs software to attack an unsuspecting system. Most of this software is referred to as malicious code or malicious software, or sometimes malware.

Compromises to Intellectual Property

Many organizations create or support the development of intellectual property as part of their business operations.

Intellectual property is defined as "the ownership of ideas and control over the tangible or virtual representation of those ideas."

Intellectual property for an organization includes trade secrets, copyrights, trademarks, and patents.

Forces of Nature

Forces of nature, force majeure, or acts of God pose the most dangerous threats, because they are unexpected and can occur with very little warning.

These threats can disrupt not only the lives of individuals, but also the storage, transmission, and use of information.

These include fire, flood, earthquake, and lightning as well as volcanic eruption and insect infestation.

Since it is not possible to avoid many of these threats, management must implement controls to limit damage and also prepare contingency plans for continued operations.

Technical Hardware Failures or Errors

Technical hardware failures or errors occur when a manufacturer distributes to users equipment containing a known or unknown flaw.

These defects can cause the system to perform outside of expected parameters, resulting in unreliable service or lack of availability.

Some errors are terminal, in that they result in the unrecoverable loss of the equipment. Some errors are intermittent, in that they only periodically manifest themselves, resulting in faults that are not easily repeated.

Technical Software Failures or Errors

This category of threats comes from purchasing software with unknown, hidden faults.

Large quantities of computer code are written, debugged, published, and sold only to determine that not all bugs were resolved.

Sometimes, unique combinations of certain software and hardware reveal new bugs.

Sometimes, these items aren't errors, but are purposeful shortcuts left by programmers for honest or dishonest reasons.

Technological Obsolescence

When the infrastructure becomes antiquated or outdated, it leads to unreliable and untrustworthy systems.

Management must recognize that when technology becomes outdated, there is a risk of loss of data integrity to threats and attacks.

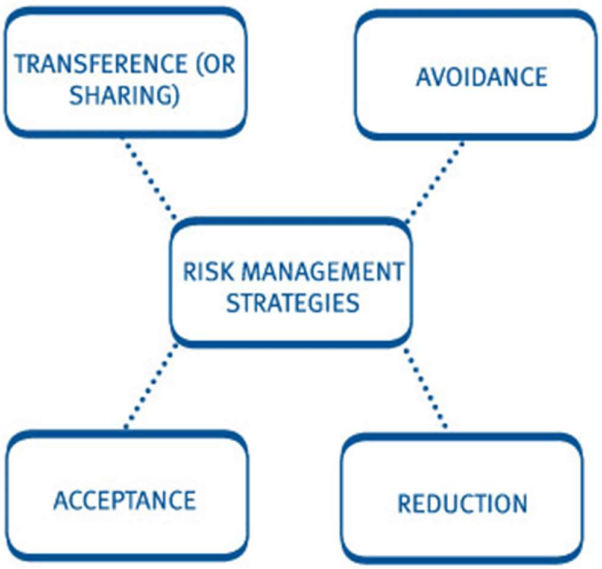
Ideally, proper planning by management should prevent the risks from technology obsolesce, but when obsolescence is identified, management must take immediate action.

5. **Risk management strategy definition**

A risk management strategy is a key part of the risk management lifecycle. After identifying risks and assessing the likelihood of them happening, as well as the impact they could have, you will need to decide how to treat them. The approach you decide to take is your **risk management strategy.** This is also sometimes referred to as risk treatment.

There are four main risk management strategies, or risk treatment options:

- Risk acceptance
- Risk transference
- Risk avoidance
- Risk reduction



Types of risk management strategy

Risk acceptance

Risk acceptance definition: *A risk is accepted with no action taken to mitigate it.*

This approach will not reduce the impact of a risk or even prevent it from happening, but that's not necessarily a bad thing. Sometimes the cost of mitigating risks can exceed the cost of the risk itself, in which case it makes more sense to simply accept the risk. After all, why spend £200,000 to prevent a £20,000 risk?

However, this approach does come with a gamble. You will need to be sure that, if the risk does occur in the future, then you will be able to deal with it when the time

comes. Because of this, it is best to accept risks only when the risk has a low chance of occurring or will have minimal impact if it does occur.

Risk transference

Risk transference definition: *A risk is transferred via a contract to an external party who will assume the risk on an organisation's behalf.*

Choosing to transfer a risk does not entirely eradicate it. The risk still exists, only the responsibility for it shifts from your organisation to another.

An example of this would be travel insurance. You don't accept the risk of a lost suitcase or an accident abroad and the costs that this would bring – you pay a travel insurance company to bear the financial consequences for you.

The same goes for the workplace. You may outsource work – and the risks that come with it - to a contractor. In finance, you may adopt a hedging strategy to protect your assets or investments.

Risk avoidance

Risk avoidance definition: *A risk is eliminated by not taking any action that would mean the risk could occur.*

If you choose this approach, you are aiming to completely eliminate the possibility of the risk occurring. One example of risk avoidance would be with investment. If, after analysing the risks associated with that investment, you deem it too risky, then you simply do not make the investment.

Treating risks by avoiding them should be reserved for risks that would have a major impact on your organisation if they were to occur. However, if you avoid every risk you come up against, you may miss out on positive opportunities. You never know, that investment you decided not to make could have paid off. That is why it's important to thoroughly analyse risks and make the most informed judgement you can.

Risk reduction

Risk reduction definition: *A risk becomes less severe through actions taken to prevent or minimise its impact.*

Risk reduction is a common strategy when it comes to risk treatment. It is sometimes known as lowering risk. By choosing this approach, you will need to work out the measures or actions you can take that will make risks more manageable.

One example of risk reduction would be within manufacturing and the risk of products being produced to incorrect specifications. Using a quality management system can lower the chance of this happening, so this would be a method of risk reduction. In the finance industry, you may face risks associated with new regulations. Implementing a digital solution to help you manage regulatory requirements can mitigate the risks of non-compliance and would therefore also be an example of risk reduction.

6. **Types of Password Attacks**
   Password Attacks:

   1. Phishing

   Phishing is when a hacker posing as a trustworthy party sends you a fraudulent email, hoping you will reveal your personal information voluntarily. Sometimes they lead you to fake "reset your password" screens; other times, the links install malicious code on your device. We highlight several examples on the OneLogin blog.

   Here are a few examples of phishing:

- **Regular phishing.** You get an email from what looks like goodwebsite.com asking you to reset your password, but you didn't read closely and it's actually goodwobsite.com. You "reset your password" and the hacker steals your credentials.
- **Spear phishing.** A hacker targets you specifically with an email that appears to be from a friend, colleague, or associate. It has a brief, generic blurb ("Check out the invoice I attached and let me know if it makes sense.") and hopes you click on the malicious attachment.
- **Smishing and vishing.** You receive a text message (SMS phishing, or smishing) or phone call (voice phishing, or vishing) from a hacker who informs you that your account has been frozen or that fraud has been detected. You enter your account information and the hacker steals it.
- **Whaling.** You or your organization receive an email purportedly from a senior figure in your company. You don't do your homework on the email's veracity and send sensitive information to a hacker.

To avoid phishing attacks, follow these steps:

- **Check who sent the email**: look at the From: line in every email to ensure that the person they claim to be matches the email address you're expecting.
- **Double check with the source**: when in doubt, contact the person who the email is from and ensure that they were the sender.
- **Check in with your IT team**: your organization's IT department can often tell you if the email you received is legitimate.

2. Man-in-the-Middle Attack

Man-in-the middle (MitM) attacks are when a hacker or compromised system sits in between two uncompromised people or systems and deciphers the information they're passing to each other, including passwords

To help prevent man-in-the-middle attacks:

- **Enable encryption on your router.** If your modem and router can be accessed by anyone off the street, they can use "sniffer" technology to see the information that is passed through it.
- **Use strong credentials and two-factor authentication.** Many router credentials are never changed from the default username and password. If a hacker gets access to your router administration, they can redirect all your traffic to their hacked servers.
- **Use a VPN.** A secure virtual private network (VPN) will help prevent man-in-the-middle attacks by ensuring that all the servers you send data to are trusted.

3. Brute Force Attack

If a password is equivalent to using a key to open a door, a brute force attack is using a battering ram. A hacker can try 2.18 trillion password/username combinations in 22 seconds, and if your password is simple, your account could be in the crosshairs.

To help prevent brute force attacks:

- Use a complex password. The difference between an all-lowercase, all-alphabetic, six-digit password and a mixed case, mixed-character, ten-digit password is enormous. As your password's complexity increases, the chance of a successful brute force attack decreases.
- Enable and configure remote access. Ask your IT department if your company uses remote access management. An access management tool like OneLogin will mitigate the risk of a brute-force attack.

- Require multi-factor authentication. If multi-factor authentication (MFA) is enabled on your account, a potential hacker can only send a request to your second factor for access to your account. Hackers likely won't have access to your mobile device or thumbprint, which means they'll be locked out of your account.

4. Dictionary Attack

A type of brute force attack, dictionary attacks rely on our habit of picking "basic" words as our password, the most common of which hackers have collated into "cracking dictionaries." More sophisticated dictionary attacks incorporate words that are personally important to you, like a birthplace, child's name, or pet's name.

To help prevent a dictionary attack:

- Never use a dictionary word as a password. If you've read it in a book, it should never be part of your password. If you must use a password instead of an access management tool, consider using a password management system.
- Lock accounts after too many password failures. It can be frustrating to be locked out of your account when you briefly forget a password, but the alternative is often account insecurity. Give yourself five or fewer tries before your application tells you to cool down.
- Consider investing in a password manager. Password managers automatically generate complex passwords that help prevent dictionary attacks.

5. Credential Stuffing

If you've suffered a hack in the past, you know that your old passwords were likely leaked onto a disreputable website. Credential stuffing takes advantage of accounts that never had their passwords changed after an account break-in. Hackers will try various combinations of former usernames and passwords, hoping the victim never changed them.

To help prevent credential stuffing:

- Monitor your accounts. There are paid services that will monitor your online identities, but you can also use free services like haveIbeenpwned.com to check whether your email address is connected to any recent leaks.
- Regularly change your passwords. The longer one password goes unchanged, the more likely it is that a hacker will find a way to crack it.
- Use a password manager. Like a dictionary attack, many credential stuffing attacks can be avoided by having a strong and secure password. A password manager helps maintain those.

