TCP/IP NETWORKING

(CET 06102)

UNIT 2

Computer Network Security Threat

NETWORK SECURITY

- Network security is the practice of protecting a computer network from unauthorized access, misuse, or attacks. It involves using tools, technologies, and policies to ensure that data traveling over the network is safe and secure, keeping sensitive information away from hackers and other threats.
- Network Security has become the central topic of cyber security with many organizations inviting applications from people who have skills in this area. The network security solutions protect various vulnerabilities of the computer systems such as users, location, data, devices, and applications

A **network** is *considered secure only when it comprises* three key components confidentiality, integrity, and availability. This combination, called the **CIA triad**, is a well-known standard used while creating network security policies for any organization.

In a world where the internet of things (IoT) is the new normal, network architecture is increasingly complex. This system is constantly under threat from hackers who are evolving and continuously finding ways to spot vulnerabilities and exploit them.

Vulnerabilities exist in several areas such as devices, data, applications, users, and locations, among others. With even the shortest period of downtime, losses can be immense.

Cybersecurity threats are acts performed by individuals with harmful intent, whose goal is to steal data, cause damage to or disrupt computing systems.

Types of Network Security

Network security is defined as the process of creating a strategic defensive approach that secures a company's data and its resources across its network. It protects the organization against any form of a potential threat or unauthorized access.

Irrespective of the organization's size, industry, or infrastructure, network security solutions protect it against the ever-evolving threat of cyberattacks.

Network Security involves access control, virus and antivirus software, application security, network analytics, types of network-related security (endpoint, web, wireless), firewalls, VPN encryption and more.

Network security comprises a wide range of technologies, devices, and processes. It refers to a body of rules and configurations uniquely designed to protect computer networks and their data.

The integrity, confidentiality, and accessibility of these computers are maintained with network security and software and hardware technologies.

These are different types of Network Security:

- **Application security**: Application security involves steps that a developer undertakes to spot, repair, and prevent security vulnerabilities at any point in the application's development.

Applications are not immune to vulnerabilities that are easy for attackers to access. Application security comprises software, hardware, and processes to plug any other vulnerabilities.

Example: Suppose the developers of an organization are encountering frequent coding errors. These errors could allow and accept unverified inputs and easily turn into SQL injection attacks without anyone noticing it. This can further lead to data leaks if a hacker finds them. In such a case, employing application security can help the organization.

- **Data loss prevention (DLP):** Data loss prevention involves taking measures to prevent employees from sharing data outside a prescribed network. It ensures that all information is transmitted safely.

Example: If an organization collects and stores sensitive personal information and data that constitute intellectual property or trade secrets, the security level should be high.

- **Email security:** Email gateways are weak links that are often the source of a security breach. When phishing attacks are refined with social engineering tactics, emails are the primary source of these attacks. With email security, such attacks can be minimized.

A secure email gateway placed either on-premises or in the cloud can prevent such malicious emails from coming through. Email encryption solutions offer protection from regulatory violations or data loss.

Example: For example, suppose an organization regularly sends emails that include personally identifiable information like name, address, bank account details, or social security numbers. In that case, the company should encrypt its emails using an email security solution.

Exchanging sensitive files or financial information by email is a potentially risky affair. This is because most emails are transmitted in plain text and are not well protected as it hops from one server to another.

Hence, if organizations deploy email encryption software, the plain text would get encrypted, making it safer for transmission since the contents of email, attachments, can be intercepted and read by an attacker.

- **Firewalls:** Firewalls are the barriers between an internal and external network, such as the internet. They use a prescribed set of protocols to regulate incoming and outgoing traffic on the network.

Firewalls are the first line of defense. If a company receives data that is not in keeping with its established set of protocols, firewalls prevent them from getting through.

Example: Firewalls guard traffic at a computer's entry point called ports, where information is exchanged with external devices. For example, a source address 165.12.2.1 is allowed to reach destination 171.14.2.2 over port 22.

Here, only trusted packets with source addresses (165.12.2.1) will be allowed to enter the destination address (171.14.2.2). Besides this, firewalls also prevent unauthorized access to a system and can make your PC invisible when you're online, preventing attempted intrusions in the first place.

- **Virtual private network (VPN):** VPN creates a secure tunnel for information passage on the internet. The tunnel is encrypted from originating point to destination point, ensuring all data transmitted and received is protected.

With telecommuting and work-from-home increasingly being the norm, employees often depend on insecure networks for the internet, leaving company data vulnerable to an attack. With VPNs, employees can be placed anywhere in the world yet have a safe network that does not leave the company data vulnerable.

A **vulnerability** is a weakness in an IT system that can be exploited by an attacker to deliver a successful attack.

Example: You are in a company whose employees travel frequently. In that case, they may end up using public Wi-Fi networks. However, if a hacker is using the same network, your employees' systems can get hacked in no time, putting the whole organization at risk.

Using a VPN adds an extra layer of security by ensuring that all the communication is encrypted.

