# Fundamentals of Information Systems Security/Access Control Systems



*Access controls* are security features that control how users and systems communicate and interact with other systems and resources.

*Access* is the flow of information between a subject and an object.

A *subject* is an active entity that requests access to an object or the data within an object. E.g.: user, program, process etc.

An *object* is a passive entity that contains the information. E.g.: Computer, Database, File, Program etc.

Access controls give organization the ability to control, restrict, monitor, and protect resource availability, integrity and confidentiality

## Contents

### Access Control Challenges[]

- *Various types of users need different levels of access* - Internal users, contractors, outsiders, partners, etc.
- *Resources have different classification levels*- Confidential, internal use only, private, public, etc.
- *Diverse identity data must be kept on different types of users* - Credentials, personal data, contact information, work-related data, digital certificates, cognitive passwords, etc.
- *The corporate environment is continually changing*- Business environment needs, resource access needs, employee roles, actual employees, etc.

### Access Control Principles[]

- *Principle of Least Privilege*: States that if nothing has been specifically configured for an individual or the groups, he/she belongs to, the user should not be able to access that resource i.e.Default no access
- *Separation of Duties*: Separating any conflicting areas of responsibility so as to reduce opportunities for unauthorized or unintentional modification or misuse of organizational assets and/or information.
- *Need to know* : It is based on the concept that individuals should be given access only to the information that they absolutely require in order to perform their job duties

### Access Control Criteria[]

The criteria for providing access to an object include

- Roles
- Groups
- Location
- Time
- Transaction Type

### Access Control Practices[]

- Deny access to systems by undefined users or anonymous accounts.
- Limit and monitor the usage of administrator and other powerful accounts.
- Suspend or delay access capability after a specific number of unsuccessful logon attempts.
- Remove obsolete user accounts as soon as the user leaves the company.
- Suspend inactive accounts after 30 to 60 days.
- Enforce strict access criteria.
- Enforce the need-to-know and least-privilege practices.
- Disable unneeded system features, services, and ports.
- Replace default password settings on accounts.
- Limit and monitor global access rules.
- Ensure that logon IDs are nondescriptive of job function.
- Remove redundant resource rules from accounts and group memberships.
- Remove redundant user IDs, accounts, and role-based accounts from resource access lists.
- Enforce password rotation.
- Enforce password requirements (length, contents, lifetime, distribution, storage, and transmission).
- Audit system and user events and actions and review reports periodically.
- Protect audit logs.

## Security Principles[]

- Fundamental Principles (CIA)
- Identification
- Authentication
- Authorization
- Non Repudiation

## Identification Authentication and Authorization []

*Identification* describes a method of ensuring that a subject is the entity it claims to be. E.g.: A user name or an account no.

*Authentication* is the method of proving the subjects identity. E.g.: Password, Passphrase, PIN

*Authorization* is the method of controlling the access of objects by the subject. E.g.: A user cannot delete a particular file after logging into the system

**Note:** There must be a three step process of Identification, Authentication and Authorization in order for a subject to access an object

### Identification and Authentication[]

### Identification Component Requirements[]

When issuing identification values to users or subjects, ensure that

- Each value should be unique, for user accountability
- A standard naming scheme should be followed

- The values should be non-descriptive of the users position or task
- The values should not be shared between the users.

### Authentication Factors[]

There are 3 general factors for authenticating a subject.

- Something a person knows- E.g.: passwords, PIN- least expensive, least secure
- Something a person has – E.g.: Access Card, key- expensive, secure
- Something a person is- E.g.: Biometrics- most expensive, most secure

**Note:** For a strong authentication to be in process, it must include two out of the three authentication factors- also referred to as two factor authentication.

### Authentication Methods[]

### Biometrics[]

- Verifies an individuals identity by analyzing a unique personal attribute or behavior
- It is the most effective and accurate method for verifying identification.
- It is the most expensive authentication mechanism
- Types of Biometric Systems
    - *Finger Print*- are based on the ridge endings, bifurcation exhibited by the friction edges and some minutiae of the finger
    - *Palm Scan*- are based on the creases, ridges, and grooves that are unique in each individuals palm
    - Hand Geometry- are based on the shape (length, width) of a persons hand and fingers
    - *Retina Scan*- is based on the blood vessel pattern of the retina on the backside of the eyeball.
    - *Iris Scan*- is based on the colored portion of the eye that surrounds the pupil. The iris has unique patterns, rifts, colors, rings, coronas and furrows.
    - *Signature Dynamics*- is based on electrical signals generated due to physical motion of the hand during signing a document
    - *Keyboard Dynamics*- is based on electrical signals generated while the user types in the keys (passphrase) on the keyboard.
    - *Voice Print*- based on human voice
    - *Facial Scan*- based on the different bone structures, nose ridges, eye widths, forehead sizes and chin shapes of the face.
    - *Handy Topography*- based on the different peaks, valleys, overall shape and curvature of the hand.
- Types of Biometric Errors
    - *Type I Error*: When a biometric system rejects an authorized individual ( false rejection rate)
    - *Type II Error*: When a biometric systems accepts imposters who should be rejected (false acceptance rate)
    - Crossover Error Rate (CER): The point at which the false rejection rate equals false acceptance rate. It is also called as Equal Error Rate (EER).

## Passwords[]

- It is the most common form of system identification and authentication mechanism
- A password is a protected string of characters that is used to authenticate an individual
- Password Management
    - Password should be properly guaranteed, updated, and kept secret to provide and effective security
    - Passwords generators can be used to generate passwords that are uncomplicated, pronounceable, non-dictionary words.
    - If the user chooses his passwords, the system should enforce certain password requirement like insisting to use special char, no of char, case sensitivity etc. )
- Techniques for Passwords Attack
    - Electronic monitoring- Listening to network traffic to capture information, especially when a user is sending her password to an authentication server. The password can be copied and reused by the attacker at another time, which is called a replay attack.
    - Access the password file- Usually done on the authentication server. The password file contains many users' passwords and, if compromised, can be the source of a lot of damage. This file should be protected with access control mechanisms and encryption.
    - Brute force attacks Performed with tools that cycle through many possible character, number, and symbol combinations to uncover a password.
    - Dictionary attacks Files of thousands of words are used to compare to the user's password until a match is found.
    - Social engineering An attacker falsely convinces an individual that she has the necessary authorization to access specific resources
- Password checkers can be used to check the strength of the password by trying to break into the system
- Passwords should be encrypted and hashed
- Password aging should be implemented
- No of logon attempts should be limited

## Cognitive Passwords[]

- Cognitive passwords are facts or opinion-based information used to verify an individual identity (e.g.: mothers maidens name)
- This is best used for helpdesk services, and occasionally used services.

## One-Time or Dynamic Passwords[]

- It is a token based system used for authentication purposes where the service is used only once
- It is used in environments that require a higher level of security than static password provides
- Types of token generators
    - Synchronous (e.g.: SecureID) - A synchronous token device/generator synchronizes with the authentication service by any of the two means.

        - Time Based: In this method the token device and the authentication service must hold the same time within their internal clocks. The time value on the token device and a secret key are used to create a one time password. This password is decrypted by the server and compares it to the value that is expected.
        - Counter Based: In this method the user will need to initiate the logon sequence on the computer and push a button on the token device. This causes the token device and the authentication service to advance to the next authentication value. This value and a base secret are hashed and displayed to the user. The user enters this resulting value along with a user ID to be authenticated.
    - Asynchronous: A token device that is using an asynchronous token-generating method uses a challenge/response scheme to authenticate the user. In this situation, the authentication server sends the user a challenge, a random value also called a nonce. The user enters this random value into the token device, which encrypts it and returns a value that the user uses as a one-time password. The user sends this value, along with a username, to the authentication server. If the authentication server can decrypt the value and it is the same challenge value that was sent earlier, the user is authenticated
- Example: SecureID
    - It is one of the most widely used time-based tokens from RSA Security
    - It uses a time based synchronous two-factor authentication

### Cryptographic Keys[]

- Uses private keys and Digital Signatures
- Provides a higher level of security than passwords.