6. Keyloggers

Keyloggers are a type of malicious software designed to track every keystroke and report it back to a hacker. Typically, a user will download the software believing it to be legitimate, only for it to install a keylogger without notice.

To protect yourself from keyloggers:

- Check your physical hardware. If someone has access to your workstation, they can install a hardware keylogger to collect information about your keystrokes. Regularly inspect your computer and the surrounding area to make sure you know each piece of hardware.

- Run a virus scan. Use a reputable antivirus software to scan your computer on a regular basis. Antivirus companies keep their records of the most common malware keyloggers and will flag them as dangerous.

7. **DoS vs DDoS**
   A **DoS attack** is a denial of service attack where a computer is used to flood a server with TCP and UDP packets. A **DDoS attack** is where multiple systems target a single system with a DoS attack. The targeted network is then bombarded with packets from multiple locations.

   During this type of attack, the service is put out of action as the packets sent over the network to **overload the server's capabilities and make the server unavailable** to other devices and users throughout the network. DoS attacks are used to shut down individual machines and networks so that they can't be used by other users.

   In addition, using a DDoS attack **makes it more complicated for the victim to recover**. Nine times out of ten the systems used to execute DDoS attacks have been compromised so that the attacker can launch attacks remotely through the use of slave computers. These slave computers are referred to as zombies or bots.

8. **Spoofing**
   Spoofing, as it pertains to cybersecurity, is when someone or something pretends to be something else in an attempt to gain our confidence, get access to our systems, steal data, steal money, or spread malware. Spoofing attacks come in many forms, including:
   - Email spoofing
   - Website and/or URL spoofing
   - Caller ID spoofing
   - Text message spoofing
   - GPS spoofing
   - Man-in-the-middle attacks
   - Extension spoofing
   - IP spoofing
   - Facial spoofing
9. **Virus vs Worms:**

10. **Risk, Risk Appetite, License Infringement and Residual Risk**
    Risk

- The term “information security risk” refers to the damage that attacks against IT systems can cause. IT risk encompasses a wide range of potential events, including data breaches, regulatory enforcement actions, financial costs, reputational damage, and more.
- Although “risk” is often conflated with “threat,” the two are subtly different. “Risk” is a more conceptual term: something that may or may not happen. A threat is a specific, actual danger.

Risk Appetite

- Risk appetite is the amount of risk an organization is willing to take in pursuit of objectives it deems have value.
- Risk appetite can also be described as an organization's *risk capacity*, or the maximum amount of residual risk it will accept after controls and other measures have been put in place.
- Risk tolerance, by contrast, is the amount of deviation from its risk appetite that an organization is willing to accept to achieve a specific objective based on parameters that include industry and vertical standards.

License Infringement
Licensing infringement is the act of using another person's protected intellectual property (IP) without permission.

Residual risk
Residual risk is the risk that remains after controls are accounted for. It’s the risk that remains after your organization has taken proper precautions.

11. Types of Data Ownership

There are several types of data ownership, including:

1. Personal ownership: This refers to the ownership of data that belongs to an individual. Personal ownership includes data such as medical records, financial records, and social media profiles.
2. Corporate ownership: This refers to the ownership of data that belongs to a business. Corporate ownership includes data such as customer information, sales data, and market research.
3. Public ownership: This refers to the ownership of data that is owned by the government or publicly-funded organizations. Public ownership includes data such as census data, weather data, and public records.
4. Joint ownership: This refers to the ownership of data that is owned by multiple individuals or organizations. Joint ownership can be established through contracts or agreements that outline the terms of use and ownership of the data.
5. Open ownership: This refers to the ownership of data that is freely available for anyone to use, share, and modify. Open ownership includes data such as open source software, creative commons licensed content, and open data initiatives.

12. Types of Attacks in Information Security

Types of Cyber Attacks

There are many varieties of cyber attacks that happen in the world today. If we know the various types of cyberattacks, it becomes easier for us to protect our networks and systems against them. Here, we will closely examine the top ten cyber-attacks that can affect an individual, or a large business, depending on the scale.

Let’s start with the different types of cyberattacks on our list:

1. Malware Attack

This is one of the most common types of cyberattacks. “Malware” refers to malicious software viruses including worms, spyware, ransomware, adware, and trojans.

The trojan virus disguises itself as legitimate software. Ransomware blocks access to the network's key components, whereas Spyware is software that steals all your confidential data without your knowledge. Adware is software that displays advertising content such as banners on a user's screen.

Malware breaches a network through a vulnerability. When the user clicks a dangerous link, it downloads an email attachment or when an infected pen drive is used.

Let’s now look at how we can prevent a malware attack:

- Use antivirus software. It can protect your computer against malware. Avast Antivirus, Norton Antivirus, and McAfee Antivirus are a few of the popular antivirus software.
- Use firewalls. Firewalls filter the traffic that may enter your device. Windows and Mac OS X have their default built-in firewalls, named Windows Firewall and Mac Firewall.
- Stay alert and avoid clicking on suspicious links.
- Update your OS and browsers, regularly.

2. Phishing Attack

Phishing attacks are one of the most prominent widespread types of cyberattacks. It is a type of social engineering attack wherein an attacker impersonates to be a trusted contact and sends the victim fake mails.

Unaware of this, the victim opens the mail and clicks on the malicious link or opens the mail's attachment. By doing so, attackers gain access to confidential information and account credentials. They can also install malware through a phishing attack.
Phishing attacks can be prevented by following the below-mentioned steps:

- Scrutinize the emails you receive. Most phishing emails have significant errors like spelling mistakes and format changes from that of legitimate sources.
- Make use of an anti-phishing toolbar.
- Update your passwords regularly.

3. Password Attack

It is a form of attack wherein a hacker cracks your password with various programs and password cracking tools like Aircrack, Cain, Abel, John the Ripper, Hashcat, etc. There are different types of password attacks like brute force attacks, dictionary attacks, and keylogger attacks.
Listed below are a few ways to prevent password attacks:

- Use strong alphanumeric passwords with special characters.
- Abstain from using the same password for multiple websites or accounts.
- Update your passwords; this will limit your exposure to a password attack.
- Do not have any password hints in the open.

4. Man-in-the-Middle Attack

A Man-in-the-Middle Attack (MITM) is also known as an eavesdropping attack. In this attack, an attacker comes in between a two-party communication, i.e., the attacker hijacks the session between a client and host. By doing so, hackers steal and manipulate data.
As seen below, the client-server communication has been cut off, and instead, the communication line goes through the hacker.
MITM attacks can be prevented by following the below-mentioned steps:

- Be mindful of the security of the website you are using. Use encryption on your devices.
- Refrain from using public Wi-Fi networks.

5. SQL Injection Attack

A Structured Query Language (SQL) injection attack occurs on a database-driven website when the hacker manipulates a standard SQL query. It is carried by injecting a malicious code into a vulnerable website search box, thereby making the server reveal crucial information.
This results in the attacker being able to view, edit, and delete tables in the databases. Attackers can also get administrative rights through this.
To prevent a SQL injection attack:

- Use an Intrusion detection system, as they design it to detect unauthorized access to a network.
- Carry out a validation of the user-supplied data. With a validation process, it keeps the user input in check.

6. Denial-of-Service Attack

A Denial-of-Service Attack is a significant threat to companies. Here, attackers target systems, servers, or networks and flood them with traffic to exhaust their resources and bandwidth.
When this happens, catering to the incoming requests becomes overwhelming for the servers, resulting in the website it hosts either shut down or slow down. This leaves the legitimate service requests unattended.

It is also known as a DDoS (Distributed Denial-of-Service) attack when attackers use multiple compromised systems to launch this attack.

Let’s now look at how to prevent a DDoS attack:

- Run a traffic analysis to identify malicious traffic.
- Understand the warning signs like network slowdown, intermittent website shutdowns, etc. At such times, the organization must take the necessary steps without delay.
- Formulate an incident response plan, have a checklist and make sure your team and data center can handle a DDoS attack.
- Outsource DDoS prevention to cloud-based service providers.

7. Insider Threat

As the name suggests, an insider threat does not involve a third party but an insider. In such a case; it could be an individual from within the organization who knows everything about the organization. Insider threats have the potential to cause tremendous damages.

Insider threats are rampant in small businesses, as the staff there hold access to multiple accounts with data. Reasons for this form of an attack are many, it can be greed, malice, or even carelessness. Insider threats are hard to predict and hence tricky.

To prevent the insider threat attack:

- Organizations should have a good culture of security awareness.
- Companies must limit the IT resources staff can have access to depending on their job roles.
- Organizations must train employees to spot insider threats. This will help employees understand when a hacker has manipulated or is attempting to misuse the organization's data.

8. Cryptojacking

The term Cryptojacking is closely related to cryptocurrency. Cryptojacking takes place when attackers access someone else’s computer for mining cryptocurrency. The access is gained by infecting a website or manipulating the victim to click on a malicious link. They also use online ads with JavaScript code for this. Victims are unaware of this as the Crypto mining code works in the background; a delay in the execution is the only sign they might witness.

Cryptojacking can be prevented by following the below-mentioned steps:

- Update your software and all the security apps as cryptojacking can infect the most unprotected systems.
- Have cryptojacking awareness training for the employees; this will help them detect crypotjacking threats.
- Install an ad blocker as ads are a primary source of cryptojacking scripts. Also have extensions like MinerBlock, which is used to identify and block crypto mining scripts.

9. Zero-Day Exploit

A Zero-Day Exploit happens after the announcement of a network vulnerability; there is no solution for the vulnerability in most cases. Hence the vendor notifies the vulnerability so that the users are aware; however, this news also reaches the attackers.

Depending on the vulnerability, the vendor or the developer could take any amount of time to fix the issue. Meanwhile, the attackers target the disclosed vulnerability. They make sure to exploit the vulnerability even before a patch or solution is implemented for it.

Zero-day exploits can be prevented by:

- Organizations should have well-communicated patch management processes. Use management solutions to automate the procedures. Thus it avoids delays in deployment.
- Have an incident response plan to help you deal with a cyberattack. Keep a strategy focussing on zero-day attacks. By doing so, the damage can be reduced or completely avoided.

