

Use Cases for FTPS

- **Banking and Finance:** FTPS enables secure transfer of financial data, such as transactions, statements, and sensitive customer information.
- **Healthcare:** FTPS is used for transferring confidential patient records, medical images, and other sensitive healthcare data.
- **E-commerce:** FTPS ensures secure exchange of product information, inventory updates, and customer data between online retailers and suppliers.

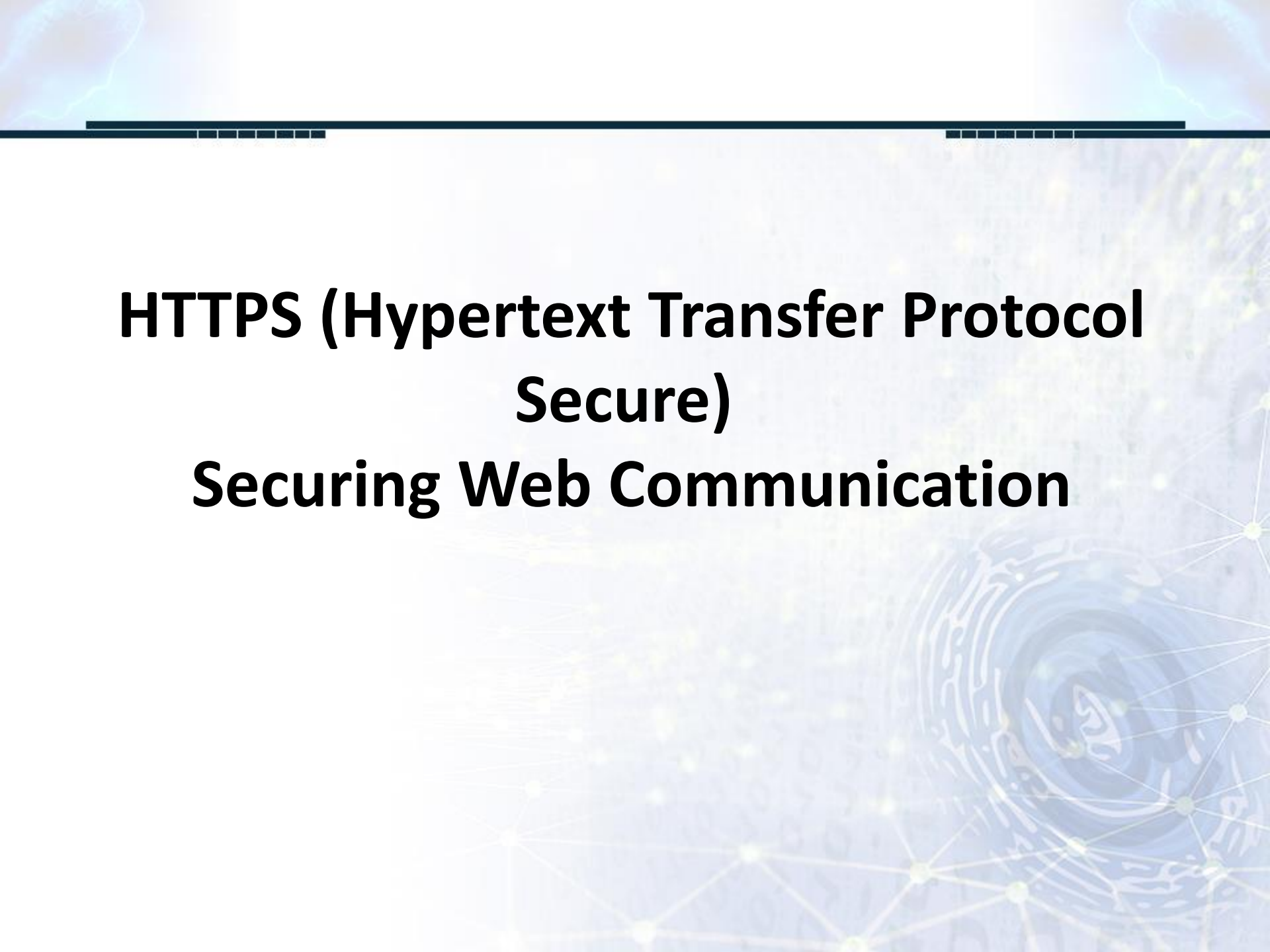


Best Practices for FTPS Implementation

1. **Use Strong Authentication:** Implement strong username/password combinations or consider additional authentication methods like certificates.
2. **Regularly Update SSL/TLS Certificates:** Keep SSL/TLS certificates up to date to maintain the security of the FTPS server.
3. **Employ Access Controls:** Restrict FTPS access to authorized users and employ granular permissions to limit access to specific files and directories.
4. **Monitor and Audit:** Implement logging and monitoring mechanisms to track FTPS activities and detect any suspicious or unauthorized actions.

Conclusion

- FTPS is a secure and reliable file transfer protocol that combines the benefits of FTP with SSL/TLS encryption.
- By implementing FTPS, organizations can ensure the confidentiality, integrity, and secure transfer of sensitive data.
- With its wide compatibility and industry adoption, FTPS remains a trusted solution for secure file transfers in various sectors.

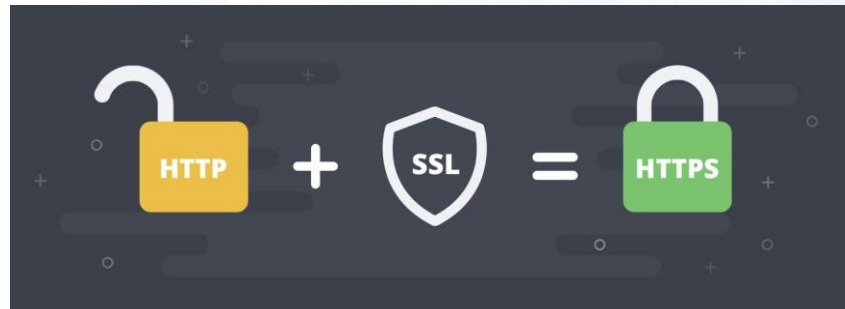


HTTPS (Hypertext Transfer Protocol Secure)

Securing Web Communication

Introduction to HTTPS

- HTTPS (Hypertext Transfer Protocol Secure) is a secure version of the HTTP protocol used for communication between web browsers and web servers.
- HTTPS adds an extra layer of security by encrypting data exchanged between the client and server, ensuring confidentiality and integrity.



How HTTPS Works

HTTPS utilizes the SSL/TLS (Secure Sockets Layer/Transport Layer Security) protocol to establish a secure connection:

Client Request: The client (web browser) initiates a request to the server using the HTTPS protocol.

Server Response: The server responds by presenting its SSL/TLS certificate to the client.

Certificate Verification: The client verifies the authenticity of the server's certificate using trusted Certificate Authorities (CAs).

Secure Connection: Once the certificate is validated, a secure connection is established, and data exchange occurs over an encrypted channel.

Encryption and Decryption: The client and server encrypt and decrypt data using symmetric encryption algorithms and a shared session key.

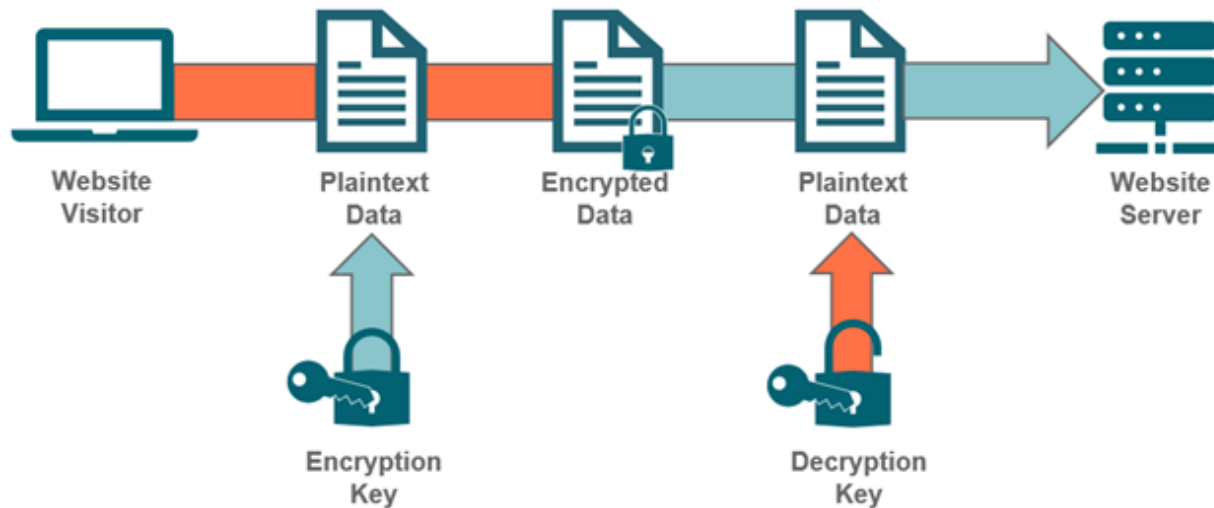
Secure Data Transfer: All subsequent data exchanged between the client and server remains encrypted, protecting it from eavesdropping and tampering.