### Passphrase[]

- A passphrase is a sequence of characters that is longer than a password and in some cases, takes the place of a password during an authentication process.
- The application transforms the pass phrase into a virtual password and into a format required by the application
- It is more secure than passwords

### Memory Cards[]

- Holds information but cannot process them
- More secure than passwords but costly
- E.g.: Swipe cards, ATM cards

### Smart Cards[]

- Holds information and has the capability to process information and can provide a two factor authentication (knows and has)
- Categories of Smart Cards

    - Contact
    - Contactless
        - Hybrid- has 2 chips and supports both contact and contactless
        - Combi- has a microprocessor that can communicate with both a contact as well as a contact reader.
- More expensive and tamperproof than memory cards
- Types of smartcard attacks
    - Fault generation: Introducing of computational errors into smart card with the goal of uncovering the encryption keys that are being used and stored on cards
    - Side Channel Attacks: These are non-intrusive attacks and are used to uncover sensitive information about how a component works without trying to compromise any type of flaw or weakness. The following are some of the examples
        - Differential Power Analysis: Examining the power emission that are released during processing
        - Electromagnetic Analysis: Examining the frequency that are emitted
    - Timing: How long a specific process takes to complete
    - Software Attacks: Inputting instructions into the card that will allow for the attacker to extract account information. The following are some of the examples
        - Microprobing: Uses needles to remove the outer protective material on the cards circuits by using ultrasonic vibrations thus making it easy to tap the card ROM chip
- Smart Card Standards
    - ISO/IEC
        - 14443-1: Physical Characteristics
        - 14443-2: Radio frequency power and signal interface
        - 14443-3: Initialization and anti collision
        - 14443-4: Transmission protocol

### Identity Management[]

- Identity Management is a broad term that encompasses the use of different products to identify, authenticate and authorize users through automated means.
- Identity management system is the management of the identity life cycle of entities (subjects or objects) during which:
- The identity is established:
    - a name (or number) is associated to the subject or object;
    - the identity is re-established: a new or additional name (or number) is connected to the subject or object;
- The identity is described:
    - one or more attributes which are applicable to this particular subject or object may be assigned to the identity;

    - the identity is newly described: one or more attributes which are applicable to this particular subject or object may be changed;

- The identity is destroyed.
- Identity Management Challenges
- Identity Management Technologies
- Authorization Principles

## Access Control Categories[]

Access controls can be implemented at various layers of a network and individual systems.

The access controls can be classified into three layers or categories, each category having different access control mechanisms that can be carried out manually or automatically.

- Administrative Controls
- Physical Controls
- Technical or Logical Controls

Each category of access control has several components that fall within it, as described

### Administrative[]

The administrative controls are defined by the top management in an organization.

### Administrative Control Components[]

#### Policy and Procedures

- A security policy is a high-level plan that states management's intent pertaining to how security should be practiced within an organization, what actions are acceptable, and what level of risk the company is willing to accept. This policy is derived from the laws, regulations, and business objectives that shape and restrict the company.
- The security policy provides direction for each employee and department regarding how security should be implemented and followed, and the repercussions for noncompliance. Procedures, guidelines, and standards provide the details that support and enforce the company's security policy.

#### Personnel Controls

- Personnel controls indicate how employees are expected to interact with security mechanisms, and address noncompliance issues pertaining to these expectations.
- Change of Status: These controls indicate what security actions should be taken when an employee is hired, terminated, suspended, moved into another department, or promoted.
- Separation of duties: The separation of duties should be enforced so that no one individual can carry out a critical task alone that could prove to be detrimental to the company.

Example: A bank teller who has to get supervisory approval to cash checks over $2000 is an example of separation of duties. For a security breach to occur, it would require collusion, which means that more than one person would need to commit fraud, and their efforts would need to be concerted. The use of separation of duties drastically reduces the probability of security breaches and fraud.

- Rotation of duties means that people rotate jobs so that they know how to fulfill the obligations of more than one position. Another benefit of rotation of duties is that if an individual attempts to commit fraud

within his position, detection is more likely to happen if there is another employee who knows what tasks should be performed in that position and how they should be performed.

#### Supervisory Structure

- Management must construct a supervisory structure which enforces management members to be responsible for employees and take a vested interest in their activities. If an employee is caught hacking into a server that holds customer credit card information, that employee and her supervisor will face the consequences?

#### Security-Awareness Training

- This control helps users/employees understand hot to properly access resources, why access controls are in place and the ramification for not using the access controls properly.

#### Testing

- This control states that all security controls, mechanisms, and procedures are tested on a periodic basis to ensure that they properly support the security policy, goals, and objectives set for them.
- The testing can be a drill to test reactions to a physical attack or disruption of the network, a penetration test of the firewalls and perimeter network to uncover vulnerabilities, a query to employees to gauge their knowledge, or a review of the procedures and standards to make sure they still align with business or technology changes that have been implemented.

### Examples of Administrative Controls[]

- Security policy
- Monitoring and supervising
- Separation of duties
- Job rotation
- Information classification
- Personnel procedures
- Investigations
- Testing
- Security-awareness and training

### Physical[]

Physical controls support and work with administrative and technical (logical) controls to supply the right degree of access control.

### Physical Control Components[]

#### Network Segregation

- Network segregation can be carried out through physical and logical means. A section of the network may contain web servers, routers, and switches, and yet another network portion may have employee workstations.
- Each area would have the necessary physical controls to ensure that only the permitted individuals have access into and out of those sections.

**Perimeter Security**

- The implementation of perimeter security depends upon the company and the security requirements of that environment.
- One environment may require employees to be authorized by a security guard by showing a security badge that contains picture identification before being allowed to enter a section. Another environment may require no authentication process and let anyone and everyone into different sections.
- Perimeter security can also encompass closed-circuit TVs that scan the parking lots and waiting areas, fences surrounding a building, lighting of walkways and parking areas, motion detectors, sensors, alarms, and the location and visual appearance of a building. These are examples of perimeter security mechanisms that provide physical access control by providing protection for individuals, facilities, and the components within facilities.

**Computer Controls**

- Each computer can have physical controls installed and configured, such as locks on the cover so that the internal parts cannot be stolen, the removal of the floppy and CD-ROM drives to prevent copying of confidential information, or implementation of a protection device that reduces the electrical emissions to thwart attempts to gather information through airwaves.

**Work Area Separation**

- Some environments might dictate that only particular individuals can access certain areas of the facility.

**Data Backups**

- Backing up data is a physical control to ensure that information can still be accessed after an emergency or a disruption of the network or a system.

**Cabling**

- There are different types of cabling that can be used to carry information throughout a network.
- Some cable types have sheaths that protect the data from being affected by the electrical interference of other devices that emit electrical signals.
- Some types of cable have protection material around each individual wire to ensure that there is no crosstalk between the different wires.
- All cables need to be routed throughout the facility in a manner that is not in people’s way or that could be exposed to any danger of being cut, burnt, crimped, or eavesdropped upon.

