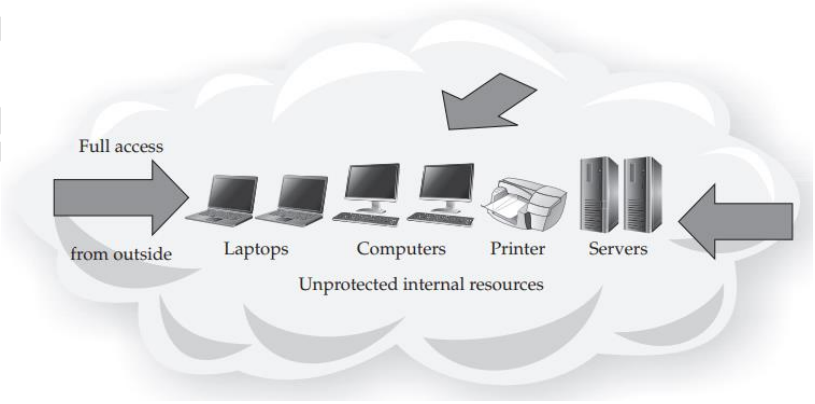
Information Security Overview

The Importance of Information Protection

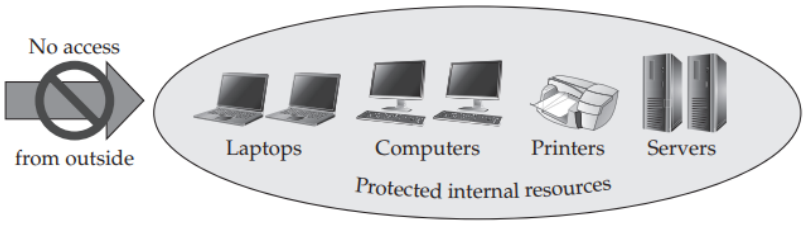
- Information is an important asset.
- In business, information is often one of the most important assets a company possesses.
- Information differentiates companies and provides leverage that helps one company become more successful than another.
- Information can be classified into different categories This is typically done in order to control access to the information in different ways, depending on its importance, its sensitivity, and its vulnerability to theft or misuse
- Companies may have confidential information, Loss or theft of confidential information could violate the privacy of individuals, reduce the company's competitive advantage, or cause damage to the company.
- Specialized information or secret information may include trade secrets, such as formulas, production details, and other intellectual property, proprietary methodologies and practices that describe how services are provided, research plans, electronic codes, passwords, and encryption keys.
- In some business sectors, the protection of information is not just desirable, it's mandatory.
- They are required by HIPAA to ensure robust security over protected health information (PHI) that consists of medical data and personally identifiable information (PII).
- Financial institutions are also required by regulations to protect customer information, PII, and financial records.
- The better your security controls are that protect all these different types of data, the greater the level of access that you can safely provide to authorized parties who need to use that data.

The Evolution of Information Security

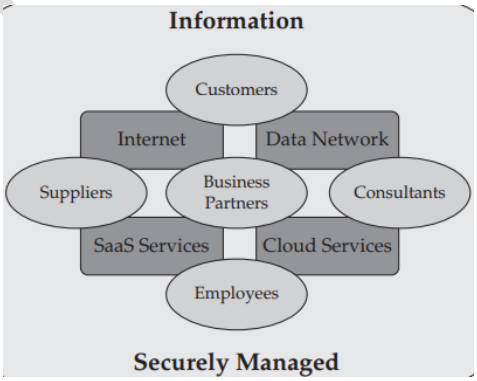
- Originally, the academic security model was "wide open" and the government security model was "closed and locked."
- Original academic open-access model



- Original government perimeter blockade model



- practices established by the **academic and government institutions** persisted until the early 1990s, and some of those practices are still around today
- When businesses started to widely embrace the Internet as a **sales channel** and business tool in the early-to-mid **1990s**, a new security model was required.
- E-commerce and business required a more blended approach of providing limited access to data in a controlled fashion, which is a more sophisticated and complex approach than that used by the earlier security models.
- As the use of **information technologies** evolved, the original all-or-nothing approaches to security no longer met the needs of information consumers. So, the practice of network security evolved.
- The concepts of intranets and extranets were developed to accommodate internal and external customers, respectively, with secured boundaries that resembled miniature versions of the firewall perimeter and VPN.
- These approaches continued through the end of the 1990s to the early part of the **2000s.**
- the first decade of the **21st century**, the Internet continued to become an increasingly critical business platform, and the network became more of a key business component.
- As more companies started doing business on the Internet, concepts such as Software-as-a-Service (SaaS) were developed to provide business services over the Internet.
- Basic viruses and worms along with the simple exploits and man-in-the-middle attacks found in the decade of the 1990s became more sophisticated, effective, and ubiquitous.
- cloud computing is moving the boundaries of the network even further away from the data center. This global interconnectedness requires a different perspective on security—we can no longer build virtual walls around our networks.
- Modern information is shared among many consumers, via many channels.



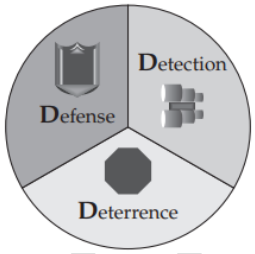
Justifying Security Investment

- How do you justify spending money on security?

- First there was FUD—fear, uncertainty, and doubt.
- **return on investment (ROI)** was used as an attempt to market security as an investment that "pays for itself." This was the standard approach to justifying information technology budgets, but it never translated well to security.
- ROI was combined with **annualized loss expectancy (ALE)**, a risk measurement strategy that combines the frequency (or probability) of a loss with the cost of that loss, to produce a yearly expected monetary value.
- The "**insurance analogy**" was developed as an alternative to value-based security justifications. People and businesses spend money on insurance—often as much as 10 percent of the value of the asset per year—even though they may never have a claim to file. They spend this money for peace of mind.
- Robust **information security practices** not only reduce risks and costs, but also provide new opportunities for revenue. In the past, security was thought of only in the context of protection (blocking access, closing holes, segmenting and separating systems and networks, and denying connections). Today that view has evolved to focus on enabling business on a global scale, using new methods of communication.
- Good security practices allow companies to perform their operations in a more integrated manner, especially with their customers.
    - **Business Agility**
        - Knowledge is power—in business, the more you know, the better you can adapt. Strong security provides insight into what is happening on the network and, consequently, in the enterprise.
        - Security allows information to be used more effectively in advancing the goals of organization because that organization can safely allow more outside groups of people to utilize the information when it is secure.
        - Automation of business processes, made trustworthy by appropriate security techniques, allows companies to focus on their core business
    - **Cost Reduction**
        - Modern security practices do reduce some costs, such as those resulting from loss of data or equipment.
        - The consequences of a security compromise can be significant. A publicized security incident can severely damage the credibility of a company, and thus its ability to acquire and retain customers.
        - An increasing number of attacks are categorized as advanced persistent threats (APTs).
        - These attacks are designed to deploy malware into a network and remain undetected until triggered for some malicious purpose.
    - **Portability**
        - Portability means that software and data can be used on multiple platforms or can be transferred/transmitted within an organization, to a customer, or to a business partner.
        - To meet the demands of today's businesses and consumers, architectures and networks need to be designed with security controls baked in as part of the development process.

Security Methodology

- Security is a paradigm, a philosophy, and a way of thinking. Defensive failures occur when blind spots exist. A defender who overlooks a vulnerability risks the exploitation of that vulnerability.
- The field of security is concerned with protecting assets in general. Information security is concerned with protecting information in all its forms, whether written, spoken, electronic, graphical, or using other methods of communication.
- Network security is concerned with protecting data, hardware, and software on a computer network.
- The basic assumptions of security are as follows:
    - We want to protect our assets.
    - There are threats to our assets.
    - We want to mitigate those threats.
- Three aspects of security can be applied to any situation—defense, detection, and deterrence. These are considered the **three Ds** of security



- **Defense** is often the first part of security that comes to mind, and usually it is the easiest aspect for people to understand. The desire to protect ourselves is instinctive, and defense usually precedes any other protective efforts. Defensive ways (stateful firewalls, network access control, web content filtering)
- Another aspect of security is **detection**. In order to react to a security incident, you first need to know about it. Detective controls on the network include audit trails and log files, system and network intrusion detection and prevention systems
- **Deterrence** is another aspect of security. It is considered to be an effective method of reducing the frequency of security compromises, and thereby the total loss due to security incidents. Many companies implement deterrent controls for their own employees, using threats of discipline and termination for violations of policy.

How to Build a Security Program

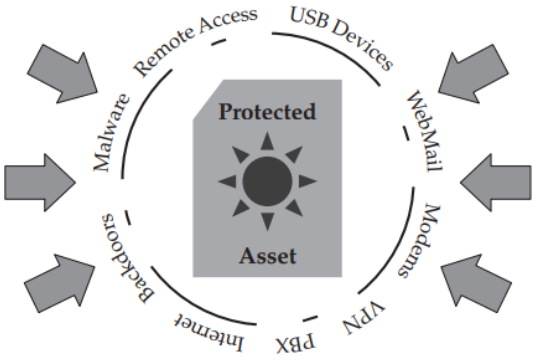
- **Authority** The security program must include the right level of responsibility and authorization to be effective.
    - A security program charter defines the purpose, scope, and responsibilities of the security organization and gives **formal authority** for the program.
    - Usually, the security organization is responsible for information protection, risk management, monitoring, and response.
- **Framework** A security framework provides a defensible approach to building the program.
    - The **security policy** provides a framework for the security effort. The policy describes the intent of executive management with respect to what must be done to comply with the business requirements.

  - **Standards** are the appropriate place for product-specific configurations to be detailed. Standards are documented to provide continuity and consistency in the implementation and management of network resources.
  - **Guidelines** for the use of software, computer systems, and networks should be clearly documented for the sake of the people who use these technologies.
- **Assessment** Assessing what needs to be protected, why, and how leads to a strategy for improving the security posture.
  - A risk analysis provides a perspective on current risks to the organization's assets.
  - A risk analysis results in a well-**defined set of risks** that the organization is concerned about. These risks can be mitigated, transferred, or accepted.
  - A **gap analysis** compares the desired state of the security program with the actual current state and identifies the differences.
  - **Remediation planning** takes into account the risks, gaps, and other objectives of the security program, and puts them together into a prioritized set of steps to move the security program from where it is today to where it needs to be at a future point.
- **Planning** Planning produces priorities and timelines for security initiatives.
  - A **roadmap** is a plan of action for how to implement the security remediation plans.
  - The roadmap is useful for managers who need the information to plan activities and to target specific implementation dates and the order of actions.
  - The **security architecture** documents how security technologies are implemented, at a relatively high level.
  - The **project plans** detail the activities of the individual contributors to the various security implementations.
- **Action** The actions of the security team produce the desired results based on the plans.
  - The actions that should be taken when a security event occurs are defined in the **incident response plan.** Advance planning for what to do when security incidents occur helps shorten the response time and provides repeatable, reliable, and effective actions to limit the scope and damage of an incident
- **Maintenance** The end stage of the parts of the security program that have reached maturity is to maintain them.
  - **Security awareness** programs are **used to educate** employees, business partners, and other stakeholders about what behaviors are expected of them, what actions they should take under various circumstances to comply with security policies, and what consequences may ensue if they don't follow the rules.

The Impossible Job

- A universal truth of security, regardless of the application, is that the job of the attacker is always easier than the job of the defender. The attacker needs only to find one weakness, while the defender must try to cover all possible vulnerabilities.
- In fact, the defender has an impossible job if the goal is to have 100 percent protection against all conceivable attacks. That is why the primary goal of security cannot be to eliminate all threats. Management may need to be educated about this concept, because they may not realize that this

is a tenet of the security profession. Every defender performs a risk assessment by choosing which threats to defend against, which to insure against, and which to ignore.



- **Mitigation** is the process of defense,
- **transference** is the process of insurance, and
- **acceptance** is deciding that the risk does not require any action.

The Weakest Link

- A security infrastructure will drive an attacker to the weakest link.
- All security controls should complement each other, and each should be equally as strong as the others. This principle is called equivalent security or transitive security.
- The weakest link will attract the greatest number of attacks. **(from low level attack to high level attack)**
- In a computer network, **firewalls are often the strongest point of defense**. They encounter their fair share of attacks, but most attackers know that properly configured firewalls are difficult to penetrate, so they will look for easier prey.
- **attacker can take the form of DSL lines** in labs or small offices that aren't firewalled, modems and other remote access systems, **Private Branch Exchange (PBX)** phone switches, home computers and laptops that are sometimes connected to the company network, unpatched web servers and other Internet-facing servers, e-mail servers (to launch attacks such as spear-phishing), and Domain Name Service **(DNS)** servers that are accessible from the Internet. All of these typically offer less resistance to attackers than firewalls offer.

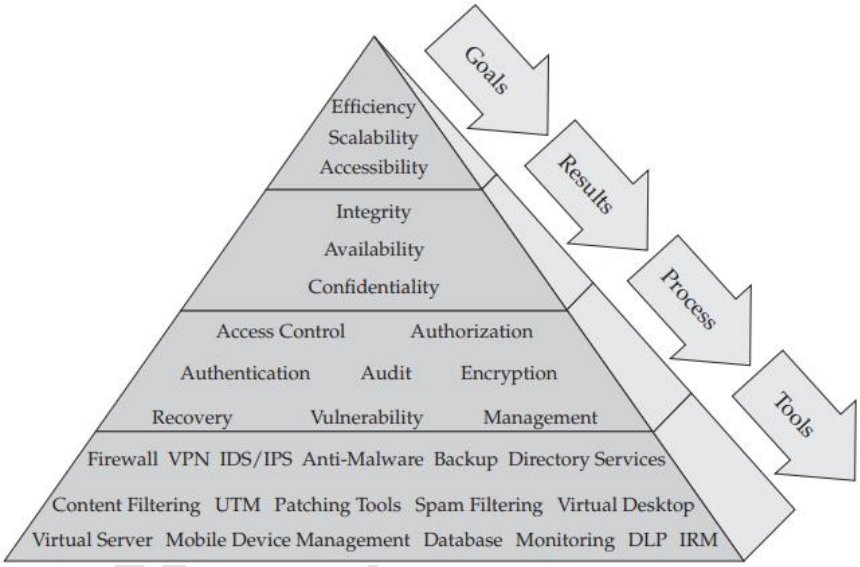
Strategy and Tactics

- A security strategy is the definition of all the architecture and policy components that **make up a complete plan for defense, detection, and deterrence**. Security tactics are the day-today practices of the individuals and technologies assigned to the protection of assets.
- **strategies are usually proactive** and **tactics are often reactive**. Both are equally important, and a successful security program needs to be both strategic and tactical in nature.
- **Strategy** is defined as a game plan, which can help the organization to achieve its mission and objectives.(how to secure, and plan to secure)

- **Tactics** are the actions, projects or events, to reach a particular point (what if attack is observed or encountered)

Business Processes vs. Technical Controls

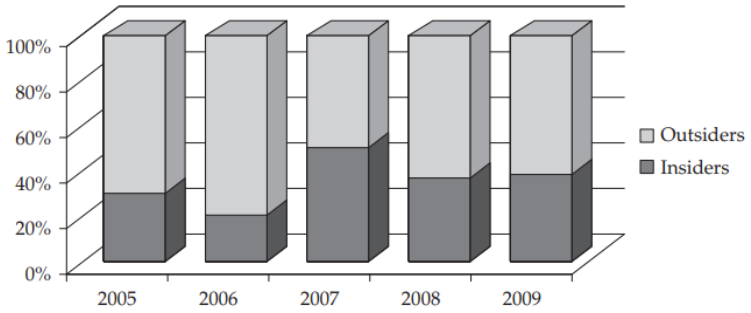
- Security technologies need to be selected on the basis of business context, so they are targeted toward specifically identified risks with clear objectives.
- Organizations that place technical controls on their network without accompanying business processes have not recognized that computers are tools for accomplishing specific objectives, and that tools should be considered within a business process in order to be effective.
- For example**, purchasing a database does not solve the problem of how to manage customer data. Customer data management is a business process that can be facilitated by a database**.



Risk Analysis

Threat Definition

- How do you know you're defending against the right threats? For example, if an organization were to simply purchase and install a firewall (and do nothing else) without identifying and ranking the various threats to their most important assets, would they be secure? Probably not.
- Consider the statistics shown in Figure. These statistics are from Verizon's 2010 Data Breach Investigations Report (DBIR), the result of a collaboration between Verizon and the U.S. Secret Service.



- Security professionals know that many real-world threats come from inside the organization, which is why just building a wall around your trusted interior is not good enough. Regardless of the breakdown for your particular organization, you need to make sure your security controls focus on the right threats. To avoid overlooking important threat sources, you need to consider all types of threats. This consideration should take into account the following **aspects of threats:**
    - *Threat vectors*
        - A threat vector is a term used to **describe where a threat originates and the path it takes to reach a target**. An example of a threat vector is an e-mail message sent from outside the organization to an inside employee, containing an irresistible subject line along with an executable attachment that happens to be a Trojan program, which will compromise the recipient's computer if opened
        -

Sources	Threats	Targets
Employee Contractor	Theft Loss	Intellectual property Trade secret

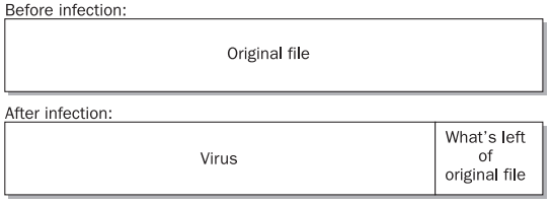
    - *Threat sources and targets*
        - we need to understand how attacks work so that you can select the best countermeasures for defense.
        - Security controls(Preventative, Detective, Deterrent, Corrective, Recovery)
    - **Types of attacks (is in detail below)**

Types of Attacks

- Any computer that is accessible from the Internet will be attacked. It will constantly be probed by attackers and malicious programs intending to exploit vulnerabilities. If you don't keep up with patches and take appropriate countermeasures, your computer will surely be compromised within a short amount of time.
- Attacks can take the form of automated, malicious, mobile code traveling along networks looking for exploit opportunities, or they can take the form of manual attempts by an attacker
- An attacker may even use an automated program to find vulnerable hosts and then manually attack the victims.
- **Malicious Mobile Code**
    - There are three generally recognized variants of malicious mobile code: **viruses**, **worms**, and **Trojans**.
    - lifecycle of malicious mobile code
        - Find
        - Exploit
        - Infect

- Repeat

- **Computer Viruses**
  - A virus is a self-replicating program that uses other host files or code to replicate.
  - Viruses can infect program files, boot sectors, hard drive partition tables, data files, memory, macro routines, and scripting files
  - **Anatomy of a Virus**
    - The damage routine of a virus (or really of any malware program) is called the payload.
    - a "harmless" virus takes up CPU cycles and storage space.
    - payloads can be intentionally destructive, deleting files, corrupting data, copying confidential information, formatting hard drives, and removing security settings.
    - Confidential financial statements and business plans have been sent out to competitors by malware.
    - Viruses cannot break hard drive read-write heads, electrocute people, or cause fires.
      - **Types of viruses**
      - If the virus executes, does its damage, and terminates until the next time it is executed, it is known as a **nonresident virus**.
      - If the virus stays in memory after it is executed, it is called a **memory-resident virus.**
      - Memory-resident viruses are also able to manipulate the operating system in order to hide from administrators and inspection tools. These are called **stealth viruses**.
      - If the virus overwrites the host code with its own code, effectively destroying much of the original contents, it is called an **overwriting virus.**
      - If the virus inserts itself into the host code, moving the original code around so the host programming still remains and is executed after the virus code, the virus is called a **parasitic virus.**
      - Viruses that copy themselves to the beginning of the file are called **prepending viruses**
      - viruses placing themselves at the end of a file are called **appending viruses.**
      - Viruses appearing in the middle of a host file are labeled **mid-infecting viruses**
      - In order for a pure **boot sector virus** to infect a computer, the computer must have booted, or attempted to boot, off an infected disk.
      - Some boot sector viruses, like Tequila, are classified as **multipartite viruses**, because they can infect both boot sectors and program files.
      - **Macro viruses** infect the data running on top of an application by using the program's macro or scripting language.