10. Watering Hole Attack

The victim here is a particular group of an organization, region, etc. In such an attack, the attacker targets websites which are frequently used by the targeted group. Websites are identified either by closely monitoring the group or by guessing. After this, the attackers infect these websites with malware, which infects the victims' systems. The malware in such an attack targets the user's personal information. Here, it is also possible for the hacker to take remote access to the infected computer.

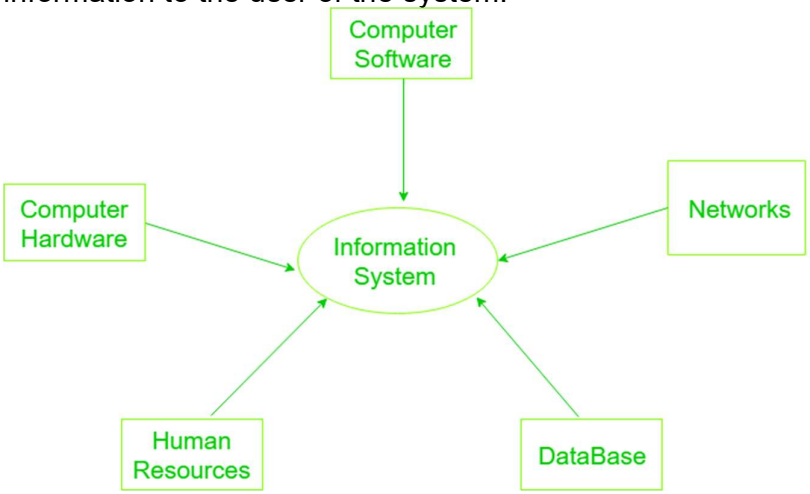
Let's now see how we can prevent the watering hole attack:

- Update your software and reduce the risk of an attacker exploiting vulnerabilities. Make sure to check for security patches regularly.
- Use your network security tools to spot watering hole attacks. Intrusion prevention systems(IPS) work well when it comes to detecting such suspicious activities.
- To prevent a watering hole attack, it is advised to conceal your online activities. For this, use a VPN and also make use of your browser's private browsing feature. A VPN delivers a secure connection to another network over the Internet. It acts as a shield for your browsing activity. NordVPN is a good example of a VPN.

Those were the top ten types of cyberattacks. Now, let us walk you through the next section of our article on types of cyberattacks.

13. **Components of Information Security**

An **Information system** is a combination of hardware and software and telecommunication networks that people build to collect, create and distribute useful data, typically in an organization. It defines the flow of information within the system. The objective of an information system is to provide appropriate information to the user, to gather the data, process the data and communicate information to the user of the system.



Components of the information system are as follows:

1. Computer Hardware:

Physical equipment used for input, output and processing. The hardware structure depends upon the type and size of the organization. It consists of an input and an output device, operating system, processor, and media devices. This also includes computer peripheral devices.

2. Computer Software:

The programs/ application program used to control and coordinate the hardware components. It is used for analysing and processing of the data. These programs include a set of instruction used for processing information.

Software is further classified into 3 types:

1. System Software
2. Application Software
3. Procedures

3. Databases:

Data are the raw facts and figures that are unorganized that are later processed to generate information. Softwares are used for organizing and serving data to the user, managing physical storage of media and virtual resources. As the hardware can't work without software the same as software needs data for processing. Data are managed using Database management system.

Database software is used for efficient access for required data, and to manage knowledge bases.

4. Network:

- Networks resources refer to the telecommunication networks like the intranet, extranet and the internet.
- These resources facilitate the flow of information in the organization.
- Networks consists of both the physical devices such as networks cards, routers, hubs and cables and software such as operating systems, web servers, data servers and application servers.
- Telecommunications networks consist of computers, communications processors, and other devices interconnected by communications media and controlled by software.
- Networks include communication media, and Network Support.

5. Human Resources:

It is associated with the manpower required to run and manage the system. People are the end user of the information system, end-user use information produced for their own purpose, the main purpose of the information system is to benefit the end user. The end user can be accountants, engineers, salespersons, customers, clerks, or managers etc. People are also responsible to develop and operate information systems. They include systems analysts, computer operators, programmers, and other clerical IS personnel, and managerial techniques.

14. **Risk Assessment**

Information security risk assessment is an essential part of enterprises management practices that provides to identify, quantify, and prioritize risks against element for risk acceptance and goals relevant to the organization.

Risk management defines a process that includes identification, management, and elimination or reduction of the likelihood of events that can negatively influence the resources of the information system to decrease security risks that potentially have the ability to affect the information system, subject to an acceptable value of

protection defines that include a risk analysis, analysis of the “cost-effectiveness” parameter, and selection, construction, and testing of the security subsystem, and the study of all elements of security.

A Security Risk Assessment (or SRA) is an assessment that contains recognizing the risks in the company, the technology and the processes to check that controls are in place to safeguard against security threats. Security risk assessments are generally required by compliance standards, including PCI-DSS standards for payment card security.

Security Risk Assessments are implemented by a security assessor who will compute all elements of the companies systems to recognize areas of risk. These can be as simple as a system that enables weak passwords, or can be more complex problems, including insecure business processes. The assessor will generally review everything from HR policies to firewall configurations while working to recognize potential risks.

15. **Vulnerability and it’s types**

A vulnerability is a weakness that can be exploited by cybercriminals to gain unauthorized access to a computer system. After exploiting a vulnerability, a cyberattack can run malicious code, install malware, and even steal sensitive data. Vulnerabilities can be exploited by a variety of methods, including SQL injection, buffer overflows, cross-site scripting (XSS), and open-source exploit kits that look for known vulnerabilities and security weaknesses in web applications.

Many vulnerabilities impact popular software, placing the many customers using the software at a heightened risk of a data breach, or supply chain attack. Such zero-day exploits are registered by MITRE as a Common Vulnerability Exposure (CVE).

1. Hardware Vulnerability:

A hardware vulnerability is a weakness which can used to attack the system hardware through physically or remotely.

For examples:

1. Old version of systems or devices
2. Unprotected storage
3. Unencrypted devices, etc.

2. Software Vulnerability:

A software error happen in development or configuration such as the execution of it can violate the security policy. For examples:

1. Lack of input validation
2. Unverified uploads
3. Cross-site scripting
4. Unencrypted data, etc.

3. Network Vulnerability:

A weakness happen in network which can be hardware or software.

For examples:

1. Unprotected communication
2. Malware or malicious software (e.g.:Viruses, Keyloggers, Worms, etc)
3. Social engineering attacks
4. Misconfigured firewalls

4. Procedural Vulnerability:

A weakness happen in an organization operational methods.

For examples:

1. Password procedure – Password should follow the standard password policy.

2. Training procedure – Employees must know which actions should be taken and what to do to handle the security. Employees must never be asked for user credentials online. Make the employees know social engineering and phishing threats.

16. Risk Identification and assessment deliverables

TABLE 7-7 Risk Identification and Assessment Deliverables

Deliverable	Purpose
Information asset classification worksheet	Assembles information about information assets and their impact on or value to the organization
Weighted criteria analysis worksheet	Assigns a ranked value or impact weight to each information asset
TVA worksheet	Combines the output from the information asset identification and prioritization with the threat identification and prioritization and identifies potential vulnerabilities in the "triples"; also incorporates extant and planned controls
Ranked vulnerability risk worksheet	Assigns a risk-rating ranked value to each uncontrolled asset–vulnerability pair

17. 10 Commandments of computer ethics

The Ten Commandments of Computer Ethics

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

18. VPN and It's Modes

Virtual Private Networks (VPNs)

A VPN is a private and secure network connection between systems that uses the data communication capability of an unsecured and public network. VPNs are commonly used to extend securely an organization's internal network connections to remote locations beyond the trusted network. The VPNC defines three VPN technologies:

- A trusted VPN, or VPN, uses leased circuits from a service provider and conducts packet switching over these leased circuits.
- Secure VPNs use security protocols and encrypt traffic transmitted across unsecured public networks like the Internet.
- A hybrid VPN combines the two, providing encrypted transmissions (as in secure VPN) over some or all of a trusted VPN network.

A VPN that proposes to offer a secure and reliable capability while relying on public networks must address:

- *Encapsulation* of incoming and outgoing data, wherein the native protocol of the client is embedded within the frames of a protocol that can be routed over the public network, as well as be usable by the server network environment.
- *Encryption* of incoming and outgoing data to keep the data contents private while in transit over the public network but usable by the client and server computers and/or the local networks on both ends of the VPN connection.
- *Authentication* of the remote computer and, perhaps, the remote user as well. Authentication and the subsequent authorization of the user to perform specific actions are predicated on accurate and reliable identification of the remote system and/or user.

A VPN is a private and secure network connection between systems that uses the data communication capability of an unsecured and public network. VPNs are commonly used to extend securely an organization's internal network connections to remote locations beyond the trusted network. The VPNC defines three VPN technologies:

- A trusted VPN, or VPN, uses leased circuits from a service provider and conducts packet switching over these leased circuits.
- Secure VPNs use security protocols and encrypt traffic transmitted across unsecured public networks like the Internet.
- A hybrid VPN combines the two, providing encrypted transmissions (as in secure VPN) over some or all of a trusted VPN network.

Transport Mode

- In transport mode, the data within an IP packet is encrypted, but the header information is not. This allows the user to establish a secure link directly with the remote host, encrypting only the data contents of the packet.
- There are two popular uses for transport mode VPNs.
- The end-to-end transport of encrypted data. In this model, two end users can communicate directly, encrypting and decrypting their communications as needed. Each machine acts as the end node VPN server and client.
- A remote access worker or teleworker connects to an office network over the Internet by connecting to a VPN server on the perimeter.