**Control Zone**

- It is a specific area that surrounds and protects network devices that emit electrical signals. These electrical signals can travel a certain distance and can be contained by a specially made material, which is used to construct the control zone.
- The control zone is used to resist penetration attempts and disallow sensitive information to “escape” through the airwaves.
- A control zone is used to ensure that confidential information is contained and to hinder intruders from accessing information through the airwaves.
- Companies that have very sensitive information would likely protect that information by creating control zones around the systems that are processing that information

## Examples of Physical Control[]

- Fences
- Locks
- Badge system
- Security guard
- Biometric system
- Mantrap doors
- Lighting
- Motion detectors
- Closed-circuit TVs
- Alarms
- Backups
- safe storage area of backups

## Technical[]

Technical controls called logical controls are the s/w tools used to restrict subject's access to objects. They can be core OS components, add-on security packages, applications, n/w h/w devices, protocols, encryption mechanisms, and access control metrics.

They protect the integrity and availability of resources by limiting the number of subjects that can access them and protect the confidentiality of resources by preventing disclosure to unauthorized subjects.

## Technical Control Components[]

### System Access

- In this type, control of access to resources is based on the sensitivity of data, clearance level of users, and user's rights and permissions. As technical control for system access can be a user name password, Kerberos implementation, biometrics, PKI, RADIUS, TACACS or authentication using smartcards.

### Network Access

- This control defines the access control mechanism to access the different network resources like the routers, switches, firewalls, bridges etc.

### Encryption and protocols

- These controls are used to protect information as it passes throughout an n/w and resides on computers. They preserve the confidentiality and integrity of data and enforce specific paths for communication to take place.

### Auditing

- These controls track activity within a n/w, on a n/w device or on a specific computer .They help to point out weakness of other technical controls and make the necessary changes.

### Network Architecture

- This control defines the logical and physical layout of the network, and also the access control mechanisms between different n/w segments.

## Examples of Technical Controls[]

- ACLs
- Routers
- Encryption
- Audit logs
- IDS
- Antivirus software
- Firewalls
- Smart cards
- Dial-up call-back systems
- Alarms and alerts

## Access Control Types[]

Each of the access control categories – administrative, physical and technical work at different levels, each at a different level of granularity and perform different functionalities based on the type.

The different types of access control are

- Preventative- Avoid undesirable events from occurring
- Detective- Identify undesirable events that have occurred
- Corrective- Correct undesirable events that have occurred
- Deterrent- Discourage security violations
- Recovery- Restore resources and capabilities
- Compensative- Provide alternatives to other controls

## Access Control Threats[]

### Denial of Service(DoS/DDoS)[]

#### Overview

- A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the means to, motives for, and targets of a DoS attack may vary, it generally consists of the concerted, malevolent efforts of a person or persons to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely.
- The purpose of DoS attacks is to force the targeted computer(s) to reset, or consume its resources so that it can no longer provide its intended service

#### Types of DoS Attacks

A DoS attack can be perpetrated in a number of ways. There are five basic types of attack:

- Consumption of computational resources, such as bandwidth, disk space, or CPU time;
- Disruption of configuration information, such as routing information;
- Disruption of state information, such as unsolicited resetting of TCP sessions;
- Disruption of physical network components.
- Obstructing the communication media between the intended users and the victim so that they can no

longer communicate adequately.

**Countermeasures**

Unfortunately, there are no effective ways to prevent being the victim of a DoS or DDoS attack, but there are steps you can take to reduce the likelihood that an attacker will use your computer to attack other computers:

- Install and maintain anti-virus software.
- Install a firewall, and configure it to restrict traffic coming into and leaving your computer.
- Follow good security practices for distributing your email address.Applying email filters may help you manage unwanted traffic.

## Buffer Overflows[]

**Overview**

- A buffer overflow is an anomalous condition where a process attempts to store data beyond the boundaries of a fixed-length buffer. The result is that the extra data overwrites adjacent memory locations. The overwritten data may include other buffers, variables and program flow data and may cause a process to crash or produce incorrect results. They can be triggered by inputs specifically designed to execute malicious code or to make the program operate in an unintended way. As such, buffer overflows cause many software vulnerabilities and form the basis of many exploits.

**Buffer Overflow Techniques**

- *Stack Buffer Overflow*
    - A stack buffer overflow occurs when a program writes to a memory address on the program's call stack outside of the intended data structure; usually a fixed length buffer.
    - Stack buffer overflow bugs are caused when a program writes more data to a buffer located on the stack than there was actually allocated for that buffer. This almost always results in corruption of adjacent data on the stack, and in cases where the overflow was triggered by mistake, will often cause the program to crash or operate incorrectly.
    - A technically inclined and malicious user may exploit stack-based buffer overflows to manipulate the program in one of several ways:
        - By overwriting a local variable that is near the buffer in memory on the stack to change the behaviour of the program which may benefit the attacker.
        - By overwriting the return address in a stack frame. Once the function returns, execution will resume at the return address as specified by the attacker, usually a user input filled buffer.
        - By overwriting a function pointer,or exception handler, which is subsequently executed.
- *Heap Buffer Overflow*
    - A heap overflow is another type of buffer overflow that occurs in the heap data area. Memory on the heap is dynamically allocated by the application at run-time and typically contains program data.
    - Exploitation goes as follows: If an application copies data without first checking to see if it fits into the chunk (blocks of data in the heap), the attacker could supply the application with a piece of data that is too large, overwriting heap management information (metadata) of the next chunk. This allows an attacker to overwrite an arbitrary memory location with four bytes of data. In most environments, this may allow the attacker control over the program execution.

**Countermeasure**

- Choice of programming language
- Use of safe libraries
- Stack-smashing protection which refers to various techniques for detecting buffer overflows on stack-allocated variables.The most common implementation being StackGuard, and SSP
- Executable space protection which is the marking of memory regions as non-executable, such that an attempt to execute machine code in these regions will cause an exception. It makes use of hardware features such as the NX bit (Non Execute bit).
- Address space layout randomization: A technique which involves arranging the positions of key data areas, usually including the base of the executable and position of libraries, heap, and stack, randomly in a process' address space.
- Deep packet inspection:It is a form of computer network packet filtering that examines the data and/or header part of a packet as it passes an inspection point, searching for non-protocol compliance, viruses, spam, intrusions or predefined criteria to decide if the packet can pass or if it needs to be routed to a different destination, or for the purpose of collecting statistical information. It also called Content Inspection or Content Processing.

## Malicious Software[]

## Password Crackers[]

## Spoofing/Masquerading[]

#### Overview

- A spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.
- Popular Spoofing Techniques
    - *Man-in-the-middle attack (MITM):*An attack in which an attacker is able to read, insert and modify at will messages between two parties without either party knowing that the link between them has been compromised. The attacker must be able to observe and intercept messages going between the two victims
    - *IP address Spoofing* : refers to the creation of IP packets with a forged (spoofed) source IP address with the purpose of concealing the identity of the sender or impersonating another computing system.
    - *URL spoofing*: A Spoofed URL describes one website that poses as another
    - *Phishing* :An attempt to criminally and fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication.
    - *Referrer spoofing*:It is the sending of incorrect referrer information along with an HTTP request, sometimes with the aim of gaining unauthorized access to a web site. It can also be used because of privacy concerns, as an alternative to sending no referrer at all.
    - *Spoofing of file-sharing Networks*: Polluting the file-sharing networks where record labels share files that are mislabeled, distorted or empty to discourage downloading from these sources.
    - *Caller ID spoofing* :This allows callers to lie about their identity, and present false names and numbers, which could of course be used as a tool to defraud or harass
    - *E-mail address spoofing:*A technique commonly used for spam e-mail and phishing to hide the origin of an e-mail message by changing certain properties of the e-mail, such as the From,

Return-Path and Reply-To fields.