HTTPS Working

How Insecure Website Communications Work (HTTP)



How Secure Website Communications Work (HTTPS)



Benefits of HTTPS

HTTPS offers numerous benefits for secure web communication:

- **Data Confidentiality:** HTTPS encrypts sensitive information, such as passwords, credit card details, and personal data, preventing unauthorized access.
- **Data Integrity:** HTTPS ensures that data remains intact during transmission, detecting any modifications or tampering attempts.
- **Authentication:** HTTPS verifies the identity of the server through SSL/TLS certificates, preventing impersonation or man-in-the-middle attacks.
- **Trust and User Confidence:** Displaying the padlock symbol and "https" in the URL instills trust in users and reassures them about the security of the website.
- **SEO Benefits:** Search engines consider HTTPS as a ranking signal, incentivizing website owners to implement HTTPS for improved search engine visibility.

Implementing HTTPS

Steps to implement HTTPS on a website:

1. Obtain an SSL/TLS certificate from a trusted Certificate Authority (CA).
2. Install the SSL/TLS certificate on the web server.
3. Configure the server to redirect HTTP traffic to HTTPS.
4. Ensure all web content (images, scripts, stylesheets, etc.) is loaded securely using HTTPS.
5. Test the HTTPS implementation to verify proper functioning and resolve any issues.

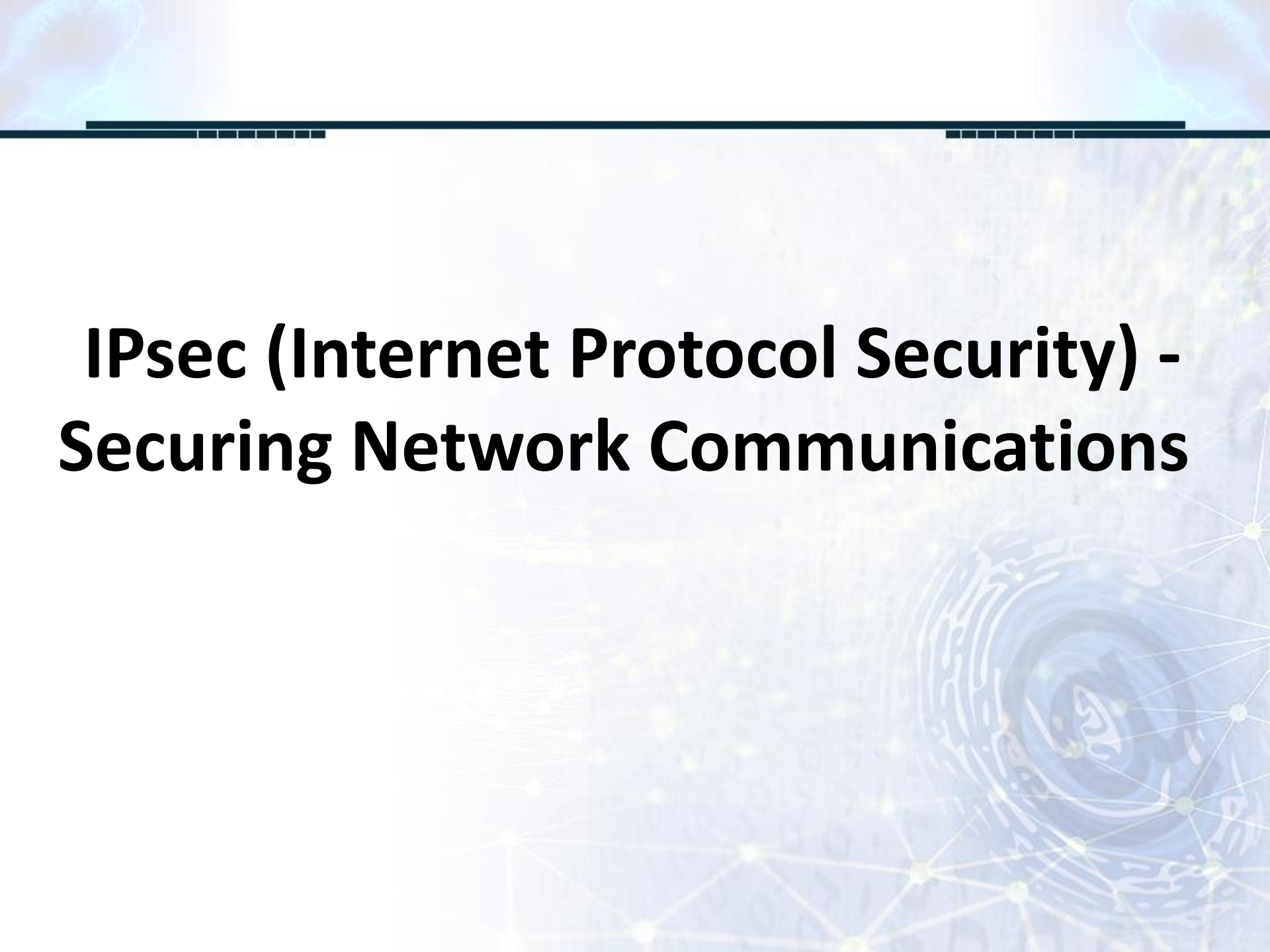
HTTPS Best Practices

Best practices for implementing and maintaining HTTPS:

- Use the latest version of the SSL/TLS protocol supported by your infrastructure.
- Enable strong cipher suites and prioritize secure encryption algorithms.
- Implement HTTP Strict Transport Security (HSTS) to enforce HTTPS usage and prevent downgrade attacks.
- Regularly renew and update SSL/TLS certificates to prevent expiration or revocation.
- Perform security audits and vulnerability scans to identify and address any weaknesses in the HTTPS configuration.

Conclusion

- HTTPS is a crucial technology for securing web communication and protecting sensitive information.
- It ensures data confidentiality, integrity, and authenticity, building trust with users and search engines.
- By implementing HTTPS correctly and following best practices, organizations can enhance the security of their websites and safeguard user data.



IPsec (Internet Protocol Security) - Securing Network Communications

Introduction to IPsec

- IPsec (Internet Protocol Security) is a suite of protocols and cryptographic techniques used to secure network communications at the IP layer.
- It provides a robust framework for ensuring the confidentiality, integrity, and authenticity of IP packets transmitted over a network.



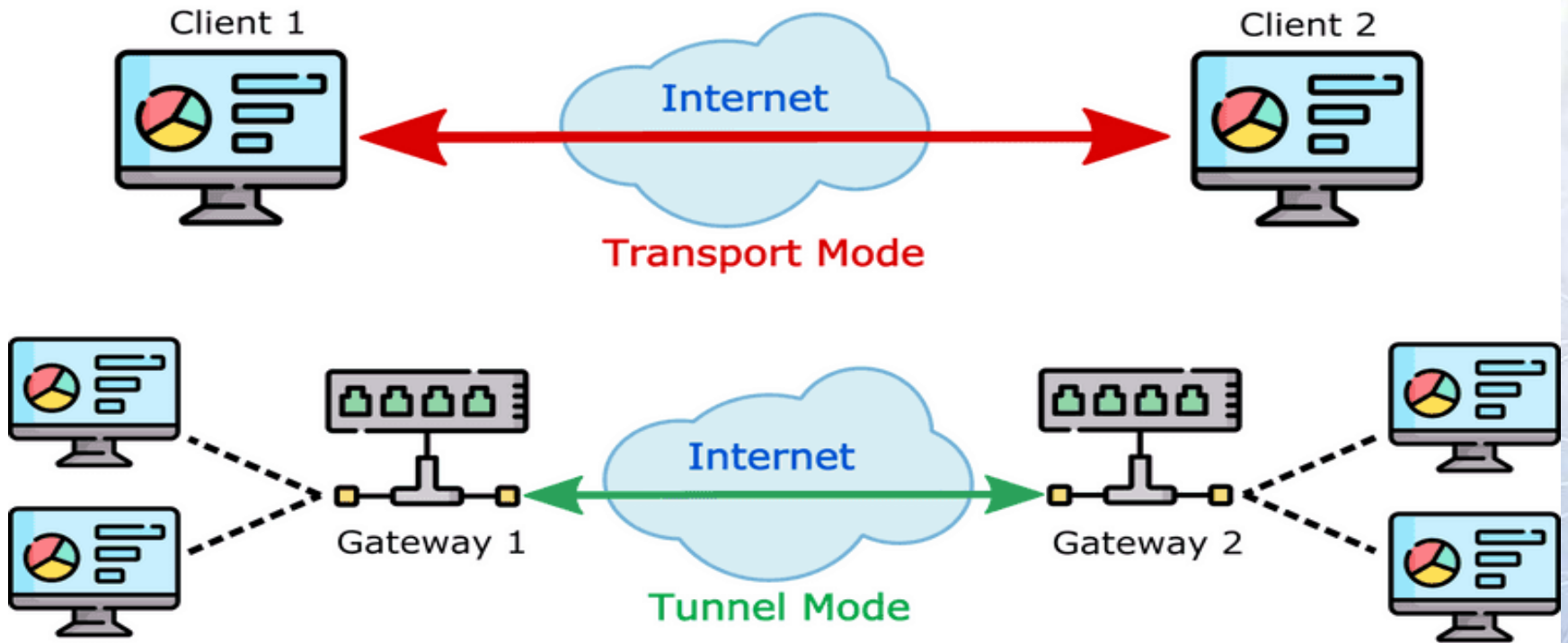
How IPsec Works?