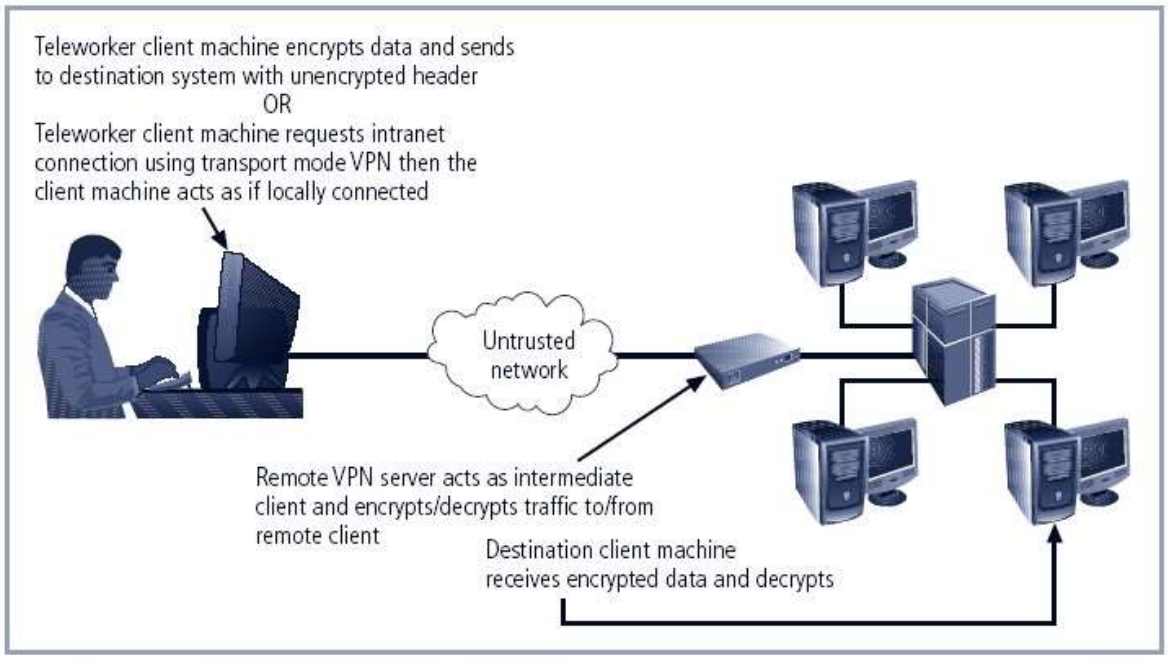


FIGURE 6-18 Transport Mode VPN

Tunnel Mode

In tunnel mode, the organization establishes two perimeter tunnel servers. These servers serve as the encryption points, encrypting all traffic that will traverse an unsecured network.

In tunnel mode, the entire client packet is encrypted and added as the data portion of a packet addressed from one tunneling server and to another. The receiving server decrypts the packet and sends it to the final address.

The primary benefit to this model is that an intercepted packet reveals nothing about the true destination system.

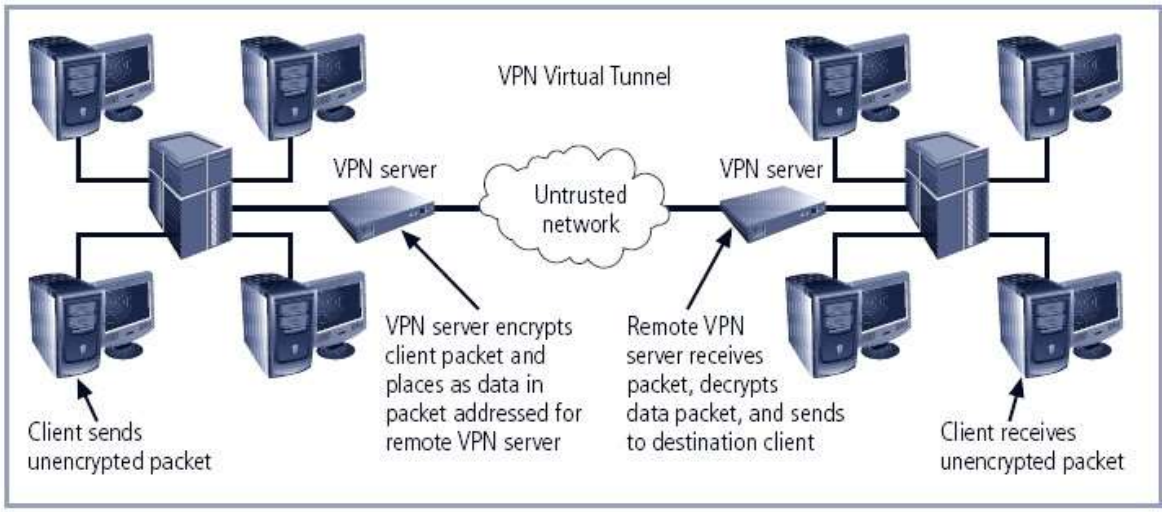


FIGURE 6-19 Tunnel Mode VPN

19. **Intrusion Detection system**

An **Intrusion Detection System (IDS)** is a system that monitors **network traffic** for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for the harmful activity or policy breaching. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms.

Although intrusion detection systems monitor networks for potentially malicious activity, they are also disposed to false alarms. Hence, organizations need to fine-tune their IDS products when they first install them. It means properly setting up the intrusion detection systems to recognize what normal traffic on the network looks like as compared to malicious activity.

Intrusion prevention systems also monitor network packets inbound the system to check the malicious activities involved in it and at once send the warning notifications.

Classification of Intrusion Detection System:

IDS are classified into 5 types:

1. **Network Intrusion Detection System (NIDS):**
   Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks. Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator. An example of a NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying to crack the firewall.
2. **Host Intrusion Detection System (HIDS):**
   Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of existing system files and compares it with the previous snapshot. If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission-critical machines, which are not expected to change their layout.
3. **Protocol-based Intrusion Detection System (PIDS):**
   Protocol-based intrusion detection system (PIDS) comprises a system or agent that would consistently resides at the front end of a server, controlling and interpreting the protocol between a user/device and the server. It is trying to secure the web server by regularly monitoring the HTTPS protocol stream and accept the related HTTP protocol. As HTTPS is un-encrypted and before instantly entering its web presentation layer then this system would need to reside in this interface, between to use the HTTPS.
4. **Application Protocol-based Intrusion Detection System (APIDS):**
   Application Protocol-based Intrusion Detection System (APIDS) is a system or agent that generally resides within a group of servers. It identifies the intrusions by monitoring and interpreting the communication

on application-specific protocols. For example, this would monitor the SQL protocol explicit to the middleware as it transacts with the database in the web server.

5. **Hybrid Intrusion Detection System :**
   Hybrid intrusion detection system is made by the combination of two or more approaches of the intrusion detection system. In the hybrid intrusion detection system, host agent or system data is combined with network information to develop a complete view of the network system. Hybrid intrusion detection system is more effective in comparison to the other intrusion detection system. Prelude is an example of Hybrid IDS.

20. **Firewall Architectures**

Firewall Architectures

Each of the firewall devices noted earlier can be configured in a number of network connection architectures.

The firewall configuration that works best for a particular organization depends on three factors: the objectives of the network, the organization's ability to develop and implement the architectures, and the budget available for the function.

Although literally hundreds of variations exist, there are four common architectural implementations of firewalls:

- Packet filtering routers
- Screened host firewalls
- Dual-homed firewalls
- Screened subnet firewalls

Packet filtering firewalls:

This is the most basic type of firewall. It examines each packet of data that enters or leaves a network, and only allows packets that meet certain criteria (such as having the correct IP address or port number) to pass through. This type of firewall is relatively simple to set up and maintain, but it does not provide much protection against more advanced threats such as malware or denial-of-service attacks. It examines the headers of packets passing through the router, and decides whether to forward or discard them based on the rules it has been configured with. Packet filtering routers can be used to block traffic based on source and destination IP addresses, port numbers, and other parameters. They are simple and efficient but lack deep inspection capabilities.

Screened host firewalls:

A screened host firewall is a host-based firewall that uses a screened gateway to protect a single host on the network. The screened gateway, which is typically a router or firewall, screens all incoming and outgoing traffic to and from the protected host. This type of firewall is typically used to protect servers, and it can be more secure than a packet filtering router, as it can inspect the contents of packets in addition to the headers.

A screened host firewall typically consists of two components: a router or firewall that acts as the screened gateway, and a host that runs the firewall software. The screened gateway is responsible for screening all incoming and outgoing traffic to

and from the host, while the host-based firewall software is responsible for enforcing the security rules on the host itself.

One of the advantages of a screened host firewall is that it can provide a high level of security for the protected host. The firewall software can be configured to block all incoming and outgoing traffic by default, and only allow specific types of traffic through. This makes it more difficult for attackers to penetrate the host, as they must first bypass the screened gateway and then the host-based firewall software.

Another advantage is that it can inspect the contents of packets in addition to the headers. This allows the firewall to detect and block malicious payloads, such as malware or exploit code, that might otherwise be able to bypass a packet filtering router.

However, one of the main disadvantages of a screened host firewall is that it only provides protection for a single host.

Dual-homed firewalls: A dual-homed firewall is a firewall that has two network interfaces, one connected to the internal network and one connected to the external network. This allows the firewall to act as a barrier between the internal and external networks, controlling and monitoring the flow of traffic between them. This type of firewall is more secure than a single-homed firewall, as it can be configured to block all incoming and outgoing traffic by default, and only allow specific types of traffic through.

One of the main advantages of a dual-homed firewall is that it can provide a high level of security for the internal network. By default, the firewall blocks all incoming and outgoing traffic, and only allows specific types of traffic through. This makes it more difficult for attackers to penetrate the internal network, as they must first bypass the firewall.

Another advantage of dual-homed firewall is that it can perform deep packet inspection, meaning it can look beyond the headers of the packets and inspect the contents of the packets. This allows the firewall to detect and block malicious payloads, such as malware or exploit code, that might otherwise be able to bypass a packet filtering router.
However, one of the main disadvantages of a dual-homed firewall is that it can be complex to set up and maintain. It requires a high level of expertise to properly configure the firewall and ensure that it is providing the desired level of security. Additionally, it may have a higher cost as it needs a separate hardware to be installed.

Screened subnet firewalls: A screened subnet firewall is similar to a screened host firewall, but it is used to protect a subnet of hosts rather than a single host. It uses a screened gateway, typically a router or firewall, to screen all incoming and outgoing traffic to and from the protected subnet. This type of firewall is typically used to protect a group of servers or workstations, and it can provide a higher level of security than a packet filtering router, as it can inspect the contents of packets in addition to the headers.

All the above firewalls can provide a layer of security to the network, but the level of security and the complexity of the configuration depend on the type of firewall used. It's essential to consider the specific needs and the complexity of the network before selecting the appropriate firewall architecture.