- **The Next Evolution of Viruses**
  - The four most popular small-form-factor programming environments are Android, Windows CE, Java, and Symbian.
  - According to McAfee, the Android OS has become the biggest target for mobile malware, with Trojans, spyware, SMS spamming malware, ransomware, and even botnets infecting mobile smartphones and tablets.
  - Tablets and smartphones have all the right components for a fast-spreading malware program. They have network connectivity, e-mail, a contact address book, and both allow additional programs and features to be added.
- **Computer Worms**
  - A computer worm uses its own coding to replicate, although it may rely on the existence of other related code to do so.
  - The key to a worm is that it does not directly modify other host code to replicate. **A worm may travel the Internet trying one or more exploits to compromise** a computer, and if successful, it then writes itself to the computer and begins replicating again.
  - Once launched, it infects the PC, harvests e-mail addresses from the user's e-mail system, and sends itself out to new recipients.
  - It adds itself into the Windows startup group so it gets executed each time Windows starts.
  - It would also infect web sites with vulnerable versions of IIS and place infected JavaScript coding on the sites.
  - **E-Mail Worms**
    - E-mail worms are a curious intersection of social engineering and automation.
    - They appear in people's inboxes as messages and file attachments from friends, strangers, and companies.
    - They pose as pornography, cute games, official patches from Microsoft, or unofficial applications found in the digital marketplace.
- **Trojans**
  - Trojan horse programs, or Trojans, work by posing as legitimate programs that are activated by an unsuspecting user.
  - After execution, the Trojan may attempt to continue to pose as the other legitimate program (such as a screensaver) while doing its malicious actions in the background.
  - If the Trojan simply starts its malicious actions and doesn't pretend to be a legitimate program, it's called **a direct-action Trojan**.
  - **Remote Access Trojans**
    - A powerful type of Trojan program called a remote access Trojan (RAT) is very popular in today's attacker circles.
    - Once installed, a RAT **becomes a back door into the compromised system** and allows the remote attackers to do virtually anything they want to the compromised PC.
    - RATs have even been known to **record video and audio from the host computer's** web camera and microphone.
    - Imagine malware that is capable of recording every conversation made near the PC. Surely confidential business meetings have been recorded.

- RATs come with server and client programs. The client portion creates server executables that are meant to be run on unsuspecting users' PCs, while the server programs can be extensively customized.

- **Zombie Trojans and DDoS Attacks**
  - Zombie Trojans infect a host and wait for their originating attacker's commands telling them to attack other hosts.
  - The attacker installs a series of zombie Trojans, sometimes numbering in the thousands. With one predefined command, the attacker can cause all the zombies to begin to attack another remote system with a **distributed denial of service (DDoS) attack.**
- **Malicious HTML**
  - The Internet allows for many different types of attacks, many of which are HTML-based.
  - Pure HTML coding can be malicious when it **breaks browser security zones** or when it can access local system files.
  - Malicious HTML has often been used to access files on local PCs, too.
  - Specially crafted HTML links can download files from the user's workstation, retrieve passwords, and delete data

Risk Analysis

- A risk analysis needs to be a part of every security effort. It should analyze and categorize the assets that need to be protected and the risks that need to be avoided, and it should facilitate the **identification and prioritization of protective elements**.
- It can also provide a means to measure the effectiveness of the overall security architecture, by tracking those risks and their associated mitigation over time to observe trends
- formal definition of risk is the probability of an undesired event (a threat) exploiting a vulnerability to cause an undesired result to an asset.

  Risk = Probability (Threat + Exploit of Vulnerability) * Cost of Asset Damage
- commonly used approach to assigning cost to risks is annualized loss expectancy (ALE).

  Annualized Loss (ALE) = Single Loss (SLE) * Annualized Rate (ARO)
- This is the cost of an undesired event—a single loss expectancy (SLE)—multiplied by the number of times you expect that event to occur in one year—the annualized rate of occurrence (ARO).

Secure Design Principles

The CIA Triad and Other Models

CIA triad—Confidentiality, Integrity, and Availability.

- **Confidentiality**
  - Confidentiality refers to the restriction of access to data only to those who are authorized to use it.
- **Integrity**
  - Integrity, which is particularly relevant to data, refers to the assurance that the data has not been altered in an unauthorized way.
- **Availability**

- availability refers to the "uptime" of computer-based services—the assurance that the service will be available when it's needed.

Defense Models

- There are two approaches you can take to preserve the confidentiality, integrity, availability, and authenticity of electronic and physical assets such as the data on your network:
  - Build a defensive perimeter around those assets and trust everyone who has access inside
  - Use many different types and levels of security controls in a layered defense-in depth approach
- **The Lollipop Model**
  - The most common form of defense, known as perimeter security, involves building a virtual (or physical) wall around objects of value.
  - Perimeter security is like a lollipop with a hard, crunchy shell on the outside and a soft, chewy center on the inside.
  - One of the limitations of perimeter security is that once an attacker breaches the perimeter defense, the valuables inside are completely exposed.
- **The Onion Model**
  - A better approach is the onion model of security. It is a layered strategy, often referred to as defense in depth. This model addresses the contingency of a perimeter security breach occurring.
  - A layered security architecture, like an onion, must be peeled away by the attacker, layer by layer, with plenty of crying.

Zones of Trust

- trust levels of networks and computer systems are known as zones of trust.
- Once you have identified the risks and threats to your business, and you know what functions are required for your business, you can begin to separate those functions into zones of trust.
- Zones of trust are connected with one another, and business requirements evolve and require communications between various disparate networks, systems, and other entities on the networks.
- IT resources vary in the extent to which they trust each other. Separating these resources into zones of trust enables you to vary the levels of security for these resources according to their individual security needs.
- Firewalls, routers, virtual LANs (VLANs), and other network access control devices and technologies can be used to separate trust zones from each other
- Trust can also be viewed from a transaction perspective. During a particular transaction, several systems may communicate through various zones of trust.
  - For example, a credit card transaction may pass through a web server, an application server, a database, and a credit-checking service on the Internet. During the transaction, all of these systems must trust each other equally, even though the transaction may cross several network boundaries.
- Segmentation allows greater refinement of access control based on the audience for each particular system, and it helps confine the communications between systems to the services that have transactional trust relationships.

Best Practices for Network Defense

stop malicious mobile code from arriving on the desktop in the first place, close holes, and make sure the users' computers are appropriately configured. If they can't click on malware, run it, or allow it on their computer, you've significantly decreased the threat of malicious attack.

- **Secure the Physical Environment**
  - Depending on your environment, PCs and laptops might need to be physically secured to their desks.
- **Password Protect Booting**
  - boot-up password before the operating system will load. This can usually be set in the CMOS/BIOS and is called a user or boot password.
- **Password Protect CMOS**
  - It is important to ensure that unauthorized users do not have access to the CMOS/BIOS settings. Most CMOS/ BIOSs allow you to set up a password to prevent unauthorized changes.
- **Disable Booting from USB and CD**
  - Disabling booting from USB storage devices and optical drives will prevent boot viruses from those devices and stop attackers from bypassing operating system security by loading a different operating system on the computer.
- **Harden the Operating System**
  - reduce the attack surface of the operating system by removing unnecessary software, disabling unneeded services, and locking down access (turning off unneeded services, Configure software settings securely, Segment the network into zones, Strengthen authentication)
- **Keep Patches Updated**
  - An attacker's best friend is an unpatched system. In most cases, the vulnerabilities used are widely known, and the affected vendors have already released patches for system administrators to apply.
- **Use an Antivirus Scanner (with Real-Time Scanning)**
  - an antivirus (AV) scanner is essential. It should be deployed on your desktop, with forced, automatic updates, and it should be enabled for real-time protection.
- **Use Firewall Software**
  - Firewalls have come a long way since their days of simple port filtering. Today's devices are stateful inspection systems capable of analyzing threats occurring anywhere in layers three through seven with software that runs directly on the computer.
- **Secure Network Share Permissions**
  - One of the most common ways an attacker or worm breaks into a system is through a network share (such as NetBIOS or SMB) with no password or a weak password.
- **Use Encryption**
  - Linux and Unix administrators should be using SSH instead of Telnet or FTP to manage their computers. The latter utilities work in plaintext over the network, whereas SSH is encrypted.
  - Encrypting File System (EFS) is one of the most exciting features in Windows. EFS encrypts and decrypts protected files and folders on the fly.

- **Secure Applications**
    - Managing your applications and their security should be a top priority of any administrator.
    - locking down applications, securing P2P services, and making sure your application programmers code securely
- **Securely Configure Applications**
    - In end-user PC environments, however, you want to keep the applications and minimize the risk at the same time. You can do this by regularly applying security patches and making sure security settings are set at the vendor's recommended settings, if not higher.
    - *Securing E-Mail* E-mail worms continue to be the number-one threat on computer systems, especially Windows systems running Outlook or Outlook Express.
    - *Blocking Dangerous* File Types Blocking dangerous file attachments is the best way to prevent exploits, given today's preferred method of e-mailing viruses and worms.
    - *Blocking Outlook File Attachments* Many administrators believe that they cannot block potentially dangerous file extensions in their network. They believe end users and management would revolt. But when management hears the statistics, they present a compelling business argument for file blocking.
- **Install Applications to Nonstandard Directories and Ports**
    - Many malware programs depend on the fact that most people install programs to default directories and on default ports. You can significantly minimize the risk of exploitation by installing programs into nonstandard directories and instructing them to use nonstandard ports.
- **Lock Down Applications**
    - limit what an end user can and cannot run on the desktop. In Windows, the administrator could set system policies to prevent the installation of new applications, take away the user's Run command, and severely limit the desktop.
- **Secure P2P Services**
    - if P2P isn't authorized in your corporate environment, eradicate it. Start by educating end users and working with management to establish penalties for unauthorized software. Then track the programs down and remove them.
- **Make Sure Programmers Program Securely**
    - Preventing SQL injection attacks can be as simple as using double quotation marks instead of single quotes. Stopping buffer-overflow attacks requires input validation.
- **Back Up the System**
    - Security experts cannot always repair the damage and put the system back to the way it was prior to the exploit. This means it's important to keep regular, tested backups of your system.

END OF UNIT1

Authentication and Authorization

Authentication

- Authentication is the process by which people prove they are who they say they are. It's composed of two parts: a public statement of identity (usually in the form of a **username**) combined with a private response to a challenge (such as a password).
- A **password** by itself, which is a means of identifying yourself through something only you should know (and today's most common form of challenge **response**), is an example of single-factor authentication.
- **Biometrics**, which use a sensor or scanner to identify unique features of individual body parts, are better than passwords because they can't be shared—the user must be present to log in.
- **Multifactor authentication** refers to **using two or more methods** of checking identity.
- **Two-factor authentication** is the most common form of multifactor **authentication smart card along with a password**

Usernames and Passwords

1. password authentication, **a challenge** is issued by a computer, and the party wishing to be identified provides a response. If **the response** can be validated, the user is said to be authenticated, and the user is allowed to access the system. Otherwise, the user is prevented from accessing the system
2. Other password-based systems, including Kerberos, are more complex.

types of password authentication systems

Local Storage and Comparison : User passwords were entered in simple machine-resident databases by administrators and were provided to users.

Securing Passwords with Encryption and Securing the Password File : modern Unix systems, the usernames are stored in the /etc/passwd file but the passwords are stored in a separate file, known as a shadow password file and located in /etc/shadow. It contains the encrypted passwords and is not world-readable.

Windows added the syskey utility, which added a layer of protection to the database in the form of additional encryption.

Central Storage and Comparison : When passwords are encrypted, authentication processes change. Instead of doing a simple comparison, the system must first take the user-entered, **plaintext** password and **encrypt it using the same algorithm** used for its storage in the password file. Next, the newly encrypted password is **compared to the stored encrypted password**. If they match, the user is authenticated.

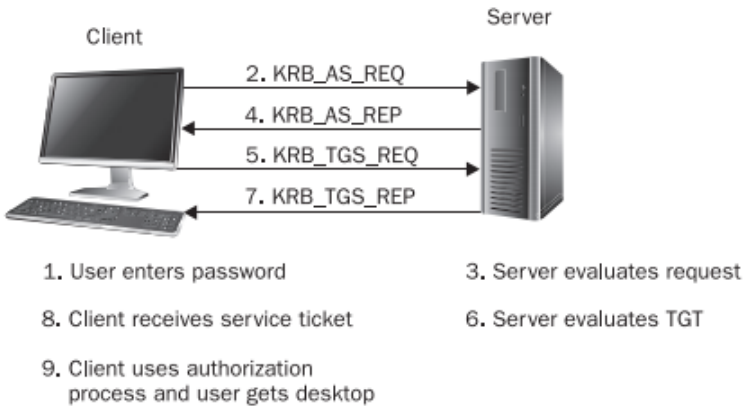
solution of **securing authentication credentials across the network** so they are not easily intercepted and replayed is to use the challenge and response authentication algorithms **Challenge Handshake Authentication Protocol**

Kerberos

Kerberos is a network authentication system based on the use of tickets

Kerberos authentication process

1. A user enters their password
2. Data about the client and possibly an authenticator is sent to the server , The authenticator is the result of using the password (which may be hashed or otherwise manipulated) to encrypt a timestamp (the clock time on the client computer). This authenticator and a plaintext copy of the timestamp accompany a login request, which is sent to the Kerberos authentication server (AS)—this is the KRB_AS_REQ message
3. The KDC checks the timestamp from the workstation against its own time. which is five minutes, by default
4. The KDC, since it maintains a copy of the user's password, can use the password to encrypt the plaintext copy of the timestamp and compare the result to the authenticator. If the results match, the user is authenticated, and a ticket-granting ticket (TGT) is returned to the client—this is the KRB_AS_REP message.
5. The client sends the TGT to the KDC with a request for the use of a specific resource, and it includes a fresh authenticator. The request might be for resources local to the client computer or for network resources. This is the KRB_TGS_REQ message, and it is handled by the TGS
6. The KDC validates the authenticator and examines the TGT. Since it originally signed the TGT by encrypting a portion of the TGT using its own credentials, it can verify that the TGT is one of its own.
7. If all is well, the KDC issues a service ticket for the requested resource—this is the KRB_TGS_REP message. part of the ticket is encrypted with the credentials of the client.
8. The client can decrypt its part of the ticket and thus knows what resource it may use. The client sends the ticket to the resource computer along with a fresh authenticator.
9. The resource computer (the client) validates the timestamp by checking whether the time is within the valid period, and then decrypts its portion of the ticket. This tells the computer which resource is requested and provides proof that the client has been authenticated.



One-Time Password Systems

- Passwords are subject to a number of different attacks. They can be captured and cracked, or used in a replay attack in which the passwords are intercepted and later used to repeat authentication
- solution to this type of attack is to use an algorithm that requires the password to be different every time it is used. this has been accomplished with the use of a one-time pad.

- When two people need to send encrypted messages, if they each have a copy of the one-time pad, each can use the day's password
- The advantage, of course, to such a system is that even if a key is cracked or deduced, it is only good for the current message. The next message uses a different key.
- Two current methods that use one-time passwords are **time-based keys and sequential keys.**
    - **Time-based** keys use hardware- or software-based authenticators that generate a random seed based on the current time of day
    - **Sequential key** systems use a passphrase to generate one-time passwords. The original passphrase, and the number representing how many passwords will be generated from it, is entered into a server. The **server generates a new password each time** an authentication request is made.

Certificate-Based Authentication

- A certificate is a collection of information that binds an identity (user, computer, service, or device) to the public key of a public/private key pair. The typical certificate includes information about the identity and specifies the purposes for which the certificate may be used, a serial number, and a location where more information about the authority that issued the certificate may be found.
- The certificate is digitally signed by the issuing authority, the certificate authority (CA).
- The infrastructure used to support certificates in an organization is called the Public Key Infrastructure (PKI).
- **authentication steps are as follows**
    1. The client issues an authentication request.
    2. A challenge is issued by the server.
    3. The workstation uses its private key to encrypt the challenge.
    4. The response is returned to the server.
    5. Since the server has a copy of the certificate, it can use the public key to decrypt the response.
    6. The result is compared to the challenge.
    7. If there is a match, the client is authenticated.
- **Two systems that use certificates for authentication are SSL/TLS and smart cards**
    - **Secure Sockets Layer (SSL**) is a certificate-based system that is used to provide authentication of secure web servers and clients and to share encryption keys between servers and clients. Transport Layer Security (TLS) is the Internet standard version (RFC 2246) of the proprietary SSL.
        - **The authentication process**
            1. The user enters the URL for the server in the browser.
            2. The client request for the web page is sent to the server.
            3. The server receives the request and sends its server certificate to the client.
            4. The client's browser checks its certificate store for a certificate from the CA that issued the server certificate.
            5. If the CA certificate is found, the browser validates the certificate by checking the signature on the server's certificate using the public key provided on the CA's certificate.

6. If this test is successful, the browser accepts the server certificate as valid.
7. A symmetric encryption key is generated and encrypted by the client, using the server's public key.
8. The encrypted key is returned to the server.
9. The server decrypts the key with the server's own private key. The two computers now share an encryption key that can be used to secure communications between the two of them

- **potential problems with ssl**
  1. Unless the web server is properly configured to require the use of SSL, the server is not authenticated to the client
  2. If the client does not have a copy of the CA's certificate, the server will offer to provide one.
  3. The process for getting a CA certificate in the browser's store is not well controlled.
  4. decision to provide a certificate to an organization for use on its web server is based on policies written by people, and a decision is made by people.

- **Smart Cards and Other Hardware-Based Devices**
  - The protection of the private key is **paramount in certificate-based authentication systems. If an attacker can obtain the private key,** they can spoof the identity of the client and authenticate. Implementations of these systems do a good job of protecting the private key, but, ultimately**, if the key is stored on the computer, there is potential for compromise.**
  - A better system would be to require that the **private key be protected and separate from the computer. Smart cards can be used for this purpose**
  - The **use of smart cards to store the private key and certificate solves the problem of protecting the keys.**

Authorization

- The counterpart to authentication is authorization. Authentication establishes who the user is; authorization specifies what that user can do.
- **User Rights**
  - Privileges or user rights are different from permissions. **User rights provide the authorization to do things that affect the entire system**. The ability to create groups, assign users to groups, log in to a system, and many more user rights can be assigned.
- **Role-Based Authorization (RBAC)**
  - Each job within a company has a role to play. Each employee requires privileges (the **right to do something**) and permissions (the **right to access particular resources** and do specified things with them) if they are to do their job.
- **Access Control Lists (ACLs)**
  - ACLs to determine whether the requested service or resource is authorized.
- **File-Access Permissions**
  - Both Windows and Unix systems use file permissions to manage access to files. The implementation varies, but it works well for both systems
  - **Windows File Permissions** (Full Control, Modify, Read and Execute, List Folder Contents, Read, Write, Special Permissions*)

- **Unix File-Access Permissions** (Execute, Read, Write, Denied)

Encryption

A Brief History of Encryption

- Once upon a time, keeping data secret was not hard. Hundreds of years ago, when few people were literate
- important secrets were kept by writing them down and hiding them from literate people.
- Persian border guards in the fourth century b.c. let blank wax writing tablets pass, but the tablets hid a message warning Greece of an impending attack. The message was simply covered by a thin layer of fresh wax.
- Scribes also tattooed messages on the shaved heads of messengers. When their hair grew back in, the messengers could travel incognito through enemy lands. When they arrived at their destination, their heads were shaved and the knowledge was revealed.

Early Codes

- Early code attempts used transposition. They simply **rearranged the order of the letters** in a message. Of course, this rearrangement had to follow some order, or the recipient would not be able to restore the message.
- early attempts at cryptography (the science of data protection via encryption) used substitution. A substitution algorithm simply replaces each character in a message with another character. **Caesar's cipher** is an example of a substitution algorithm. To create these messages, you list the alphabet across a page and agree with the recipient on the starting letter—suppose you agree to start with the fourth letter of the alphabet, D. Starting with this letter, you write down a new alphabet under the old.
- A→D, B→E……Z→C
- Eventually, of course, **variations of substitution algorithms appeared**. These algorithms used multiple alphabets and could not be cracked by simple frequency analysis.
- This complex, **polyalphabetic algorithm**, developed by the 16th century French diplomat, Blaise de Vigenère, was not broken for 300 years.

More Modern Codes

- The modern stream and block ciphers used today are sophisticated encryption algorithms that run on high-speed computers, but their origins were in simple physical devices used during colonial times.

Symmetric-Key Cryptography

- It means the key needed to encrypt message is the same used for decrypt message
- **stream ciphers** are often produced in code today, a modern example being RC4.
- While a stream cipher works on one character at a time, **block ciphers** work on a block of many bits at a time.(eg : DES[data encryption standard], Advanced Encryption Standard (AES) has now replaced DES and Triple DES)

Key Exchange

- These single-key, symmetric algorithms work fine as long as the key can somehow be shared between the parties that wish to use it.