IPsec operates in two main modes: Transport mode and Tunnel mode:

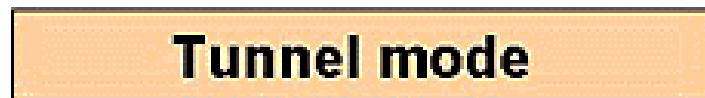
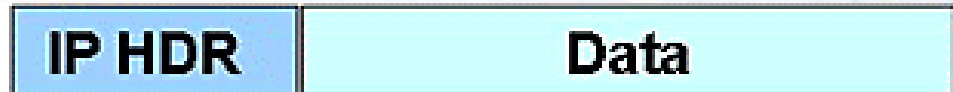
1. **Transport Mode:** Protects the data payload of IP packets, leaving the original IP header intact. It is typically used for end-to-end communication within a network.
2. **Tunnel Mode:** Encrypts the entire IP packet, including the original IP header, and encapsulates it within a new IP packet. It is often used for secure communication between networks.

IPsec Working

IPSec Modes



IPsec Modes

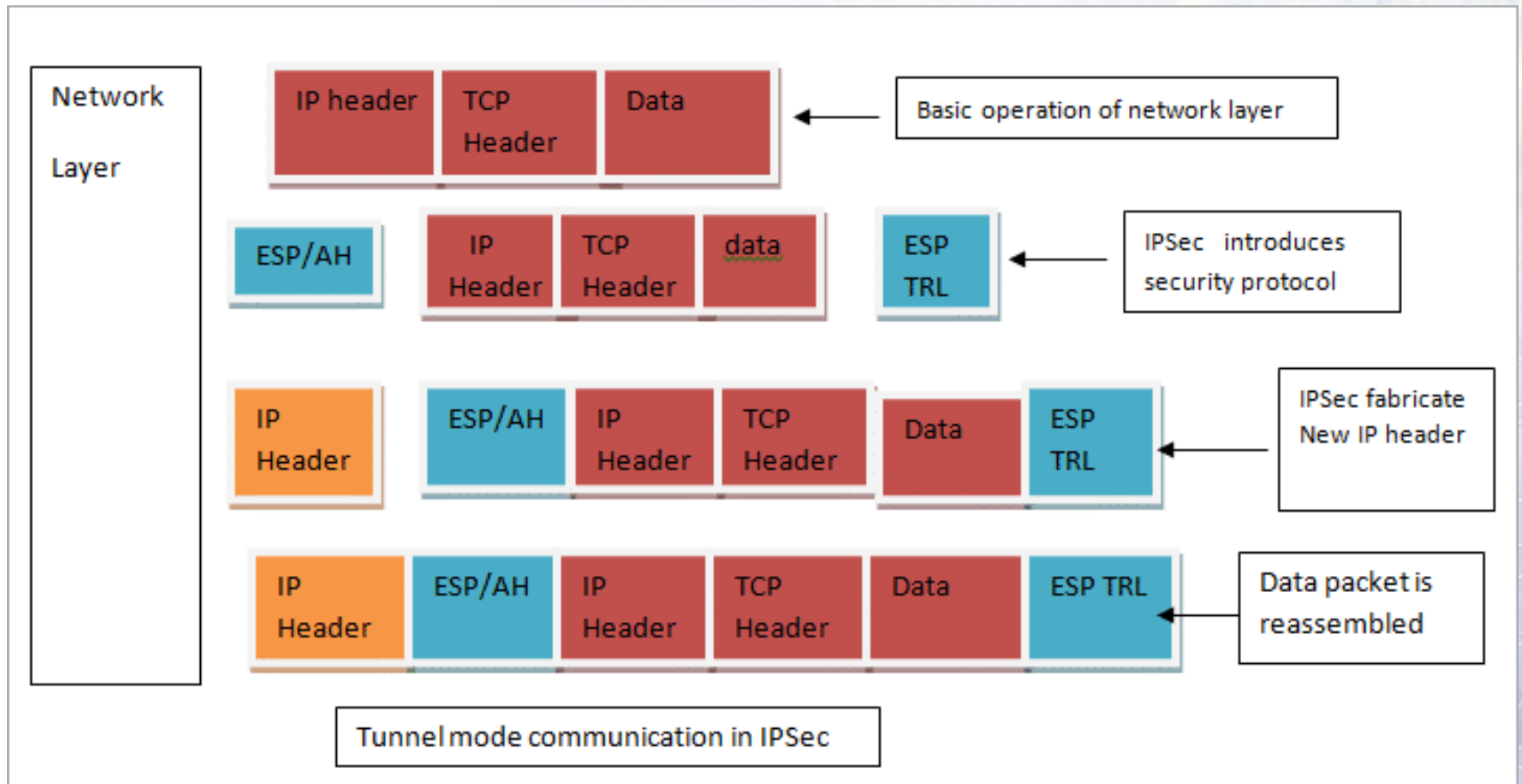


Components of IPsec

IPsec consists of several key components:

1. **Authentication Header (AH):** Provides data integrity and authentication of IP packets.
2. **Encapsulating Security Payload (ESP):** Offers data confidentiality, integrity, and authentication through encryption and encapsulation.
3. **Security Associations (SA):** Establishes the security parameters, including encryption algorithms, authentication methods, and key management, between two communicating entities.
4. **Key Management:** Involves the secure exchange, generation, and management of cryptographic keys used by IPsec for encryption and authentication.

Tunnel Mode Detail



Benefits of IPsec

IPsec offers numerous advantages for securing network communications:

1. **Confidentiality:** Encrypts IP packets, preventing unauthorized access and eavesdropping of sensitive data.
2. **Integrity:** Verifies the integrity of IP packets, ensuring they have not been tampered with during transit.
3. **Authentication:** Authenticates the source of IP packets, preventing spoofing and unauthorized access.
4. **Seamless Integration:** IPsec can be implemented at the network layer, providing security for all applications and protocols that use IP.
5. **Interoperability:** IPsec is a widely supported standard, allowing secure communication between different vendors and platforms.