- *Login spoofing* : A technique used to obtain a user's password. The user is presented with an ordinary looking login prompt for username and password, which is actually a malicious program, usually called a Trojan horse under the control of the attacker. When the username and password are entered, this information is logged or in some way passed along to the attacker, breaching security.

**Countermeasures**

- Be skeptical of e-mails indicating that you need to make changes to your accounts or warnings indicating that accounts will be terminated without you doing some type of activity online.
- Call the legitimate company to find out if this is a fraudulent message.
- Review the address bar to see if the domain name is correct.
- When submitting any type of financial information or credential data, an SSL connection should be set up, which is indicated in the address bar (https://) and a closed-padlock icon in the browser at the bottom-right corner.
- Do not click on an HTML link within an e-mail. Type the URL out manually instead.
- Do not accept e-mail in HTML format.

## Emanations[]

**Overview**

- All electronic devices emit electrical signals. These signals can hold important information, and if an attacker buys the right equipment and positions himself in the right place, he could capture this information from the airwaves and access data transmissions as if he had a tap directly on the network wire.

**Countermeasure**

- Tempest: Tempest is the name of a program, and now a standardized technology that suppresses signal emanations with shielding material. Vendors who manufacture this type of equipment must be certified to this standard. In devices that are Tempest rated, other components are also modified, especially the power supply, to help reduce the amount of electricity that is used unlike the normal devices which have just an outer metal coating, referred to as a Faraday cage. This type of protection is usually needed only in military institutions, although other highly secured environments do utilize this type of safeguard.
    - Tempest Technologies: Tempest technology is complex, cumbersome, and expensive, and therefore only used in highly sensitive areas that really need this high level of protection. Two alternatives to Tempest exist
        - White Noise: White noise is a uniform spectrum of random electrical signals. It is distributed over the full spectrum so that the bandwidth is constant and an intruder is not able to decipher real information from random noise or random information.
        - Control Zone: Some facilities use material in their walls to contain electrical signals. This prevents intruders from being able to access information that is emitted via electrical signals from network devices. This control zone creates a type of security perimeter and is constructed to protect against unauthorized access to data or compromise of sensitive information.

## Shoulder Surfing[]

#### Overview

- Shoulder surfing refers to using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is particularly effective in crowded places because it's relatively easy to observe someone as they:
    - Fill out a form
    - Enter their PIN at an automated teller machine or a POS Terminal
    - Use a calling card at a public pay phone
    - Enter passwords at a cybercafe, public and university libraries, or airport kiosks.
    - Enter a digit code for a rented locker in a public place such as a swimming pool or airport.
- Shoulder surfing is also be done at a distance using binoculars or other vision-enhancing devices. Inexpensive, miniature closed-circuit television cameras can be concealed in ceilings, walls or fixtures to observe data entry. To prevent shoulder surfing, it is advised to shield paperwork or the keypad from view by using one's body or cupping one's hand.
- Recent automated teller machines now have a sophisticated display which discourages shoulder surfers. It grows darker beyond a certain viewing angle, and the only way to tell what is displayed on the screen is to stand directly in front of it.
- Certain models of credit card readers have the keypad recessed, and employ a rubber shield that surrounds a significant part of the opening towards the keypad. This makes shoulder-surfing significantly harder, as seeing the keypad is limited to a much more direct angle than previous models. Taken further, some keypads alter the physical location of the keys after each keypress. Also, security cameras are not allowed to be placed directly above an ATM.

### Object Reuse[]

#### Overview

- Object reuse issues pertain to reassigning to a subject media that previously contained one or more objects.
- The sensitive information that may be left by a process should be securely cleared before allowing another process the opportunity to access the object. This ensures that information not intended for this individual or any other subject is not disclosed.
- For media that holds confidential information, more extreme methods should be taken to ensure that the files are actually gone, not just their pointers.

#### Countermeasures

- Sensitive data should be classified by the data owners.
- How the data is stored and accessed should also be strictly controlled and audited by software controls.
- Before allowing one subject to use media that was previously used, the media should be erased or degaussed. If media holds sensitive information and cannot be purged, there should be steps on how to properly destroy it so that there is no way for others to obtain this information.

### Data Remanence[]

#### Overview

- Data remanence is the residual representation of data that has been in some way been nominally erased or removed. This residue may be due to data being left intact by a nominal delete operation, or through physical properties of the storage medium.

- Data remanence may make inadvertent disclosure of sensitive information possible, should the storage media be released into an uncontrolled environment.

**Countermeasures**

- Classes of Countermeasures
    - *Clearing*
        - Clearing is the removal of sensitive data from storage devices in such a way that there is assurance, proportional to the sensitivity of the data, that the data may not be reconstructed using normal system functions. The data may still be recoverable, but not without unusual effort.
        - Clearing is typically considered an administrative protection against accidental disclosure within an organization. For example, before a floppy disk is re-used within an organization, its contents may be cleared to prevent their accidental disclosure to the next user.
    - *Purging*
        - Purging or sanitizing is the removal of sensitive data from a system or storage device with the intent that the data can not be reconstructed by any known technique.
        - Purging is generally done before releasing media outside of control, such as before discarding old media, or moving media to a computer with different security requirements.
- Methods to Countermeasure
    - Overwriting
        - A common method used to counter data remanence is to overwrite the storage medium with new data. This is often called a wiping or shredding a file or disk. Because such methods can often be implemented in software alone, and may be able to selectively target only part of a medium, it is a popular, low-cost option for some applications.
        - The simplest overwrite technique writes the same data everywhere -- often just a pattern of all zeros. At a minimum, this will prevent the data from being retrieved simply by reading from the medium again, and thus is often used for clearing.
    - Degaussing
        - Degaussing is the removal or reduction of a magnetic field. Applied to magnetic media, degaussing may purge an entire media element quickly and effectively. A device, called a degausser, designed for the media being erased, is used.
        - Degaussing often renders hard disks inoperable, as it erases low-level formatting which is only done at the factory, during manufacture. Degaussed floppy disks can generally be reformatted and reused.
    - Encryption
        - Encrypting data before it is stored on the medium may mitigate concerns about data remanence. If the decryption key is strong and carefully controlled (i.e., not itself subject to data remanence), it may effectively make any data on the medium unrecoverable. Even if the key is stored on the medium, it may prove easier or quicker to overwrite just the key, vs the entire disk.
        - Encryption may be done on a file-by-file basis, or on the whole disk.
    - Physical destruction

    - Physical destruction of the data storage medium is generally considered the most certain way to counter data remanence, although also at the highest cost. Not only is the process generally time-consuming and cumbersome, it obviously renders the media unusable. Further, with the high recording densities of modern media, even a small media fragment may contain large amounts of data.
    - Specific destruction techniques include:
        - Physically breaking the media apart, by grinding, shredding, etc.
        - Incinerating
        - Phase transition (i.e., liquification or vaporization of a solid disk)
        - Application of corrosive chemicals, such as acids, to recording surfaces
        - For magnetic media, raising its temperature above the Curie point

## Backdoor/Trapdoor[]

### Overview

- A backdoor is a malicious computer program or particular means that provide the attacker with unauthorized remote access to a compromised system exploiting vulnerabilities of installed software and bypassing normal authentication.
- A backdoor works in background and hides from the user. It is very similar to a virus and therefore is quite difficult to detect and completely disable.
- A backdoor is one of the most dangerous parasite types, as it allows a malicious person to perform any possible actions on a compromised computer. The attacker can use a backdoor to
    - spy on a user,
    - manage files,
    - install additional software or dangerous threats,
    - control the entire system including any present applications or hardware devices,
    - shutdown or reboot a computer or
    - attack other hosts.
- Often a backdoor has additional harmful capabilities like keystroke logging, screenshot capture, file infection, even total system destruction or other payload. Such parasite is a combination of different privacy and security threats, which works on its own and doesn’t require to be controlled at all.
- Most backdoors are autonomic malicious programs that must be somehow installed to a computer. Some parasites do not require the installation, as their parts are already integrated into particular software running on a remote host. Programmers sometimes left such backdoors in their software for diagnostics and troubleshooting purposes. Hackers often discover these undocumented features and use them to break into the system.