- A way to solve this problem was first proposed by Whitfield Diffie and Martin Hellman. The Diffie-**Hellman key agreement protocol** uses two sets of mathematically related keys and a complex mathematical equation that takes advantage of this relationship.

Public Key Cryptography

- Another method for exchanging a session key is to use public key cryptography. This algorithm is asymmetric—it uses a set of related keys. If one key is used to encrypt the message, the other is used to decrypt it, and vice versa.
- One of the key pairs is known as the private key and the other as the public key. **Public keys are exchanged** and **private keys are kept secret**.
- In addition to its use for key exchange, public key cryptography is used to create digital signatures.

Key Exchange

- Public/private key pairs can be used to exchange session keys.
- each party that needs to exchange keys generates a key pair.
- The public keys are either exchanged among the parties or kept in a database.
- The private keys are kept secret.

Public Key Infrastructure

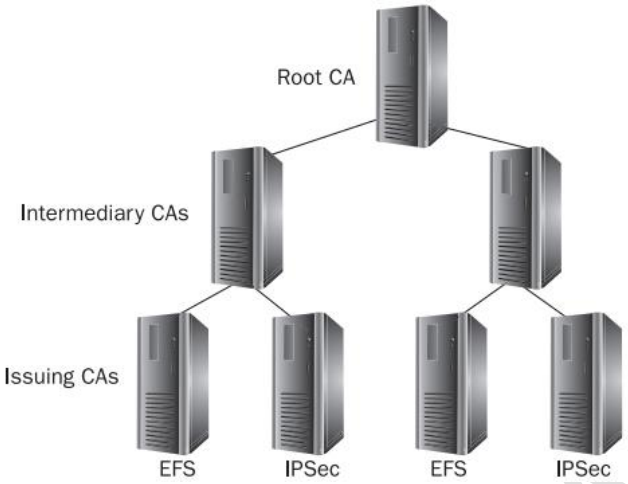
- Public Key Infrastructure (PKI) has become one of the most prevalent forms of encryption in modern electronic transactions.
- An associated key pair is bound to a security principal (user or computer) by a **certificate**. The certificate also makes the security principal's public key available, while the related private key is kept hidden.
- A certificate authority (CA) issues, catalogs, renews, and revokes certificates under the management of a policy and administrative control.

Structure and Function

- Multiple CAs can be arranged in a hierarchy for security, redundancy, and geographical and functional diversity.

CA Hierarchy

- one root CA provides CA certificates for another level of CAs. While there are many hierarchical designs that can be arranged, the classic, best practice design is displayed



Certificate Templates and Enrollment

- CAs integrated with Active Directory, called Enterprise CAs, issue many different types of **certificates, based on built-in certificate templates**. **Enrollment can be automatic, manual** with automatic issuance, or manual and approved by a CA Administrator.

Revocation

- Certificates do a have **a validity period**, or time during which they may be used, and any certificate-aware application should be designed to check this time frame before approving use of the certificate. Nevertheless, **keys might be compromised**, and **users leave the company**—what then? A certificate can be revoked

Role Separation

- Each user and administrator of certificate services plays a role.
- Specific CA roles are CA Administrator and CA Manager.
- The CA Administrator manages the CA
- CA Manager manages certificates.

Cross-Certification

- Just as multiple Windows domains or forests can inadvertently multiply within an organization, so can multiple CA hierarchies be created.
- If **this is the case and trust between the hierarchies** is required or if you need to establish trust between two hierarchies belonging to different organizations, Windows Server 2003 or higher CA hierarchies can cross-certify with other Windows Server 2003 or higher CA hierarchies and some third-party product CA hierarchies.

Storage Security

Storage Security Evolution

- **3.5-inch floppy disk drives**
- next generation of storage devices**, compact discs (CDs) and digital video discs (DVDs)**

- **Flash drives** (USB sticks and the like) have exploded in popularity
- many organizations try to ban their use, but everybody has one—so policies prohibiting these devices are hard to enforce outside of controlling the USB ports on every computer in the environment.
- They are prone to both malware and girlfriend exploits, in the same way floppies were—even more so, in the age of **"autorun" (automatic execution of any code that is on the device, immediately upon connecting it)**
- Flash drives are a significant source of malware infections in many environments.
- **Portable hard drives**, like flash drives, are cheap and plentiful. With their large storage capacities, they carry all the same threats.
- The newest form of portable storage is the **solid-state drive (SSD).** SSD devices combine the best features of flash drives and portable hard drives

Modern Storage Security

- Modern storage solutions have moved away from the endpoint computers to the network.
- Network-attached storage (NAS) and storage area networks (SANs) consist of large hard drive arrays with a controller that serves up their contents on the network.
- **NAS** can be **accessed by** most computers and other **devices on the network**
- **SAN is typically used by servers.**

Storage Infrastructure

- Storage infrastructure can often be found on a dedicated LAN, with servers, arrays, and NAS appliances
- Storage can also be located in multiple sites, including geographically diverse regional distributions, and even third-party and Internet locations
- In securing these components, you must take into account three primary categories:
    - **Storage networks**
        - Separation of duties should be applied within the storage infrastructure. Since all storage devices are connected physically, either over a network or through a storage connection protocol, separating access to the physical servers prevents a storage administrator from connecting a rogue server into the environment and then provisioning it access to restricted logical unit numbers (LUNs). A LUN is the mechanism an array uses to present its storage to a host operating system.
        - Isolating data traffic between LUNs via the switch is accomplished through the use of zoning—comparable to virtual LANs (VLANs) in the network world. Zoning creates a protected zone where only identified devices within that zone are allowed to communicate with each other.
        - When a storage administrator configures zoning for the infrastructure, there are two types of zoning to choose from: port zoning and World Wide Name (WWN) zoning.
            - **Port Zoning** The most notable characteristic of port zoning is that the accessibility of the host to the LUNs is defined by the switch port. The

advantage to zoning in this manner is that an intruder cannot connect a host to the switch

- **WWN Zoning** The alternative to port zoning, in which the zones are created relative to the ports the servers are connected to on the switch, is WWN zoning, which defines the individual zone based on the WWN ID of the host bus adapter (HBA). The WWN is very much like the MAC address of a network card.

- **Arrays**
  - When LUNs are created**, it is necessary for the array to provide a screen to prevent the data that resides on the array from being accessed by other hosts** that are able to connect to the array.
  - Storage arrays are therefore equipped with a mechanism that provides protection known as **LUN masking.**
  - **LUN masking** adds a layer of protection to the data once that data resides on the storage array
- **Servers**
  - As long as the data "rests" on the server, the potential to access that data exists. Many options are available to protect that data while it is at rest on the server.
  - The concern of the storage administrator is what happens if someone is able to access the data either locally or remotely.
  - In the worst-case scenario, an attacker may obtain access to the server and escalate his authority to attempt to read the data. In order to keep the data secure in this scenario, it is necessary to implement data encryption.

Administration Channel

- **Administration of the storage environment** should be done through a network that is **separate from the main corporate network.**
- Malware, rogue administrators, and attackers all need to rely on a corporate network to gain unauthorized access to administration functions they can exploit to compromise infrastructure

Risks to Data

- **Access by an Unauthorized System**
  - Suppose you have removed a disk from a server and placed it on another server—what happens to the file protection that was put in place by the original system? The disk is now owned by the new OS, and, as administrator or root of this rogue system, you can now change permissions and access the data.
- **Access by Unauthorized Person**
  - All data that is controlled by a server is at risk of the authorization mechanisms of the system itself being compromised and thereby exposing the data to an attacker.

Risk Remediation

- **Confidentiality Risks**

	Defense	**Detection**	**Deterrence**	**Residual risks**

Data Leakage, Theft, Exposure, Forwarding	block inappropriate data access	monitoring software to track data flow	Establish security policies	moves data around in an untraceable manner
Espionage, Packet Sniffing, Packet Replay	Encrypt data	keep track of data access	employ contract	Data can be stolen from the network
Inappropriate Administrator Access	Reduce the number of administrators	administrative access logs	Establish security policies	Because administrators have full control, they can abuse their access privileges either intentionally or accidentally
Storage Persistence after destroying	disk wiping or file shredding	isn't much that can be done	Establish data-wiping requirements before selecting a storage product	Data can remain on physical media long after it is thought to have been deleted.
Storage Platform Attacks	strong compartmentalization and role-based access control	Implement an IDS	Employ strong legal representation	Data can be stolen directly from the SAN, and you may find out about it after the fact or not at all.
Misuse of Data	Block the ability to send e-mail	Use watermarking	Employ a strict security policy	People can find ways around controls

- **Integrity Risks**

	Defense	**Detection**	**Deterrence**	**Residual risks**
Malfunctions	select has appropriate RAID	integrity verification software	isn't much that can be done	Technology failures that damage data may result in operational or compliance risk
Data Deletion and Data Loss	stored and housed in more than one location	Maintain and review audit logs	educational and awareness programs	Once critical data is gone, if it can't be restored, it is gone forever.
Data Corruption and Data Tampering	Utilize version control software to maintain archive copies	Use integrity-checking software	Maintain educational and awareness programs	Corrupted or damaged data can cause significant issues

Accidental Modification	Utilize version control software to maintain archive copies	Use integrity-checking software	Maintain educational and awareness programs	Corrupted or damaged data can cause significant issues

- **Availability Risks**

	Defense	**Detection**	**Deterrence**	**Residual risks**
Denial of Service	Implement firewalls	intrusion detection systems	Work with your legal department	they can be hard to track
Outage (unreachability)	employ a solid disaster recovery plan	Employ monitoring tools	little can be done to stop them from happening.	switch over to the disaster recovery environment.
Instability and Application Failure	all software updates are applied	Implement service monitoring	contracts with storage suppliers	little can be done to stop them from happening
Slowness	redundant storage system	Monitor response time of applications	Establish contract language with storage manufacturers	loss of efficiency and effective downtime

Best Practices

- **Zoning**
  - Port-based zoning improves security through control of the connections between hosts and the storage array.
- **Arrays**
  - Arrays have been developed over time to provide LUN masking as a form of protecting LUNs from access by unauthorized servers.
- **Servers**
  - must ensure that the server environment itself is controlled and monitored.
  - It is important that servers be configured securely, and that the equipment is located in a secure facility with access control and monitoring.
- **Staff**
  - When hiring individuals to manage and secure the storage environment, the requisite skill set should include solid knowledge of storage security practices.
- **Offsite Data Storage**
  - Storing data offsite (securely) is a critical aspect of any organization's business continuity process.

Database Security

General Database Security Concepts

- Modern databases must meet different goals. They must be reliable, provide for quick access to information, and provide advanced features for data storage and analysis.
- Architecturally, relational databases function in a client-server manner (although they can certainly be used as part of multitier applications)
- **Databases can be used in various capacities, including:**
    - **Application support** Ranging from simple employee lists to enterprise-level tracking software
    - **Secure storage of sensitive information** Relational databases offer one of the most secure methods of centrally storing important data.
    - **Online transaction processing (OLTP)** OLTP services are often the most common functions of databases in many organizations. These systems are responsible for receiving and storing information that is accessed by client applications and other servers
    - **Data warehousing** Many organizations go to great lengths to collect and store as much information as possible.

Understanding Database Security Layers

relational databases can support a wide array of different types of applications and usage patents, they generally utilize security at multiple layers.

Server-Level Security

- very important to physically protect databases in order to prevent unauthorized users from accessing database files and data backups.
- If an unauthorized user can get physical access to your servers, it's much more difficult to protect against further breaches.

Network-Level Security

- Databases are designed as network applications, you must take reasonable steps to ensure that only specific clients can access these machines.
- "best practices" for securing databases include limiting the networks and/or network addresses that have direct access to the computer.
- Another security practice involves changing the default port on which the server listens.(eg : 80 port to 81 port)

Data Encryption

- modern databases support encrypted connections between the client and the server
- Data encryption is also an important security feature in areas outside of the network layer. Often, database administrators will make backups of their data and store them on file servers.
- data encryption can be effectively used *within* a database. Many types of systems store sensitive data, such as credit card numbers and passwords.
- potential problem lies in the fact that database developers and administrators often require full permissions on these tables in order to do their jobs. One way to obscure this data is to encrypt values that are stored in database tables.

Operating System Security

- On most platforms, database security goes hand in hand with operating system security. Network configuration settings, file system permissions, authentication mechanisms, and operating system encryption features can all play a role in ensuring that databases remain secure.
- Windows-based operating systems, only the NTFS file system offers any level of file system security.

Managing Database Logins

- Most database systems require users to enter some authentication information before they can access a database.
- many relational database products that operate on Microsoft's Windows operating system platform can utilize the security features of a domain-based security model.
- organizations are increasingly turning to biometric-based authentication (authentication through the use of fingerprint identification, retinal scans, and related methods), as well as smart-card and token-based authentication.
- integrated security is highly recommended, both for ease of use and for ease of management.
- systems administrators can start and stop the services and can move or delete database files.

Database Roles and Permissions

- In order to actually access a database, the user's login must be authorized to use it.
- Generally, database administrators will create "groups" or "roles," and each of these will contain users.
- a database administrator might create a role that allows Sales Staff to insert and update data in a specific table. Users of this role might also be able to call certain stored procedures, views, and other database objects.
- Another role might be created for Sales Managers. This role may be provided with the ability to delete sales-related data and make other changes within the database.
- Through the use of roles, database administrators can easily control which users have which permissions.

Object-Level Security

- Tables, however, are the fundamental unit of data storage. Each table is generally designed to refer to some type of entity (such as an Employee, a Customer, or an Order). Columns within these tables store
- details about each of these items (FirstName or CustomerNumber are common examples).
- Permissions are granted to execute one or more of the most commonly used **SQL commands.** These commands are
    - **SELECT** Retrieves information from databases. SELECT statements can obtain and combine data from many different tables, and can also be used for performing complex aggregate calculations.
    - **INSERT** Adds a new row to a table.
    - **UPDATE** Changes the values in an existing row or rows.
    - **DELETE** Deletes rows from a table.
- The ANSI Standard SQL language provides for the ability to use three commands for administering permissions to tables and other database objects:
    - **GRANT** Specifies that a particular user or role will have access to perform a specific action.
    - **REVOKE** Removes any current permissions settings for the specified users or roles.
    - **DENY** Prevents a user or role from performing a specific action.

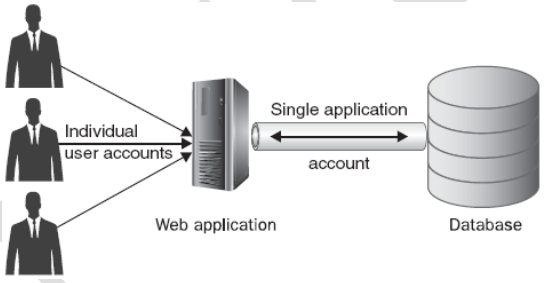
Using Other Database Objects for Security

- high-level look at the three commonly used database objects and how they can be used to better manage security settings.
- **Views**
    - Views are generally defined simply as the result of a SELECT query. This query, in turn, can pull information from many different tables and can also perform common calculations on the data.

- **Stored Procedures**
  - databases offer developers the ability to create and reuse SQL code through the use of objects called *stored procedures*. Stored procedures can be used to perform any function that is possible through the use of standard SQL commands.
- **Triggers**
  - Triggers are designed to automatically be "fired" whenever specification actions take place within a database.

Using Application Security

- To implement this type of functionality using database-level permissions settings, in the real world, this process can be difficult to implement and maintain.
- For these reasons, many modern database systems implement what is generally known as *application-level security*. In this method, a single database account is used by an application. This account provides the application with access to all of the databases, information, and operations that might be required by any users of the application.
- Application security allows you to limit the number of database accounts and thus, by limiting the number of actual accounts that have database access, limit your exposure to external hacking attempts.
- Large and complex database applications often enforce their own security based on business rules that are stored and enforced within the application itself.



- **Limitations of Application-Level Security**
  - You should also keep in mind that any defects or vulnerabilities in the application could easily translate into a security breach—users could access and modify without proper authorization.
  - The second major concern related to application-level security is that it does not provide any type of protection for users that can bypass the application.
- **Supporting Internet Applications**
  - A common network configuration for Internet-based applications is to prevent direct access to the databases from all but the most trusted servers (or, sometimes, networks).
  - A potential point of weakness in this setup is that the overall strength of the security is dependent on the safety of the web servers.
  - First, web- and standard-client applications often use a "**connection string**" to store authentication information. For administration purposes, this information is often stored in configuration files that can be modified, as needed. It's important to ensure that these files are properly protected (through the use of encryption and file system permissions) to prevent the usability of this information in the case that it is compromised.

- If someone has a database connection string, they will generally be able to use it to gain full access to your databases.
- Better yet, the use of authentication mechanisms that are integrated with the operating system (such as Windows Authentication in the Microsoft world) can help reduce or eliminate this potential problem.

Database Backup and Recovery

- An integral part of any overall database security strategy should be providing for database backup and recovery.
- Backups serve many different purposes. Most often, it seems that systems administrators perform backups to protect information in the case of server hardware failures.
- The real challenge is in determining what backup strategies apply to your own environment.
- First, resources such as storage space, network bandwidth, processing time, and local disk I/O bandwidth are almost always limited
- So, how do you decide what to protect? One method is to classify the importance of the relative types of information you need to protect.

high-level data protection requirements

Resource	Importance	Notes
OLTP server	Critical	Information can't be easily re-created, and data loss will lead to inaccurate or misleading reports.
E-mail server	High	Recovering lost messages and user mailboxes is very difficult.
Decision-support server (data warehouse)	Medium	Information can be regenerated from other sources.
Intranet web server	Medium	Content is important, but is replicated among multiple machines as part of development processes.

A Sample Categorization of Data Based on Importance

- **Determining Backup Constraints**
  - Once you have a reasonable idea of what your organization needs to back up, it's time to think about ways in which you can implement a data protection strategy. It is of critical importance that you define your business requirements before you look at the technical requirements for any kind of data protection solution.
- **Determining Recovery Requirements**
  - It's important to keep in mind that the purpose of data protection is not to create backups. The real purpose is to provide the ability to recover information, in case it is lost.
  - The question they should ask is the following: "If we lose data due to failure or corruption, how long will it take to get it back?"

Machine	Amount of Data (est.)	Backup Window	Acceptable Downtime	Acceptable Data Loss	Other Requirements
Server 1 (file/ print services)	14GB	>12 hours	1 day	1 day	General file/ print server
Server 2 (file services)	>17GB	>6 hours	3 hours	4 hours	Engineering file server

SQL Server 1 (sales OLTP)	>6GB	>12 hours	30 minutes	1 hour	Sales order entry; must support point-in-time recovery
Shipping server	>17.5GB	>2 hours	5 minutes	None	Must remain online at all times; transactions cannot be lost

Sample Data Protection Requirements Worksheet Based on Business Requirements

- **Types of Database Backups**
  - **Full backups** This type of backup consists of making a complete copy of all of the data in a database.
  - **Differential backups** This type of backup consists of copying all of the data that has changed since the last full backup. Since differential backups contain only changes
  - **Transaction log backups** Relational database systems are designed to support multiple concurrent updates to data. In order to manage contention and to ensure that all users see data that is consistent to a specific point in time, data modifications are first written to a transaction log file.

Keeping Your Servers Up to Date

- In order to ensure that known vulnerabilities and server problems are repaired, you must apply the latest security and application patches.
- you should always review available updates and find out if the servers you manage have problems that are potentially solved by an update
- If so, plan to install the updates as soon as you can test and deploy them.

Database Auditing and Monitoring

- The idea of accountability is an important one when it comes to network and database security. The process of auditing involves keeping a log of data modifications and permissions usage.
- users that are attempting to overstep their security permissions (or users that are unauthorized altogether) can be detected and dealt with before significant damage is done.
- There's another benefit to implementing auditing: when users know that certain actions are being tracked, they might be less likely to attempt to snoop around your databases.
- In many cases, auditing too much information can decrease system performance. Also, audit logs can take up significant disk space.
- At a minimum, most database administrators should configure logging of both successful and failed database login attempts.
- **Reviewing Audit Logs**
  - In order for auditing to be truly useful, systems and database administrators should regularly review the data that has been collected. It is only through this activity that potential problems in security settings can be detected before they get worse.
  - The challenge with reviewing audit logs is in determining what information is useful. Unfortunately, there's no simple method that will work for all situations.
- **Database Monitoring**
  - Although auditing can provide an excellent way to track detailed actions, sometimes you just want to get a quick snapshot of who's using the server and for what purpose.
  - By establishing a performance and usage baseline, you will be able to quickly identify any potential misuse of the system. For example, using the Windows Performance Toolkit

(WPT) that is part of Microsoft's server-side operating systems, you can track many statistics related to database usage.