21. **Cryptography Tools**

Cryptography Tools

Public Key Infrastructure (PKI) is an integrated system of software, encryption methodologies, protocols, legal agreements, and third-party services that enables users to communicate securely.

PKI systems are based on public-key cryptosystems and include digital certificates and certificate authorities (CAs).

PKI Protects Information Assets in Several Ways:

Authentication. Digital certificates in a PKI system permit parties to validate the identity of other parties in an Internet transaction.

Integrity. A digital certificate demonstrates that the content signed by the certificate has not been altered while being moved from server to client.

Privacy. Digital certificates keep information from being intercepted during transmission over the Internet.

Authorization. Digital certificates issued in a PKI environment can replace user IDs and passwords, enhance security, and reduce some of the overhead required for authorization processes and controlling access privileges.

Nonrepudiation. Digital certificates can validate actions, making it less likely that customers or partners can later repudiate a digitally signed transaction.

Digital Signatures

An interesting thing happens when the asymmetric process is reversed, that is, the private key is used to encrypt a short message.

The public key can be used to decrypt it, and the fact that the message was sent by the organization that owns the private key cannot be refuted.

This is known as nonrepudiation, which is the foundation of digital signatures.

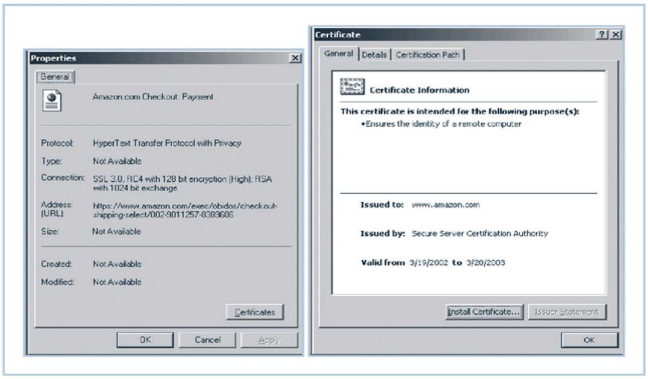
Digital signatures are encrypted messages that are independently verified by a central facility (registry) as authentic.

Digital Certificates and Certificate Authorities

As alluded to earlier, a digital certificate is an electronic document, similar to a digital signature, attached to a file certifying that this file is from the organization it claims to be from and has not been modified from the originating format.

A certificate authority is an agency that manages the issuance of certificates and serves as the electronic notary public to verify their worth and integrity.

Below diagram shows digital certificates



Hybrid Systems

In practice, asymmetric key encryption is not widely used except in the area of certificates. Instead, it is more often used in conjunction with symmetric key encryption creating a hybrid system.

The current process is based on the Diffie-Hellman Key Exchange method, which is a way to exchange private keys without exposure to any third parties using public key encryption.

With this method, asymmetric encryption is used as a method to exchange symmetric keys so that two organizations can conduct quick, efficient, secure communications based on symmetric encryption.

Diffie-Hellman provided the foundation for subsequent developments in public key encryption.

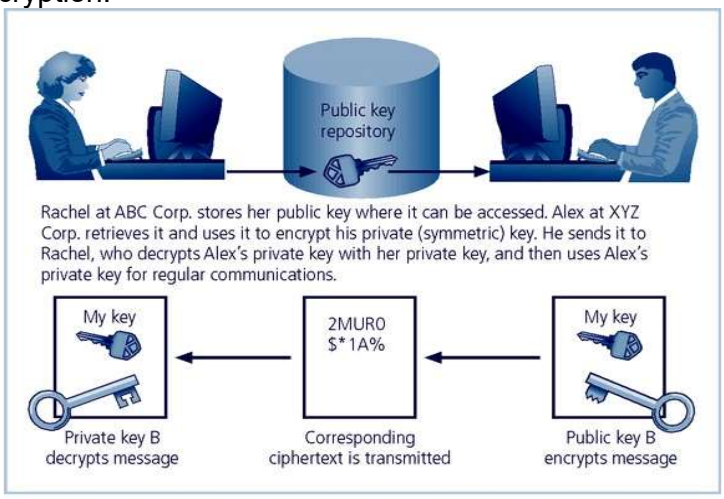


FIGURE 8-17 Hybrid Encryption Example

Steganography

Steganography is a process of hiding information and has been in use for a long time.

The word "steganography" is derived from the Greek words steganos meaning "covered" and graphein meaning "to write."

The most popular modern version of steganography involves hiding information within files that appear to contain digital pictures or other images.

Most computer graphics standards use a combination of three color values (red, blue, and green (RGB)) to represent a picture element, or pixel.

Each of the three color values usually requires an 8-bit code for that color's intensity (e.g., 00000000 for no red and 11111111 for maximum red).

This inability to perceive difference on the part of humans provides the steganographer with one bit per color (or three bits per pixel) to use for encoding data into an image file.

Some applications are capable of hiding messages in .bmp, .wav, .mp3, and .au files, as well as in unused storage space on CDs and DVDs.

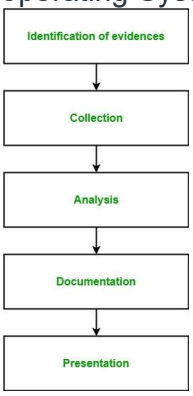
22. Symmetric and Asymmetric Key Encryption

Symmetric Key Encryption	Asymmetric Key Encryption
It only requires a single key for both encryption and decryption.	It requires two keys, a public key and a private key, one to encrypt and the other one to decrypt.
The size of cipher text is the same or smaller than the original plain text.	The size of cipher text is the same or larger than the original plain text.
The encryption process is very fast.	The encryption process is slow.
It is used when a large amount of data is required to transfer.	It is used to transfer small amounts of data.
It only provides confidentiality.	It provides confidentiality, authenticity, and non-repudiation.
The length of key used is 128 or 256 bits	The length of key used is 2048 or higher
In symmetric key encryption, resource utilization is low as compared to asymmetric key encryption.	In asymmetric key encryption, resource utilization is high.
It is efficient as it is used for handling large amount of data.	It is comparatively less efficient as it can handle a small amount of data.
Security is less as only one key is used for both encryption and decryption purpose.	It is more secure as two keys are used here- one for encryption and the other for decryption.
The Mathematical Representation is as follows- P = D (K, E(P)) where K –> encryption and decryption key P –> plain text D –> Decryption E(P) –> Encryption of plain text	The Mathematical Representation is as follows- P = D(Kd, E (Ke,P)) where Ke –> encryption key Kd –> decryption key D –> Decryption E(Ke, P) –> Encryption of plain text using encryption key Ke . P –> plain text

Symmetric Key Encryption	Asymmetric Key Encryption
Examples: 3DES, AES, DES and RC4	Examples: Diffie-Hellman, ECC, El Gamal, DSA and RSA

23. Digital Forensics in Information Security

Digital Forensics is a branch of forensic science which includes the identification, collection, analysis and reporting any valuable digital information in the digital devices related to the computer crimes, as a part of the investigation. In simple words, Digital Forensics is the process of identifying, preserving, analyzing and presenting digital evidences. The first computer crimes were recognized in the 1978 Florida computers act and after this, the field of digital forensics grew pretty fast in the late 1980-90's. It includes the area of analysis like storage media, hardware, operating System, network and applications. It consists of 5 steps at high level:



1. **Identification of evidence:** It includes of identifying evidences related to the digital crime in storage media, hardware, operating system, network and/or applications. It is the most important and basic step.
2. **Collection:** It includes preserving the digital evidences identified in the first step so that they doesn't degrade to vanish with time. Preserving the digital evidences is very important and crucial.
3. **Analysis:** It includes analyzing the collected digital evidences of the committed computer crime in order to trace the criminal and possible path used to breach into the system.
4. **Documentation:** It includes the proper documentation of the whole digital investigation, digital evidences, loop holes of the attacked system etc. so that the case can be studied and analysed in future also and can be presented in the court in a proper format.
5. **Presentation:** It includes the presentation of all the digital evidences and documentation in the court in order to prove the digital crime committed and identify the criminal.

Purpose:
Digital forensics is used in both criminal and private investigations.
Traditionally, it is associated with criminal law where evidence is collected to support or negate a hypothesis before the court. Collected evidence may be used as part of intelligence gathering or to locate, identify or halt other crimes. As a result, data gathered may be held to a less strict standard than traditional forensics.
In civil cases, digital forensic teams may help with electronic discovery (eDiscovery). A common example is following unauthorized network intrusion. A forensics examiner will attempt to understand the nature and extent of the attack, as well as try to identify the attacker.
As encryption becomes more widespread, the forensic investigation becomes harder, due to the limited laws compelling individuals to disclose encryption keys.