### Countermeasure

- Powerful antivirus and anti-spyware products

## Dictionary Attacks[]

### Overview

- Dictionary attacks are launched by programs which are fed with a lists (dictionaries) of commonly used words or combinations of characters, and then compares these values to capture passwords.
- Once the right combination of characters is identified, the attacker can use this password to authenticate herself as a legitimate user.
- Sometimes the attacker can even capture the password file using this kind of activity.

**Countermeasures**

To properly protect an environment against dictionary and other password attacks, the following practices should be followed:

- Do not allow passwords to be sent in cleartext.
- Encrypt the passwords with encryption algorithms or hashing functions.
- Employ one-time password tokens.
- Use hard-to-guess passwords.
- Rotate passwords frequently.
- Employ an IDS to detect suspicious behavior.
- Use dictionary cracking tools to find weak passwords chosen by users.
- Use special characters, numbers, and upper- and lowercase letters within the password.
- Protect password files.

## Bruteforce Attacks[]

**Overview**

- Brute force is defined as “trying every possible combination until the correct one is identified.”
- The most effective way to uncover passwords is through a hybrid attack, which combines a dictionary attack and a brute force attack
- A brute force attack is also known as an exhaustive attack.
- These are usually used for wardialing in hopes of finding a modem that can be exploited to gain unauthorized access.

**Countermeasures**

For phone brute force attacks, auditing and monitoring of this type of activity should be in place to uncover patterns that could indicate a wardialing attack:

- Perform brute force attacks to find weaknesses and hanging modems.
- Make sure only necessary phone numbers are made public.
- Provide stringent access control methods that would make brute force attacks less successful.
- Monitor and audit for such activity.
- Employ an IDS to watch for suspicious activity.
- Set lockout thresholds.

## Social Engineering[]

**Overview**

- Social engineering is a collection of techniques used for manipulation of the natural human tendency to

trust in order to obtain information that will allow a hacker to gain unauthorized access to a valued system and the information that resides on that system.

- Forms of a Social engineering attack
    - Physical: the workplace, the phone, your trash(dumpster diving), and even on-line
    - Psychological: Persuasion
    - Reverse Social Engineering

**Common Social Engineering Attacks**

- At work Place
    - In the workplace, the hacker can simply walk in the door, like in the movies, and pretend to be a maintenance worker or consultant who has access to the organization. Then the intruder struts through the office until he or she finds a few passwords lying around and emerges from the building with ample information to exploit the network from home later that night
    - Another technique to gain authentication information is to just stand there and watch an oblivious employee type in his password.
- On Phone/Help Desk
    - It its the most prevalent type of social engineering attack.
    - A hacker will call up and imitate someone in a position of authority or relevance and gradually pull information out of the user.
    - Help desks are particularly prone to this type of attack. Hackers are able to pretend they are calling from inside the corporation by playing tricks on the PBX or the company operator, so caller-ID is not always the best defense
    - Help desks are particularly vulnerable because they are in place specifically to help, a fact that may be exploited by people who are trying to gain illicit information
- Dumpster Diving
    - Dumpster diving, also known as trashing, is another popular method of social engineering. A huge amount of information can be collected through company dumpsters (trash can).
    - The following items turn to be a potential security leaks in our trash:
        - company phone books which can give the hackers names and numbers of people to target and impersonate
        - organizational charts contain information about people who are in positions of authority within the organization
        - memos provide small tidbits of useful information for creating authenticity
        - company policy manuals show hackers how secure (or insecure) the company really is
        - calendars of meetings may tell attackers which employees are out of town at a particular time
        - system manuals, printouts of sensitive data or login names and passwords may give hackers the exact keys they need to unlock the network.
        - disks and tapes can be restored to provide all sorts of useful information.
        - company letterhead and memo forms
- Online

    - One way in which hackers can obtain online passwords is through an on-line form: they can send out some sort of sweepstakes information and ask the user to put in a name (including e-mail address – that way, she might even get that person's corporate account password as well) and password.
    - E-mail can also be used for more direct means of gaining access to a system. For instance, mail attachments sent from someone of authenticity can carry viruses, worms and Trojan horses

- Persuasion
    - This a technique where the hackers themselves teach social engineering from a psychological point-of-view, emphasizing how to create the perfect psychological environment for the attack.
    - Basic methods of persuasion include: impersonation, ingratiation, conformity, diffusion of responsibility, and plain old friendliness.Regardless of the method used, the main objective is to convince the person disclosing the information that the social engineer is in fact a person that they can trust with that sensitive information. The other important key is to never ask for too much information at a time, but to ask for a little from each person in order to maintain the appearance of a comfortable relationship
        - Impersonation generally means creating some sort of character and playing out the role.Some common roles that may be played in impersonation attacks include: a repairman, IT support, a manager, a trusted third party or a fellow employee
        - Conformity is a group-based behavior, but can be used occasionally in the individual setting by convincing the user that everyone else has been giving the hacker the same information requested. When hackers attack in such a way as to diffuse the responsibility of the employee giving the password away, that alleviates the stress on the employee.

- Reverse Social Engineering
    - This is when the hacker creates a persona that appears to be in a position of authority so that employees will ask him for information, rather than the other way around. If researched, planned and executed well, reverse social engineering attacks may offer the hacker an even better chance of obtaining valuable data from the employees; however, this requires a great deal of preparation, research, and pre-hacking to pull off.

**Countermeasures**

- Having proper security policies in place which addresses both physical and psychological aspects of the attack
- Providing proper training to employees, helpdesk personnel

## Access Control Technologies[]

### Single Sign-On[]

**Introduction**

- SSO is a technology that allows a user to enter credentials one time and be able to access all resources in primary and secondary network domains

**Advantages**

- Reduces the amount of time users spend authenticating to resources.
- Enable the administrator to streamline user accounts and better control access rights
- Improves security by reducing the probability that users will write down their passwords

- Reduces the administrators time in managing the access permissions

**Limitations**

- Every platform application and resource needs to accept the same type of credentials, in the same format and interpret their meaning in the same way.

**Disadvantages**

- Once an individual is in, he is in, thus giving a bigger scope to an attacker

## Kerberos[]

**Introduction**

- Kerberos is an authentication protocol that was designed in mid-1980 as part of MIT's project Athena.
- It works in a C/S model and is based on symmetric key cryptography
- It is widely used in UNIX systems and also the default authentication method for windows 2k and 2k3 and is the de-facto standard for heterogeneous networks.