UNIT 3

Secure Network Design

Design of the network plays an integral role in an organization's ability to effectively manage and secure access to its data the boundary between an organization's network and the Internet or a peered network, much akin to a parcel property line, is known as an *electronic security perimeter (ESP)*.
Design of the network will play an integral role both in defining those electronic boundaries and in enabling an organization to effectively protect, manage, a secure access to information assets within that perimeter.

Introduction to Secure Network Design

All information systems create risks to an organization, and whether or not the level of risk introduced is acceptable is ultimately a business decision. Controls such as firewalls resource isolation, hardened system configurations, authentication and access control systems, and encryption can be used to help mitigate identified risks to acceptable levels.

Acceptable Risk

- Acceptable level of risk depends on the individual organization and its ability to tolerate risk Management's risk tolerance is expressed through the policies, procedures, and guidelines issued to the staff.

Designing Security into a Network

- Security is often an overlooked aspect of network design, and attempts at retrofitting security on top of an existing network can be expensive and difficult to implement properly. Influences on network design include budgets, availability requirements, the network's size and scope, future growth expectations, capacity requirements, and management's tolerance of risks.

Network Design Models

- Essential elements can be translated into network design, such as using firewalls and authentication systems for controlling traffic movement around the network, using the network to segregate traffic of differing sensitivity levels, and using monitoring systems to detect unauthorized activities.

Designing an Appropriate Network

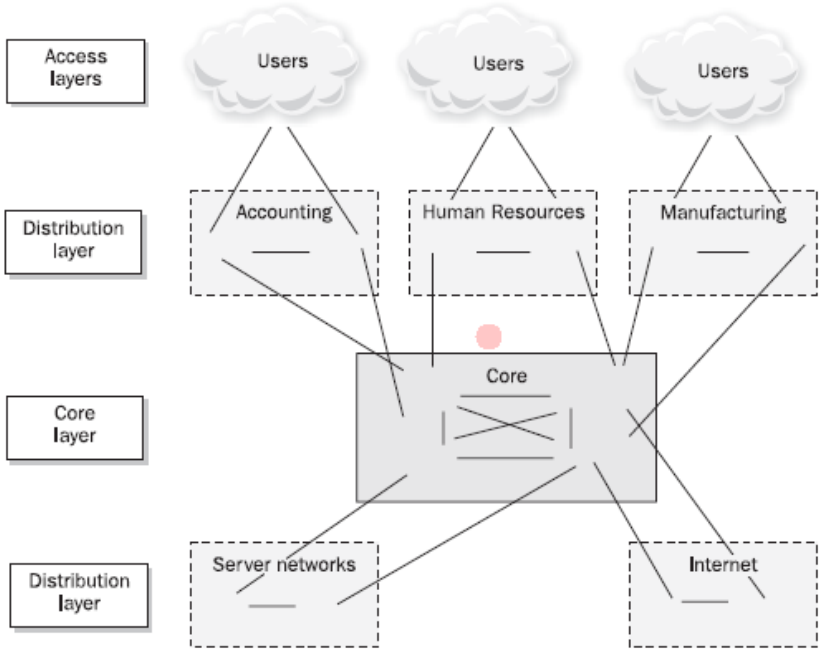
- To design and maintain a network that supports the needs of its users, network architects and engineers must have a solid understanding of what those needs are.
- The best way to do this is to involve those architects and engineers in the application development process. By getting involved early in the development cycle, engineers can suggest more secure designs and topologies, and additionally can assure the project team that they have a clear understanding of the security considerations and capabilities.
- It is important to understand their expectations and needs with regard to performance, security, availability, budget, and the overall importance of the new project.

The Cost of Security

- Security control mechanisms have expenses associated with their purchase, deployment, and maintenance, and implementing these systems in a redundant fashion can increase costs significantly.

Performance

- When determining the appropriate network technology, be sure that it can meet the bandwidth requirements projected for three to five years in the future. Otherwise, expensive replacements or upgrades may be required.
- Applications and networks that have low tolerance for latency, such as those supporting video and voice streaming, will obviously require higher performance network connections and hardware.
- The Cisco Hierarchical Internetworking model, uses three main layers commonly referred to as the core, distribution, and access layers:
- **Core layer** Forms the network backbone and is focused on moving data as fast as possible between distribution layers. Because performance is the core layer's primary focus, it should not be used to perform CPU-intensive operations such as filtering, compressing, encrypting, or translating network addresses for traffic.
- **Distribution layer** Sits between the core and the access layer. This layer is used to aggregate access-layer traffic for transmission into and out of the core.
- **Access layer** Composed of the user networking connections.



Availability

- Network availability requires that systems are appropriately resilient and available to users on a timely basis (meaning, when users require them). The opposite of availability is denial of service, which is when users cannot access the resources they need on a timely basis.
- Depending on the specific business and risk factors, redundancy often increases both cost and complexity. Determining the right level of availability and redundancy is an important design element, which is best influenced by a balance between business requirements and resource availability.
- Designers can and should consider maintaining multiple Internet links to different Internet service providers to insulate an organization from problems at any one provider.

- A true high-availability design will incorporate redundant hardware components at the switch, network, firewall, and application levels. When eliminating failure points, be sure to consider all possible components.

Security

- Each element on a network performs different functions and contains data of differing security requirements. Some devices contain highly sensitive information that could damage an organization if disseminated to unauthorized individuals, such as payroll records, internal memorandums, customer lists, and even internal job-costing documents.
- When designing and implementing security in network and system architectures, it is helpful to identify critical security controls and understand the consequences of a failure in those controls.
- Perimeter security is only as strong as its weakest link. Without adequate security on each external connection, the security of the internal network becomes dependent on the security of these other connected networks.
- Strong security will ensure that these connections cannot be used as a back door into the internal network.

Wireless Impact on the Perimeter

- Network perimeter security is only useful if there are adequate physical security controls to prevent an unauthorized user from simply walking up to and plugging into the internal network.
- Organizations that deploy wireless solutions must recognize and mitigate risks associated with an unauthorized individual gaining connectivity to the corporate LAN via wireless signal leakage outside of the corporate-controlled premises.
- In addition to signal-leakage problems, flaws have been discovered in the encryption mechanisms used to protect wireless traffic. Thus, wireless networks are at significant risk for having network communications intercepted and monitored by unauthorized parties.
- Administrators have augmented wireless control mechanisms with VPN solutions to provide strong authentication and encryption of wireless traffic to achieve appropriate levels of security for wireless data and for accessing internal resources.

Remote Access Considerations

- Most corporate networks permit user access to internal resources from remote locations. While some corporations still maintain dial-up access as a backup or secondary solution, remote access is now generally provided via a VPN solution.
- Despite their usefulness, VPNs have a significant impact on the corporate network perimeter. Depending on how they are configured, VPNs can enable remote workstations to connect as if they were physically connected to the local network, though they remain outside the protection of the corporate security infrastructure.

Internal Security Practices

- Organizations that deploy firewalls strictly around the perimeter of their network leave themselves vulnerable to internally initiated attacks, which are statistically the most common threats today.
- When designing internal network zones, if there is no reason for two particular networks to communicate, explicitly configure the network to block traffic between those networks, and log any attempts that hosts make to communicate between them.

  Intranets

- The main purpose of an *intranet* is to provide internal users with access to applications and information. Intranets are used to house internal applications that are not generally available to external entities, such as time and expense systems, knowledge bases, and organization bulletin boards.
- An organization may want to provide public Internet access to certain systems. For example, for an organization to receive Internet e-mail, the e-mail server must be made available to the Internet.
- Because these systems are publicly accessible, they can and will come under attack from malicious users. By housing them on a segregated network, a successful attack against these systems still leaves a firewall between the successful attacker and more sensitive internal resources.

Extranets

- Extranets are application networks that are controlled by an organization and made available to trusted external parties, such as suppliers, vendors, partners, and customers.

DMZ Networks and Screened Subnets

Outbound Filtering

- Failure to restrict outbound access creates a number of significant risks to the corporation and its infrastructure, such as users accessing services that do not comply with corporate security policies or that do not have legitimate business purposes.

Web Access Considerations

- Web filtering today can be handled via a variety of specialized products and appliances, including some cloud-based offerings the use of a proxy service gives a corporation several additional options when controlling user traffic.
- A proxy server can also log, record, and report on user Internet usage, which can deter employees from wasting their days browsing web sites or visiting web sites not appropriate or relevant to their job function

Network Device Security

How to use routers and switches to increase the security of the network. Routers and switches have been managed by using a command-line interface (CLI), but interfaces have evolved over time toward graphical configuration solutions. CLIs are still available, but *web user interfaces (web UIs)* have become ubiquitous and are the most commonly used configuration tools these days "all-in-one" devices such as *unified threat management (UTM)* platforms (firewalls combined with network antivirus, web filtering, application network communication control, IPS, and other network-oriented security functions, often bundled into switches both large and consumer sized).

Switch and Router Basics

TCP/IP provides all the necessary components and mechanisms to transmit data between two computers over a network

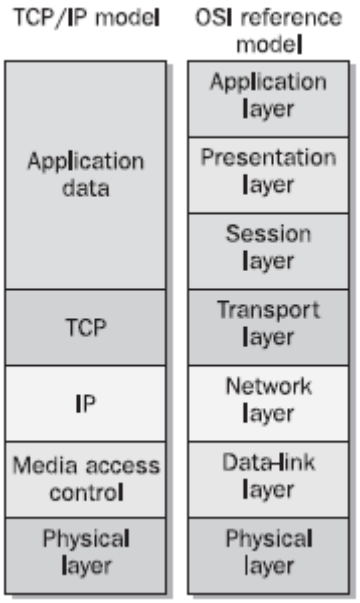
MAC Addresses, IP Addresses, and ARP

- Each device on a network actually has two network-related addresses: a layer two address known as the *Media Access Control (MAC) address* (also known as the *hardware address* or *physical address*), and a layer three address known as the *IP address*.

- To send traffic, a device must have the destination device's IP address as well as a MAC address. Knowing the destination device's host name, the sending device can obtain the destination device's IP address using protocols such as *Domain Name Service (DNS)*. To ascertain a MAC address, the host uses the *Address Resolution Protocol (ARP)* note that no authentication or verification is done for any ARP replies that are received. This facilitates an attack known as *ARP poisoning*

TCP/IP

- The fundamental purpose of TCP/IP is to provide computers with a method of transmitting data from one computer to another over a network. The purpose of a firewall is to control the passage of TCP/IP packets between hosts and networks.
- In actuality, TCP/IP is a suite of protocols and applications that perform discrete functions corresponding to specific layers of the Open Systems Interconnection (OSI) model.



Ports and TCP/IP

- To enable communications within the TCP/IP stack and to facilitate connections between two hosts, most well-known services are run on universally known ports.
- Firewalls base some or all of their access control decisions on the port information contained within packet headers. Without universally known ports, providers of services would need to inform each of heir users of the proper ports to use. For example, port 80 is the well-known port for HTTP, and almost all web servers on the Internet are configured to service HTTP requests on port 80.
- The source port is normally assigned semi-randomly by the TCP (or UDP) process on the source host

Hubs

- Hubs were dumb devices used to solve the most basic connectivity issue: how to connect more than two devices together. They transmitted packets between devices connected to them, and they functioned by retransmitting each and every packet received on one

port out through all of its other ports without storing or remembering any information about the hosts connected to them.

- This created scalability problems for legacy half-duplex Ethernet networks, because as the number of connected devices and volume of network communications increased, collisions became more frequent, degrading performance.
- Although most modern "hubs" offer 100-Mbps full-duplex or gigabit connectivity (there are no half-duplex connections in gigabit networks hub still cannot address the scaling problem of a single broadcast domain. For that reason, hubs are rarely used.

Switches

- Switches were developed to overcome the historical performance shortcomings of hubs. Switches are more intelligent devices that learn the various MAC addresses of connected devices and transmit packets only to the devices they are specifically addressed to. Since each packet is not rebroadcast to every connected device, the likelihood that two packets will collide is significantly reduced.
- To reduce a network's exposure to ARP poisoning attacks, segregate sensitive hosts between layer three devices or use *virtual LAN (VLAN)* functionality on switches. For highly sensitive hosts, administrators may wish to statically define important MAC entries, such as the default gateway.

Routers

- Routers operate at layer three, the network layer of the OSI model, and the dominant layer three protocol in use today is Internet Protocol version 4 (IPv4). Routers are primarily used to move traffic between different networks, as well as between different sections of the same network. Routers learn the locations of various networks in two different ways: dynamically via routing protocols and manually via administratively defined static routes.
- Rogue or malicious routes in the network can disrupt normal communications or cause confidential information to be rerouted to unauthorized parties. While a number of routing protocols, such a Routing Information Protocol version 2 (RIPv2), Open Shortest Path First (OSPF), and the Border Gateway Protocol (BGP), can perform authentication, a common method is to disable or filter routing protocol updates on necessary router interfaces.

Routing Protocols

- *Distance-vector protocols* are more simplistic, are better suited for smaller networks (less than 15 routers), and require less CPU power on the devices that run them. Distance-vector protocols maintain tables of distances to other networks. Distance is measured in terms of *hops*, with each additional router that a packet must pass through being considered a hop. The most popular distance-vector protocol is the Routing Information Protocol (RIP).
- *Link-state protocols* were developed to address the specific needs of larger networks. Link state protocols use several different metrics to determine the best route to another network, and they maintain maps of the entire network that enable them to determine alternative and parallel routing paths to remote networks. Open Shortest Path First (OSPF) and Intermediate System to Intermediate System (IS-IS) are examples of link-state protocols.

Network Hardening

The more steps and time you take to patch and harden a device, the more secure it will be.

Patching

- Patches and updates released by the product vendor should be applied in a timely manner.
- Quick identification of potential problems and installation of patches to address newly discovered security vulnerabilities can make the difference between a minor inconvenience
  and a major security incident.

Switch Security Practices

- Network nodes are not directly aware that switches handle the traffic they send and receive, effectively making switches the silent workhorse of a network.
- Other than sometimes offering an administrative interface, layer two switches do not maintain layer three IP addresses, so hosts cannot send traffic to them directly.
- MAC addresses are unique for every network interface card, and switches can be configured to allow only specific MAC addresses to send traffic through a specific port on the switch.
- Switches can also be used to create *virtual local area networks (VLANs)*, layer two broadcast domains that are used to further segment LANs.

Access Control Lists

- Routers have the ability to perform IP packet filtering Access control lists (ACLs) can be configured to permit or deny TCP, UDP, or other types of traffic based on the source or destination address, or both, as well as on other criteria such as the TCP or UDP port numbers contained in a packet.
- Additionally, ACLs are often used to protect the router itself, and for other more advanced functions. It is a best practice to use an ACL to allow only the management stations or hosts on a network used by administrative staff authorized to log in to the network devices to connect to the administrative services (such as Telnet, SSH, or HTTP) on a router.

Disabling Unused Services

- Routers run services that are not required for the process of routing packets. Taking steps to disable and protect such services can increase the overall security of the network.

Proxy ARP

- Proxy ARP allows one host to respond to ARP requests on behalf of the real host. This is commonly used on a firewall that is proxying traffic for protected hosts.

Network Discovery Protocols

- Opportunity for anyone sniffing the network to learn a significant amount of information about the network topology. These protocols are not actively used, they should be disabled, and if they are used, careful attention should be paid to securing them as much as possible.

Other Extraneous Services

- All routers provide a number of services that can be disabled if they are not needed.
- **Diagnostic Services: -** Most routers have a number of diagnostic services enabled for certain UDP and TCP services, including echo, charge, and discard. These services should be disabled when not in use for troubleshooting or testing.

- **BOOTP Server: -** Routers can be used to provide DHCP addresses to clients through the BOOTP service.
- **TFTP Server: -** the Trivial File Transfer Protocol (TFTP) server can be used to simply transfer configuration files and software upgrades to and from the router.
- **Finger Server: -** The finger service can be queried to see who is logged in to the router and from where.
- **Web Server: -** Many vendors provide a web server for making configuration changes. If the router will not be managed in this manner, the web server can be disabled.

Administrative Practices

- SSH is recommended, as Telnet is sent over the network in clear text a web interface can be accessed via a browser, or the router can be monitored and managed via the Simple Network Management Protocol (SNMP)
- Securing each of these management protocols is of paramount importance, so they cannot be abused by attackers.
- Another important step when hardening network devices is to configure a banner that is displayed whenever a connection is established as part of the login process, often called a login banner or message-of-the-day (MOTD) banner.

Remote Command Line

- A more secure alternative, most routers support the Secure Shell (SSH) protocol. SSH provides the same interface and access as Telnet, but it encrypts all communications.
- Many network devices maintain one password to access the device and a second password to access configuration commands, commonly called “privileged” or “enable” access.

Centralizing Account Management (AAA)

- In large-scale environments, it is cumbersome to synchronize and maintain individual user accounts on each network switch, router, and device. While it is possible to automate and simplify local account management through scripting or tools, most network devices can be configured to authenticate against a central account repository via authentication, authorization, and accounting (AAA).
- *Authentication* is the component that determines if an incoming connection is allowed, *authorization* determines what level of access or privilege the authenticated account is allowed, and *accounting* keep track of everything that the authenticated and authorized account does.

Simple Network Management Protocol (SNMP)

- Network devices can also be monitored and managed via Simple Network Management Protocol (SNMP), which provides a centralized mechanism for monitoring and configuration. SNMP can be used to monitor such things as link operation, port status and statistics, and CPU load via *Management Information Base Object Identifiers (MIB OIDs)*, a structured format database that describes objects within a device that can be monitored or managed by SNMP or another management protocol.
- As SNMP has evolved as a tool, and its capabilities have expanded, its security has improved. The first version, SNMPv1, was originally released in 1988, and as with many other software protocols at the time, there was little consideration for the security of the protocol itself.

- SNMPv2 addressed many of the issues with SNMPv1, including performance, but added significant complexity.
- SNMPv3, the current version, doesn't change the protocol functionally but adds the capability of encryption, message integrity, and authentication of traffic.

Internet Control Message Protocol (ICMP)

- The Internet Control Message Protocol (ICMP) provides a mechanism for reporting TCP/ IP communication problems, as well as utilities for testing IP layer connectivity. It is an invaluable tool when troubleshooting network problems.

ECHO and Traceroute

- Echo requests and replies, more commonly known as *pings*, are used to determine if another host is available and reachable across the network.
- An attacker can use ping to scan publicly accessible networks to identify available hosts, though more experienced attackers avoid ping and use more stealthy methods of host identification.

Unreachable Messages

- Another type of ICMP message is a Type 3 Destination Unreachable message. A router will return an ICMP Type 3 message when it cannot forward a packet because the destination address or service specified is unreachable.

Directed Broadcasts

- The first and last IP addresses of any given network are treated as being special. These addresses are known as the network address and the broadcast address, respectively. Sending a packet to either of these addresses is akin to sending an individual packet to each host on that network. Thus, someone who sends a single ping to the broadcast address on a subnet with 75 hosts could receive 75 replies.
- This functionality has become the basis for a genre of attacks known as *bandwidth amplification attacks*.

Redirects

- ICMP redirects are used in the normal course of network operation to inform hosts of a more efficient route to a destination network.

Anti-Spoofing and Source Routing

- Another type of attack used against networks is to insert fake or spoofed information in TCP/IP packet headers in the hopes of being taken for a more trusted host.
- In addition to spoofed packets, routers should be configured to drop packets that contain source routing information. Source routing is used to dictate the path that a packet should take through a network.

Logging

- As with any device, it is a good idea to maintain logs for routers. Routers are able to log information related to ACL activity as well as system-related information.

Firewalls

Firewalls have been one of the most popular and important tools used to secure networks since the early days of interconnected computers.

Overview

- Firewalls are the first line of defense between the internal network and untrusted networks like the Internet. You should think about firewalls in terms of what you really need to protect, so you will achieve the right level of protection for your environment.

The Evolution of Firewalls

- First-generation firewalls were simply permit/deny engines for **layer three traffic**, working much like a purposed access control list appliance.
- Second-generation firewalls were able to keep track of active network sessions, putting their functionality effectively at **layer four**. These were referred to as *stateful firewalls* or, less commonly, *circuit gateways*. capability to block *man-in-the-middle (MITM)* attacks from other IP addresses
- The third generation of firewalls ventured into the application layer—**layer seven**. These "application firewalls" were able to decode data inside network traffic streams for certain well-defined, preconfigured applications such as HTTP (the language of the web),
- DNS (the protocol for IP address lookups), and older, person-to-computer protocols such as FTP and Telnet.