➢Web and DNS Filtering

- Domain Name System (DNS) filtering allows organizations to stop domain-based attacks, such as DNS hijacking, tunneling, etc. Likewise, URL filtering prevents users and applications from accessing suspicious URLs, which could be linked to malicious websites. These web security tool help enterprises enforce acceptable-use policies while protecting them from harmful content.
- Example: if a user attempts to access a malicious website, the web filter checks its database of categorized sites. If the domain has been flagged, it'll block access entirely.

➢Anti-Malware Software

- Anti-malware and next-gen antivirus software is one of the better-known network security measures. This software keeps environments secure by monitoring, scanning for, and removing malware.
- This software employs a range of detection techniques, including signature-based scanning, heuristic analysis, and behavioral monitoring. Together, they identify and neutralize various types of malware, including viruses, worms, Trojans, ransomware, and spyware.

➢Intrusion Prevention System(IPS)

- An intrusion Prevention System is also known as Intrusion Detection and Prevention System. It is a network security application that monitors network or system activities for malicious activity. The major functions of intrusion prevention systems are to identify malicious activity, collect information about this activity, report it, and attempt to block or stop it.

➢Sandboxing

- Sandboxing is a cybersecurity technique in which files are opened or code is performed on a host computer that simulates end-user operating environments in a secure, isolated environment. To keep threats off the network, sandboxing watches the code or files as they are opened and searches for harmful activity.

LIST OF NETWORK SECURITY DEVICES

1. Firewalls

- A firewall is the safety layer that regulates the connections that can take place within a network.

2. VPN’s

- VPN Gateways are utilized to create a secure connection to the remote systems.

3. Anti Virus

- It is used to identify, monitor, and filter out all kinds of malware.

4. URL Filtering

- URL filtering will keep the end-users secured by prohibiting them to access malicious websites.

5. IDS system

Techniques for Testing Network Security

Testing network security involves various techniques designed to identify vulnerabilities and ensure robust protection against threats. Penetration testing simulates cyberattacks to uncover weaknesses that could be exploited by hackers.

1. Network Scanning

- In this technique, a port scanner is utilized to recognize all the hosts connected to the network. Network Services are also scanned, like FTP and HTTP. This ultimately helps in confirming whether the ports are configured to allow only secured network services or not.

2. Vulnerability Scanning

- Vulnerability Scanner assists in finding the weakness of the system or network. It delivers data on the security loopholes which can be enhanced.

3. Ethical Hacking

- This is hacking performed to recognize probable threats to a system or network. This assists to identify if unauthorized access or malicious attacks are possible.

4. Password Cracking

- This technique can be utilized to crack weak passwords. This can enable implementing a policy with minimum password criteria which ends up in establishing strong passwords and is hard to crack.

5. Penetration Testing

Pentest is an attack done on a network or system to discover Security flaws. Under Penetration Testing Technique the Servers, web application, mobile devices, endpoints, wireless devices, and network devices, are all compromised to know the vulnerability.

BENEFITS OF NETWORK SECURITY

- The following are the main benefits of network security:

➢ **Functionality.** Network security ensures the ongoing high performance of the networks that businesses and individual users rely on.

➢ **Privacy and security.** Many organizations handle user data and must ensure the confidentiality, integrity and availability of data on a network, known as the *CIA triad*. Network security prevents the security breaches that can expose PII and other sensitive information, damage a business's reputation and result in financial losses.

➢ **Intellectual property protection.** Intellectual property is key to many companies' ability to compete. Securing access to intellectual property related to products, services and business strategies helps organizations maintain their competitive edge.

➢ **Compliance.** Complying with data security and privacy regulations, such as HIPAA and GDPR, is legally required in many countries. Secure networks are a key part of adhering to these mandates

CHALLENGES OF NETWORK SECURITY

- **Evolving network attack methods.** The biggest network security challenge is the rate at which cyber attacks evolve. Threat actors and their methods constantly change as technology changes. For example, new technology, such as block chain, has led to new types of malware attacks, such as crypto jacking. As a result, network security defense strategies must adapt to these new threats.
- **User adherence.** As mentioned, security is every network user's responsibility. It can be difficult for organizations to ensure that everyone is adhering to network security best practices, while simultaneously evolving those strategies to address the newest threats.
- **Remote and mobile access.** More companies are adopting bring your own device policies, which means a more distributed and complex network of devices for organizations to protect. Remote work is also more prevalent. This makes wireless security more important, as users are more likely to be using a personal or public network when accessing company networks.
- **Third-party partners.** Cloud providers, managed security services and security product vendors often get access to an organization's network, opening new potential vulnerabilities

Network Security VS. Cyber Security

Network security focuses primarily on securing network infrastructure, including the network edge, routers, and switches.

Cyber security includes network security and covers additional areas, such as data storage and transportation.

Network security and cyber security differ mainly in network planning. A cyber security plan includes within it a network security plan.

However, network security plans can exist independent of cyber security.