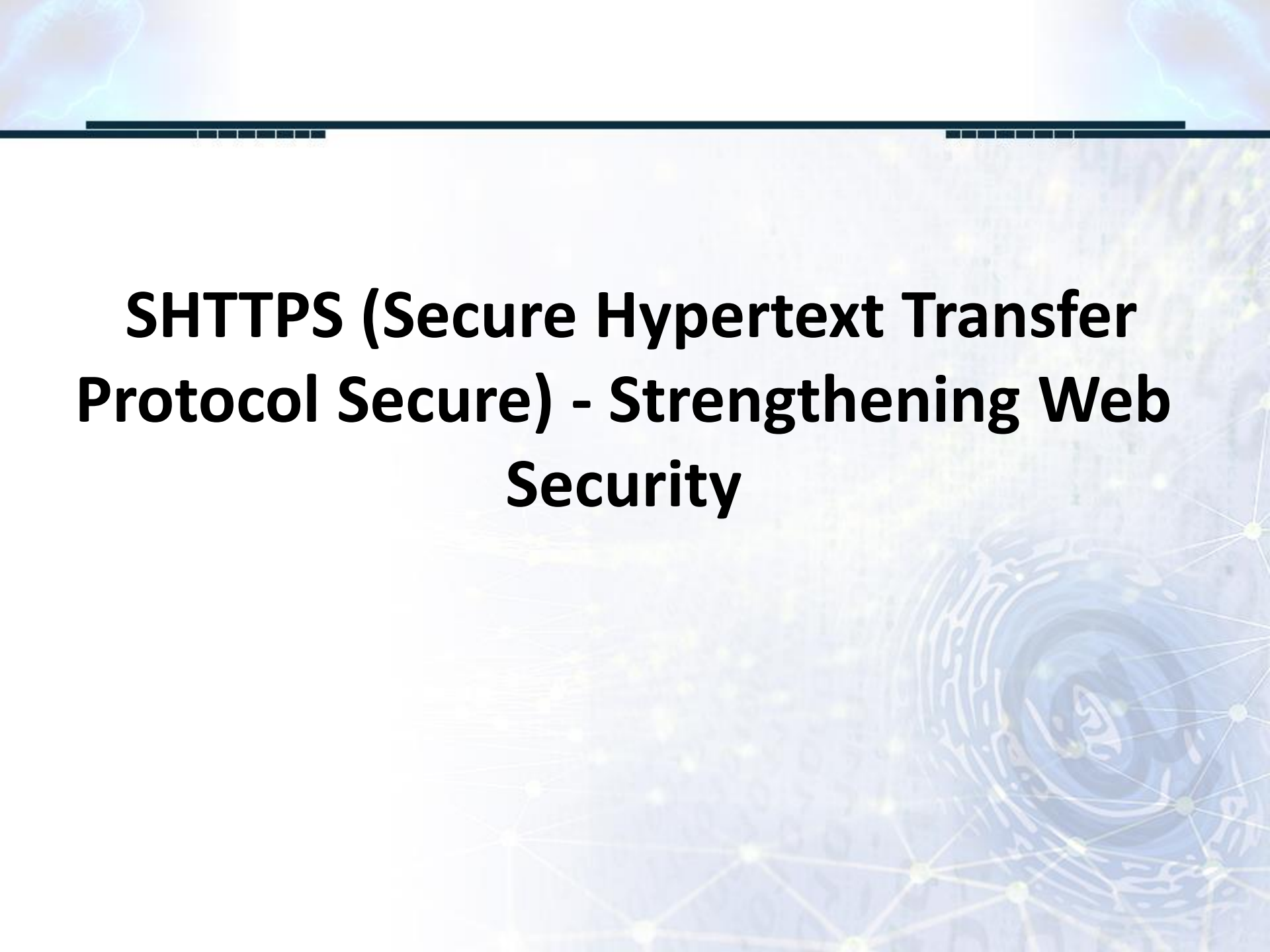
IPsec Implementation

Steps to implement IPsec in a network:

1. **Assess Network Requirements:** Determine the specific security needs and objectives of the network.
2. **Plan IPsec Policy:** Define security policies, including encryption algorithms, authentication methods, and key management approaches.
3. **Configure IPsec Devices:** Configure IPsec parameters on network devices, such as routers, firewalls, or VPN concentrators, based on the defined policies.
4. **Test and Monitor:** Perform thorough testing to ensure IPsec is functioning correctly and continuously monitor the network for any potential issues or vulnerabilities.

Conclusion

- IPsec is a powerful security protocol suite that protects network communications at the IP layer, ensuring confidentiality, integrity, and authenticity.
- By implementing IPsec correctly and following best practices, organizations can secure their network infrastructure and protect sensitive data from unauthorized access.



SHTTPS (Secure Hypertext Transfer Protocol Secure) - Strengthening Web Security

Introduction to SHTTPS

- SHTTPS (Secure Hypertext Transfer Protocol Secure) is an enhanced version of HTTPS that integrates additional security measures.
- It combines the secure communication features of HTTPS with additional mechanisms to protect against various web security threats.



Why SHTTPS?

- Traditional HTTPS provides secure communication between clients and servers, but SHTTPS further strengthens web security by addressing specific vulnerabilities and attacks.
- SHTTPS aims to mitigate risks related to website tampering, data integrity, and man-in-the-middle attacks.

Key Features of SHTTPS

SHTTPS incorporates the following key features to enhance web security:

- **Subresource Integrity (SRI):**
 - SRI ensures that external resources, such as scripts and stylesheets, loaded by a webpage are not tampered with during transit.
 - It uses cryptographic hashes to verify the integrity of the resources, allowing the browser to block or warn if any modifications are detected.
- **Certificate Transparency (CT):**
 - CT is a framework that provides public auditing and monitoring of SSL/TLS certificates issued by Certificate Authorities (CAs).
 - It aims to detect and mitigate misissued or fraudulent certificates, enhancing trust and accountability in the certificate ecosystem.
- **HTTP Public Key Pinning (HPKP):**
 - HPKP allows website operators to specify a list of cryptographic hashes of their SSL/TLS public keys in the HTTP response header.
 - This helps protect against rogue or compromised CAs by instructing the browser to only accept specific public keys for future connections to the website.

Benefits of SHTTPS

SHTTPS offers several advantages for web security:

- **Enhanced Protection:** SHTTPS strengthens the overall security of websites by addressing specific vulnerabilities and threats.
- **Tamper Detection:** SRI helps ensure the integrity of external resources and prevents unauthorized modifications.
- **Certificate Accountability:** CT provides transparency and oversight of SSL/TLS certificates, reducing the risk of misissued or fraudulent certificates.
- **Key Validation:** HPKP allows website operators to enforce the use of specific public keys, protecting against compromised or unauthorized certificates.
- **User Trust:** Implementing SHTTPS demonstrates a commitment to web security, enhancing user confidence and trust in the website.

Implementing SHTTPS

Steps to implement SHTTPS on a website:

- **Enable HTTPS:** Ensure that your website is already using HTTPS for secure communication.
- **Subresource Integrity (SRI):** Implement SRI by adding integrity attributes to external resource references (e.g., script and stylesheet tags) in your web pages.
- **Certificate Transparency (CT):** Utilize CT logs and monitoring services to track and validate SSL/TLS certificates issued for your website.
- **HTTP Public Key Pinning (HPKP):** Carefully consider the implications of HPKP, as it requires careful management of public keys and potential risks associated with pinning.

Conclusion

- SHTTPS is an advanced approach to web security, integrating additional measures to strengthen HTTPS and protect against specific vulnerabilities.
- By implementing SHTTPS and leveraging its features, website owners can enhance the integrity, trustworthiness, and overall security of their web presence.



SSH (Secure Shell) - Secure Remote Access and File Transfer

Introduction to SSH

- SSH (Secure Shell) is a cryptographic network protocol that provides secure remote access and file transfer between two systems.
- It offers a secure alternative to traditional remote access protocols like Telnet and FTP.
- SSH ensures the confidentiality, integrity, and authenticity of data exchanged between client and server.