24. Security Maintenance Model

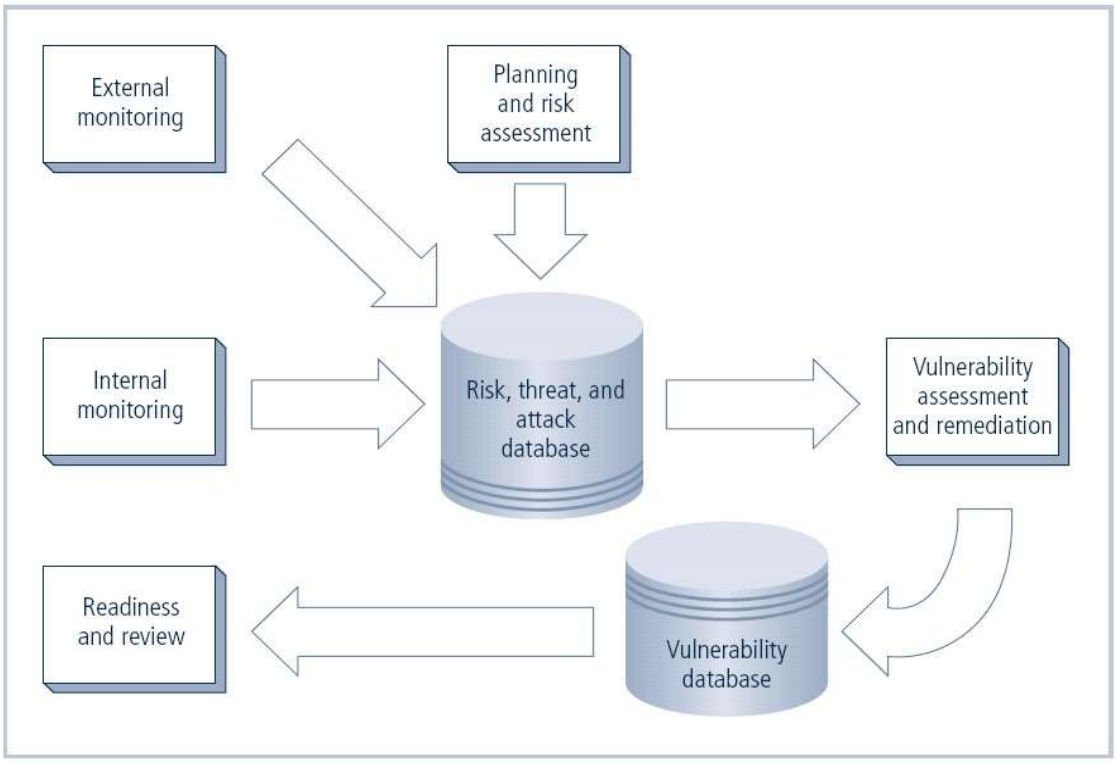


FIGURE 12-1 The Maintenance Model

The five domains of the security maintenance model are external monitoring, planning and risk assessment, internal monitoring, readiness and review, and vulnerability assessment and remediation.
External monitoring focuses on evaluating external threats to the organization. These include hackers, other companies, other governments, and so on. It provides early awareness of new and upcoming threats and threat agents, as well as new vulnerabilities. This ensures the company can come up with a plan of defense.

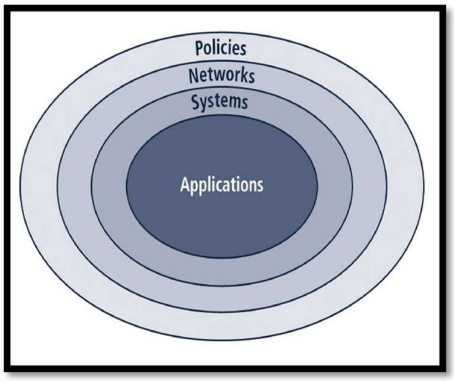
Planning and risk assessment focuses on identifying ongoing information security activities and managing the risks associated with them. For example, if a certain practice, such as password storage, is analyzed and revealed to leave the company vulnerable to attack, this step analyzes how to reform the practice to mitigate the risk.

Internal monitoring focuses on identifying the state of the organization's networks, information systems, and defenses. They look at their current system and where there may be vulnerabilities that need to be addressed, such as a backdoor. This way, the company can protect itself internally.

Readiness and review focuses on the continuance of the information security program and the continued improvement of it. This includes policy and program reviews to ensure everything is accurate and offers the needed protection. They also rehearse the measures they have taken to see if they are falling short and need to be improved.

Vulnerability assessment and remediation focuses on remediating the vulnerabilities identified in the rest of the maintenance process. It works to solve these vulnerabilities in a timely manner so that the company is not at risk for long. This involves penetration testing so that the company can see where the system is vulnerable and then work to rectify that.

25. Bull's eye Model



Bull's Eye Model Layers

- Policies – the outer layer in the bull's eye diagram
- Networks – the place where threats from public networks meet the organization's networking infrastructure; in the past, most information security efforts have focused on networks, and until recently information security was often thought to be synonymous with network security
- Systems – computers used as servers, desktop computers, and systems used for process control and manufacturing systems
- Application – all applications systems, ranging from packed applications such as office automation and e-mail programs, to high-end ERP packages and custom application software developed by the organization

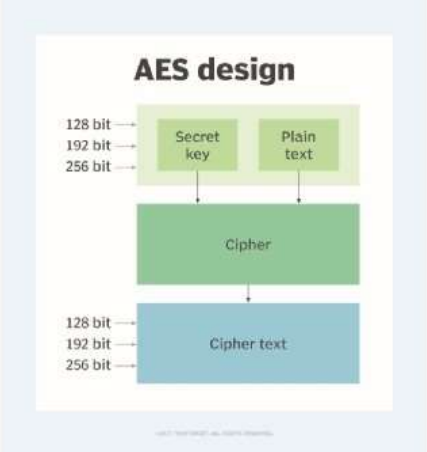
26. AES Algorithm

The Advanced Encryption Standard (AES) is a symmetric key encryption algorithm that is widely used to secure sensitive data. It was first adopted by the U.S. government in 2002 and has since become an international standard for encryption. It uses a fixed block size of 128 bits and key sizes of 128, 192 or 256 bits. The algorithm works by taking plaintext as input and applying a series of mathematical operations, including substitution and permutation, to produce the ciphertext. The key is used to control the specific operations applied to the plaintext, making it unique to that key.

In AES algorithm, the plaintext is transformed through several rounds of operations, each round includes Substitution-Permutation Network (SPN) structure and uses a unique round key derived from the original key. The process of encryption and decryption is done through a specific set of operations such as substitution, permutation and XOR (Exclusive OR) on the plaintext with round key.

To provide an example, let's take an AES-128 encryption of plaintext "Hello World". The plaintext is divided into 128-bit blocks, and a 128-bit key is used to encrypt the data. The algorithm applies 10 rounds of operations, including substitution and permutation, to each block using the key. The resulting ciphertext will be a string of random characters that are unreadable without the key. To decrypt the ciphertext, the same key is used to reverse the mathematical operations and reveal the original plaintext.

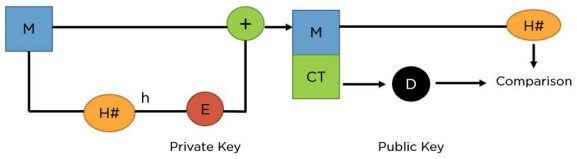
It is important to note that the AES algorithm is considered to be a highly secure encryption method and has been widely adopted in various industries, including finance, healthcare, and government.



27. RSA Algorithm

The RSA encryption algorithm is a widely-used public key encryption method that is based on the mathematical properties of large prime numbers. It is named after its inventors, Ron Rivest, Adi Shamir, and Leonard Adleman.

The RSA algorithm works by generating a pair of large prime numbers, referred to as the "public key" and "private key." The public key can be freely distributed and used to encrypt messages, while the private key is kept secret and used to decrypt messages



RSA can also encrypt and decrypt general information to securely exchange data along with handling digital signature verification.

Steps in RSA Algorithm

- Choose two large prime numbers (p and q)
- Calculate n = p*q and z = (p-1)(q-1)
- Choose a number e where 1 < e < z
- Calculate d = e-1mod(p-1)(q-1)
- You can bundle private key pair as (n,d)
- You can bundle public key pair as (n,e)

Encryption/Decryption Function
Once you generate the keys, you pass the parameters to the functions that calculate your ciphertext and plaintext using the respective key.

- If the plaintext is m, ciphertext = me mod n.
- If the ciphertext is c, plaintext = cd mod n

To understand the above steps better, you can take an example where p = 17 and q=13. Value of e can be 5 as it satisfies the condition 1 < e < (p-1)(q-1).
N = p * q = 221
D = e-1mod(p-1)(q-1) = 29
Public Key pair = (221,5)
Private Key pair = (221,29)
If the plaintext(m) value is 10, you can encrypt it using the formula me mod n = 82.
To decrypt this ciphertext(c) back to original data, you must use the formula cd mod n = 29.
You can now look at the factors that make the RSA algorithm stand out versus its competitors in the advantages section.

28.3 Basic Operations on Cryptography

1. Encryption: Encryption is the process of converting plaintext into an unreadable form called ciphertext. This is done using an algorithm and a secret key. The key is used to encrypt and decrypt the data, and it must be kept secret to maintain the security of the encrypted data. There are several types of encryption such as symmetric encryption, asymmetric encryption, and block cipher encryption. Symmetric encryption uses the same key for both encryption and decryption. Asymmetric encryption uses a public key for encryption and a private key for decryption. Block cipher encryption, it breaks the plaintext into fixed-size blocks and encrypts them one block at a time.
2. Decryption: Decryption is the reverse process of encryption. It is used to convert the ciphertext back into plaintext using the same key that was used to encrypt the data,

or if it's an asymmetric encryption, the corresponding private key. Decryption allows authorized users to read and understand the original message.

3. Hashing: Hashing is a one-way process of converting plaintext into a fixed-length output called a hash. Hashing is used to ensure the integrity of data by detecting any changes made to the original data. Hashing is a one-way function, which means that it is not possible to determine the original plaintext from the hash. Common hashing algorithms include SHA-256 and MD5. Hashing is often used in digital signature, and password storage.

29. What is the difference between configuration management and change management?4M

Configuration management and change management are related but distinct concepts in IT operations.

Configuration management is the process of identifying, organizing, and controlling the different versions, configurations and relationships of the components in a system. It includes the processes of identifying, controlling, maintaining, and auditing the different versions of software, hardware, and documentation that make up a system. This process ensures that the system is stable and reliable, and that it can be recovered or restored in the event of an incident or failure.

Change management, on the other hand, is the process of controlling and tracking changes to a system. It includes the processes of identifying, evaluating, approving, implementing, and monitoring changes to the system. This process ensures that changes to the system are introduced in a controlled and orderly manner, that they are tracked, and that they are reversible if necessary. Change management also ensures that changes to the system do not cause unintended consequences or disruptions to the system or to the business.

In summary, Configuration management is the process of managing the different versions, configurations, and relationships of the components in a system, while change management is the process of controlling and tracking changes to a system. Both are important for maintaining the stability, reliability and security of the system.

30. Explain Non-technical aspects of security?3M

Non-technical aspects of security refer to the human and organizational factors that can impact the overall security of an organization. These include:

1. Security awareness: Ensuring that all employees are aware of security threats, policies and procedures, and best practices for protecting sensitive data and systems.
2. Employee training: Providing ongoing training and education to employees to help them understand the importance of security and how to identify and prevent security breaches.
3. Policy and procedures: Implementing clear and comprehensive policies and procedures that outline the roles and responsibilities of employees and the organization in maintaining security.
4. Risk management: Identifying, assessing, and mitigating potential security risks, and regularly reviewing and updating risk management strategies.
5. Physical security: Ensuring that the organization's physical facilities, including buildings and computer equipment, are secure and protected against unauthorized access and damage.