Common Network Security Threats and Attacks

Common network security threats include malicious software (malware), phishing schemes, Distributed Denial of Service (DDoS). Many network security issues create the additional risk of regulatory non-compliance. Defending against these threats involves utilizing a broad set of technologies including firewalls, network segmentation, intrusion prevention systems (IPS), and tools that can help organizations implement zero trust security principles.

Network security threats are specific attack methods that exploit those vulnerabilities. There are multiple ways to launch such attacks.

All of them should be part of network security policies.

Computer Network Threat is any possible malicious attack that seeks to unlawfully access data, disrupt digital operations or damage information.

Malware

Malware is a program that attacks information systems. There are various types of malware, each designed to perform specific malicious activities.

For example, ransomware encrypts files and holds it for ransom, spyware covertly spies on victims, and Trojans infiltrate systems.

Threat actors use malware to achieve various objectives, such as stealing or secretly copying sensitive data, blocking access to files, disrupting system operations, or making systems inoperable.

Phishing

Phishing is a type of fraud that occurs when a threat actor impersonates a reputable entity in person, via email, or other communication forms.

Threat actors often use phishing emails to spread malicious attachments or links that perform various functions, such as extracting the victim's account information or login credentials.

Bots

A bot is a small program that automates web requests with various goals. Bots perform their tasks without any human intervention, for example, scanning website content and testing stolen credit card numbers.

A bot attack utilizes automated web requests to defraud, manipulate, or disrupt applications, websites, end-users, or APIs.

Bot attacks were originally used primarily for spam and denial of service, but have evolved into complex enterprises with economies and infrastructure that enables waging additional, more damaging attacks.

DDoS Attacks

A Distributed Denial of Service (DDoS) attack employs multiple compromised computer systems to attack a target and cause a denial of service for the targeted resource’s users.

It sends a flood of messages, malformed packets, or connection requests to the target system, forcing it to slow down or entirely shut down, denying service to real systems and users.

DDoS attacks can target a website, server, and other network resources.

Internal Security Threats

Over 90% of cyberattacks are caused by human error. This can take the form of phishing attacks, careless decision-making, weak passwords, and more.

Insider actions that negatively impact your business's network and sensitive data can result in downtime, loss of revenue, and disgruntled customers.

Man-in-the-Middle attacks

MITM attacks occur when attackers hijack connections between network devices or between a network and external devices.

By doing so, attackers can eavesdrop on traffic, extracting data transfers and information that can be used in social engineering attacks or sold to third-parties.

While they are commonly associated with remote working, MITM attacks can occur in any situation where devices interact via log-in portals.

This makes secure Single Sign On (SSO) systems and network encryption essential.

SQL injection attacks

In SQL injection attacks, criminals target poorly configured search boxes on otherwise legitimate websites.

By entering malicious code, attackers can harvest information entered into those search fields, providing valuable data for social engineering assaults.

Unauthorized access

Unauthorized access refers to attackers accessing a network without receiving permission.

Among the causes of unauthorized access attacks are weak passwords, lacking protection against social engineering, previously compromised accounts, and insider threats.

Privilege escalation

Once attackers penetrate your network, they can use privilege escalation to expand their reach.

Horizontal privilege escalation involves attackers gaining access to additional, adjacent systems, and vertical escalation means attackers gain a higher level of privileges for the same systems.

Vulnerability is a weakness that can be exploited by cybercriminals to gain unauthorized access to a computer system.

After exploiting a vulnerability, a cyberattack can run malicious code, install malware, and even steal sensitive data.

Exploit (in its noun form) is a segment of code or a program that maliciously takes advantage of vulnerabilities or security flaws in software or hardware to infiltrate and initiate a denial-of-service (DoS) attack or install malware, such as spyware, ransomware, Trojan horses, worms, or viruses.

Attack is an information security threat that involves an attempt to obtain, alter, destroy, remove, implant or reveal information without authorized access or permission.

It happens to both individuals and organizations. There are many different kinds of attacks, including but not limited to passive, active, targeted, clickjacking, brandjacking, botnet, phishing, spamming, inside and outside.

Threat is a potential negative action or event facilitated by a vulnerability that results in unwanted impact to a computer system or application.

Method to Combat Computer Network Security Threat

➢Keep your software and systems fully up to date

Often cyber attacks happen because your systems or software aren't fully up to date, leaving weaknesses. So cybercriminals exploit these weaknesses to gain access to your network. Once they are in – it's often too late to take preventative action.

To counteract this, it's smart to invest in a patch management system that will manage all software and system updates, keeping your system resilient and up to date.

➢Ensure Endpoint Protection

Endpoint protection protects networks that are remotely bridged to devices. Mobile devices, tablets and laptops that are connected to corporate networks give access paths to security threats. These paths need to be protected with specific endpoint protection software.

➢Install a Firewall

Putting your network behind a firewall is one of the most effective ways to defend yourself from any cyber attack. A firewall system will block any brute force attacks made on your network and/or systems before it can do any damage, something we can help you with.