**Kerberos Components**

- Key Distribution Center (KDC)
    - Holds all users and services secret key and info about the principles in the database
    - Provides an authentication service with the help of a service called AS
    - Provides key distribution functionality
    - Provides a ticket granting service (TGS)
- Secret Keys are the keys shared between principle and KDC generally using symmetric key cryptography algorithm that are used to authenticate the principles and communicate securely
- Principles are users, applications or any network services
- A ticket is a token generated by KDC and given to a principle when one principle need to authenticate another principle
- Realm is a set of principles. A KDC can be responsible for one or more realms. Realms allow an administrator to logically group resources and users.
- Session Keys are the keys shared between the principles that will enable them communicate security

**Kerberos Authentication Process**

- User enters username and password into the workstation (WS)
- The Kerberos s/w on the workstation sends the username to the Authentication Server (AS) on the KDC.
- The AS generates a Ticket Granting Ticket (TGT) encrypting it with the user's secret key stored in DB with the help of TGT and sends it to the user.
- The password entered by the user is transformed into a secret key using which the ticket (TGT) is decrypted and thus the user gains access to the WS.
- Suppose the user wants to use the printer, the users system send the TGT to the TGS on the KDC
- The TGS generates a new ticket with two instances of a session key, one encrypted with the user's secret key and the other encrypted with the print server's secret key. This ticket may also contain an authenticator which contains info on user.
- The new ticket is sent to the users system which is used to authenticate with the print server.

- The user's system decrypts and extracts the session key, adds a second authenticator set of identification information to the ticket and sends the ticket onto the print server.
- The print server receives the ticket, decrypts and extracts the session key, and decrypts and extracts the two authenticators in the ticket. If the printer server can decrypt and extract the session key, it knows that the KDC created the ticket, because only the KDC has the secret key that was used to encrypt the session key. If the authenticator information that the KDC and the user put into the ticket matches, then the print server knows that it received the ticket from the correct principal.

#### Weakness of Kerberos

- The KDC can be a single point of failure. If the KDC goes down, no one can access needed resources. Redundancy is necessary for the KDC.
- The KDC must be able to handle the number of requests it receives in a timely manner. It must be scalable.
- Secret keys are temporarily stored on the users' workstation, which means it is possible for an intruder to obtain these cryptographic keys.
- Session keys are decrypted and reside on the users' workstations, either in a cache or in a key table. Again, an intruder can capture these keys.
- Kerberos is vulnerable to password guessing. The KDC does not know if a dictionary attack is taking place.
- Network traffic is not protected by Kerberos if encryption is not enabled.

## SESAME[]

#### Introduction

- SESAME (Secure European Systems for Applications in a Multi-vendor Environment) is a SSO technology that was developed to extend Kerberos functionality and improve upon its weakness.
- SESAME uses a symmetric and asymmetric cryptographic technique to protect exchanges of data and to authenticate subjects to network resources.
- SESAME uses digitally signed privileged Attribute Certificates (PAC) to authenticate subjects to objects. PAC contains the subject's identity, access capabilities for the object, access time period, and life time of the PAC

## Security Domain[]

#### Introduction

- A domain is a set of resources that are available to a subject.
- A security domain refers to the set the resources working under the same security policy and managed by the same group.
- Domains can be separated by logical boundaries, such as
    - Firewalls with ACL's
    - Directory services making access decisions
    - Objects that have their own ACL's indicating which individual or group can access them.
- Domains can be architected in a hierarchical manner that dictates the relationship between the different domains and the ways in which subjects within the different domains can communicate.
- Subjects can access resources in domains of equal or lower trust levels.

### Thin Clients[]

#### Introduction

- Thin clients are diskless computers that are sometimes called as dumb terminals.
- It is based on C/S technology where a user is supposed to logon to a remote server to use the computing and network resources.
- When the user starts the client, it runs a short list of instructions and then points itself to a server that will actually download the operating system, or interactive operating software, to the terminal. This enforces a strict type of access control, because the computer cannot do anything on its own until it authenticates to a centralized server, and then the server gives the computer its operating system, profile, and functionality.
- Thin-client technology provides another type of SSO access for users, because users authenticate only to the central server or mainframe, which then provides them access to all authorized and necessary resources.

## Access Control Models[]

#### Introduction

- An access control model is a framework that dictates how subjects access objects.
- It uses access control technologies and security mechanisms to enforce the rules and objectives of the model.
- There are three main types of access control models:
    - Discretionary,
    - Mandatory, and
    - Nondiscretionary (also called role-based).

### Discretionary Access Control[]

- The control of access is based on the discretion (wish) of the owner
- A system that uses DAC enables the owner of the resource to specify which subjects can access specific resources
- The most common implementation of DAC is through ACL's which are dictated and set by the owners and enforced by the OS.
- Examples: Unix, Linux, Windows access control is based on DAC
- DAC systems grant or deny access based on the identity of the subject. The identity can be user identity or a group identity (Identity based access control)

### Mandatory Access Control[]

- This model is very structured and strict and is based on a security label (also known as sensitivity label) attached to all objects
- The subjects are given security clearance by classifying the subjects as secret, top secret, confidential etc.) and the objects are also classified similarly
- The clearance and the classification data is stored in the security labels, which are bound to the specific subject and object.
- When the system makes a decision about fulfilling a request to access an object it is based on the clearance of the subject. The classification of the object and the security policy of the system

- This model is used and is suitable for military systems where classifications and confidentiality is of at most important
- SE Linux, by NSA, trusted Solaris are examples of this model
- Security label are made up of a classification and categories, where classification indicates the security level and the categories enforce need to know rules.

### Non Discretionary or Role Based Access Control[]

- A RBAC is based on user roles and uses a centrally administered set of controls to determine how subjects and objects interact.
- The RBAC approach simplifies the access control administration
- It is a best system for a company that has high employee turnover.
- Note: The RBAC can be generally used in combination with MAC and DAC systems

### DAC VS MAC VS RBAC[]

| Model | Access Control Owner | Sec Policy enforced by |
|---|---|---|
| DAC | Data Owners | ACL |
| MAC | Operating Systems | Security Labels |
| RBAC | Administrator | Roles/ Functional Position |

## Access Control Techniques[]

Different access control technologies are available to support the different access control models.

- Rule-Based Access Control
- Constrained User Interface
- Access Control Matrix
- Content Dependant Access Control
- Context Dependant Access Control

### Rule-Based Access Control[]

- Rule-based access control uses specific rules that indicate what can and cannot happen between a subject and an object.
- A subject should meet a set of predefined rules before it can access an object.
- It is not necessarily an identity based i.e. it can be applicable to all the users or subjects irrespective of their identities.
- E.g.: Routers and firewall use rules to filter incoming and outgoing packets

### Constrained User Interface[]

- Constrained user interfaces restrict user’s access ability by not allowing them to request certain functions or information, or to have access to specific system resources.
- There are three major types of restricted interfaces:
    - Menus and Shells:

- Database Views
- Physically Constrained Interfaces.

### Access Control Matrix[]

- An access control matrix is a table of subjects and objects indicating what actions individual subjects can take upon individual objects.
- The access rights that are assigned to individual subjects are called capabilities and that assigned to objects are called Access Control Lists (ACL).
- This technique uses a capability table to specify the capabilities of a subject pertaining to specific objects. A capability can be in the form of a token, ticket, or key.
  - Each row is a capability and each column is an ACL for a given user.
  - Kerberos uses a capability based system where every user is given a ticket, which is his capability table.
- ACL's are list of subjects that are authorized to access a specific object and they define what level of authorization is granted ( both at individual and at group level)
- ACL's map values from the access control matrix to the object.
- Note: A capability table is bound to a subject, whereas an ACL is bound to an object.

### Content Dependant Access Control[]

- Access to the objects is based on the content within the object.
- Example: Database Views, E-mail filtering etc.

### Context Dependant Access Control[]

- The access decisions are based on the context of a collection of information rather than on the sensitivity of the data.
- Example: A firewall makes a context-based access decisions when they collect state information on a packet before allowing it into the network.

## Access Control Administration[]

Access control administration can be done in two ways.

- Centralized
- Decentralized.