Application Control

- Web-based meeting and collaboration software might be approved for use on the Internet, but the file-sharing capabilities might be restricted.
- First- and second-generation firewalls could restrict simple applications that functioned on well-known ports. Back then, applications were well behaved, communicating on assigned ports that were well documented, so they were easy to control.
- Security administrators were concerned about different types of software that could violate security policies, such as:
    - **Peer-to-peer file sharing** Direct system-to-system communication from an inside workstation to another one on the Internet
    - **Browser-based file sharing** Web sites that provide Internet file storage via a web browser, which allow trusted people inside an organization's network to copy files outside the security administrator's area of control
    - **Web mail** Mail services with the capability to add file attachments to messages, providing a path to theft and leakage of confidential materials
    - **Internet proxies and circumventors** Services running on the Internet or on local workstations explicitly designed to bypass security controls like web filtering
    - **Remote access** Remote administration tools, usually used by system administrators to support internal systems from the Internet, which could be abused by Internet attackers

When Applications Encrypt

- Applications that want to bypass firewalls may encrypt their traffic. This makes the firewall's job more difficult by rendering most of the communication unreadable.
- Blocking all encrypted traffic isn't really feasible except in highly restricted environments where security is more important than application functionality, and a "permit by exception" policy blocks all encrypted application traffic except for that on a whitelist of allowed, known applications.

Must-Have Firewall Features

Application Awareness

- The firewall must be able to process and interpret traffic at least from OSI layers three through seven. At layer three, it should be able to filter by IP address; at layer four by port; at layer five network sessions by; at layer six by

data type, and, most significantly, at layer seven to properly manage the communications between applications.

Accurate Application Fingerprinting

- The firewall should be able to correctly identify applications, not just based on their outward appearance, but by the internal contents of their network communications as well.

Granular Application Control

- The firewall also needs to be able to identify and characterize the features of applications so they can be managed appropriately.

Bandwidth Management (QoS)

- The Quality of Service (QoS) of preferred applications, which might include Voice over IP (VoIP) for example, can be managed through the firewall based on real-time network bandwidth availability.

Core Firewall Functions

Network Address Translation (NAT)

- NAT is usually implemented in a firewall separately from the policy or rule set. It is useful to remember that just because a NAT has been defined to translate addresses between one host and another, it does not mean those hosts will be able to communicate. This is controlled by the policy defined in the firewall rule set.

Static NAT

- A static NAT configuration always results in the same address translation. The host is defined with one local address and a corresponding global address in a 1:1 relationship, and they don't change. The static NAT translation rewrites the source and destination IP addresses as required for each packet as it travels through the firewall.

Dynamic NAT

- Dynamic NAT is used to map a group of inside local addresses to one or more global addresses. The global address set is usually smaller than the number of inside local addresses, and the conservation of addresses intended by RFC 1918 is accomplished by overlapping this address space.
- One advantage of dynamic NAT over static NAT is that it provides a constantly changing set of IP addresses from the perspective of an Internet-based attacker, which makes targeting individual systems difficult.

Port Address Translation

- With Port Address Translation (PAT), the entire inside local address space can be mapped to a single global address. This is done by modifying the communication port addresses in addition to the source and destination IP addresses. Thus, the firewall can use a single IP address for multiple communications by tracking which ports are associated with which sessions.
- PAT provides an increased level of security because it cannot be used for incoming connections. However, a downside to PAT is that it limits connection-oriented protocols, such as TCP.

Auditing and Logging:-Firewalls are excellent auditors. Given plenty of disk space or remote logging capabilities, they can record any traffic that passes through them. Attack attempts will

leave evidence in logs, and if administrators are watching systems diligently, attacks can be detected before they are successful.

Additional Firewall Capabilities

Application and Website Malware Execution Blocking

- If the end users were sophisticated enough to recognize the virus writers' tricks, these viruses wouldn't get very far. Modern malware can execute and spread itself without the intervention of end users. Through automatic, browser-based execution of code (via ActiveX or Java, for example), simply opening a web page can activate a virus.
- Adobe PDF files can also transmit malware, due to their extensive underlying application framework.

Antivirus

- Firewalls that are sophisticated enough to detect malware can (and should) block it on the network. Worms that try to propagate and spread themselves automatically on the network, and malware that tries to "phone home," can be stopped by the firewall, confining their reach.

Intrusion Detection and Intrusion Prevention

- Firewalls can provide IDS and IPS capabilities at the network perimeter, which can be a useful addition or substitution for standard purpose-built intrusion detection and prevention systems, especially in a layered strategy.

Web Content (URL) Filtering and Caching

- Today's firewalls are demonstrating web content filtering capabilities that rival those of purpose-built systems, so you may be able to save money by doing the filtering on the firewall—especially if it doesn't cost extra.

E-Mail (Spam) Filtering

- As with web content filtering, modern firewalls can subtract the spam from your e-mail messages before they get delivered to your mail server.

Enhance Network Performance

- Firewalls need to be able to run at "wire speed"—fast enough to avoid bottlenecking application traffic. They should be able to perform all the functions that have been enabled without impacting performance.

Firewall Design

- All communications must pass through the firewall.
- The firewall permits only traffic that is authorized.
- In a failure or overload situation, a firewall must always fail into a "deny" or closed state, under the principle that it is better to interrupt communications than to leave systems unprotected.
- The firewall must be designed and configured to withstand attacks upon itself.

Firewall Strengths and Weaknesses

- A firewall is just one component of an overall security architecture. Its strengths and weaknesses should be taken into consideration when designing network security.

Firewall Strengths

- Firewalls are excellent at enforcing security policies.
- Firewalls are used to restrict access to specific services.
- Firewalls are transparent on the network—no software is needed on end-user workstations.

- Firewalls can provide auditing.

Firewall Weaknesses

- Firewalls are only as effective as the rules they are configured to enforce.
- Firewalls cannot stop social engineering attacks or an authorized user intentionally using their access for malicious purposes.

Firewall Placement

- A firewall is usually located at the network perimeter, directly between the network and any external connections. However, additional firewall systems can be located inside the network perimeter to provide more specific protection to particular hosts with higher security requirements.

Firewall Configuration

- When building a rule set on a firewall Build rules from most to least specific. Most firewalls process their rule sets from top to bottom and stop processing once a match is made. Placing your popular rules first Or second, instead of 30th or 31st, will save the processor from going through over 30 rules for every packet.

Wireless Network Security

- The security problems of wireless networking taxed the best minds in IT for years. At conferences and exhibitions, wireless security salespeople often issued statements like this: "Wireless insecurities and threats are made possible by a new advanced technology developed in recent years to provide novel forms of mobile networking." To keep things in perspective: at that time, war driving and open wireless home networks were ever-present; today, it's common knowledge that identity theft and insecure Wi-Fi can lead to serious consequences.
- This public awareness is fortunate, as most modern smartphones have the power to intercept WEP-encrypted wireless and to crack the keys with free software in a matter of minutes.
- The first wireless local area network (LAN) was operational in 1969—four years before Ethernet's birth. In fact, this network, the *ALOHA packet radio net* deployed by the University of Hawaii, gave Bob Metcalfe from Xerox PARC an idea that led to the creation of the *CSMA/CD algorithm* used in all modern TCP/IP networks.
- securing a wireless network requires understanding how protocols and signals work—along with wireless threats and countermeasures.

Radio Frequency Security Basics

many network and IT security professionals lack essential knowledge about radio technology

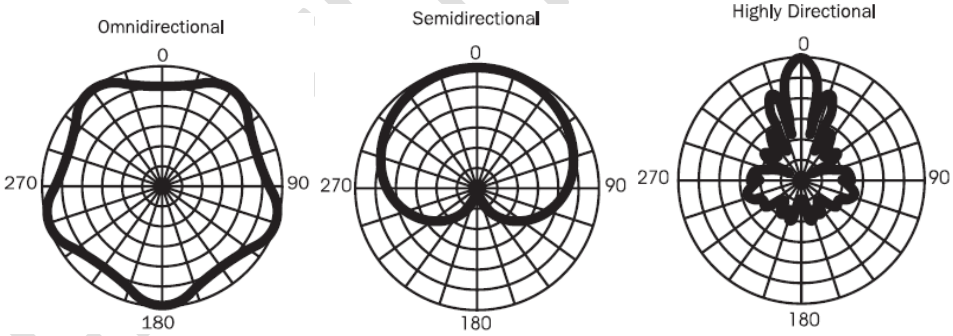
Security Benefits of RF Knowledge

- **Proper Network Design**
  - Poorly designed wireless networks are unfortunately quite common and easy for attackers to spot; they possess low resistance to attacks and tend to slow down to a standstill if network traffic overhead is increased by VPN deployment and rich content such as streaming voice and video.
- **The Principle of Least Access**
  - The WLAN must be installed and designed in such a way as to encompass your premises' territory and minimize outside signal leakage as much as possible.
- **Distinguishing Security Violations from Malfunctions**

- Is it radio interference, or has someone launched a DoS attack? Are these SYN TCP packets coming because the sending host cannot receive SYN-ACK properly, or is an attacker trying to flood your servers

- **Compliance with FCC(**Federal Communications Commission) **Regulations**
  - wireless LAN devices operate in unlicensed bands, these wireless networks can break regulations only by using inappropriately high transmission power.
- **Layer One Security Solutions**
  - tuning the transmitter's output power, choosing the right frequency, selecting the correct antennas, and positioning those antennas in the most appropriate way to provide a quality link where needed
- **Importance of Antenna Choice and Positioning**
  - A radio frequency signal is a high-frequency alternating current (AC) passed along the conductor and radiated into the air via an antenna. The emitted waves propagate away from the antenna in a straight line and form RF beams or lobes, which are dependent on antenna horizontal and vertical beam-width values. There are three generic types of antennas, which can be further divided into subtypes:

Omnidirectional	Semidirectional	Highly Directional
Mast mount omni	Patch antenna	Parabolic dish
Pillar mount omni	Panel antenna	Grid antenna
Ground plane omni	Sectorized antenna	
Ceiling mount omni	Yagi antenna	



- Yagis are frequently deployed in medium-range point-to-point bridging links, whereas highly directional antennas are used when long-range point-to-point connectivity is required. Highly directional antennas are sometimes used to blast through obstacles such as thick walls.

Controlling the Range of Your Wireless Devices via Power Output Tuning

- correct antenna positioning. Another method is to adjust the transmitter power output to suit your networking needs and not the attackers'.
- Gain is a fundamental RF term and has already been referred to several times. Gain describes an increase in RF signal amplitude
- The transmitting power output is estimated at two points on a wireless system. The first point is the *intentional radiator (IR),* which includes the transmitter and all cabling and connectors but excludes the antenna. The second point is the power actually irradiated by the antenna, or *equivalent isotropically radiated power (EIRP).*

- *Free space path loss* is the biggest cause of energy loss on a wireless network. It happens because of the radio wave front broadening and transmitted signal dispersion (think of a force decreasing when it is applied to a larger surface area).

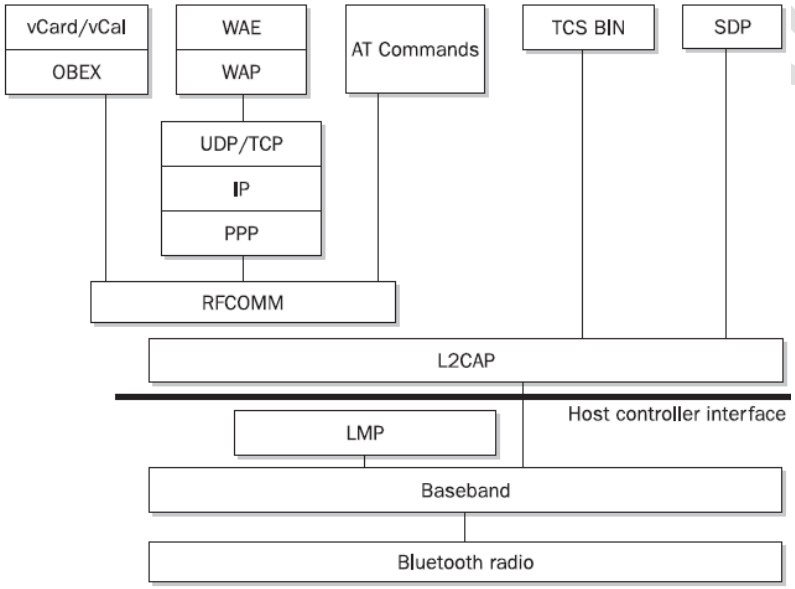
Interference, Jamming, and the Coexistence of Spread Spectrum Wireless Networks

- The basic concepts of spread spectrum communications are necessary for an understanding of interference, jamming, and the coexistence of wireless networks. Spread spectrum refers to wide-frequency low-power transmission, as opposed to narrowband transmission, which uses just enough spectrum to carry the signal and has a very large SNR.
- When the link between communicating devices is established, the two devices must agree on a variety of parameters such as communication channels. Such agreement is done via unencrypted frames sent by both parties. Anyone running a wireless sniffer can determine the characteristics of a wireless link after capturing a few management frames off the air. Thus, the only security advantage brought to civil wireless networks by implementing spread spectrum technology is the heightened resistance of these networks to interference and jamming as compared to narrowband transmission.
- There are two ways to implement spread spectrum communications:
    - Frequency hopping spread spectrum (FHSS)
        - In FHSS, a pseudorandom sequence of frequency changes (hops) is followed by all hosts participating in a wireless network
    - Direct sequence spread spectrum (DSSS)
        - DSSS combines a meaningful data signal with a high-rate pseudorandom "noise" data bit sequence, designated as processing gain or chipping code
- In Europe, 13 channels are allocated for 802.11b/g use, making access point coallocation more flexible (however, only the channels from 10 to 13 are used in France and 10 to 11 in Spain). All 14 channels can be used in Japan. Channel allocation has high relevance to the much-discussed issue of *rogue access points.*
- **There are various definitions for a "rogue access point" and, therefore, different ways of dealing with the problem:**
    - **Access points and bridges that belong to neighboring LANs and interfere with your LAN by operating on the same or overlapping channels**
        - Ensure your data is encrypted, and an authentication mechanism is in place
    - **Access points, bridges, USB adapters, and other wireless devices installed by users without permission from enterprise IT management**
        - strictly defined ban on unauthorized wireless devices
    - **Access points or other wireless devices installed by intruders to provide a back channel into the corporate LAN, effectively bypassing egress filtering on the firewall**
        - Investigate if someone has seen the potential intruder and check the information provided

<u>Data-Link Layer Wireless Security Features, Flaws, and Threats</u>

- **802.11 and 802.15 Data-Link Layer in a Nutshell**
    - layer two operations of commonly used wireless networks such as 802.11 LANs and Bluetooth networks
    - A wireless LAN's mode of operation is also dissimilar to that of Ethernet. Because a radio transceiver can only transmit or receive at a given time on a given frequency, all 802.11-compliant networks are half-duplex.

- wireless network clients the access point acts as a hub, making packet sniffing an easy task. Because detecting collisions on a wireless network is not possible, the Carrier Sense Media Access/Collision Avoidance (CSMA/CA) algorithm is used on wireless LANs instead of Ethernet's CSMA/ CD algorithm.
- If a wireless host loses connectivity to the network, another exchange of reassociation, request, and response frames takes place. Finally, a deauthentication frame can be sent to an undesirable host.
- MIMO, in the context of Wi-Fi, is still half-duplex, but MIMO allows a fancy way to "hide" or get around the duplex limitation by simultaneously transmitting in both directions (send and receive) on different antennas.
- Bluetooth wireless networks can function in circuit-switching (voice communications) and packet-switching (TCP/IP) modes, which can be used simultaneously. The Bluetooth stack is more complicated than its 802.11 counterparts, spanning all the OSI model layers.



- The Link Manager Protocol (LMP) is responsible for setting up the link between two Bluetooth devices.
- The Logical Link Control and Adaptation Protocol (L2CAP) is responsible for controlling the upperlayer protocols.
- RFCOMM is a cable replacement protocol that interfaces with the core Bluetooth protocols. The Service Discovery Protocol (SDP) is present so that Bluetoothenabled devices can gather information about device types, services, and service specifications to set up the connection between devices. Finally, there are a variety of application-layer protocols such as TCS BINARY and AT Commands; these are telephony control protocols that allow modem and fax services over Bluetooth.

- **802.11 and 802.15 Data-Link Layer Vulnerabilities and Threats**
  - The main problem with layer two wireless protocols is that in both 802.11 and 802.15 standards, the management frames are neither encrypted nor authenticated. Anyone can log, analyze, and transmit them without necessarily being associated with the target network.
  - the information presented by management frames is only a tiny fraction of the problem. The attacker can easily knock wireless hosts offline by sending deauthenticate and disassociate frames. Even worse, the attacker can insert his or her machine as a rogue access point by

spoofing the real access point's MAC and IP addresses, providing a different channel to associate, and then sending a disassociate frame to the target host(s).

- **Closed-System SSIDs, MAC Filtering, and Protocol Filtering**
  - *Closed-system SSID* is a feature of many higher-end wireless access points and bridges. It refers to the removal of SSID from the beacon frames and/or probe response frames, thus requiring the client hosts to have a correct SSID in order to associate. This turns SSID into a form of shared authentication password. the wireless network (**SSID**) will not broadcast.
  - MAC filtering, unlike closed-system SSID, is a common feature that practically every modern access point supports.
  - Nevertheless, MAC filtering may stop *script kiddie* (unsophisticated) attackers from associating with the network.
  - protocol filtering is less common than closed systems and MAC address filtering; it is useful only in specific situations and when it is sufficiently selective. For example, when the wireless hosts only need web and mail traffic
- **Built-in Bluetooth Network Data-Link Security and Threats**
  - Bluetooth has a well-thought-out security mechanism covering both data authentication and confidentiality.
  - Bluetooth communication channel involves five steps:
    1. An initialization key is generated by each device using the random number, BD_ADDR, and shared PIN.
    2. Authentication keys (sometimes called *link keys*) are generated by both ends.
    3. The authentication keys are exchanged using the initialization key, which is then discarded.
    4. Mutual authentication via a challenge-response scheme takes place.
    5. Encryption keys are generated from authentication keys, BD_ADDR, and a 128-bit random number.

Wireless Vulnerabilities and Mitigations

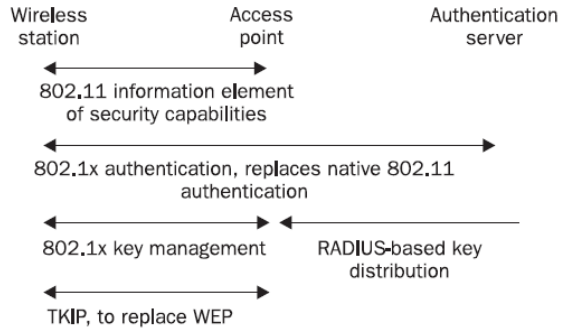
- **five types of wireless attacks**
  - **Wired Side Leakage**
    - On wireless networks, reconnaissance involves promiscuously listening for wireless packets using a wireless sniffer so the attacker can begin to develop a footprint of the wireless network.
    - When deploying wireless, you need to ensure that, like a firewall, ingress as well as egress are considered.
  - **Rogue Access Points**
    - The definition of a *rogue AP* is an unsanctioned wireless access point connected to your physical network. Any other visible AP that's not yours is simply a neighboring access point.
  - **Misconfigured Access Points**
    - Enterprise wireless LAN deployments can be riddled with misconfigurations. Human error coupled with different administrators installing the access points and switches can lead to a variety of misconfigurations.
  - **Wireless Phishing**

- users may unknowingly connect to a wireless network that they believe is the legitimate access point but that has, in fact, been set up as a honeypot or open network specifically to attract unsuspecting victims.

- **Client Isolation**
  - client isolation allows people to access the Internet and other resources provided by the access point, minus the LAN capability. When securing a Wi-Fi network, isolation is a necessity. Typically the feature is disabled by default, so ensure that it's enabled across all access points.