➢Control access to your systems

One of the attacks that you can receive on your systems can be physical, having control over who can access your network is really really important. Somebody can simply walk into your office or enterprise and plug in a USB key containing infected files into one of your computers allowing them access to your entire network or infect it.

It’s essential to control who has access to your computers.

➢Passwords

Having the same password setup for everything can be dangerous. Once a hacker figures out your password, they now have access to everything in your system and any application you use.

Having different passwords setup for every application you use is a real benefit to your security, and changing them often will maintain a high level of protection against external and internal threats.

Technique for Securing Network Devices, Software and Data

Data security is the practice of protecting digital information from unauthorized access, corruption, or theft throughout its entire lifecycle.

It's a concept that encompasses every aspect of information security from the physical security of hardware and storage devices to administrative and access controls, as well as the logical security of software applications. It also includes organizational policies and procedures.

Data security *involves* deploying tools and technologies that enhance the organization's visibility into where its critical data resides and how it is used.

Ideally, *these tools should be able to apply protections* like encryption, data masking, and redaction of sensitive files, and should automate reporting to streamline audits and adhering to regulatory requirements.

Software security is the protection of software applications and digital experiences from unauthorized access, use, or destruction.

For Software Security you need to invest in multiple tools along with focused developer training and tool customization and integration before you'll see a return on your security investment.

Below are software security strategies:-

- Patch your software and systems

Many attackers exploit known vulnerabilities associated with old or out-of-date software. To impede common attacks, ensure that all your systems have up-to-date patches. Regular patching is one of the most effective software security practices.

➢Strong Passwords and Encryptions

Setting a strong password on any electronic device used to store personal information is an important measure to protect privacy and is a requirement of the Privacy Policy for electronic devices and media such as computers, laptops, and smartphones.

Passwords help to prevent against unauthorized access to personal information. However, basic password measures can be defeated by a determined individual and the underlying data are generally not protected.

If the password is in any way compromised or bypassed, the data are readable. For this reason, it is much better to use a combination of password protection and encryption.

Encryption goes one step further than password protection and is an easy and effective way to lessen the likelihood of a privacy breach. **Encryption** is the method by which information is converted into secret code that hides the information's true meaning.

➢Educate and train users

Employee training should be a part of your organization's security DNA. Having a well-organized and well-maintained security training curriculum for your employees will go a long way in protecting your data and assets.

Include awareness training for all employees and secure coding training for developers. Do it regularly, not just once a year.

And conduct simulations like phishing tests to help employees spot and shut down social engineering attacks.

➢Automate routine tasks

Attackers use automation to detect open ports, security misconfigurations, and so on. So you can't defend your systems using only manual techniques.

Instead, automate day-to-day security tasks, such as analyzing firewall changes and device security configurations. Automating frequent tasks allows your security staff to focus on more strategic security initiatives.

➢Enforce least privilege

Ensure that users and systems have the minimum access privileges required to perform their job functions.

Enforcing the principle of least privilege significantly reduces your attack surface by eliminating unnecessary access rights, which can cause a variety of compromises.

That includes avoiding “privilege creep,” which happens when administrators don’t revoke access to systems or resources an employee no longer needs.

Privilege creep can occur when an employee moves to a new role, adopts new processes, leaves the organization, or should have received only temporary or lower-level access in the first place.

➢Create a robust IR plan

No matter how much you adhere to software security best practices, you'll always face the possibility of a breach. But if you prepare, you can stop attackers from achieving their mission even if they do breach your systems.

Have a solid incident response (IR) plan in place to detect an attack and then limit the damage from it.

An IRP is a set of documents that acts as a roadmap if you are faced with a cyber-emergency. Think of it as a manual in case of danger.

It should be thorough and consider every aspect that arises out of your risk assessment and what should be done in each case. These should be test-run as well.

➢Document your security policies

Maintain a knowledge repository that includes comprehensively documented software security policies.

Security policies allow your employees, including network administrators, security staff, and so on, to understand what activities you're performing and why.

Also, it's not enough just to have policies. Make sure everybody reads them. At a minimum, make that part of the onboarding process for new employees.

➢Segment your network

Segment your network is an application of the principle of least privilege. Proper network segmentation limits the movement of attackers.

Identify where your critical data is stored, and use appropriate security controls to limit the traffic to and from those network segments.

➢Integrate security into your SDLC

Integrate software security activities into your organization's software development life cycle (SDLC) from start to finish. Those activities should include architecture risk analysis, static, dynamic, and interactive application security testing, SCA, and pen testing.

Building security into your SDLC does require time and effort at first. But fixing vulnerabilities early in the SDLC is vastly cheaper and much faster than waiting until the end. Ultimately, it reduces your exposure to security risks.

➢Monitor user activity

Trust, but verify. Monitoring user activities helps you ensure that users are following software security best practices. It also allows you to detect suspicious activities, such as privilege abuse and user impersonation/ masquerade.