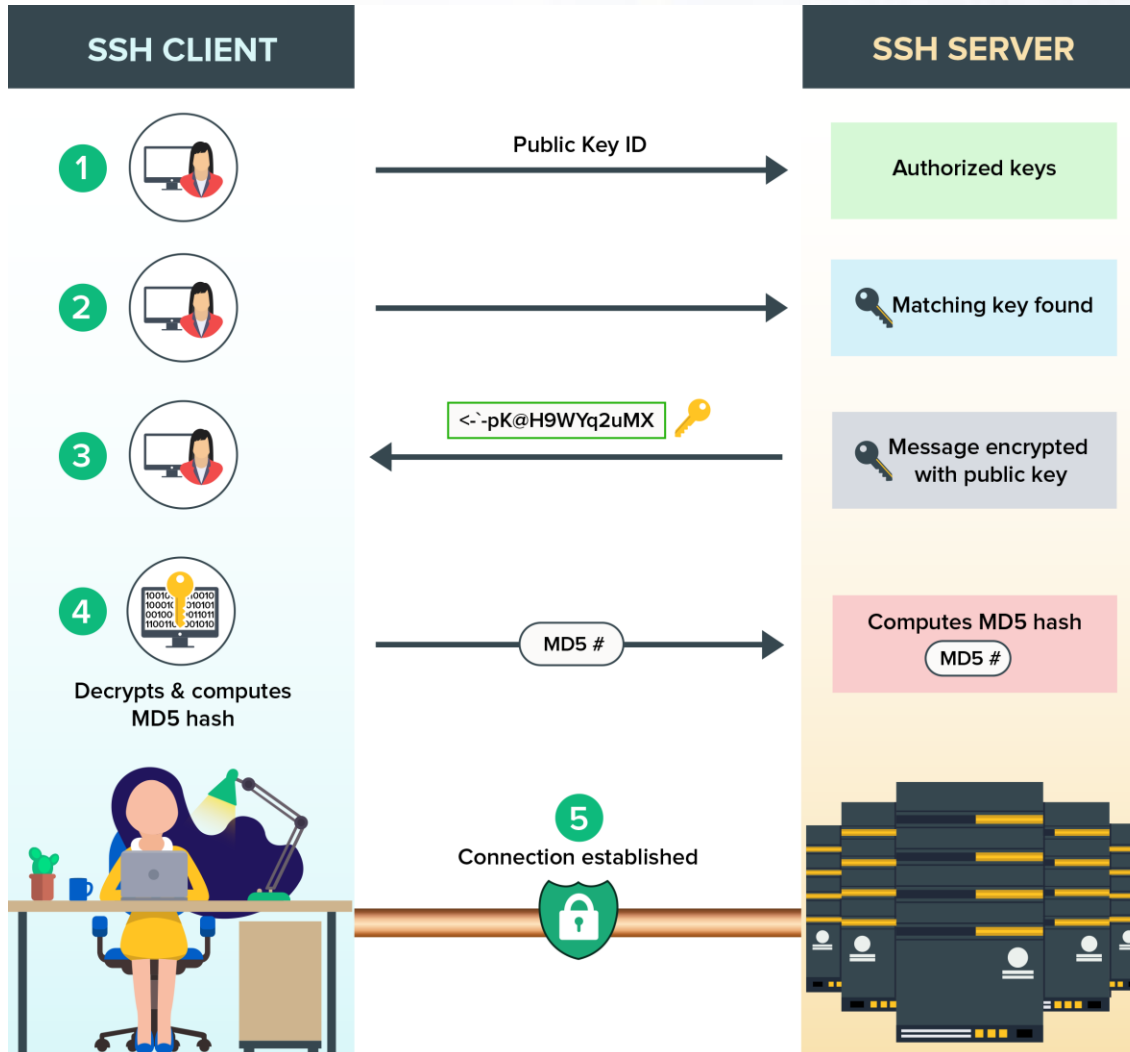


How SSH Works

SSH uses public-key cryptography and encryption to establish a secure connection:

1. **Client Authentication:** The client initiates a connection to the server using SSH and provides its public key.
2. **Server Authentication:** The server presents its public key to the client, which the client verifies to ensure the authenticity of the server.
3. **Session Key Exchange:** Both client and server agree on a session key, which is used for symmetric encryption and decryption of data during the session.
4. **Secure Data Exchange:** All subsequent data exchanged between the client and server is encrypted using the session key.
5. **Command Execution and File Transfer:** The client can securely execute remote commands or transfer files to and from the server.

HTTPS Working



Benefits of SSH

SSH offers several advantages for secure remote access and file transfer:

- **Encryption:** All data transmitted over SSH is encrypted, protecting it from unauthorized access or interception.
- **Authentication:** SSH uses public-key cryptography for user authentication, ensuring secure access to remote systems.
- **Data Integrity:** SSH verifies the integrity of data during transmission, preventing tampering or unauthorized modification.
- **Port Forwarding:** SSH allows secure tunneling of other protocols, enabling remote access to services running on a server's local network.
- **Cross-Platform Compatibility:** SSH is available on various operating systems, making it widely accessible for remote administration.

SSH Implementation

Steps to implement SSH for remote access and file transfer:

1. Install an SSH server on the remote system you want to access.
2. Generate an SSH key pair on the client machine.
3. Configure the SSH server to allow remote access using the generated SSH public key.
4. Use an SSH client (e.g., OpenSSH, PuTTY) to establish a secure connection to the remote system using the SSH key pair.

SSH Best Practices

Best practices for implementing and using SSH:

- Use strong and unique SSH key pairs for authentication.
- Disable password-based authentication to enhance security.
- Regularly update SSH software and apply security patches.
- Implement firewall rules to allow SSH access only from trusted IP addresses.
- Monitor SSH logs for suspicious activity and enable two-factor authentication for added security.

Conclusion

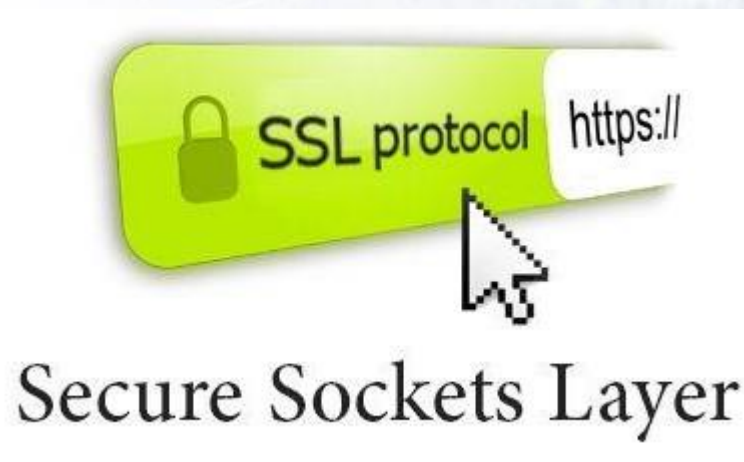
- SSH is a critical protocol for secure remote access and file transfer.
- It provides encryption, authentication, and data integrity, ensuring secure communication between client and server.
- By implementing SSH correctly and following best practices, organizations can protect sensitive information and maintain secure remote administration.



SSL (Secure Sockets Layer) - Ensuring Secure Communication

Introduction to SSL

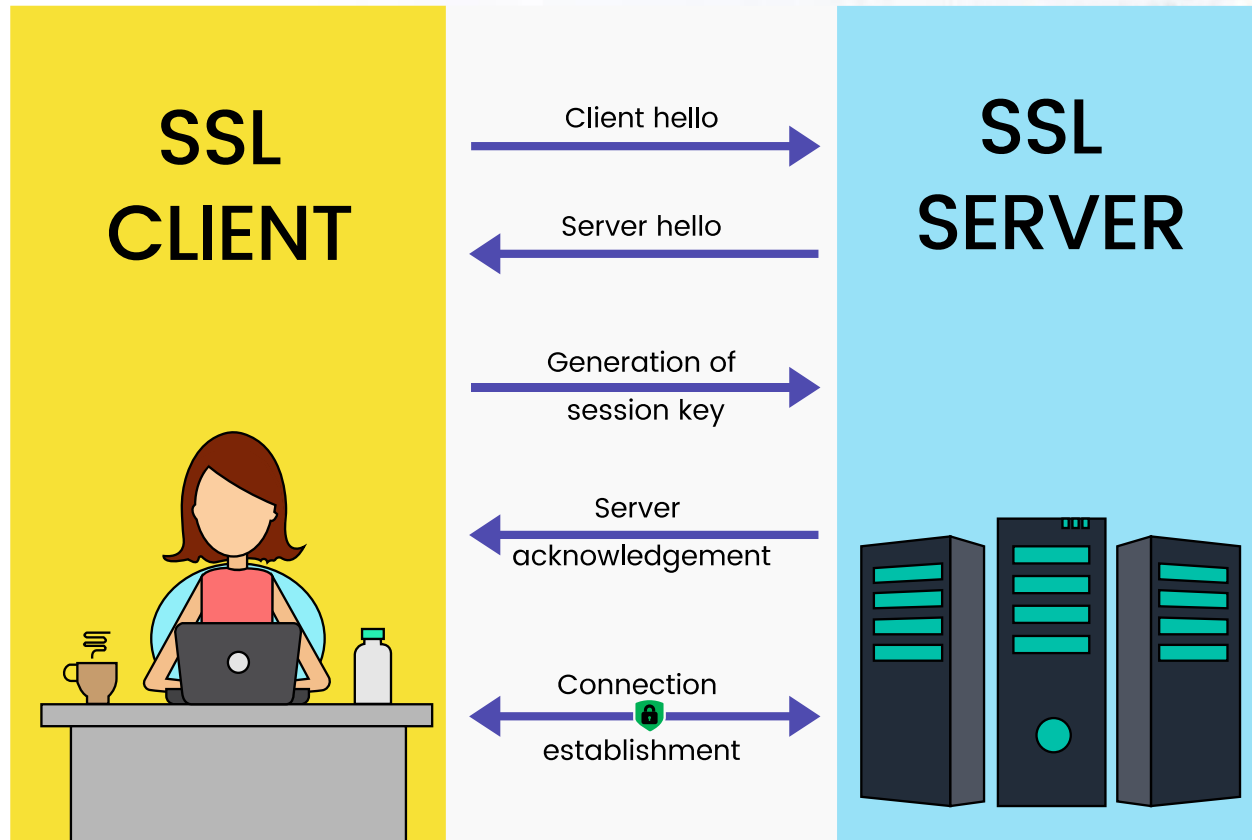
- SSL (Secure Sockets Layer) is a cryptographic protocol that provides secure communication over the internet.
- It ensures the confidentiality, integrity, and authenticity of data transmitted between clients and servers.
- SSL has been succeeded by Transport Layer Security (TLS), but the term "SSL" is still commonly used.