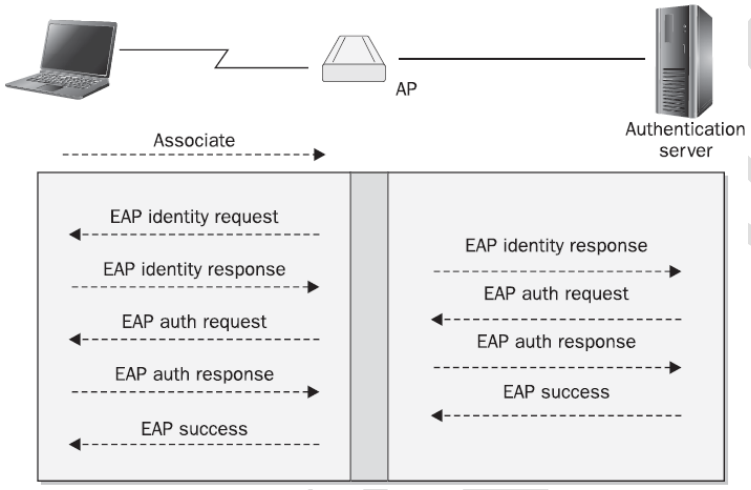
Wireless Network Hardening Practices and Recommendations

- **Wireless Security Standards**
  - 802.11i, this standard is now widely known as WPA2, which stands for Wi-Fi Protected Access version 2. WPA2 replaced WPA, which was a hybrid of the old, insecure WEP standard that was backward compatible for existing wireless infrastructures.
  - WPA used RC4 encryption, which is weaker than the AES encryption used in WPA2.
- **Temporal Key Integrity Protocol and Counter Mode with CBC-MAC Protocol**
  - The WPA2 architecture can be split on two "layers:" encryption protocols and 802.11x port-based access control protocols.
  - The Temporal Key Integrity Protocol (TKIP) and the Counter Mode with CBC-MAC Protocol (CCMP) are WPA2 encryption protocols on 802.11 LANs. TKIP encrypts each data packet with a unique encryption key. To increase key strength
  - **TKIP includes four additional algorithms:**
    1. A cryptographic message integrity check to protect packets
    2. An initialization-vector (IV) sequencing mechanism that includes hashing
    3. A per-packet key-mixing function to increase cryptographic strength
    4. A rekeying mechanism to provide key generation every 10,000 packets
- **802.1x-Based Authentication and EAP Methods**
- **802.1x**
- On wireless networks, 802.1x can also be used for the dynamic distribution of WEP keys. Because wireless LANs have no physical ports, an association between the wireless client and the access point is assumed to be a network access port. In terms of 802.1x, the wireless client is defined as a *supplicant* (or *peer*), and the access point, as an *authenticator* (similar to an Ethernet switch on wired LANs). Finally, an authentication server is needed on the wired network segment to which the access point is connected. This service is usually provided by a RADIUS server supplied with some form of user database, such as native RADIUS, LDAP, NDS, or Active Directory. Wireless gateways can implement the authentication server, as well as the authenticator functionality



802.1x/TKIP functionality

- **EAP**
  - EAP is an advanced replacement of CHAP under PPP, designed to run over local area networks (EAP over LAN [EAPOL] describes how EAP frames are encapsulated within Ethernet, Token Ring, or FDDI frames). EAP frame exchange between the supplicant, authenticator, and authentication server is summarized



- **EAP authentication process commonly implemented EAP types**
  - EAP-MD5 is the base level of EAP support by 802.1x devices. It is the first EAP type that duplicates CHAP operations.
  - EAP-TLS (Transport Layer Security) provides mutual certificate-based authentication. It is built on the SSLv3 protocol and requires deployed certificate authority
  - EAP-LEAP (Lightweight EAP or EAP-Cisco Wireless) is a Cisco-proprietary EAP type, implemented on Cisco access points and wireless clients.
  - PEAP (Protected EAP, an IETF standard) and EAP-TTLS (Tunneled Transport Layer Security are other forms of EAP. EAP-TTLS supports multiple legacy authentication methods, including PAP, CHAP, MS-CHAP, MS-CHAPv2, and EAP-MD5.

- **Wireless Intrusion Detection and Prevention**
  - suspicious events to look for on a wireless LAN include Probe requests (a good indication of someone using active scanning mode)
  - Beacon frames from unsolicited access points or ad hoc wireless clients
  - Floods of disassociate/deauthenticate frames (man-in-the-middle attack?)
  - Associated but not authenticated hosts (attempts to guess the shared key?)
  - Multiple incorrect SSIDs on closed networks (SSID brute-forcing?)
  - Frames with unsolicited and duplicated MAC addresses
  - ARP spoofing and other attacks originating from wireless LANs
- **Wireless IPS and IDS**
  - Wireless IPS identifies wireless attacks using wireless sensors. These wireless sensors typically use the same Wi-Fi radios that are found in access points, which is why many

vendors allow for dual usage of access points, both for access as well as for detecting attacks.

- The Wi-Fi protocol allows channels to be assigned to various frequencies, with one channel assigned to each frequency. In heavily congested wireless environments, using different channels (or frequencies) allows the administrator to minimize interference, which is also referred to as *co-channel interference.*

- **Bluetooth IPS**
  - Bluetooth attacks have affected many organizations but most significantly retailers. Attackers have identified ways in which to hack point of sale systems and register keypads by inserting a Bluetooth radio. Either a malicious employee or fake technician opens the point of sale system or register keypad and attaches a Bluetooth broadcasting radio to the device. As credit cards are swiped, they're simultaneously broadcast to the neighboring airspace. If the attacker is nearby, either in the store or in the parking lot, he or she simply uses a Bluetooth device to listen and receive these credit card numbers.
  - There are three classes of Bluetooth devices commonly differentiated by their range. Class 3 devices are the ones most of us are familiar with and usually include Bluetooth headsets. With a limited range of approximately 1 meter, they don't serve attackers well. Therefore, attackers commonly use Class 2 and Class 3 devices, which can be easily purchased online for under $20.

Wireless Network Positioning and Secure Gateways

- The final point to be made about wireless network hardening is related to the position of the wireless network in the overall network design topology.
- A secure wireless gateway with stateful or proxy firewalling capability must separate the wireless network from the wired LAN.
- The most common approach today is to have APs that can be connected anywhere on the LAN, but create an encrypted tunnel back to the controller and send all traffic through it before it hits the local network.
- The controller will run firewalling and IDS/IPS capabilities to check this traffic before it is exposed to the internal network.
- Higher-end specialized wireless gateways combine access point, firewalling, authentication, VPN concentrator, and user roaming support capabilities.

UNIT 4

Intrusion Detection And Prevention Systems

- Intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) are important tools in a computer security arsenal.
- An IDS can be network based or host based: a network IDS is referred to as a NIDS, whereas a host-based IDS is referred to as a HIDS. Additionally, a NIDS and HIDS can *detect* traffic of interest, or if they are further configured to prevent a specific action from happening

IDS Concepts

- *Intrusion detection (ID)* is the process of monitoring for and identifying specific malicious traffic. Most network administrators do ID all the time without realizing it.
- Security administrators areconstantly checking system and security log files for something suspicious.
- An antivirus scanner is an ID system when it checks files and disks for known malware.
- An IDS can take the form of a software program installed on an operating system, but today's commercial network-sniffing IDS/IPS typically takes the form of a hardware appliance because of performance requirements.
- When the IDS notices a possible malicious threat, called an *event,* it logs the transaction and takes appropriate action.
- If the threat is high risk, the IDS will alert the appropriate people.

Threat Types

Attacks or Misuse

- *Attacks* are unauthorized activity with malicious intent using specially crafted code or techniques.
- *Misuse* refers to unauthorized events without specially crafted code. In this case, the offending person used normally crafted traffic or requests and their implicit level of authorization to do something malicious.

Network Protocol Attacks

- Protocols are designed to perform functions, not to be secure. Malicious network protocol attacks interfere with the normal operation of the process.
- **Flag Exploits** Abnormally crafted network packets are typically used for DoS attacks on host machines, to skirt past network perimeter defenses (bypassing access control devices),to impersonate another user's session (attack on integrity), or to crash a host's IP stack(DoS).
- Malicious network traffic works by playing tricks with the legitimate format settings of the IP protocol. For instance, using a specially crafted tool, an attacker can set incompatible sequences of TCP flags, causing destination host machines to issue responses other than the normal responses, resulting in session hijacking or more typically a DoS condition.
- **Fragmentation and Reassembly Attacks** although not quite the security threat they once were, IP packets can be used in *fragmentation* attacks.
- Attacks can use fragment offset values to cause the packets to maliciously reassemble and intentionally force the reassembly of a malicious packet

Application Attacks

- Although network protocol attacks abound, most security threats exploit the host's application layer.

- Application attacks include misappropriated passwords, cross-site scripting, malicious URLs, password cracking Attempts, rootkit software, illegal data manipulation, unauthorized file access.
- **Content Obfuscation** Most IDSs look for known malicious commands or data in a network packet's data payload. A byte-by-byte comparison is done between the payload and each potential threat signature in the IDS's database. If something matches, it's flagged as an event. This is how "signature-based" IDSs work. Someone has to have the knowledge to write the "signature."
- Because byte scanning is relatively easy to do, attackers use encoding schemes to hide their malicious commands and content. *Encoding* schemes are non-plaintext character representations that eventually get converted to plaintext for processing.
- Encoding can be used to obscure text and data used to create malicious commands. Attackers employ all sorts of tricks to fool IDSs
- **Data Normalization:-**Normalization reassembles fragments into single whole packets, converts encoded characters into plain ASCII text, fixes syntax mistakes, removes extraneous characters, converts tabs to spaces, removes common hacker tricks, and does its best to convert the data into its final intended form.

Threats an IDS Cannot Detect

- If an outside hacker uses social engineering tricks to get the CEO's password, not many IDSs will notice
- If the webmaster accidentally posts a confidential document to a public directory available to the world, the IDS won't notice.
- If an attacker uses the default password of an administrative account that should have been changed right after the system was installed, few IDSs will notice.

First-Generation IDS

- First-generation IDSs focused almost exclusively on the benefit of early warning resulting from accurate detection.IDSs never get over 90 percent accuracy against a wide spectrum of real-world attack traffic.
- When an IDS misses a legitimate threat, it is called a *false negative*. Most IDS are plagued with even higher false Positive rates, however.
- IDSs have high false positive rates. A false positive is when the IDS says there is a security threat by "alerting," but the traffic is not malicious or was never intended to be malicious(benign condition).

Second-Generation IDS

- The net effect of most IDSs being fairly accurate and none being highly accurate has resulted in vendors and administrators using other IDS features for differentiation.
- *Second-generation* IDSs do that and work to simplify the administrator's life by offering a bountiful array of back-end options. They offer intuitive end-user interfaces, intrusion prevention, centralized device management, event correlation, and data analysis.
- Second-generation IDSs do more than just detect attacks—they sort them, prevent them, and attempt to add as much value as they can beyond mere detection.

IDS Types and Detection Models

- All IDSs follow one of two intrusion detection models—*anomaly* (also called *profile, behavior, heuristic,* or *statistical*) detection or *signature* (knowledge-based) detection although some systems use parts of both when it's advantageous.

Host-Based IDS

- A *host-based IDS* (HIDS) is installed on the host it is intended to monitor. The host can be a server, workstation, or any networked device (such as a printer, router, or gateway).
- A HIDS installs as a service or daemon, or it modifies the underlying operating system's kernel or application to gain first inspection authority.

Network-Based IDS (NIDS)

- *Network-based IDSs* (NIDSs) are the most popular IDSs, and they work by capturing and analyzing network packets speeding by on the wire. Unlike a HIDS, a NIDS is designed to protect more than one host. It can protect a group of computer hosts, like a server farm, or monitor an entire network.

  Packet-Level Drivers

  - Network packets are captured using a packet-level software driver bound to a network interface card. Most commercial IDSs have their own packet-level drivers and packet-sniffing software.

  Promiscuous Mode

  - If you are going to set up an IDS, make sure its network interface card has a *promiscuous mode* and is able to inspect all traffic passing by on the wire.

  Sensors for Network Segments

  - A *network segment* can be defined as a single logical packet domain. For a NIDS, this definition means that all network traffic heading to and from all computers on the same network segment can be physically monitored.
  - NIDS inspection device to which all network traffic is copied, known as a *span port,* or a traffic repeater device, known as a *sensor* or *tap*.

Anomaly-Detection (AD) Model

- If an IDS looks only at network packet headers for differences, it is called *protocol anomaly detection*
- The goal of AD is to be able to detect a wide range of malicious intrusions, including those for which no previous detection signature exists. events AD systems can monitor and trigger alerts
- Unusual user account activity
- High CPU utilization
- Inappropriate protocol use
- Unusual workstation login location

AD Advantages

- AD systems are great at detecting a sudden high value for some metric.

AD Disadvantages

- AD systems base their detection on deviation from what's normal, they tend to work well in static environments, such as on servers that do the same thing day in and day out.

Signature-Detection Model

- *Signature-detection* or *misuse* IDSs are the most popular type of IDS, and they work by using databases of known bad behaviors and patterns.
- The defined patterns of code are called *signatures,* and often they are included as part of a governing *rule* when used within an IDS.

  Signature-Detection Rules

- Unique signature byte sequence
- Protocol to examine (such as TCP, UDP, ICMP)
- IP port requested
- IP addresses to inspect (destination and source)
- Action to take if a threat is detected (such as allow, deny, alert, log, disconnect)

Advantages of Signature Detection

- Signature-detection IDSs are proficient at recognizing known threats. Once a good signature is created, signature detection IDSs are great at finding patterns.

Disadvantages of Signature Detection

- **Cannot Recognize Unknown Attacks** Just like antivirus scanners, signature-detection IDSs are not able to recognize previously unknown attacks.
- **Performance Suffers as Signatures or Rules Grow** because each network packet or event is compared against the signature database, or at least a subset of the signature database, performance suffers as rules increase.

IDS Features

IDS End-User Interfaces

- IDS end-user interfaces let you configure the product and see ongoing detection activities. You should be able to configure operational parameters, rules, alert events, actions, log files, and update mechanisms.
- IDS interfaces come in two flavors: syntactically difficult command prompts or less-functional GUIs.

Intrusion-Prevention Systems (IPS)

- Going far beyond mere monitoring and alerting, second-generation IDSs are being called *intrusion-prevention systems* (IPSs). They either stop the attack or interact with an external system to put down the threat.
- For an IPS to cooperate with an external device, they must share a common scripting language, API, or some other communicating mechanism. Another common IPS method is for the IDS device to send reset (RST) packets to both sides of the connection, forcing both source and destination hosts to drop the communication.

IPS Disadvantages

- A well-known consequence of IPSs is their ability to exacerbate the effects of a false positive. With an IDS, a false positive leads to wasted log space and time, as the administrator researchesthe threat's legitimacy. IPSs are proactive, and a false positive means a legitimate service or host is being denied. Malicious attackers have even used prevention countermeasures as a DoS attack.

IDS Management

- Central to the IDS field are the definitions of *management console* and *agent*. An IDS agent (which can be a *probe, sensor,* or *tap*) is the software process or device that does the actual data collection and inspection.
- IDS management consoles usually fulfill two central roles: configuration and reporting. If you have multiple agents, a central console can configure and update multiple distributed agents at once.

IDS Logging and Alerting

Alerts

- Alerts are high-priority events communicated to administrators in real time. The IDS's policy determines what security threats are considered high risk, and the priority level is set accordingly.
- Alerts should be quick and to the point; however, they need to contain enough information for the incident responder to track down the event.

Logs

- IDS log files record all detected events regardless of priority and, after its detection engine, have the greatest influence on the speed and use of an IDS. IDS logs are used for data analysis and reporting.

IDS Deployment Considerations IDS Fine-Tuning

- Fine-tuning an IDS means doing three things: increasing inspection speed, decreasing false positives, and using efficient logging and alerting.

Increasing Inspection Speed

- Strategy is to let other faster perimeter devices do the filtering. Routers and firewalls are usually faster than IDSs, so, when possible, configure the packet filters of your routers and firewalls to deny traffic that should not be on your network in the first place.
- The more traffic that you can block with the faster device, the higher performing your IDS will be.

Decreasing False Positives

- In most instances, false positives will outweigh all other events. Track them all down, rule out maliciousness, and then appropriately modify the source or IDS to prevent them.

IPS Deployment Plan

- Here are the steps to a successful IPS deployment:

1. Document your environment's security policy.
2. Define human roles.
3. Decide the physical location of the IPS and sensors.
4. Configure the IPS sensors and management console to support your security policy.
5. Plan and configure device management (including the update policy).
6. Review and customize your detection mechanisms.
7. Plan and configure any prevention mechanisms.
8. Plan and configure your logging, alerting, and reporting.
9. Deploy the sensors and console (do not encrypt communication between sensors and links to lessen troubleshooting).
10. Test the deployment using IPS testing tools (initially use very broad rules to make sure the sensors are working).
11. Encrypt communications between the sensors and console.
12. Test the IPS setup with actual rules.
13. Analyze the results and troubleshoot any deficiencies.
14. Fine-tune the sensors, console, and logging, alerting, and reporting.
15. Implement the IPS system in the live environment in monitor-only mode.
16. Validate alerts generated from the IPS.
17. One at a time, set blocking rules for known reliable alerts that are important in your environment.
18. Continue adding blocking rules over time as your confidence in each rule increases.
19. Define continuing education plans for the IPS administrator.
20. Repeat these steps as necessary over the life of the IPS.

Security Information and Event Management (SIEM)

- Multiple security systems can report to a centralized *Security Information and Event Management (SIEM) system,* bringing together logs and alerts from several disparate sources.
- SIEM platforms take the log files, find commonalities (such as attack types and threat origination), and summarize the results for a particular time period.
- SIEMs have a huge advantage over individual IDS systems because they have the capability to collect and analyze many different sources of information to determine what's really happening. As a result, the SIEM can significantly reduce false positives by verifying information based on other data.

Data Aggregation

- SIEMs collect information from every available source that is relevant to a security event. These sources take the form of alerts, real-time data, logs, and supporting data.

Alerts

- The SIEM's key function is to validate security alerts using many different sources of data to reduce false positives, so only the most reliable alerts get sent on to the security administrator.

Real-Time Data

- Real-time data such as network flow data (for instance, Cisco's Net Flow and similar traffic monitoring protocols from other vendors) gives the SIEM additional information to correlate.

Logs

- Logs are different from events, in that they are a normal part of system activity and usually meant for debugging purposes. Logs can be an important additional data source for a SIEM, however. Logs contain valuable information about what's happening on a system, and they can give the SIEM a deeper view into what's happening.

Supporting Data

- You can enhance the quality of a SIEM's correlation even more by providing the SIEM with supporting data that has been previously collected. Data can be imported into the SIEM, and it will use that data to make comparative determinations.

Analysis

- A SIEM takes all the data given to it and makes decisions, so the security administrator can focus on the most important alerts. For this reason, event correlation is a SIEM's most important feature. The correlation engine of every SIEM product is its most distinguishing feature. The better the analysis, the cleaner the end result.

Operational Interface

- For all the data collected by the SIEM and its resulting alerts to be human-readable, it must present the information in a way that an administrator can understand at a glance.
- Alerting is the other way the SIEM interacts with humans. Whereas the dashboard performs a pull type of data transfer to the administrator (because the administrator must go to the SIEM, log in, and intentionally look for the information), alerts represent a push technique that doesn't require human diligence to notice something important is happening.

Voice over IP (VoIP) and PBX Security

- Attackers have been targeting computing systems for the last 25 years or so using intentionally exploitative behavior such as hacking and denial of service attacks.

Background

- When you layer a VoIP system on top of an IP network, you combine the risks associated with both, creating a superset of new risks as of result. Here are two examples
- Many VoIP systems are server-based and rely on common operating systems (mainly Windows and Linux) to run their hardware interface. Therefore, they are susceptible to a class of problems that from a voice systems perspective were not previously a threat.
- IP-based voice protocols, while providing low-cost, advanced end-user features and reliable transport mechanisms for voice traffic, also give attackers a new method for exploiting voice systems and additional avenues for compromising data networks in general.
- **Consider the components of a modern enterprise IP-based phone or video system:**
- **Call control elements (call agents)**
    - Internet protocol private branch exchange (IPPBX)
    - Session border controllers (SBCs)
- **Gateways and gatekeepers**
    - Dial peers
    - Multi-conference units (MCUs) and specialized conference bridges
- **Hardware endpoints**
    - Phones
    - Video codecs
    - Soft clients and software endpoints
- **IP phones**
    - Desktop video clients
    - IP-based smartphone clients
- **Contact center components**
    - Automated call distribution (ACD) and interactive voice response (IVR) systems
    - Call center integrations and outbound dialers
    - Call recording systems
- **Voicemail systems**

list of protocols commonly used on enterprise networks, the PTN, and Internet

- H.248 (also known as Megaco)
- Media gateway control protocol (MGCP)
- Session initiation protocol (SIP)
- H.323
- Secure real-time transport protocol (SRTP)
- real-time protocol (RTP), real-time control protocol (RTCP), and real-time streaming protocol (RTSP)
- Short message service (SMS)
- **In traditional carrier networks (as defined by AT&T to support direct distance dialing or DDD … this was "in the beginning" for telephony), switches were defined by a class hierarchy that separated them into five different roles.**
    - **Class 1** International gateways handing off and receiving traffic from outside the U.S and Canadian networks
    - **Class 2** Tandem switches interconnecting whole regions
    - **Class 3** Tandem switches connecting major population centers within a region

- **Class 4** Tandem switches connecting the various areas of a city or towns in a region
- **Class 5** Switches connecting subscribers and end-users

- The portability of IP and flexibility of VoIP have allowed enterprises to provide their own transport across significant geographical distances, as they are no longer relegated to the functions and features of a PBX.
- Some of the main drivers behind the development of VoIP technology are the opportunities for cost savings, from lowering the cost of structured cabling by sharing Ethernet connections to advanced features like VoIP backhaul and global tail-end hop-off.