➢Measure

Define key metrics that are meaningful and relevant to your organization. Well-defined metrics will help you assess your security posture over time.

There's no silver bullet when it comes to securing your organization's assets. But you can make your organization a much more difficult target by sticking to the fundamentals.

Security Layers

Layered security is a network security approach that deploys multiple security controls to protect the most vulnerable areas of your technology environment where a breach or cyberattack could occur.

The purpose of a multi-layered security approach is to ensure that each individual component of your cybersecurity plan has a backup to counter any flaws or gaps.

Implementing multi-layered security is crucial to protect your network, users, and business-critical data.

Here are 12 essential security layers you should have in place:-

- Firewall. The first line of defense in your network security, a firewall monitors incoming and outgoing network traffic based on a set of rules.

A firewall acts as a barrier between a trusted network and an untrusted network, only allowing into your network traffic that has been defined in the security policy.

- **Patch Management.** Outdated software is full of vulnerabilities, or security holes, that offer hackers an easy way into your network. "Patching" refers to the process of distributing and applying updates to software and firmware.

Patches are important because they address functionality errors or bugs, boost performance, and close the security gaps that would otherwise leave your systems, software, and applications vulnerable to cyberattacks.

- **Multi-Factor Authentication.** Enabling multi-factor authentication (MFA) is one of the most important things you can do to reduce the risk of a cyberattack.

Also commonly known as two-factor authentication, MFA requires multiple forms of verification to access an application, account, or corporate network.

For example, after entering your password, you may be prompted to enter a one-time code sent via text message or push notification.

These additional forms of authentication prevent hackers from exploiting weak or compromised end-user credentials to access your network.

- **Endpoint Protection.** Think about all the devices your business uses not only laptops, workstations, and mobile devices but also printers, scanners, copiers, security cameras, smart devices (e.g., thermostats), and more.

Every device connected to your network is a potential entry point for hackers. All of these entry points, known as "endpoints," need to be included in your organization's cybersecurity plan.

- **Web Content Filtering.** This software blocks users' access to websites and online content deemed inappropriate or dangerous.

Content can be blocked by specific categories designated at the organization level as well as based on databases of sites and sources that are known threats and/or considered high-risk for malware or phishing attempts.

- Email Filtering. Email remains one of the most common cyberattack vectors, with 94% of malware delivered by email. Opportunistic cybercriminals know it takes only a single click on a malicious link for an end-user to unwittingly grant access to their entire corporate network.

Filtering emails at the gateway reduces this risk and helps to protect your users and your business from email-borne cyber threats such as phishing attacks, ransomware, viruses and malware, and business email compromise.

- Security Awareness Training and Phishing Simulations. Could your employees spot a phishing email if it slipped past your email filter and into their inbox? More than one-third of reported data breaches involve phishing emails.

When building your cybersecurity layers, training on cybersecurity basics and best practices is essential to help end-users identify phishing emails and other common cyber scams that threaten your network's security.

This training can be reinforced through periodic phishing simulations, which test users on their vigilance in recognizing suspicious emails, further strengthening your defenses.

- Sophisticated Password Policy. Up to 73% of passwords in use are duplicates, which means if your password is leaked in one data breach, any other account using that password is also compromised.

Password policies set organization-wide rules about password strength and complexity (e.g., irregular capitalization and special characters) to prevent password re-use, prohibit weak passwords, and improve your network security.

- Dark Web Monitoring. The dark web is home to many illegal activities, including the sale of sensitive and personally-identifying information stolen during data breaches.

Employee credentials are a best-seller on the dark web, used by cybercriminals to access an organization's confidential data, send email spam, install malware, and more.

- Dark web monitoring tools scan the dark web for email addresses and passwords associated with your company's domain so you can identify and address these vulnerabilities before they can be exploited by a hacker.

- Physical Security. Does your security plan account for internal threats? Firewalls can't protect your valuable data from being copied and stolen via a USB drive.

That's why your security layers must also include the physical security of your IT infrastructure. Physical security measures restrict access to and protect your on-premises infrastructure and spaces in which data is stored.

Examples of such measures include access control systems, keycards and door locks, security cameras and surveillance, and security personnel.

- Business Continuity and Disaster Recovery. In the event of a disaster such as a cyberattack, are you sure your data is protected? Business continuity and disaster recovery (BCDR) solutions can mitigate the downtime and damage associated with a cyberattack, allowing you to restore your data and operations from a backup.

Two important reminders: 1) Isolate your backups to ensure that if your network is breached, your backups can't also be accessed and encrypted; and 2) Ensure your business continuity plan is documented, tested, and regularly updated.

- Managed Detection and Response. How do you detect when someone or something has gotten past your other layers of protection? Managed detection and response (MDR) is an advanced security solution that combines next-generation monitoring software and a 24/7 (human-staffed) security operations center to identify and isolate suspicious behavior on your network in real-time and immediately detain confirmed threats to prevent spread.

If your preventative measures fail, MDR acts as the security camera that catches a cybercriminal sneaking onto your network and the alarm system that alerts you to the breach.