6. Incident response planning: Having a plan in place to respond quickly and effectively to security incidents, including the identification and containment of breaches, the preservation of evidence, and the restoration of services.
7. Third-party security: Managing the security risks associated with third-party vendors and contractors, including reviewing and monitoring their security practices and ensuring compliance with organizational security policies.
8. Compliance: Understanding and adhering to relevant laws, regulations, and industry standards related to security, such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA).

All these non-technical aspects of security are important to protect the organization from various types of security breaches and to ensure the continuity of the business. These aspects should be continuously monitored and updated in order to keep up with the changing security landscape.

31. Major subject areas recommended for security maintenance

The major subject areas recommended for security maintenance include:

Access control: This includes managing and controlling access to systems, networks, and data. It includes the implementation of authentication mechanisms, as well as the management of user accounts and permissions.

Network security: This includes the protection of networks and network infrastructure from unauthorized access or attack. It includes the implementation of firewalls, intrusion detection and prevention systems, and network segmentation.

Malware protection: This includes the protection of systems and networks from malware, such as viruses, worms, and Trojan horses. It includes the implementation of anti-virus software, as well as the management of software updates and patches.

Data security: This includes the protection of data from unauthorized access, alteration, or destruction. It includes the implementation of encryption, as well as the management of data backups and disaster recovery plans.

Incident response and incident management: This includes the processes and procedures in place to detect, respond to, and recover from security incidents. It includes the development of incident response plans and the management of incident response teams.

Security awareness and training: This includes the training and education of employees on security

32. Technical Aspects of Information Security

- **Authenticity** – Authentication defines that users are who they request to be. Availability defines that resources are available by authorized parties; “denial of service” attacks, which are the subject matter of national news, are attacks against availability.

  The concerns of information security professionals are access control and Nonrepudiation. Authorization defines the power that it can have

over distinguishing authorized users from unauthorized users, and levels of access in-between. Authenticity defines the constant checks that it can have to run on the system to make sure sensitive places are protected and working perfectly.

- **Integrity** – Integrity defines that information is protected against unauthorized changes that are not perceptible to authorized users; some incidents of hacking compromise the integrity of databases and multiple resources.
- **Accuracy** – The accuracy and completeness of information systems and the data supported within the systems should be an administration concern. Information which has been inappropriately changed or destroyed (by external or employees) can impact the organization. Each organization should make controls to provide that data entered into and saved in its automated files and databases are complete and accurate, and provide the accuracy of disseminated data.
- **Confidentiality** – The principle of confidentiality defines that only the sender and the intended recipient(s) must be able to create the content of a message. Confidentiality have compromised if an unauthorized person is able to create a message.
- **Access Control** – The principle of access control decides who must be able to access what. For example, it must be able to define that user A can view the data in a database, but cannot refresh them. User A can be allowed to create updates as well. An access-control mechanism can be install to provide this.

  Access control is associated to two areas including role management and rule management. Role management apply on the user side, whereas rule management targets on the resources side.

33. Non-technical Aspects of Implementation

- Other parts of implementation process are not technical in nature, dealing with the human interface to technical systems
- This includes creating a culture of change management as well as considerations for organizations facing change

The Culture of Change Management

- Prospect of change can cause employees to build up resistance to change
- The stress of change can increase the probability of mistakes or create vulnerabilities
  - Resistance to change can be lowered by building resilience for change

Reducing Resistance to Change from the Start

- The more ingrained the previous methods and behaviors, the more difficult the change ▪ Best to improve interaction between affected members of organization and project planners in early project phases
- Three-step process for project managers: communicate, educate, and involve

Developing a Culture that Supports Change

- Ideal organization fosters resilience to change

- Resilience: organization has come to expect change as a necessary part of organizational culture, and embracing change is more productive than fighting it
- To develop such a culture, organization must successfully accomplish many projects that require change

34. **Security Education Training and Awareness**

Security Education, Training, and Awareness Program

- As soon as general security policy exists, policies to implement security education, training, and awareness (SETA) program should follow
- SETA is a control measure designed to reduce accidental security breaches
- Security education and training builds on the general knowledge the employees must possess to do their jobs, familiarizing them with the way to do their jobs securely
- The SETA program consists of three elements: security education; security training; and security awareness.

Security awareness training in most organizations focuses on familiarizing the employees with the organizational security policy. The security awareness focus for users may include:

- educating users on the creation of good passwords
- do's and don'ts for maintaining workstations
- informing users of email and Internet access policies
- employee responsibility for computer security
- reporting procedures
- emergency procedures
- The focus for security awareness for system administrators may include:
  - training on how to configure systems securely
  - education on user account management policies
  - secure remote access for support of systems

35. **Cost Benefit Analysis**

Cost-benefit analysis (CBA) is a method used to evaluate a project by comparing its losses and gains — essentially a quantified and qualified list of pros and cons. CBA is a useful way to assess business projects because it reduces the evaluation complexity to a single price figure. As you can imagine, this makes CBA an invaluable tool when it comes to explaining the intricacies and selling the value of a robust cyber security strategy to key stakeholders.

36. **Honeypot**

A honeypot is a security mechanism that creates a virtual trap to lure attackers. An intentionally compromised computer system allows attackers to exploit vulnerabilities so you can study them to improve your security policies. You can apply a honeypot to any computing resource from software and networks to file servers and routers.

Honeypots are a type of deception technology that allows you to understand attacker behavior patterns. Security teams can use honeypots to investigate cybersecurity breaches to collect intel on how cybercriminals operate. They also reduce the risk of false positives, when compared to traditional cybersecurity measures, because they are unlikely to attract legitimate activity.

Honeypots vary based on design and deployment models, but they are all decoys intended to look like legitimate, vulnerable systems to attract cybercriminals.

Production vs. Research Honeypots

There are two primary types of honeypot designs:

- **Production honeypots**—serve as decoy systems inside fully operating networks and servers, often as part of an intrusion detection system (IDS). They deflect criminal attention from the real system while analyzing malicious activity to help mitigate vulnerabilities.
- **Research honeypots**—used for educational purposes and security enhancement. They contain trackable data that you can trace when stolen to analyze the attack.

Types of Honeypot Deployments

There are three types of honeypot deployments that permit threat actors to perform different levels of malicious activity:

- **Pure honeypots**—complete production systems that monitor attacks through bug taps on the link that connects the honeypot to the network. They are unsophisticated.
- **Low-interaction honeypots**—imitate services and systems that frequently attract criminal attention. They offer a method for collecting data from blind attacks such as botnets and worms malware.
- **High-interaction honeypots**—complex setups that behave like real production infrastructure. They don't restrict the level of activity of a cybercriminal, providing extensive cybersecurity insights. However, they are higher-maintenance and require expertise and the use of additional technologies like virtual machines to ensure attackers cannot access the real system.

37. **Attack vs Vulnerability**

Parameters	Attack	Vulnerability
1. Definition	An attack is an act or event that harms a system	Vulnerability is some flaw or weakness in a computer system.
2. Motive	Attack is intentional way to destroy a system	Vulnerability is unintentional, which could exist in system design, business operations, installed software, and network configurations.
3. Type	Attack can be active or passive.	This can be hardware, software or network vulnerabilities.
4. Operation	Attack is done from out or inside the network.	Vulnerability is an internal problem.
5. Example	Example: Cross-site scripting, SQL injection, Viruses etc.	Example: Buffer ov

38. Scanning an Analysis Tools

Scanning and Analysis Tools

Scanning tools are typically used as part of an attack protocol to collect information that an attacker would need to launch a successful attack.

The attack protocol is a series of steps or processes used by an attacker, in a logical sequence, to launch an attack against a target system or network.

- **Fingerprinting**: systematic survey of all of target organization's Internet addresses collected during the footprinting phase
- Fingerprinting reveals useful information about internal structure and operational nature of target system or network for anticipated attack
- These tools are valuable to network defender since they can quickly pinpoint the parts of the systems or network that need a prompt repair to close the vulnerability

Port Scanners

Port scanning utilities (or port scanners) are tools used by both attackers and defenders to identify (or fingerprint) the computers that are active on a network, as well as the ports and services active on those computers, the functions and roles the machines are fulfilling, and other useful information.

These tools can scan for specific types of computers, protocols, or resources, or their scans can be generic.

The more specific the scanner is, the better it can give attackers and defenders information that is detailed and will be useful later. However, it is also recommended that you keep a generic, broad-based scanner in your toolbox as well.

Firewall Analysis Tools

There are several tools that automate the remote discovery of firewall rules and assist the administrator in analyzing the rules to determine exactly what they allow and what they reject.

Incidentally, administrators who feel wary of using the same tools that attackers use should remember:

1. Regardless of the nature of the tool that is used to validate or analyze a firewall's configuration, it is the intent of the user that will dictate how the information gathered will be used.
2. In order to defend a computer or network well, it is necessary to understand the ways it can be attacked.

Thus, a tool that can help close up an open or poorly configured firewall will help the network defender minimize the risk from attack.

Operating System Detection Tools

Detecting a target computer's OS is very valuable to an attacker, because once the OS is known, all of the vulnerabilities to which it is susceptible can easily be determined. There are many tools that use networking protocols to determine a remote computer's OS.

As most OSs have a unique way of responding to ICMP requests, these tools are very reliable in finding matches and thus detecting the OSs of remote computers. System and network administrators should take note of this and plan to restrict the use of ICMP through their organization's firewalls and, when possible, within its internal networks.

Vulnerability Scanners

An "active" vulnerability scanner is one that initiates traffic on the network in order to determine security holes.

As a class, this type of scanner identifies exposed usernames and groups, shows open network shares, and exposes configuration problems and other vulnerabilities in servers.
A passive vulnerability scanner is one that listens in on the network and determines vulnerable versions of both server and client software.
Passive scanners are advantageous in that they do not require vulnerability analysts to get approval prior for testing.
These tools simply monitor the network connections to and from a server to gain a list of vulnerable applications.
Furthermore, passive vulnerability scanners have the ability to find client-side vulnerabilities that are typically not found in active scanners.