### Centralized Access Control[edit]

- Here one entity (dept or an individual) is responsible for overseeing access to all corporate resources.
- This type of administration provides a consistent and uniform method of controlling users access rights.
- Example: RADIUS, TACACS and Diameter

#### RADIUS

- It is a c/s authentication protocol that authenticates and authorizes remote users.
- The access server houses the users credentials
- It is an open standard protocol developed by Livingston enterprises.

**TACACS**

- TACACS has been through three generations: TACACS, Extended TACACS (XTACACS), and TACACS+.
    - TACACS combines its authentication and authorization processes,
    - XTACACS separates authentication, authorization, and auditing processes and
    - TACACS+ is XTACACS with extended two-factor user authentication.
- TACACS uses fixed passwords for authentication and TACACS+ allows users to use dynamic (one-time) passwords, which provides more protection.
- TACACS+ provides basically the same functionality as RADIUS with a few differences in some of its characteristics.
    - TACACS+ uses TCP as its transport protocol, while RADIUS uses UDP.
    - RADIUS encrypts the user's password only as it is being transmitted from the RADIUS client to the RADIUS server. Other information, as in the username, accounting, and authorized services, is passed in clear text. This is an open invitation for attackers to capture session information for replay attacks. TACACS+ encrypts all of this data and thus does not have the vulnerabilities that are inherent in the RADIUS protocol
    - The RADIUS protocol combines the authentication and authorization functionality whereas TACACS+ uses a true AAA architecture, which separates the authentication, authorization, and accounting functionalities thus giving the ability to authenticate remote users. TACACS+ also enables to define more granular user profiles, which can control the actual commands that users can carry out

**Note:**RADIUS is the appropriate protocol when simplistic username/password authentication can take place and users only need an Accept or Deny for obtaining access, as in ISPs. TACACS+ is the better choice for environments that require more sophisticated authentication steps and tighter control over more complex authorization activities, as in corporate networks

**Diameter**

- Diameter is a protocol that has been developed to build upon the functionality of RADIUS and overcome many of its limitations. The creator of this protocol decided to call it Diameter as a play on the term RADIUS, as in the diameter is twice the radius.
- Diameter is another AAA protocol that provides the same type of functionality as RADIUS and TACACS+ but also provides more flexibility and capabilities to meet the new demands of today's complex and diverse networks where we want our wireless devices and smart phones to be able to authenticate themselves to our networks and we use roaming protocols, Mobile IP, PPPoE and etc.
- Diameter provides a base protocol, which defines header formats, security options, commands, and AVPs (Attribute Value Pairs). This base protocol allows for extensions to tie in other services, such as VoIP, FoIP, Mobile IP, wireless, and cell phone authentication. So Diameter can be used as an AAA protocol for all of these different uses.
- RADIUS and TACACS+ are client/server protocols, which mean that the server portion cannot send unsolicited commands to the client portion. The server portion can only speak when spoken to. Diameter is a peer-based protocol that allows either end to initiate communication.
    - This functionality allows the Diameter server to send a message to the access server to request the user to provide another authentication credential if she is attempting to access a secure resource.
    - This functionality also allows the Diameter server to disconnect the user if necessary for one reason or another.

- Diameter is backward compatible with RADIUS, uses UDP and AVPs, and provides proxy server support.
- It has better error detection and correction functionality and failover properties than RADIUS, thus provides better network resilience.
- Diameter also provides end-to-end security through the use of IPSec or TLS, which is not available in RADIUS.
- Diameter has the functionality and ability to provide the AAA functionality for other protocols and services because it has a large AVP set. RADIUS has 28 (256) AVPs and Diameter has 232. So, more AVPs allow for more functionality and services to exist and communicate between systems.
- Diameter provides the following AAA function
    - Authentication
        - PAP, CHAP, EAP
        - End-to-end protection of authentication information
        - Replay attack protection
    - Authorization
        - Redirects, secure proxies, relays, and brokers
        - State reconciliation
        - Unsolicited disconnect
        - Reauthorization on demand
    - Accounting
        - Reporting, ROAMOPS accounting, event monitoring

### Decentralized Access Control[]

- A decentralized access control administration method gives control of access to the people closer to the resources
- In this approach, it is often the functional manager who assigns access control rights to employees.
- Changes can happen faster through this type of administration because not just one entity is making changes for the whole organization.
- There is a possibility for conflicts to arise that may not benefit the organization as because different managers and departments can practice security and access control in different ways.
- There is a possibility of certain controls to overlap, in which case actions may not be properly proscribed or restricted.
- This type of administration does not provide methods for consistent control, as a centralized method would.

## Access Control Monitoring(IDS/IPS)[]

Access Control Monitoring is a method of keeping track of who attempts to access specific network resources

The ACM system can fall into two categories: Intrusion Prevention System (IPS) and Intrusion Detection System (IDS)

### Intrusion Detection Systems[]

## Basic Concepts[]

Intrusion detection is the process of detecting an unauthorized use of, or attack upon, a computer, network, or a telecommunication infrastructure.

IDS are designed to aid in mitigating the damage that can be caused by hacking, or breaking into sensitive computer and network systems.

**Common Components of an IDS**

- Sensors: collect traffic and user activity data and send it to an analyzer.
- Analyzer: detects an activity that it is programmed to deem as fishy and sends an alert to the administrative interface.
- Administrative Interface: Report the alert details.

**Common Functions of an IDS**

- Watch for attacks
- Parse audit logs
- Protect system files
- Alert administrators during attacks
- Expose a hackers technique
- Illustrate which vulnerabilities need to be addressed
- Help track down individual hackers

## IDS Types[]

- Network-Based IDS: A network-based IDS (NIDS) uses sensors, which are either host computers with the necessary software installed or dedicated appliances—each with its network interface card (NIC) in promiscuous mode. The NIC driver captures all traffic and passes it to an analyzer to look for specific types of patterns.
- Host-Based IDS: A host-based IDS (HIDS) can be installed on individual workstations and/or servers and watch for inappropriate or anomalous activity. HIDSs are usually used to make sure users do not delete system files, reconfigure important settings, or put the system at risk in any other way.

## IDS Technologies[]

Both HIDS and NIDS can employ the following technologies

- Knowledge or Signature Based
- Statistical Anomaly Based
- Rule Based

**Knowledge or Signature Based**

- These are knowledge based systems where some knowledge is accumulated about specific attacks and a model called signatures is developed.
- The main disadvantage of these systems is they cannot detect new attacks and a few signatures need to be written and continuously updated.
- Also known as misuse-detection system

- Attacks
    - Land Attacks ( packets modified to have the same s/c and destination IP)

**Security Humor:** Attacks or viruses that have been discovered in production environments are referred to as being "in the wild." Attacks and viruses that exist but have not been released are referred to as being "in the zoo."