Without a detection and response tool, it can take more than 200 days to discover a data breach, giving hackers plenty of time to plan and execute a devastating attack before you are even aware of a problem.

User Access Control

Access control is a method of limiting access to a system or to physical or virtual resources. It is a process by which users can access and are granted certain prerogative/ privilege to systems, resources or information.

Access control is a security technique that has control over who can view different aspects, what can be viewed and who can use resources in a computing environment. It is a fundamental concept in security that reduces risk to the business or organization.

Access control systems *perform* identification, authentication, and authorization of users and entities by evaluating required login credentials that may include passwords, pins, bio-metric scans or other authentication factors.

There is multi-factor authentication which requires two or more authentication factors which is often an important part of the layered defense to protect access control systems.

Access control is a method of limiting access to a system or to physical or virtual resources. It is a process by which users can access and are granted certain prerogative to systems, resources or information.

Access control is a security technique that has control over who can view different aspects, what can be viewed and who can use resources in a computing environment.

It is a fundamental concept in security that reduces risk to the business or organization. To establish a secure system, electronic access control systems are used that depend on user credentials, access card readers, auditing and reports to track employee access to restricted business locations and areas.

These systems include access control panels to prohibit entry to sensitive areas like alarms and lock down areas to prevent unauthorized access or operations.

Access control systems perform identification, authentication, and authorization of users and entities by evaluating required login credentials that may include passwords, pins, bio-metric scans or other authentication factors.

Access control is a security technique that has control over who can view different aspects, what can be viewed and who can use resources in a computing environment. It is a fundamental concept in security that reduces risk to the business or organization.

Access control is a fundamental component of data security that dictates who's allowed to access and use company information and resources.

Through authentication and authorization, access control policies make sure users are who they say they are and that they have appropriate access to company data.

Two Types of Access Control

- Physical Access Control

Physical access control restricts entry to campuses, buildings, rooms and physical IT assets.

- Logical Access Control

Logical access control limits connections to computer networks, system files and data.

Authentication Factors

- Password or PIN
- Bio-metric measurement (fingerprint & retinal scan)
- Card or Key
- Knowledge Factor

Authentication Mechanism

- Two-factor authentication
- Multi factor authentication
- one-time password
- Three-factor authentication
- Bio metrics
- Hard Tokens
- Soft Tokens
- Contextual Authentication
- Device identification

ELEMENTS OF ACCESS CONTROL

1.Identification

Identification is the process of determining who someone is and verifying their identity. It's not always easy, especially when dealing with large groups of people in a short span of time.

- The two main methods of identification are user IDs and badges.

➢**User IDs** - User IDs are unique identifiers assigned to each user in the system. They are used to track user activity and tie access to specific individuals. User IDs should be difficult to guess and should not contain any clues about the user's identity or role. IDs are often tied to accounts and profiles that contain additional user information.

➢**Badges B.** - Badges serve as physical identification. They are cards or tags worn visibly by users. Badges allow security personnel to quickly identify authorized

2.Authentication

Access control limits access to information and data, depending on the person's role, identity, or authorization level. Authentication is one part of this process; it makes sure the user is who they say they are. Authentication schemes are the backbone of access control. They are responsible for verifying who you are and what you're allowed to do once authenticated.

- It is commonly implemented through passwords and biometrics.

➢**Passwords** - Passwords are secret words or phrases used to authenticate user identities. They should be strong enough to resist guessing and brute force attacks. Strong password policies enforce minimum length, complexity, and periodic changing of passwords. Multifactor authentication can be implemented by requiring a password plus a one-time code sent to the user.

➢**Biometrics authentication** - Biometrics authenticate users based on unique physical characteristics. Examples include fingerprints, retina and iris scans, facial recognition, and voice recognition. Biometrics provide a convenient hands-free authentication and higher security than passwords alone. However, biometric systems require specialized scanners and enrollment of user biometrics.

3.Authorization

Authorization is the means of regulating who can access what. The two types of authorization are discretionary and mandatory. Discretionary authorizations are granted by an entity, such as an owner or administrator, to individuals based on their need to protect the resource from unauthorized access. Mandatory authorizations are granted to people with common needs while being protected from unauthorized access.

Once identified and authenticated, users must be authorized to access specific resources. Authorization defines the user's permissions within the system.

- Two common methods are access control lists and role-based access control.

➢ **Access control lists** - Access control lists outline exactly which resources a user can access. Permissions are assigned to the user's unique ID. While flexible, ACLs can be complex to manage as permissions change.

➢ **Role-based access control** - Role-based access control grants access based on the user's role within the organization. Roles come with predefined permissions, making user administration simpler. However, defining roles with the proper permissions requires careful planning.