How SSL Works

- SSL handshake process:
- **Client Hello:** The client initiates a connection request to the server, presenting its supported SSL/TLS versions and cipher suites.
- **Server Hello:** The server responds by selecting the appropriate SSL/TLS version and cipher suite from the client's options.
- **Certificate Exchange:** The server sends its SSL certificate to the client, containing the server's public key and digitally signed by a trusted Certificate Authority (CA).
- **Client Authentication:** If required, the client presents its own SSL certificate to the server for authentication.
- **Session Key Exchange:** The client and server establish a session key for symmetric encryption and decryption of data during the session.
- **Secure Data Exchange:** All subsequent data exchanged between the client and server is encrypted using the session key.
- **Session Closure:** When the session ends, the client and server exchange closure messages to properly terminate the connection.

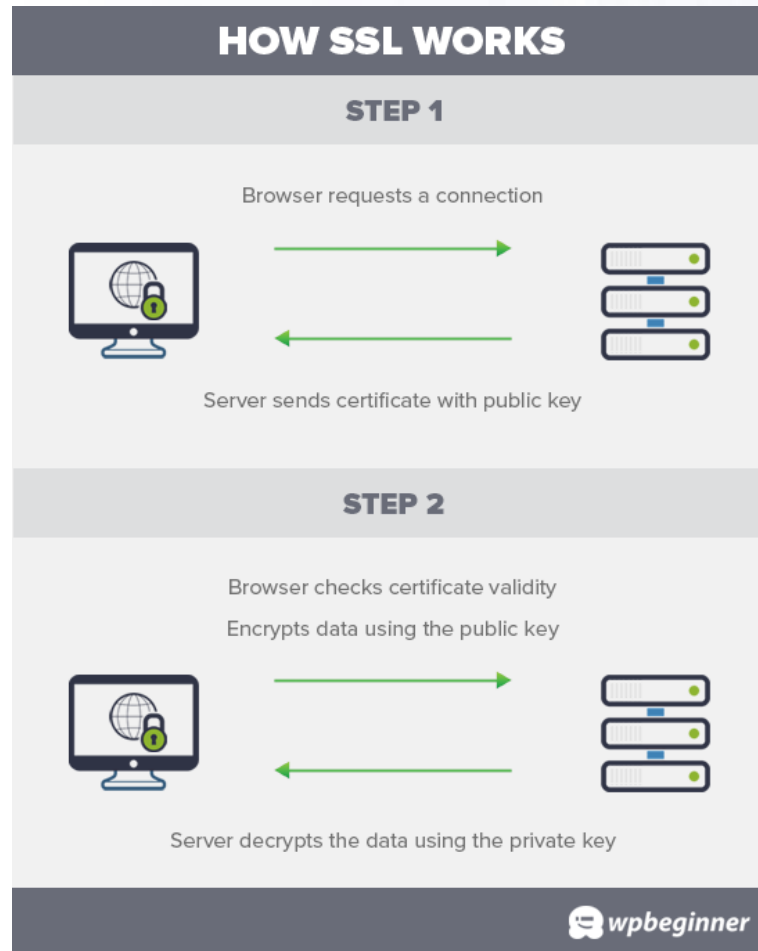
SSL Working



SSL Certificate

- SSL certificates play a crucial role in SSL/TLS communication:
- They are digital files that bind an organization's identity with a public key.
- Issued by trusted Certificate Authorities (CAs), SSL certificates provide authenticity and trust to the SSL/TLS connection.
- SSL certificates contain information such as the domain name, organization name, CA's digital signature, and the public key.

SSL Working with certificate



Benefits of SSL

- SSL provides several advantages for secure communication:
- **Data Encryption:** SSL encrypts sensitive information, such as login credentials and financial details, ensuring their confidentiality.
- **Data Integrity:** SSL ensures that data remains intact during transmission, preventing unauthorized modification.
- **Authentication:** SSL certificates verify the identity of the server, assuring users that they are connecting to the intended website and not an imposter.
- **Trust and User Confidence:** Displaying the padlock symbol and "https" in the URL enhances trust and reassures users about the security of the website.
- **Compliance:** SSL is often required to meet regulatory and compliance standards, such as PCI DSS for secure payment processing.

SSL Implementation

Steps to implement SSL on a website:

- Obtain an SSL certificate from a trusted CA.
- Install the SSL certificate on the web server.
- Configure the server to use SSL/TLS protocols and enable HTTPS.
- Test the SSL implementation to ensure it is functioning correctly.

SSL Best Practices

Best practices for SSL implementation and management:

- Keep SSL certificates up to date and renew them before expiration.
- Use strong encryption algorithms and secure cipher suites.
- Implement HTTP Strict Transport Security (HSTS) to enforce HTTPS usage.
- Regularly monitor and audit SSL configurations for vulnerabilities.
- Educate users on how to identify SSL indicators, such as padlock symbols and "https" in URLs.

Conclusion

- SSL is a vital technology for ensuring secure communication over the internet.
- It provides data encryption, authentication, and integrity, fostering trust and user confidence.
- By implementing SSL correctly and following best practices, organizations can enhance the security of their online services and protect sensitive information.



TLS (Transport Layer Security) - Ensuring Secure Communication

Introduction to TLS

- TLS (Transport Layer Security) is a cryptographic protocol that provides secure communication over the internet.
- It is the successor to SSL (Secure Sockets Layer) and offers enhanced security features.
- TLS ensures the confidentiality, integrity, and authenticity of data transmitted between clients and servers.

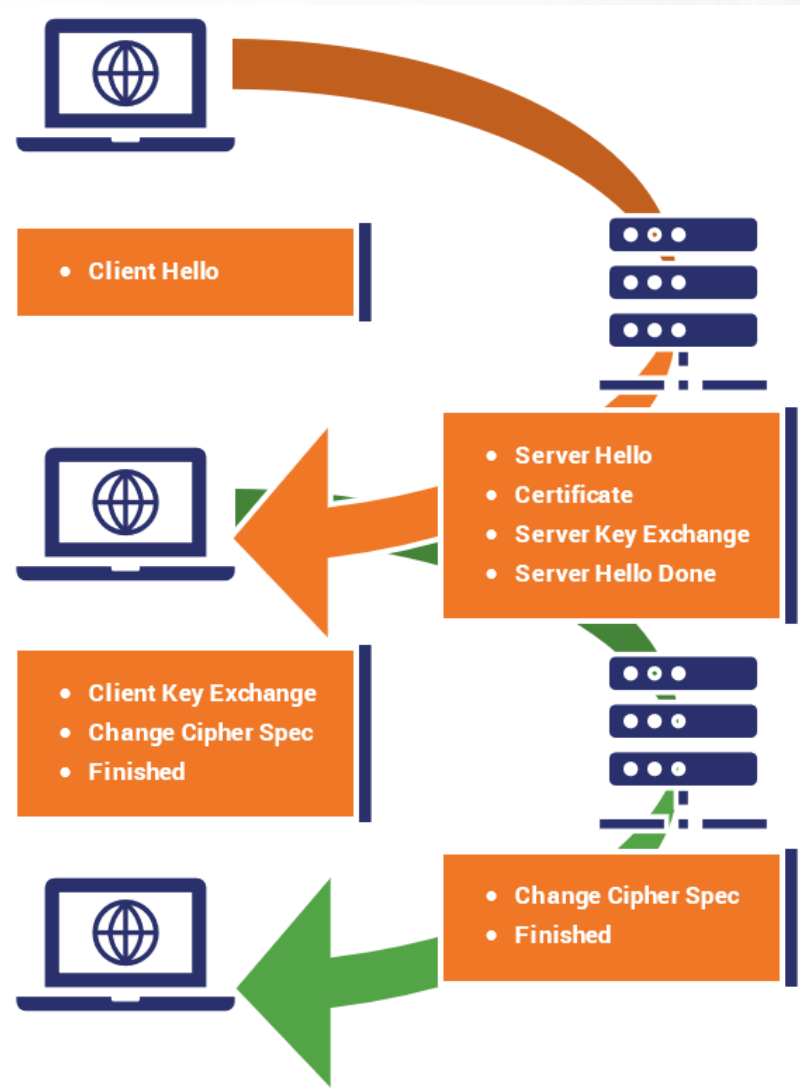


How TLS Works

TLS handshake process:

1. **Client Hello:** The client initiates a connection request to the server, presenting its supported TLS versions and cipher suites.
2. **Server Hello:** The server responds by selecting the appropriate TLS version and cipher suite from the client's options.
3. **Certificate Exchange:** The server sends its TLS certificate to the client, containing the server's public key and digitally signed by a trusted Certificate Authority (CA).
4. **Client Authentication:** If required, the client presents its own TLS certificate to the server for authentication.
5. **Key Exchange:** The client and server negotiate a shared secret key for symmetric encryption and decryption of data during the session.
6. **Secure Data Exchange:** All subsequent data exchanged between the client and server is encrypted using the shared secret key.
7. **Session Closure:** When the session ends, the client and server exchange closure messages to properly terminate the connection.