VoIP Components

Call Control

- The call control element (the "brains" of the operation) of a VoIP system can be either a purposed appliance, a piece of software that runs on a common or specialized server operating system, or a piece of network hardware embedded or integrated into another networking component such as a switch blade or software module (soft switch).
- Original IP phone systems were traditional digital time-division multiplexing (TDM)
- Primarily responsible for call setup and teardown, signaling, device software serving, and feature configuration, call control is one of the easier pieces of the voice infrastructure to protect.
- If you use a hosted or SaaS-based VoIP system, take the time to analyze how the provider manages security and ensure that its vulnerability management program supports the level of risk you are willing to accept.

Voice and Media Gateways and Gatekeepers

- The voice (or media) *gateway* is the pathway to the outside world. This component is what allows termination to a PSTN, transcoding between TDM and IP networks, media termination, and other types of analog/digital/IP interface required in today's multimedia rich IP infrastructures.
- *Gatekeepers,* not to be confused with gateways, provide intelligence and control certain routing and authentication, authorization, and accounting (AAA) security functions. They can also perform and assist with certain types of address translation, and can consolidate administrative control elements such as call detail records (CDR), communication with monitoring and management systems, and bandwidth management for a given zone.

MCUs

- Conferencing and collaboration is used extensively within and across all enterprises as part of the fundamental communications capability that connects all users to each other.
- At the heart of this technology is the Conference Bridge, or multi-conference unit (MCU), a multiport bridging system for audio, video, and multimedia collaboration.
- Special attention should be paid to MCU functionality, whether they are hosted on premise or externally, in order to make sure they are secure.

Consider the following:

- The easier it is to use, the more people will use it—even the ones you don't want to use it.
- Convenience and ease of use need to be balanced with secure practices.
- A problem with an MCU can affect a lot of users at once.
- MCUs can connect different types of media; require those facilities to be secured.

Hardware Endpoints

- Endpoint compromises today are frequently targeted at mobile devices, and much of the attention in the industry right now is focused on how to secure the mobile environment.
- Modern VoIP phones have a fair bit of intelligence built into them and offer a previously unavailable avenue—some phones have a built-in layer two switch and are capable of executing XML scripts or Java code locally. Video codecs run all kinds of custom code required for video conferencing and content sharing and are sometimes directly exposed to the Internet.

Software Endpoints

- a piece of software that runs on a PC or mobile device and acts like a hardware endpoint by registering to the call control element(s) as a device. Why would you install a soft client on a mobile device, which already has mobile capability? Two reasons: Cost is, of course, the first one.
- In many places, data usage on a cell phone is less costly than calling minutes, and by running a soft client, you convert what would otherwise be cellular usage minutes into an IP data stream (thank the "unlimited data plan" for this being a viable option).
- Second, by running the soft client, you can extend your enterprise features to the mobile user, including functionality not typically available on mobile devices such as consolidated extension-based or URI dialing.

Call and Contact Center Components

- Call centers have made a remarkable evolutionary leap, from initially being used as a place to take orders and field complaints, to being a strategic asset that most enterprises cannot survive without.
- The two core components of any call center are automatic call detection (ACD) and interactive voice response (IVR). Simply put, the ACD moves calls around, and the IVR collects information from the caller and queues those calls in the appropriate places, based on defined variables such as agent skills

Voicemail Systems

- Major component of a VoIP-based telephony system is the voicemail system. Auto attendants, direct inward system access (DISA) features used for manual call forwarding, automatic call forwarding, and other voicemail features are a "standard" component of enterprise life, which nearly everyone has come to expect and rely on.

VoIP Vulnerabilities and Countermeasures

Three main exploitable paths from which you may be attacked: The "low-tech" hacks Attacks on server, appliance, or hardware infrastructure Advanced threats directed against specific systems or protocols

Old Dogs, Old Tricks: The Original Hacks

- A vulnerability in the Dual-tone multi-frequency signaling (DTMF) dialing systems of the time, when he found that a toy whistle from a cereal box could be used to produce a 2600 Hz sound to manipulate the communication protocol of public phone systems to obtain free long distance.
- While most modern IP-based systems are smart enough not to fall for the old DTMF Tricks there are hundreds, even thousands, of exploited gateways.

Assessment Audit

- What is your externally facing profile? Are there exposed numbers that can reach internal systems and access them?
- If so, do those internal systems have password or PIN protection? What complexity?

- If simple access is required for any reason, can you audit access?

Action Steps

- Enforce password requirements for system access. Delete old and unused mailboxes as soon as possible Limit exposure where possible by using fewer external dial-in numbers;
- Pay attention to call forwarding and who is allowed to use the feature to send calls outside of your perimeter.

Vulnerabilities and Exploits

- *Vulnerability* means a weakness that has not yet been used to compromise a perimeter, whereas *exploit* is a compromised vulnerability.

Network

- Inspecting packets takes resources and adds transit time, which can lead to an adversarial relationship between the teams working to move packets from place to place seamlessly and the teams trying to ensure that legitimate data is contained within those packets.

Servers

- As with any server-based system, understand your key weaknesses and most vulnerable areas.

Appliances

- The common modern practice for many Manufacturers today is to buy OEM hardware from one of the big server suppliers and to run either a proprietary OS or custom version of a commodity operating system to create their "appliance."

The Protocols

- At the heart of the family of VoIP technologies are the specific protocols that enable the transit and real-time conversations that IP networks were not originally designed to handle.

  Protocol: H.248 (Megaco)

  - **Known Compromises and Vulnerabilities** DoS attacks using malformed packets targeted at port 2944 / sctp.

  Recommendations

  - A suitable approach is to use encryption for call setup

  Protocol: MGCP

  - **Known Compromises and Vulnerabilities** Interference with authorized calls or setup of unauthorized calls via barge-in or intercept, and rerouting or dropping legitimate callsin- progress

  Recommendations

  - use IPSec (AH or ESP) as a protection

  Protocol: SIP (Session Initiation Protocol)

  - Application layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants.
  - **Known Compromises and Vulnerabilities** DoS, DDoS, flooding, SPAM over Internet Telephony (SPIT)

  Recommendations

  - Best practices are always to turn off any unneeded services for any protocol

PBX

A Private Branch Exchange (PBX) is a computer-based switch that can be thought of as a local phone company.

- Multiple extensions
- Voicemail

- Call forwarding
- Fax management
- Remote control (for support)

Hacking a PBX

- To gain confidential information (espionage)
- To cause damages by crashing the PBX

Administrative Ports and Remote Access

- Vendors often require remote access via a modem to be able to support and upgrade the PBX.
- This port is the number one hacker entry point. An attacker can connect to the PBX via the modem; or if the administrative port is shared with a voice port, the attacker can access the port from outside the PBX by calling and manipulating the PBX to reach the administrative port.
- Just as with administrative privileges for computers, when attackers have remote administrative privileges, "they own the box" and can use it to make international calls or shut down the PBX.

Voicemail

- An attacker can gain information from voicemail or even make long-distance phone calls using a "through-dial" service.

Denial of Service

- PBXs store their voicemail data on a hard drive. An attacker can leave a long message, full of random noises, in order to make compression less effective—whereby a PBX might have to store more data than it anticipated.

Securing a PBX

- Connect administrative ports only when necessary. Protect remote access with a third-party device or a dial-back.
- Review the password strength of your users' passwords. If you require dial through, limit it to a set of predefined needed numbers.

TEM: Telecom Expense Management

- TEM program can help automate the process of getting to the goodies, the high-quality information you need to tell quickly if you have a security problem related to your phone system.
- There are many firms armed with specialized software ready to help you collect, organize, understand, interpret, and audit your telephone bills, all for a modest gain-share or percentage of savings fee (an interesting side note and case in point, that's how bad telecom bills are companies will *guarantee* that they will save you *so* much money that they will derive their compensation purely from a percentage of the money they save you or get back for.

Operating System Security Models

Operating System Models

- The *operating system security model* (also known as the *trusted computing base,* or TCB) is simply the set of rules, or protocols, for security functionality.
- Security commences at the network protocol level and maps all the way up to the operations of the operating system.
- An effective security model protects the entire host and all of the software and hardware that operate off it.

The Underlying Protocols Are Insecure

- If the underlying protocols are insecure, then the operating system is at risk. What's frightening about this insecurity is that while the language of the Internet is TCP/IP, effective security functionality was not added to TCP/IP until version 6 in the late 1990s.

We've known about TCP/IP's lack of security for a long time. The protocol's main Problems are as follows:

- **Vulnerable to spoofing** Spoofing is the term for establishing a connection with a forged sender address.
- **Vulnerable to session hijacking** An attacker can take control of a connection by intercepting the session key and using it to insert his own traffic into an established TCP/IP communication session
- **Predictable sequence guessing** The sequence number used in TCP connections is a 32-bit number, so the odds of guessing the correct ISN would seem to be exceedingly low.
- **No authentication or encryption** the lack of authentication and encryption with TCP/IP is a major weakness.
- **Vulnerable to SYN flooding** SYN flooding takes advantage of the three-way handshake in establishing a connection.

The security benefits of TCP/IP version 6 include

- IPSec security
- Authentication and encryption
- Resilience against spoofing
- Data integrity safeguards
- Confidentiality and privacy

Access Control Lists

- Much of the security functionality afforded by an operating system is via the ACL. Access control comes in many forms, but in whatever form it is implemented, it is the foundation of any security functionality.
- In Windows, an ACL is associated with each system object. Each ACL has one or more *access control entries (ACEs),* each consisting of the name of a user or a group of users.
- Each ACE identifies a security principal and specifies a set of access rights that are allowed, denied, or audited for that security principal.
- A *discretionary* access control list (DACL) that identifies the users and groups who are allowed or denied access
- A *system* access control list (SACL) that controls how access is audited

MAC vs. DAC

- *Mandatory access control* requires that access control policy decisions be beyond the control of the individual owners of an object. MAC is generally used in systems that require a very high level of security.
    - Better suited to environments with rigid information
    - Effective access restrictions
- Access control lists can be further refined into both required and optional settings. This refinement is carried out more precisely with ***discretionary access control*** and is implemented by discretionary access control lists (DACLs).

- Individual users may determine the access controls.
- Not suited for the military

- The difference between discretionary access control and its counterpart, mandatory access control, is that DAC provides an entity or object with access privileges it can pass to other entities. Depending on the context in which they are used, these controls are also called rule-based access control (RBAC) and identity-based access control (IBAC).

Classic Security Models

Three of the most famous security models are Bell-LaPadula, Biba, and Clark- Wilson**.**

Bell-LaPadula

- The Bell-LaPadula model was designed to prevent users and processes from reading above their security level.

Biba

- Biba is often known as a reversed version of Bell-LaPadula, as it focuses on integrity labels, rather than sensitivity and data classification

Clark-Wilson

- Clark-Wilson attempts to define a security model based on accepted business practices for transaction processing.

Reference Monitor

The Reference Monitor Concept

- The National Institute of Standards and Technologies describes the reference monitor concept as an object that maintains the access control policy. It does not actually change the access control information; it only provides information about the policy.

The main elements of an effective reference monitor are that it is

- **Always on** Security must be implemented consistently and at all times for the entire system and for every file and object.
- **Tamperproof** It must be impossible for an attacker to attack the access mediation mechanism such that the required access checks are not performed and authorizations not enforced.
- **Lightweight** It must be small enough to be subject to analysis and tests, proving its effectiveness.

Windows Security Reference Monitor

- The Windows Security Reference Monitor (SRM) is responsible for validating Windows process access permissions against the security descriptor for a given object. The Object Manager then, in turn, uses the services of the SRM while validating the process's request to access any object.

Trustworthy Computing

The four goals of the Trustworthy Computing initiative are

- **Security** As a customer, you can expect to withstand attack. In addition, you can expect the data is protected to prevent availability problems and corruption.
- **Privacy** You have the ability to control information about yourself and maintain privacy of data sent across the network.
- **Reliability** When you need your system or data, they are available.

- **Business integrity** the vendor of a product acts in a timely and responsible manner, releasing security updates when a vulnerability is found.
- *Secure by design* simply means that all vulnerabilities are resolved prior to shipping the product. Secure by design requires three steps.
    - *Build a secure architecture.* This is imperative. Software needs to be designed with security in mind first and then features.
    - *Add security features.* Feature sets need to be added to deal with new security vulnerabilities.
    - *Reduce the number of vulnerabilities in new and existing code.* The internal process at Microsoft was revamped to make developers more conscious of security issues while designing and developing software.

International Standards for Operating System Security

Common Criteria

- Common Criteria certification is intended to be the Good Housekeeping seal of approval for the information security sector, offering a consistent, rigorous, and independently verifiable set of evaluation requirements for hardware and software,

Common Criteria Sections

These are the three parts of the Common Criteria:

- Part 1 is the introduction to the Common Criteria. It defines the general concepts and principles of information technology security evaluation and presents a general model of evaluation.
- Part 2 details the specific security functional requirements and details a criterion for Expressing
- Part 3 details the security assurance requirements and defines a set of assurance components as a standard way of expressing

Protection Profiles and Security Targets

- A *protection profile* defines a standard set of security requirements for a specific type of product (for example, operating systems, databases, or firewalls). During Common Criteria evaluation, the product is tested against a specific PP providing reliable verification of the product's security capabilities.
- The *security target* description includes an overview of the product, potential security threats, detailed information on the implementation of all security features included in the product, and any claims of conformity against a PP at a specified (evaluation assurance levels)EAL.

Problems with the Common Criteria

- **Administrative overhead** the overhead involved with gaining certification takes a huge amount of time and resources.
- **Expense** Gaining certification is extremely expensive.
- **Labor-intensive certification** The certification process takes months.
- **Need for skilled and experienced analysts** Availability of information security professionals with the required experience is still lacking.

UNIT 5

Virtual Machines and Cloud Computing

- Virtual computers aren't the only platforms based on virtualization technology. Virtual networks, which can emulate just about any router or switch fabric, and virtual storage, which can expand or contract as needed, complete the triangle. Servers, networks, and storage together, all virtualized, make up the world of cloud computing.

Virtual Machines

- In addition to securing the VMs themselves, additional steps are needed to secure the virtual environment as a whole. The risks associated with VMs are a superset of those associated with physical servers along with a new set of risks based on the controllability of the individual virtual machines through a centralized management platform (sometimes referred to as a *hypervisor* or *virtual machine monitor*).
- **Protecting the Hypervisor**
    - The hypervisor is responsible for managing all guest OS installations on a VM server, and the service console provides a centralized location for managing all the servers in a virtual environment. As a result, a compromise of the hypervisor or service console has the potential to inflict significant damage as this would effectively allow all security controls on the virtual servers to be bypassed.
    - Hypervisor and service console servers need to be properly patched and secured, as well as logically separated through the use of isolated networks with strict access controls.
    - Firewalls should be used to block access attempts from the virtual machines to the management consoles.
    - administrative access should be strictly controlled.
    - Multifactor authentication—using *tokens* (portable digital one-time password generators), biometrics, and smart cards—is a better choice for hypervisor access.
    - Limiting the number of administrators and their privileges is another practice that can reduce the risks of hypervisor attacks via administrator accounts.
- **Protecting the Guest OS**
    - Typically, the hypervisor manages access to hardware resources so that each guest OS is able to access only its own allocated resources, such as CPU, memory, and storage, but not those resources allocated to other guest OSs.
    - This characteristic is known as *partitioning* and is designed to protect each guest OS from other guest OS instances, so attacks and malware are unable to "cross over." Partitioning also reduces the threat of *side-channel attacks* that take advantage of hardware usage characteristics to crack encryption algorithms or implementations.
    - The hypervisor monitors and tracks the state of its guest OSs, which is a function commonly referred to as *introspection*.
- **Protecting Virtual Storage**
    - security for virtualization is focused on controlling access to the files on the virtual hard drive and the overall configuration of the storage network.
- **Protecting Virtual Networks**

- The hypervisor can present the guest OS with either physical or virtual network interfaces. Typically, hypervisors provide three choices for network configurations:
  - **Network bridging** The guest OS has direct access to the actual physical network interface cards (NIC) of the real server hardware.
  - **Network Address Translation (NAT)** The guest OS has virtual access to a simulated physical NIC that is connected to a NAT emulator by the hypervisor.
  - **Host-only networking** A guest OS has virtual access to a virtual NIC that does not actually route to any physical NIC.

Cloud Computing

- Cloud computing provides a way to increase capacity or add capabilities on the fly without investing in new infrastructure, training new personnel, or licensing new software. It encompasses any subscription-based or pay-per-use service that, in real time over the Internet, extends existing IT capabilities.
- Cloud computing services are gaining in popularity among businesses that want to save money and improve the efficiency of their computing resource consumption.
- Cloud computing is attractive to small businesses and startup companies that don't have many options for establishing basic computing infrastructure in a fast and cost-effective manner.
- Video and audio conferencing, collaboration tools, and sales force automation are cited as good examples of services that can be successfully migrated to, or implemented in, a cloud.
- Select vendors based on their willingness to comply with customer requirements and their dedication to protecting customer information and environments as well as their previous track record in providing cloud services.

- **Types of Cloud Services**
- The following are the most common types of services with which we find the term "cloud" associated.
  1. **Infrastructure-as-a-Service (IaaS)** This type of service allows consumers to provision processing, storage, and networking resources, allowing them to deploy and run their own operating systems or applications in their own cloud environment.
  2. **Software-as-a-Service (SaaS)** This type of cloud computing delivers a single application through the browser to customers using a multitenant architecture.
  3. **Utility computing** Companies that offer storage and virtual servers that IT can access on demand.
  4. **Platform-as-a-Service (PaaS)** This form of cloud computing delivers development environments as a service. You build your own applications that run on the provider's infrastructure and are delivered to your users via the Internet from the provider's servers.
  5. **Web services in the Cloud** Web service providers offer APIs that enable developers to exploit functionality over the Internet, rather than delivering full-blown applications.
  6. **Managed service providers (MSP)** One of the oldest forms of cloud computing, a managed service is basically an application exposed to IT rather than to end users.
  7. **Service commerce platforms** a service commerce platform is a service hub that users interact with, such as an expense management system, to order travel or secretarial services from a common platform that then coordinates the service delivery and pricing within the specifications set by the user.
  8. **Internet integration** The integration of cloud-based services mainly serving SaaS providers using in-the-cloud integration technology.

- **Cloud Computing Security Benefits**
    1. **Centralized data** Data leakage through laptop data loss and backup tape loss could conceivably be reduced by cloud computing using thin client technology.
    2. **Monitoring** Centralized storage is easier to control and monitor.
    3. **Forensics and incident response** With IaaS providers, a dedicated forensic server can be built in the same cloud as the corporate servers but placed offline, ready to be used and brought online as required. It can also reduce evidence acquisition time, allowing immediate analysis of compromised servers. In addition, servers can now be cloned and the cloned disks instantly made available to the Cloud forensics server.
    4. **Password assurance testing** For organizations that routinely crack passwords to check for weaknesses, password cracking times can be significantly decreased.
    5. **Logging** Effectively unlimited storage for logging, with reduced concerns about insufficient disk space being allocated for system logging.
    6. **Testing security changes** Vendor updates and patches, as well as configuration changes for security purposes, can be applied using a cloned copy of the production server, with low-cost impact testing and reduced startup time.
    7. **Security infrastructure** SaaS providers that offer security technologies to customers share the costs of those technologies among their customers who use them.