Security Access Control Methods

Discretionary Access Control (DAC)

DAC is defined as an access control policy enforced over all subjects and objects granting information access that allows the subject to:

- Pass the information to other subjects or objects
- Grant its privileges to other subjects
- Change security attributes of subjects, object, systems, or system components
- Choose security attributes associated with newly-created or revised objects
- Change rules governing access control

A good example of DAC would be giving someone Editor privileges for a folder in Google Drive.

That person can share information, give the same privileges to others, change other users' ability to edit/read information, and choose security attributes for any other assets in the folder.

Mandatory Access Control (MAC)

MAC is an access control policy uniformly enforced across all subjects and objects, ultimately placing restrictions on DAC. MAC controls limit a subject's access by preventing:

- Passing the information to unauthorized subjects or objects
- Giving its privileges to others
- Changing security attributes on subjects, object, systems, or system components
- Changing access control rules

MAC limits users' ability to share information. This is where traditional Google Drive controls often create problems because they only allow file and folder owners to give Edit, Read, and Comment permissions.

While Edit permissions essentially establish DAC, Read, and Comment limit access but do not give a user the right to edit an asset directly.

Rule-Based Access Control (RAC)

RBAC collects all the access permissions a user needs to complete their job function, both explicitly outlined and implicitly needed, and maybe inherited through a hierarchy. A single role may apply to one user or a group of users.

Under RBAC, you assign users access based on their job functions. Therefore, people in the marketing department have access to the networks, systems, and applications they need to do their jobs.

This might include your customer relationship management (CRM) application, corporate blog, social media accounts, folders that marketing uses in a shared drive, and your collaboration tool.

Additionally, not everyone on the marketing team will have the same access to resources. Your social media manager may be the only person with access to those accounts but does not have access to your corporate blog or CRM.

Additionally, you also need to remember that departments may need to have similar access to resources for different reasons. Your sales team might need access to your CRM and some of the same folders in a shared drive.

As the company's application ecosystem grows, managing access becomes more challenging.

Attribute-based Access Control (ABAC)

The Access Control family (AC) control "AC-3 Access Enforcement" subsection 13 explains that ABAC is a policy that restricts system access using a combination of:

- Organizational attributes, like job function
- Action attributes, like read, write, and delete
- Environmental attributes, like time of day and geolocation
- Resource attributes, like data type or application
- ABAC enables organizations to set privileges and dynamically grant access, making it useful in dynamic cloud environments.

Role-Based Access Control (RBAC)

Role-Based Access Control is designed to allow or restrict access based on specific roles with outlined business responsibilities as opposed to an individual user.

An employee's role in an organization determines the permissions that the individual is granted and ensures that lower-level employees can't access sensitive information or perform high-level tasks.

RBAC is the most common form of managing user permissions. This method is designed using access rights that are built on variable attributes, such as resource needs, job, environment, location, and more.

This makes it simple for owners to manage users in groups based on their role or position, rather than assigning permissions to each specific individual. RBAC largely eliminates discretion when providing access to objects.

For example, a human resources specialist should not have permissions to create network accounts; this should be a role reserved for network administrators.

Companies largely depend on this model to secure their sensitive data and critical applications Improve operational efficiency, enhance compliance, giving administrators increased visibility, reducing cost, and decreasing risk of breaches and data leakage.

Role-based security is a flexible and secure method for managing user permissions.

Identity-Based Access Control (IBAC)

IBAC is a simplified security method that dictates whether the person using is permitted or denied to a given electronic resource based on their individual visual or biometric identity.

Therefore, a user will be permitted or denied access to an electronic resource based on if their identity can be matched with a name that appears on an access control list.

Using this, network administrators can more effectively manage activity and access based on individual needs. Some of the advantages of the identity-based security approach include he ability to exercise very fine-grained control over two can use which services, and which functions those individuals are actively performing.

Also, there is the benefit of being able to enforce access control policy across a variety of devices, such as smartphones, tablets, and PCs.

History-Based Access Control (HBAC)

The decisions made by this access control management system are based fundamentally on past security actions.

Historical activities of the user determine whether or not he or she is going to be granted access.

This requires real-time evaluation of the user's history of activities, such as the time between requests, the content of requests, which doors have been recently opened, etc.

As an example, access to a certain service or data source can be granted or declined on the user's past behavior, e.g. the request interval exceeds one query per second.

Organizational-Based Access Control (OBAC)

OBAC helps when evaluating the security policies and permissions of larger entities with multiple users, such as third-party companies.

This method grants a high degree of scalability and expressiveness. Each security policy is defined by and for an organization within the larger system.

Thus, the specification of the security policy is completely parameterized by the organization so that it is possible to handle simultaneously several security policies associated with different organizations.

Responsibility Access Control

Responsibility-based systems limit entry or access based on their responsibilities in an organization.

Employees can only access information that is necessary for them to carry out their official duties. Factors such as responsibility, job competence and authority are used to determine who is responsible enough to have access to certain information.

This ensures that low- level employees, do not access sensitive data of a business that may be used against the company.

Technologies used in User Access Control

➢Near Field Communication (NFC)

This is a short-range wireless connectivity technology that uses magnetic field induction to enable communication between devices when they're touched together or brought within a few centimeters of each other.