TSL Working



TLS Versions and Cipher Suites

TLS supports various versions and cipher suites to ensure secure communication:

- **TLS versions:** TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3 (the latest version).
- **Cipher suites:** Combinations of encryption algorithms, authentication methods, and key exchange protocols.

Benefits of TLS

TLS provides several advantages for secure communication:

- **Strong Encryption:** TLS uses robust encryption algorithms to protect data from unauthorized access.
- **Data Integrity:** TLS ensures that data remains intact during transmission and detects any tampering attempts.
- **Authentication:** TLS certificates verify the identity of the server, assuring users they are connecting to the correct website.
- **Forward Secrecy:** TLS supports forward secrecy, ensuring that even if a private key is compromised, past communications remain secure.
- **Compatibility:** TLS is widely supported by modern web browsers and applications, enabling secure communication across platforms.

TLS Implementation

Steps to implement TLS on a website:

1. Obtain a TLS certificate from a trusted CA.
2. Install the TLS certificate on the web server.
3. Configure the server to use TLS protocols and enable HTTPS.
4. Regularly update TLS software and libraries to stay protected against vulnerabilities.

TLS Best Practices

Best practices for TLS implementation and management:

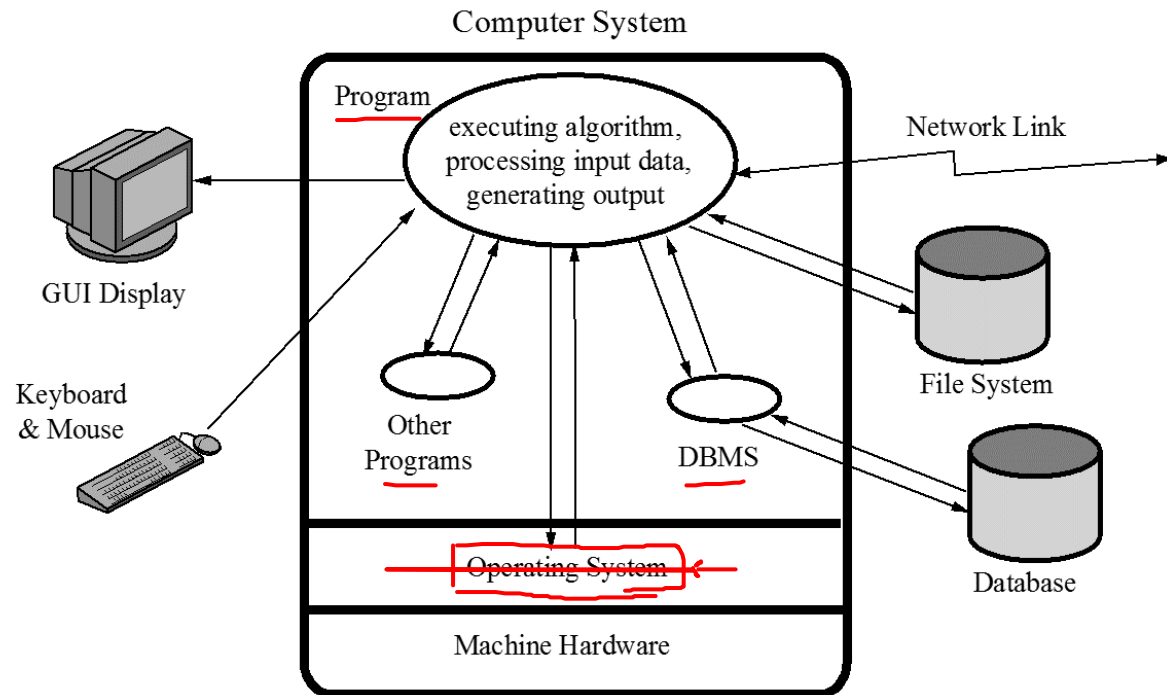
- Use the latest TLS version supported by your infrastructure.
- Select strong cipher suites that prioritize security and performance.
- Enable Perfect Forward Secrecy (PFS) to enhance security.
- Implement strict certificate validation and revocation checking.
- Regularly monitor and audit TLS configurations for vulnerabilities.

Conclusion

- TLS is a critical technology for ensuring secure communication over the internet.
- It offers strong encryption, data integrity, and authentication, enhancing the overall security of online services.
- By implementing TLS correctly and following best practices, organizations can protect sensitive information and establish trust with their users.

Operating System Security

Recall... Abstract View of Program



Operating System Security

Computer are rarely used in isolation

- Usually connected to some kind of network, Internet etc.

Networked computers

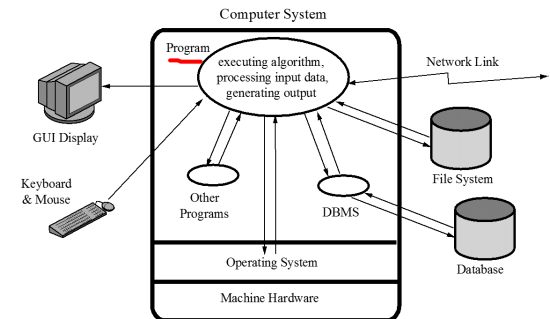
- ensure secure operation in networked environment

New threat?

- Attackers coming from the network.
- Network-facing programs on computers may be buggy.
- Users may be hurt via online communication.

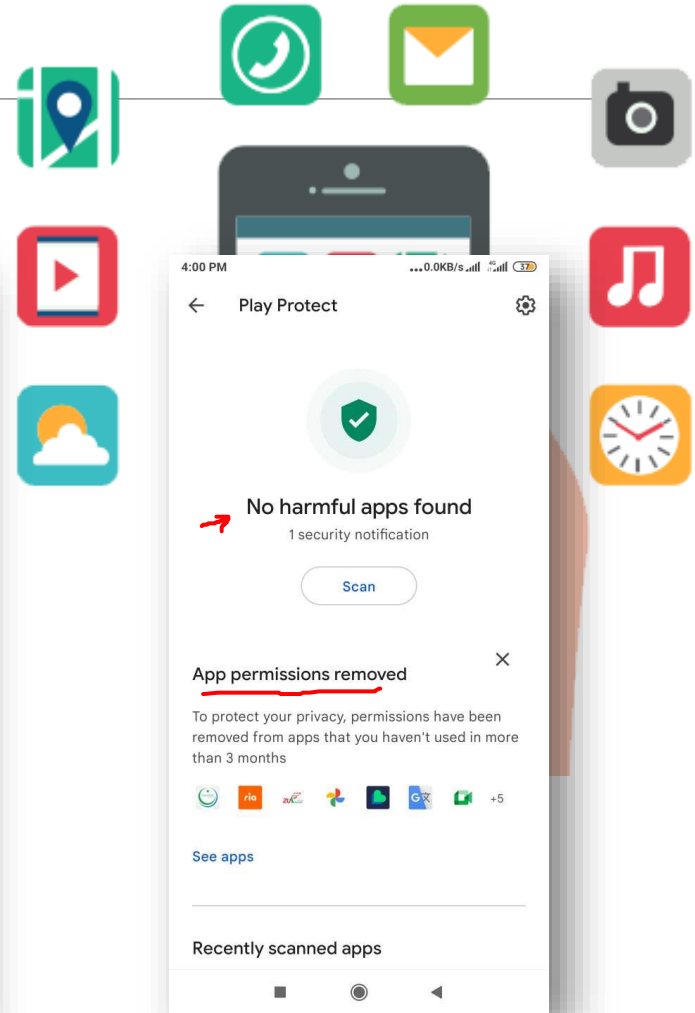
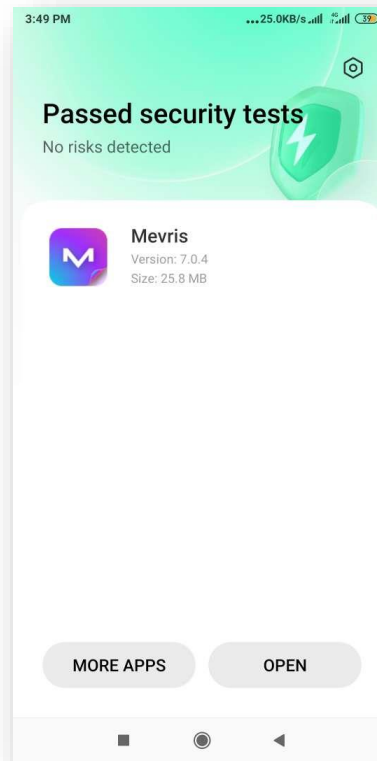
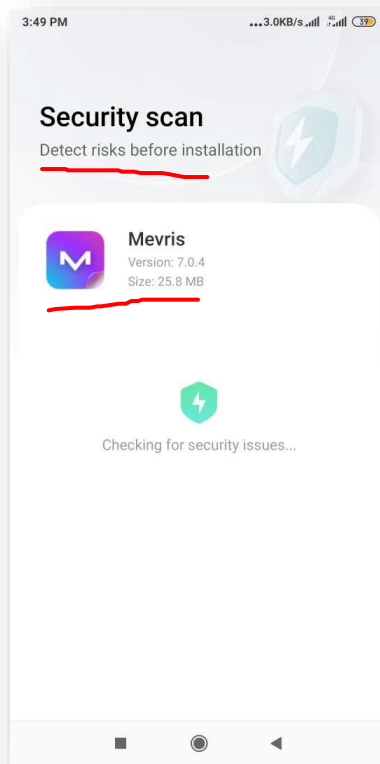
Security mechanisms