**Statistical Anomaly Based**

- These are behavioral based systems, which do not use any predefined signatures, but rather are put in a learning mode to build a profile by continually sampling the environments normal activities.
- The longer the IDS is put in a learning mode, in most instances, the more accurate a profile it will build and the better protection it will provide.
- Once a profile is build, a different profile is build based on the same sampling on all the future traffic and the data are compared to identify the abnormalities.
- Also known as profile-based systems
- Advantages
    - Can detect new attacks including 0 day attacks
    - Can also detect low and slow attacks in which an attacker tries to stay beneath the radar by sending a few packets at a time over a longer period of time.
- Disadvantages
    - Developing a correct profile to reduce false positives can be difficult.
    - There is a possibility for an attacker to integrate his/her activities into the behavior pattern of the n/w traffic. This can be controlled by ensuring that there are no attack activities currently underway while the IDS are in learning mode.
    - The success factors for these systems are based on determining proper threshold in order to reduce/avoid false positives (threshold set to too low) or false negatives (threshold set to too high)
- Attacks
    - Bring the IDS offline by DoS and send the IDS incorrect data in order to distract the n/w and security individuals to make them busy chasing wrong packets, while the real attack takes place.
- Techniques
    - Protocol Anomaly based:
        - These types of IDS have specific knowledge of each protocol that they will be monitoring.
        - The IDS builds a profile (model) of each protocol's normal usage and uses it to match with the profile build during the actual operation.
        - Common protocol vulnerabilities
            - At the DLL, the ARP does not have any protection against ARP attacks where bogus data can be inserted into its table.
            - At the n/w layer, the ICMP can be used in a LOKI attack to move data from one place to another, when this protocol was designed to only be used to send status information. This data can be a code which can be made to be executed by the

backdoor on a compromised system.

        - IP headers can be easily modified for spoofed attacks ( one acting as other)
        - At the TL, TCP packets can be injected into the connection between the two systems for a session hijack attack.

    - Traffic Anomaly based:

        - These systems have traffic-anomaly filters, which detect changes in traffic patterns as in DoS attacks or a new service that appears on the network.
        - Once there is a profile that is built that captures the baselines of an environment's ordinary traffic, all future traffic patterns are compared to that profile.
        - As with all filters, the thresholds are tunable to adjust the sensitivity, to reduce the number of false positives and false negatives.
        - Since this is a type of statistical anomaly– based IDS, it can detect unknown attacks

**Rule Based**

- Rule-based intrusion detection is commonly associated with the use of an expert system.
- An expert system is made up of a knowledge base, inference engine, and rule-based programming.
    - Knowledge is represented as rules, and the data that is to be analyzed is referred to as facts.
    - The knowledge of the system is written in rule-based programming (IF situation THEN action). These rules are applied to the facts, the data that comes in from a sensor, or a system that is being monitored.
- Example :Consider the Rule-*IF a root user creates File1 AND creates File2 SUCH THAT they are in the same directory THEN there is a call to AdministrativeTool1 TRIGGER send alert.* This rule has been defined such that if a root user creates two files in the same directory and then makes a call to a specific administrative tool, an alert should be sent.
- The more complex the rules, the more demands on software and hardware processing requirements
- Cannot detect new attacks
- Techniques
    - State Based IDS

        - A state transition takes place when a variable's value changes, which usually happens continuously within every system.
        - In a state-based IDS, the initial state is the state prior to the execution of an attack, and the compromised state is the state after successful penetration.
        - The IDS has rules that outline what state transition sequences should sound an alarm. The activity that takes place between the initial and compromised state is what the state-based IDS looks for, and it sends an alert if any of the state-transition sequences match its preconfigured rules.
        - This type of IDS scans for attack signatures in the context of a stream of activity instead of just looking at individual packets. It can only identify known attacks and requires frequent updates of its signatures.

    - Model Based IDS

        - In a model-based IDS, the product has several scenario models that represent how specific attacks and intrusions take place. The models outline how the system would behave if it

were under attack, the different steps that would be carried out by the attacker, and the evidence that would be available for analysis if specific intrusions took place.

- The IDS takes in the audit log data and compares it to the different models that have been developed, to see if the data meets any of the models' specifications. If the IDS finds data in an audit log that matches the characteristics in a specific model, it sends an alert.

### IDS Sensors[]

- Network-based IDSs use sensors for monitoring purposes. A sensor, which works as an analysis engine, is placed on the network segment the IDS is responsible for monitoring.
- The sensor receives raw data from an event generator and compares it to a signature database, profile, or model, depending upon the type of IDS.
- If there is some type of a match, which indicates suspicious activity, the sensor works with the response module to determine what type of activity needs to take place (alerting through instant messaging, page, e-mail, or carry out firewall reconfiguration, and so on).
- The sensor's role is to filter received data, discard irrelevant information, and detect suspicious activity.
- A monitoring console can be used to monitor all sensors and supplies the network staff with an overview of the activities of all the sensors in the network, but the difficulty arises in a switched environment, where traffic is forwarded through a VPN and is not rebroadcast to all the ports.This can be overcome using Spanning Ports by mirroring the traffic from all the ports to one monitored port.
- Sensor Placement
  - Sensors can be placed outside of the firewall to detect attacks
  - Inside the firewall (in the perimeter network) to detect actual intrusions.
  - At highly sensitive areas, DMZs, and on extranets
- Multiple Sensors can be used in high traffic environments to ensure all packets are investigated. Also If necessary to optimize network bandwidth and speed, different sensors can be set up to analyze each packet for different signatures. That way, the analysis load can be broken up over different points.

### Intrusion Prevention System[]

The traditional IDS only detects that something bad may be taking place and sends an alert. The goal of an IPS is to detect this activity and not allow the traffic to gain access to the target in the first place.

An IPS is a preventative and proactive technology, whereas an IDS is a detective and after-the-fact technology.

There has been a long debate on IPS and it turned out to be an extension of IDS and everything that holds for IDS also holds for IPS apart for IPS being preventative and IDS being detective. **Honey Pots**

#### Honey Pots

## Access Control Assurance[]

### Basic Concepts[]

*Accountability* is the method of tracking and logging the subject's actions on the objects.

*Auditing* is an activity where the users/subjects actions on the objects are monitored in order to verify that the sensitivity policies are enforced and can be used as an investigation tool.

#### Advantages of Auditing

- To track unauthorized activities performed by individuals.
- Detect intrusion.
- Reconstruct events and system conditions.
- Provide legal resource material and produce problem reports.

**Note**: A security professional should be able to access an environment and its security goals ,know what actions should be audited ,and know what is to be done with that information after it is captured – without wasting too much disk space , CPU power & staff time.

**What to Audit?**

- System-level events
    - System performance
    - Logon attempts (successful and unsuccessful)
    - Logon ID
    - Date and time of each logon attempt
    - Lockouts of users and terminals
    - Use of administration utilities
    - Devices used
    - Functions performed
    - Requests to alter configuration files
- Application-level events
    - Error messages
    - Files opened and closed
    - Modifications of files
    - Security violations within application
- User-level events
    - Identification and authentication attempts
    - Files, services, and resources used
    - Commands initiated
    - Security violations

**Review of Audit Information**

- Audit trails can be reviewed manually or through automated means.
- Types of audit reviews
    - Event oriented: done as and when an event occurs.
    - Periodic: done periodically to access the health of the system.
    - Real time: done with the help of automated tools as and when the audit information gets created.
- Audit trail analysis tools: These tools helps in reducing/filtering the audit log information that is not necessary and provides only those information necessary for auditing.
- Types of audit trail analysis tools

- audit reduction tools : these tools reduces the amount of information within an audit log, discards mundane tasks information and records system performance ,security and user functionality information that are necessary for auditing.
- Variance – detection tools: these tools monitor computer and resource usage trends and detect variations unusual activities e.g. : an employee logging into the machine during odd hours.
- Attack signature – detection: these tools parse the audit logs based on some predefined patterns in the database. If a pattern matches any of the pattern or signature in the database, it indicates that an attack has taken place or is in progress.
- Key stroke monitoring.

**Protecting Audit Data and Log Information**

- Audit logs should be protected by implementing strict access control.
- The integrity of the data should be ensured with the use of digital signatures, message digest tools ,and strong access control.
- The confidentiality can be protected with encryption and access controls and can be stored on CD-ROM’S to prevent loss or modification of the data. The modification of logs is often called as scrubbing.
- Unauthorized access attempts to audit logs should be captured and reported.