This includes authenticating credit cards, enabling physical access, transferring small files and jumpstarting more capable wireless links

➢Internet of Things (IoT)

This is IP-based communication between all components of access control technologies, which are IP-enabled intelligent devices. They use the internet to establish communication between them.

➢Radio Frequency Identification (RFID)

RFID technology uses radio waves to identify people or objects. There is a device that reads information contained in a wireless device or “tag” from a distance without making any physical contact or requiring a line of sight.

RFID uses radio waves to perform AIDC function. AIDC stands for Automatic Identification and Data Capture technology which performs object identification and collection and mapping of the data.

An antenna is an device which converts power into radio waves which are used for communication between reader and tag. RFID readers retrieve the information from RFID tag which detects the tag and reads or writes the data into the tag.

- Physical Access Control System (PACS)

This is based on personal information card verification (PIV) card and card reader. This technology is used for government and security-related areas. It involves a two-step authentication process.

- Power over Ethernet (PoE)

This technology uses cables that carry both data signals and power to supply the access control components like IP cameras, telephones, access controllers, routers, access points, and other elements. This is a very cost-effective access control technology.

➢Mobile Access Control

The mobile devices are converted into electronic key fobs by installing an application on them, which uses wireless technology for communication. The mobile device can also be used to manage and control the entire access control system of a particular area or building.

➢Bluetooth Access control

This uses the power of Bluetooth-enabled devices. The data transferred between two devices through a frequency hopping spectrum spread radio interface, which operates in the ISM band of frequency. It is effective up to 800 feet distance and 50Mbit/sec data rate.

➢Wired Access Control Technologies

These include CAT6 cable communication, PoE access, and traditional wiring solutions. The communication between different components may take place through different communication protocols.

This is a generalized category of wireless technologies used in the access control system. Bluetooth, NFC, RFID, mobile, and others fall in this category of access control technologies.

Usefulness and Importance of User Access Control

✓Simplified Management

One of the most appealing aspects of using access control systems is the ability to simplify the management process of handling employee credentials, entrance security, and tracking. Using access control systems provides you with the ability to track and monitor all entryway activity from one remote location.

✓Keep Track of All Activity

When you have an access control system in place, it is much easier to keep track of all activity, whether from your own employees or even guests, visitors, and delivery drivers.

If you experience a break-in or a theft incident, you will have the ability to recall who has accessed your building and each individual room where the access control system is activated and in use.

✓Easily Adjust Access Times

With modern access control systems, you can easily set specific access times for employees, visitors, and even entire groups of people. Whether you want to set access times for employees during work hours or if you are hosting guests for a day-long gathering, you can adjust access dates and times remotely with just a few steps.

Adjusting access times can be done within seconds and will not interfere with the security protocols you currently have in place.

✓Require Specific Credentials for Access

It is also possible to require specific credentials for access when using your access control system. Using badges that indicate specific credentials can also keep better track of who is provided access to what locations and spaces throughout your building or workplace.

✓Eliminate the Hassle of Using Traditional Keys

If you are tired of creating keys and keeping track of keys, transitioning to the use of an access control system is a must. Eliminating the hassle of using traditional keys is one of the most appealing aspects of implementing access control systems for any business, regardless of size.

Without the use of traditional keys, you will no longer need to keep track of keys that are out in the world, or whether a key has been copied and shared with others.

✓Streamline the Entering and Exiting of Your Building or Business

When you want to know who is coming and going in and out of your business on a daily basis, an access control system is essential.

Streamlining access to your building will help save time while allowing for more focus on what is most important for the growth of your business.

Keep track of and monitor traffic without using manual labor to get the job done.

✓Improve Security and Minimize Risk

Transitioning to access control systems is one of the fastest ways to boost security for your business location and building itself.

Implementing access control systems not only helps to keep better track of who is coming and going to your place of business, but it also provides in-depth details of who is always accessing individual rooms and locations, for significantly increased security.

If there is ever a security breach, an attempted hacking, or even a break-in, it is much easier to track logged reports of who has accessed what area of your building. Access control systems are incredibly helpful with any criminal investigations involving theft, burglary, and break-ins.

Using access control systems is one of the best ways to keep better track of employees, visitors, and ultimately, the security of your work or place of business. With an access control system, maintain peace of mind while always maximizing the protection and security of your business.

User Account

User Access is the authorization given to users that enables them to access specific resources on the network, such as data files, applications, printers and scanners.

User permissions also designate the type of access; for example, can data only be viewed (read only) or can they be updated (read/write).

A **user account** is an identity created for a person in a computer or computing system. User accounts can also be created for machine entities, such as service accounts for running programs, system accounts for storing system files and processes, and root and administrator accounts for system administration.

Account is a set of credentials for participating in a network. In a typical network, each user needs an account to access resources on the network, such as shared folders, printers, or applications. Accounts provide a way of identifying users on a network and are the foundation for network security.