- **Security Considerations**
    - When evaluating the need for cloud computing services, you should consider private data and public data separately. Private data, such as client information, requires stricter security controls than public data that is intended to be shared with a larger Internet audience.
    - Cloud computing also raises some additional concerns that need to be addressed, beyond those of traditional data centers. For instance, knowing and controlling the location of data is important for many reasons, not the least of which is regulatory.
    - cloud service providers have many data centers and leverage virtualization of servers, network, and storage to provide elastic environments that **can be scaled on demand**.
    - VMware has a feature called Distributed Resource Scheduler, which continuously monitors utilization across guest OSs and allocates available resources among virtual machines, providing capacity expansion by automatically migrating live virtual machines to different physical servers.
    - For sensitive and private data, colocation is also a concern. Cloud computing providers typically store data from multiple customers on the same hardware infrastructure, stating that suitable controls are in place to provide logical separation of data for different customers;

- **Cloud Computing Risks and Remediations**
    - **Availability** Cloud services can be thought of as being comparable to the Internet itself. On the Internet, availability issues are managed by using redundant service providers so a failure at one provider will not result in a loss of service.
    - **Data persistence** What happens to data when it is deleted from the cloud?
    - **Patriot Act ramifications** The U.S. government has the right to monitor and capture all traffic from a service provider on demand.
    - **Compliance ramifications** Some government regulations do not allow cloud computing.
    - **PCI compliance** Requires that you know and can demonstrate exactly where and on what physical server your data resides.

- **Migration** You may need physical-to-cloud and cloud-to-physical capability to move data into the cloud from your local computing environment, or vice versa.
- **Confidentiality** The responsibility for controlling data in a cloud environment is shared between the cloud provider and the customer. Isolating data is only as effective as the virtualization technologies used to build the cloud and the controls and practices implemented by the providers. Any data that an organization is concerned about keeping private should be housed in a private network or private cloud, not in a public cloud.

- **Cloud Computing Security Incidents**

Date reported	Provider	Service	Incident type	Summary
1/30/2009	Ma.gnolia	Ma.gnolia	Data loss	Ma.gnolia suffers major data loss, data gone for good
3/13/2009	Microsoft Corporation	Sidekick	Data loss	Microsoft Sidekick outage left customers without access to service and lost data
4/28/2010	Paychex, Inc.	Payroll 401(k) and Employee Benefits	Data loss	Payroll and 401k servicing company erroneously merges account data of two businesses
8/9/2010	Evernote Corporation	Evernote	Data loss	A small percentage of Evernote users' data lost
11/1/2010	DreamHost	Web Hosting	Denial of Service	DreamHost Cardiff distributed denial of service attack
11/4/2010	Intuit.com	Web Hosting	Denial of Service	www.websites.intuit.com denial of service attack
11/17/2010	Sitelutions	DNS	Denial of Service	Sitelutions suffers distributed denial of service attack
1/21/2011	Whirlpool	Forum	Denial of Service	Whirlpool Forum hit with distributed denial of service attack

- **Cloud Security Technologies**
  - Communication encryption
  - File-system encryption
  - Auditing
  - Traditional network firewalls
  - Application firewalls
  - Content filtering
  - Intrusion detection
  - Geographic diversity

- **Vendor Security Review**
- Perform a third-party vendor security review to validate the security practices of cloud computing providers that you are considering.
    - Physical security
    - Backups and/or data protection
    - Administrator access
    - Firewalls
    - Hypervisor security
    - Customer and instance isolation
    - Intrusion detection and anomaly monitoring
    - Data transmission security
    - Data storage security
- **Risk and Remediation Analysis**
    - The following categories of risks are divided according to the classic "CIA" triad of Confidentiality, Integrity, and Availability—the concepts that information security professionals are tasked with protecting.
    - We attempt to apply security controls consistent with the three *D*s of security—Defense, Detection, and Deterrence—in an effort to mitigate risks using the principle of layered Security
    - **Confidentiality Risks**
        - **Data leakage, theft, exposure, forwarding** The loss of information such as customer data and other types of intellectual property through intentional or unintentional means. There are four major threat vectors for data leakage: theft by outsiders, malicious sabotage by insiders (including unauthorized data printing, copying, or forwarding), inadvertent misuse by authorized users and mistakes created by unclear policies.
            - **Defense:** Employ software controls to block inappropriate data access
            - **Detection:** Use water-marking and data classification
            - **Deterrence:** Establish clear and strong language in contractual agreements
            - **Residual risk:** Data persistence within the cloud vendor environment
        - **Espionage, packet sniffing, packet replay** The unauthorized interception of network traffic for the purpose of gaining information intentionally, using tools to capture network packets or tools to reproduce traffic and data that was previously sent on a network.
            - **Defense:** Encrypt data at rest as well as data in transit
            - **Detection:** Not much can be done today
            - **Deterrence:** Transfer the risk of unauthorized access
            - **Residual risk:** Data can be stolen from the network through tools that take advantage of network topologies
    - **Integrity Risks**
        - These risks affect the validity of information and the assurance that the information is correct. Some government regulations are particularly concerned with ensuring that data is accurate. If information can be changed without warning, authorization, or an audit trail, its integrity cannot be guaranteed.
        - **Malfunctions** Computer and storage failures that can cause data corruption.
            - **Defense:** Make sure the service provider you select has appropriate RAID redundancy built into its storage network and that creating archives of important data is part of the service.
            - **Detection:** Employ integrity verification software that uses checksums or other means of data verification.

        - **Deterrence:** Owing to the nature of the data and the fact that there is no human interaction, little can be accomplished.
        - **Residual risk:** Technology failures that damage data may result in operational or compliance risks
    - **Data deletion and data loss** Accidental or intentional destruction of any data, including financial, company, personal, and audit trail information. Destruction of data owing to computer system failures or mishandling.
        - **Defense:** In the cloud environment, ensure that your critical data is redundantly stored and housed with more than one cloud service provider.
        - **Detection:** Maintain and review audit logs that relate to data deletion.
        - **Deterrence:** Maintain education and awareness programs for individuals who access and manage data. Ensure that appropriate data owners are assigned who have full authority and control over data.
        - **Residual risk:** Once critical data is gone, if it can't be restored it is gone forever.

Secure Application Design

- While the deployment environment can help protect the application to some extent, every application must be secure enough to protect itself from whatever meaningful attacks the deployment environment cannot prevent, for long enough for the operator to notice and respond to attacks in progress.

Secure Development Lifecycle

- A secure development lifecycle (SDL, or sometimes SSDL, for secure software development lifecycle) is essentially a development process that includes security practices and decision making inputs.
- The SDL itself is created, operated, measured, and changed over time following a business process lifecycle. Sometimes people call the process of developing and maintaining an SDL and other application security activities an *application security assurance program*.
- **SDL contains three primary elements:**
    1. Security activities that don't exist at all in the original lifecycle; for instance, threat Modeling.
    2. Security modifications to existing activities; for instance, adding security checks to existing peer reviews of code.
    3. Security criteria that should affect existing decisions; for instance, the number of open high-severity security issues when a decision to ship is made.

Application Security Practices

- **Security Training**
    - security training program for development teams includes technical security awareness training.
- **Secure Development Infrastructure**
    - Project contacts must be registered in case any application security issues occur, and licenses for secure development tools must be acquired.
- **Security Requirements**
    - Security requirements may include access control matrices, security objectives (which specify actions attackers with specific privileges should not be able to perform).

- **Secure Design**
  - Secure design activities usually revolve around secure design principles and patterns.
- **Threat Modeling**
  - Threat modeling is a technique for reviewing the security properties of a design and identifying potential issues and fixes.
- **Secure Coding**
  - Secure coding includes using safe or approved versions of functions and libraries, eliminating unused code.
- **Security Code Review**
  - To find security issues by inspecting application code, development teams may use static analysis tools, manual code review, or a combination.
- **Security Testing**
  - To find security issues by running application code, developers and independent testers perform repeatable security testing
- **Security Documentation**
  - When an application will be operated by someone other than the development team, the operator needs to understand what security the application needs the deployment environment to provide.

Web Application Security

- several web application security concerns to be considered
  - SQL injection
  - Forms and scripts
  - Cookies and session management
  - General attacks
- **SQL Injection**
  - *SQL* (Structured Query Language) is standardized by the American National Standards Institute (ANSI) and serves as a common language for communicating with databases. Every database system adds some proprietary features to the basic ANSI SQL. *SQL injection* is a technique to inject crafted SQL into user input fields that are part of web forms—it is mostly used to bypass custom logins to web sites. the attacker will enter '**a**' **or** "**1**"="**1**" for the username, and any password at all, because it will be ignored. The resulting SQL looks like this:
  - select * from users where username='a' or "1"="1"--' and password='whatever'
  - **Solutions for SQL Injection**
    - Filter all input fields for apostrophes (') to prevent unauthorized logins.
    - Filter all input fields for SQL commands like insert, select, union, delete, and exec to prevent server manipulation. (Make sure you do this after filtering for the apostrophes.)
    - Limit input field length (which will limit attackers' options), and validate the input length with server-side scripts.
- **Forms and Scripts**
  - Attackers can exploit the data embedded inside forms and can trick the web application into either exposing information about another user or to charge a lower price in e-commerce applications.
  - **Three methods of exploiting forms are these:**

- Disabling client-side scripts
- Passing parameters in the URLs
- Passing parameters via hidden fields

- **Client-Side Scripts**
  - Some developers use client-side scripts to validate input fields in various ways:
    - Limit the size of the input fields
    - Disallow certain characters (such as apostrophes)
    - Perform other types of validation (these can be specific to each site)
- **Passing Parameters via URLs**
  - A form has two methods of passing data: post and get. The post command sends the data in the content stream and the get command sends the data in the URL. Attackers can exploit the get command to send invalid or incorrect data, or to send malicious code.
  - http://somesite/checkout.asp?totalprice=100 This can be done simply by changing the URL like this http://somesite/checkout.asp?totalprice=50
- **Passing Data via Hidden Fields**
  - The post method sends the data using the POST HTTP command. Unlike get, this method doesn't reveal the data in the URL, but it can be exploited rather easily as well.
- **Solving Data-Transfer Problems**
  - The developer can prevent attackers from modifying data that is supposed to be hidden by managing the session information, by using GUIDs, or by encrypting the information.
  - **Managing Session Information** Most server-side scripting technologies allow the developer to store session information about the user—this is the most secure method to save session specific information because all the data is stored locally on the web server machine.
  - **Encrypting Data** The developer can pass encrypted data rather than passing the data in cleartext.

- **Cookies and Session Management**
  - Web *sessions* are implemented differently by each server-side scripting technology, but in general they start when the user enters the web site, and they end when the user closes the browser or the session times out.
  - Attackers can abuse both sessions and cookies, and this section will deal with the various risks:
    - Session theft
    - Managing sessions by sending data to the user
    - Web server cookie attacks
    - Securing sessions
  - **Session Theft**
    - Suppose that a user logs in to a web site that uses sessions. The web site tags the session as authenticated and allows the user to browse to secure areas for authenticated users. An attacker could modify the data in the cookie, however. Assume the cookie contains someemail@site.com, and each time we access the site we can automatically access restricted areas.
  - **Managing Sessions Without Sending Data to the User**

- Some users disable cookies (to protect their privacy), which means they also don't allow session management (which requires cookies).

- **Web Server Cookie Attacks**
  - An attacker can exhaust the resources of a web server using cookie management by opening many connections from dedicated software. Since this software will not send "close" events as a browser does when it is closed, the session will not be deleted until a timeout elapses. During this time, the session's information is saved either in the memory or in the hard drive, consuming resources.
- **Securing Session Tracking**
  - The best way to secure session tracking is to use a hard-to-guess identifier that is not derived from the user's data, such as an encrypted string or GUID, and to tie this identifier to the IP address of the user.

- **General Attacks**
  - **Vulnerable Scripts**
    - Some publicly used scripts (which are essentially the same as web applications) contain bugs that allow attackers to view or modify files or even take over the web server's computer.
  - **Brute-Forcing Logins**
    - An attacker can try to brute-force the login (either a standard web login or a custom ASP) using a dictionary. There are a number of ways to combat brute-force attacks:
      - Limit the number of connections per second per IP address (define this either at the firewall level or at the server-side script level)
      - Force users to choose strong passwords that contain upper- and lowercase letters and digits
  - **Buffer Overflows**
    - overflows can be used to gain control over the web server.

Client Application Security

- Writing a secure application is difficult, because every aspect of the application, like the GUI, network connectivity, OS interaction, and sensitive data management, requires extensive security knowledge in order to secure it.
- From the administrator's point of view, there are a number of security issues to keep in mind:
  - Running privileges
  - Administration
  - Application updates
  - Integration with OS security
  - Adware and spyware
  - Network access
- **Running Privileges**
  - An administrator should strive to run an application with the fewest privileges possible. Doing so protects the computer against several threats:
    - If the application is exploited by attackers, they will have the privileges of the application. If the privileges are low enough, the attackers won't be able to take the attack further.
    - Low privileges protect the computer from an embedded Trojan (in the application) because the Trojan will have fewer options at its disposal.
    - When an application has low privileges, the user won't be able to save data in sensitive areas (such as areas belonging to the OS) or even access key network resources.

- **Application Administration**
  - Most applications offer some type of interface for administration (mostly for application configuration), and each administration method poses security risks that must be addressed, such as these:
    - INI/Conf file (The most basic method of administrating an application is to control it via text-based files.)
    - GUI
    - Web-based control (web interface)
- **Integration with OS Security**
  - When an application is integrated with OS security, it can use the security information of the OS, and even modify it when needed. This is sometimes required by an application, or it may be supplied as an optional feature.
- **Application Updates**
  - Keeping applications up to date with the latest security patches is one of the most important security measures that you can take.
  - This section covers some mechanisms for easily updating applications:
    - Manual updates
    - Automatic updates
    - Semi-automated updates
    - Physical updates

Remote Administration Security

- Most of today's applications offer remote administration as part of their features, and it's crucial that it be secure.
- **Reasons for Remote Administration**
  - Remote administration is needed for various reasons:
  - **Relocated servers** An administrator needs an interface to administer any relocated web servers (computers that belong to an organization but that are physically located at the ISP).
  - **Outsourced services** Managing security products requires knowledge that some organizations don't possess, so they often outsource their entire security management to a firm specializing in that area.
  - **Physical distance** An administrator may need to manage a large number of computers in the organization. Some organizations span several buildings (or cities), and physically attending the computers can be a tedious and time-consuming task.
- **Remote Administration Using a Web Interface**
  - **advantages of remote web administration**
    - **Quick development time** Developing a web interface is faster than developing a GUI client, in terms of development, debugging, and deployment.
    - **OS support** A web interface can be accessed from all the major OSs by using a browser (unless the developers used an OS-specific solution, like ActiveX, which only runs on Windows).
    - **Accessibility** A web interface can be accessed from any location on the Internet. An administrator can administrate even if he's not in the office.
    - **User learning curve** An administrator knows how to use a browser, so the learning curve for the administrator will be shorter.

- **remote web administration has some disadvantages**
    - **Accessibility** Because web administration is accessible from anywhere on the Internet, it's also accessible to an attacker who may try to hack it.
    - **Browser control** Because a browser controls the interface, an attacker doesn't need to deploy a specific product control GUI (which might be hard to come by).
    - **Support** Web-based applications are typically easier to support and maintain.
- **Authenticating Web-Based Remote Administration**
- **HTTP Authentication Methods**
    - **Basic authentication** When a page requires basic authentication, it replies to the browser with error code 401 (unauthorized) and specifies that basic authentication is required.
    - **Digest authentication** Digest authentication uses MD5 to hash the username and password, using a challenge supplied by the web server.
    - **Secure Sockets Layer (SSL)** SSL can be configured to require a client certificate (optional) and authenticate a user only if they have a known certificate.
    - **Encrypted basic authentication** Basic authentication can be used in conjunction with regular SSL, thus encrypting the entire session, including the BASE64 encoded username and password (which is very weak encoding, easy to decode—this is not encryption).
    - **CAPTCHA** This is a popular method of verifying that the person on the other end is a human being, by showing a distorted image of letters and numbers and requiring the user to type them in correctly.

Physical Security

Classification of Assets

- *Classification of assets* is the process of identifying physical assets and assigning criticality and value to them in order to develop concise controls and procedures that protect them effectively.
- **The classification of corporate physical assets will generally fall under the following categories:**
    - **Computer equipment** Servers, network-attached storage (NAS) and storage area networks (SANs), desktops, laptops, tablets, pads, etc.
    - **Communications equipment** Routers, switches, firewalls, modems, private branch exchanges (PBXs), fax machines, etc.
    - **Technical equipment** Power supplies, uninterruptable power supplies (UPSs), power conditioners, air conditioners, etc.
    - **Storage media** Many older systems use storage media devices like magnetic tapes, DATs, CD-ROMs, and Zip drives, so it is still good to be familiar with them.
    - **Furniture and fixtures** Racks, NEMA-rated enclosures, etc.
    - **Assets with direct monetary value** Cash, jewelry, bonds, stocks, credit cards, personal data, cell phones, etc.

Physical Vulnerability Assessment

- A physical security vulnerability assessment, much like its information security counterpart, relies upon measurements of exposure to an applicable risk.

- **Buildings**
  - Take a walk around the building and look for unlocked windows and doors. Check for areas of concealment/obstruction such as bushes/shrubs directly beneath windows.
- **Computing Devices and Peripherals**
  - Verify lockdown and accessibility of systems and peripherals. Unattended systems should be logged off or have their screens locked.
  - Password-protect the BIOS with a complex password.
  - Disable system booting from floppy/CD/DVD/USB drives in the system setup.
  - Remove or disable unused modems and network ports.
- **Documents**
  - Documents should already be classified as part of your data classification and information owner matrixes and policies. Look for Confidential or "Eyes Only" documents lying around, Post-it notes with passwords and credentials, documents not collected from print jobs and faxes, and documents in the trash or recycle bin that should have been shredded.
- **Records and Equipment**
  - The category of records and equipment deserves the same consideration as any other crucial asset. No matter how dependent we become as a society upon electronically storing and processing records, there will always be the file cabinet containing paper records.

Choosing Site Location for Security

- As they say in real estate, "Location is everything." When it comes to physical security this particular saying hits close to home. When choosing a location for a data center or office site, survivability should be considered more important than cost.
- **There are many security considerations for choosing a secure site location**
  - **Accessibility** (If a site is located too remotely to be practical, usability and commutability are affected)
  - **Lighting** (Proper lighting, especially for organizations with 24×7 operations, should be evaluated and taken into consideration.)
  - **Proximity to other buildings** (Know who your neighbors are.)
  - **Proximity to law enforcement and emergency response** (if an emergency service unit were to be called to respond to an incident at this location, it has to respond quickly)
  - **RF and wireless transmission interception** (wireless hacking and hijacking become more of a threat. Other airborne" protocols that should be taken into consideration include radio frequency devices)

Securing Assets: Locks and Entry Controls

- Anything of value that is capable of "growing legs and wandering away" should have a lock or be secured in a location that has a lock.
- **Doors and File Cabinets**
  - Make sure the lock on the door functions correctly and can withstand sufficient force.
- **Laptops**
  - Laptops at the office, when not in transport, should be physically locked to the desk or in the docking station.
- **Data Centers, Wiring Closets, Network Rooms**

  - All of these areas should have common access controls, as they all perform a similar function. Make sure these rooms are kept locked. If automatic entry-tracking mechanisms are not in use, ensure an access log is kept.
- **Entry Controls**
  - you must first consider the site in which the entry controls will be deployed.
- **Building Access Control Systems**
  - access control systems that control entrance into the building or entrance to a special parking lot that is common to the entire building.
- **Building and Employee IDs**
  - Typically, one of the first things any organization does after hiring new employees is to provide them with ID badges. Building and/or employee identification should be displayed at all times, and anyone who lacks a visible ID should be challenged.
- **Biometrics**
  - A *biometric device* is classified as any device that uses distinctive personally identifiable characteristics or unique physical traits to positively identify an individual.
- **Security Guards**
  - A security guard is employed by an organization, company, or agency to patrol, guard, monitor, preserve, protect, support, and maintain the security and safety of personnel and property.

Physical Intrusion Detection

- **Closed-Circuit Television**
  - Physical intrusion detection, much like its information counterpart, requires forethought, planning, and tuning to obtain optimal effectiveness.
  - Placement of CCTV devices should be thought out with financial and operational limitations in mind. Some possible initial areas for device placement include: high-traffic areas, critical function areas (such as parking structures, loading docks, and research areas), cash handling areas, and areas of transition (such as the hallway leading from a conference room to a sensitive location).
  - Ensure that the cabling used for CCTV devices is not readily accessible, so that no one can easily tap into transmissions. Lighting will also play a critical role in the effectiveness of the camera.
- **Alarms**
  - Alarms should be tested at least monthly, and a test log should be kept. Points of entry and exit should be fitted with intrusion alarms.
  - A response plan should be in effect, and everyone who will be responding to an incident must know exactly what their roles and responsibilities are.