Packet Sniffers

A packet sniffer or network protocol analyzer is a network tool that collects copies of packets from the network and analyzes them.
It can provide a network administrator with valuable information for diagnosing and resolving networking issues.
In the wrong hands, a sniffer can be used to eavesdrop on network traffic.
Typically, to use these types of programs most effectively, the user must be connected to a network from a central location. To use a packet sniffer legally, the administrator must:

1) Be on a network that the organization owns
2) Be under direct authorization of the owners of the network
3) Have knowledge and consent of the content creators

Wireless Security Tools

An organization that spends all of its time securing the wired network and leaves wireless networks to operate in any manner is opening itself up for a security breach.
As a security professional, you must assess the risk of wireless networks.
A wireless security toolkit should include the ability to sniff wireless traffic, scan wireless hosts, and assess the level of privacy or confidentiality afforded on the wireless network.

Access Control Devices

A successful access control system includes a number of components, depending on the system's needs for authentication and authorization.
Strong authentication requires at least two of the forms of authentication listed below to authenticate the supplicant's identity. When a second factor is required to verify the supplicant's identity, this is frequently a physical device.
The technology to manage authentication based on what a supplicant knows is widely integrated into the networking and security software systems in use across the IT industry.

Authentication

Authentication is the validation of a supplicant's identity.
There are four general ways in which authentication is carried out:

- What a supplicant knows
- What a supplicant has
- What a supplicant is
- What a supplicant produces

39. Briefly describe the different ways for protecting remote connections

Protecting Remote Connections

Installing Internetwork connections requires using leased lines or other data channels provided by common carriers, and therefore these connections are usually permanent and secured under the requirements of a formal service agreement.

In the past, organizations provided remote connections exclusively through dial-up services like Remote Authentication Service (RAS).

Since the Internet has become more widespread in recent years, other options such as virtual private networks (VPNs) have become more popular.

Dial-Up

It is a widely held view that these unsecured, dial-up connection points represent a substantial exposure to attack.

An attacker who suspects that an organization has dial-up lines can use a device called a war dialer to locate the connection points.

A war dialer is an automatic phone-dialing program that dials every number in a configured range and checks to see if a person, answering machine, or modem picks up.

Some technologies, such as RADIUS systems, TACACS, and CHAP password systems, have improved the authentication process.

RADIUS and TACACS

RADIUS and TACACS are systems that authenticate the credentials of users who are trying to access an organization's network via a dial-up connection.

The Remote Authentication Dial-In User Service system places the responsibility for authenticating each user in the central RADIUS server. When a remote access server receives a request for a network connection from a dial-up client, it passes the request along with the user's credentials to the RADIUS server, which then validates the credentials and passes the resulting decision (accept or deny) back to the accepting RAS.

Similar in function to the RADIUS system is the Terminal Access Controller Access Control System (TACACS). TACACS, like RADIUS, is a centralized database and validates the user's credentials at this TACACS server.

Securing Authentication with Kerberos

Kerberos uses symmetric key encryption to validate an individual user to various network resources. Kerberos keeps a database containing the private keys of clients and servers—in the case of a client, this key is simply the client's encrypted password.

The Kerberos system knows these private keys and can authenticate one network node (client or server) to another.

Kerberos consists of three interacting services, all of which use a database library:

1. Authentication server (AS), which is a Kerberos server that authenticates clients and servers.
2. Key Distribution Center (KDC), which generates and issues session keys.
3. Kerberos ticket granting service (TGS), which provides tickets to clients who request services.

In Kerberos, a ticket is an identification card for a particular client that verifies to the server that the client is requesting services and that the client is a valid member of the Kerberos system and therefore authorized to receive services.

The ticket consists of the client's name and network address, a ticket validation starting and ending time, and the session key, all encrypted in the private key of the server from which the client is requesting services.

SESAME

The Secure European System for Applications in a Multivendor Environment (SESAME) is similar to Kerberos in that the user is first authenticated to an authentication server and receives a token.

The token is then presented to a privilege attribute server (instead of a ticket granting service as in Kerberos) as proof of identity to gain a privilege attribute certificate (PAC).

SESAME also builds on the Kerberos model by adding additional and more sophisticated access control features, more scalable encryption systems, as well as improved manageability, auditing features, and the delegation of responsibility for allowing access.

Virtual Private Networks (VPNs)

(Q. 18)

40. Short list the various roles for staffing the information security functions. 2M

Information security functions require a range of roles to be staffed in order to effectively protect an organization's information assets. Some of the various roles include:

1. Chief Information Security Officer (CISO) - responsible for the overall strategy, planning, and management of the organization's information security program.
2. Information Security Manager - responsible for managing and implementing the day-to-day operations of the information security program.
3. Security Analyst - responsible for monitoring and analyzing security-related data to identify potential threats and vulnerabilities.
4. Security Engineer - responsible for designing, implementing, and maintaining security systems and infrastructure.
5. Incident Response Coordinator - responsible for managing and coordinating the organization's incident response efforts.
6. Compliance Officer - responsible for ensuring compliance with relevant laws, regulations, and standards related to information security.
7. Penetration Tester - responsible for simulating real-world attacks on the organization's systems and infrastructure to identify vulnerabilities.
8. Security Architect - responsible for designing and implementing the organization's overall security architecture.
9. Security Administrator - responsible for maintaining and managing security-related systems and software.

41. **Information security project plan**

Information Security Project Management

- Once organization's vision and objectives for information security are understood, the process for creating project plan can be defined
- Major steps in executing project plan are:
- Planning the project
- Supervising tasks and action steps
- Wrapping up
- Each organization must determine its own project management methodology for IT and information security projects

Developing the Project Plan

- Creation of project plan can be done using work breakdown structure (WBS)
- Major project tasks in WBS are
- work to be accomplished;
- individuals assigned;
- start and end dates;
- amount of effort required;
- estimated capital and noncapital expenses;
- and identification of dependencies between/among tasks

Financial Considerations

- No matter what information security needs exist, the amount of effort that can be expended depends on funds available
- Cost benefit analysis must be verified prior to development of project plan
- Both public and private organizations have budgetary constraints, though of a different nature
- To justify an amount budgeted for a security project at either public or for-profit organizations, it may be useful to benchmark expenses of similar organizations

Priority Considerations

- In general, the most important information security controls should be scheduled first Implementation of controls is guided by prioritization of threats and value of threatened information assets

Time and Scheduling Considerations

- Time impacts dozens of points in the development of a project plan, including:
- Time to order, receive, install, and configure security control
- Time to train the users
- Time to realize return on investment of control

Staffing Considerations

- Lack of enough qualified, trained, and available personnel constrains project plan Experienced staff is often needed to implement available technologies and develop and implement policies and training programs

Procurement Considerations

- IT and information security planners must consider acquisition of goods and services There may be many constraints on the selection process for equipment and services in most organizations, specifically in the selection of service vendors or products from

manufacturers/suppliers

- These constraints may eliminate a technology from realm of possibilities

Organizational Feasibility Considerations

- Policies require time to develop; new technologies require time to be installed, configured, and tested
- Employees need training on new policies and technology, and how new information security program affects their working lives
- Changes should be transparent to system users unless the new technology is intended to change procedures (e.g., requiring additional authentication or verification)

Training and Indoctrination Considerations

- Size of organization and normal conduct of business may preclude a single large training program on new security procedures/technologies
- Thus, organization should conduct phased-in or pilot approach to implementation

Scope Considerations

- Project scope: concerns boundaries of time and effort-hours needed to deliver planned features and quality level of project deliverables
- In the case of information security, project plans should not attempt to implement the entire security system at one time

The Need for Project Management

- Project management requires a unique set of skills and thorough understanding of a broad body of specialized knowledge
- Most information security projects require a trained project manager (a CISO) or skilled IT manager versed in project management techniques

Supervised Implementation

- Some organizations may designate a champion from the general management community of interest to supervise implementation of information security project plan
- An alternative is to designate a senior IT manager or CIO to lead implementation Optimal solution is to designate a suitable person from information security community of interest
- It is up to each organization to find the most suitable leadership for a successful project implementation

Executing the Plan

- Negative feedback ensures project progress is measured periodically
- Measured results compared against expected results
- When significant deviation occurs, corrective action taken
- Often, project manager can adjust one of three parameters for task being corrected: effort and money allocated; scheduling impact; quality or quantity of deliverable

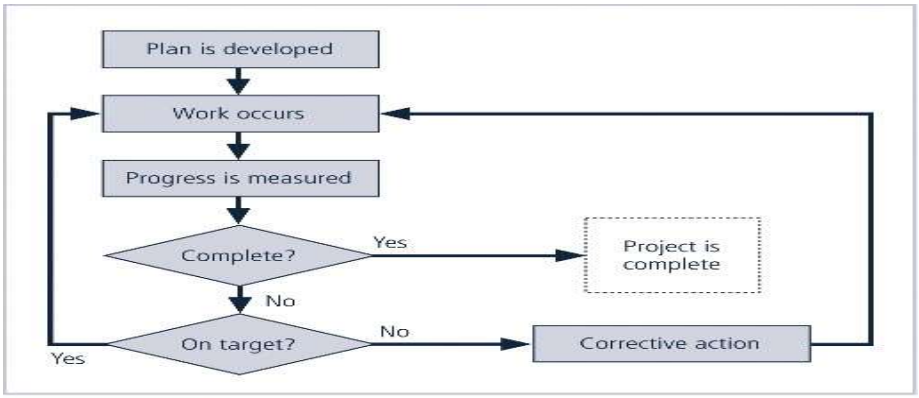


FIGURE 10-1 Negative Feedback Loop

Project Wrap-up

- Project wrap-up is usually handled as procedural task and assigned to mid-level IT or information security manager
- Collect documentation, finalize status reports, and deliver final report and presentation at wrap-up meeting
- Goal of wrap-up is to resolve any pending issues, critique overall project effort, and draw conclusions about how to improve the process for the future

42. **Triple DES**

The Triple DES encryption process

Triple DES operates in three steps: Encrypt-Decrypt-Encrypt (EDE). It works by taking three 56-bit keys (K1, K2 and K3) known as a key bundle and encrypting first with K1, decrypting next with K2 and encrypting a last time with K3. A Triple DES two-key version exists, where the same algorithm runs three times but K1 is used for the first and last steps. This two-key variant was retired in 2015.