- Authentication; Access Control
- Secure Communication (using cryptography)
- Logging & Auditing
- Intrusion Prevention and Detection



Mobile Operating System Security

Mobile computing devices:



Mobile Operating System Security

Mobile computing devices:

New threat?

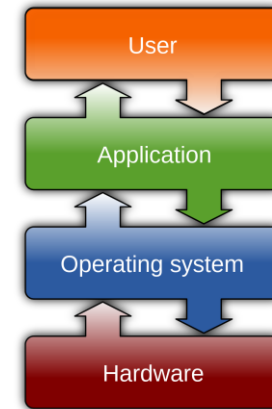
- Apps (programs) may be malicious.
- More tightly connected with personal life of the user e.g. personal health and banking apps.

Security mechanisms?

- Isolation of each app.
- Users assess risks of apps.
- Risk communication.

→ **Google Play Protect**

<https://support.google.com/googleplay/answer/2812853?hl=en>



Use Google Play Protect to help keep your apps safe and your data private

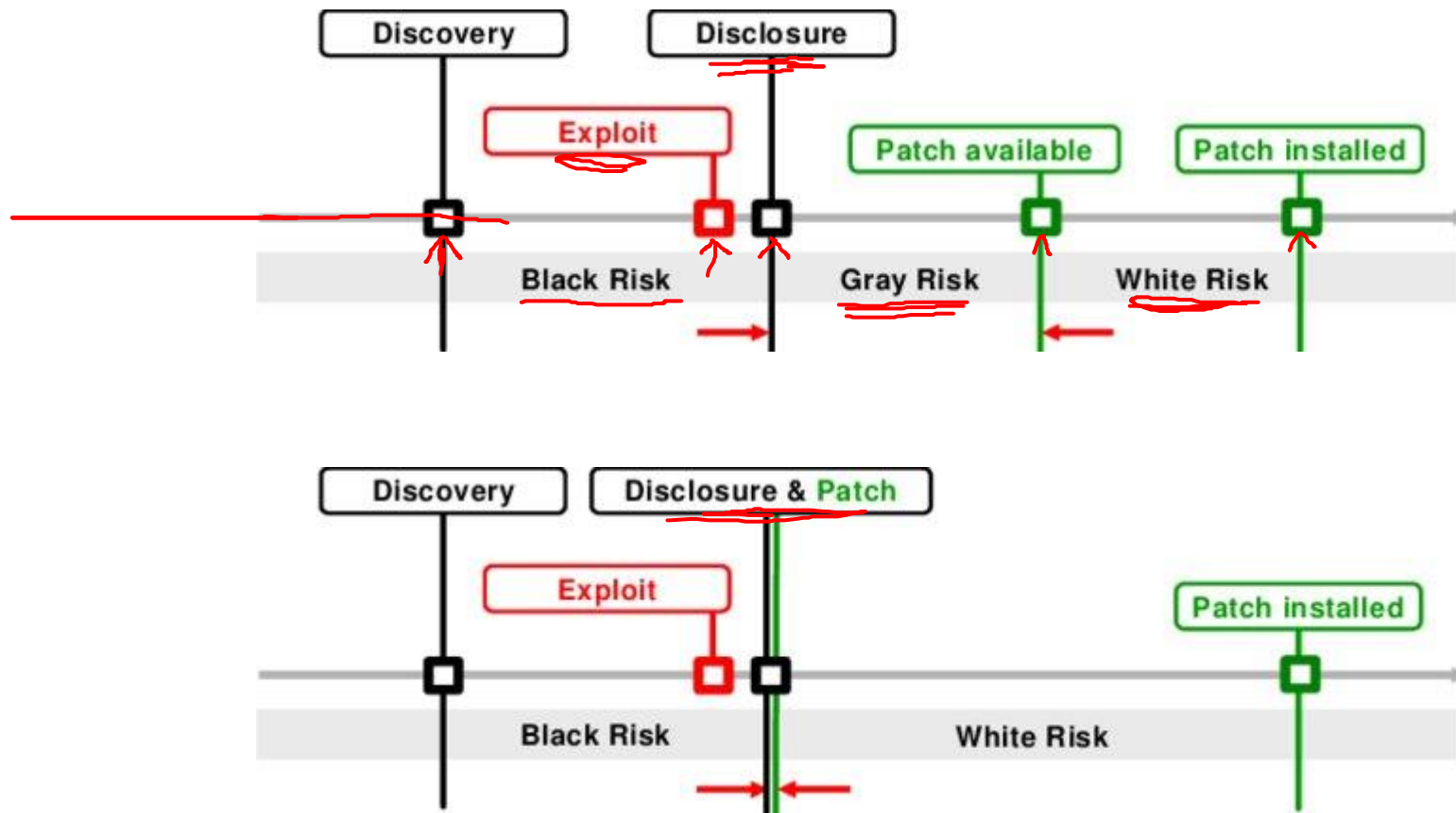
Google Play Protect checks your apps and devices for harmful behavior.

- It runs a safety check on apps from the Google Play Store before you download them.
- It checks your device for potentially harmful apps from other sources. These harmful apps are sometimes called malware.
- It warns you about potentially harmful apps.
- It may deactivate or remove harmful apps from your device.
- It warns you about detected apps that violate our [Unwanted Software Policy](#) by hiding or misrepresenting important information.
- It sends you privacy alerts about apps that can get user permissions to access your personal information, violating our [Developer Policy](#).
- It may reset app permissions to protect your privacy on certain Android versions.

Operating System Hardening

Operating Systems' Risks

Vulnerability, Exploit, Patch...



Operating Systems Hardening

- The idea of OS hardening is to minimize a computer's exposure to current and future threats by fully configuring the operating system and removing unnecessary applications.

- Updates in Windows
- Patch Management System in Linux/Unix

- Basic steps

- Install and patch the operating system

- Harden and configure the operating system to adequately address the identified security needs of the system by:

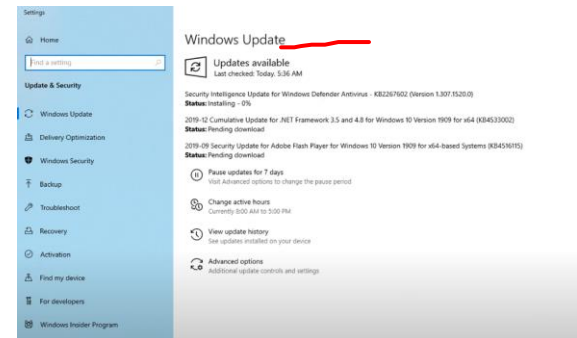
- ➔ ■ Removing unnecessary services, applications, and protocols

- ➔ ■ Configuring users, groups, and permissions

- ➔ ■ Configuring resource controls

- Install and configure additional security controls, such as anti-virus, host-based firewalls, and intrusion detection system (IDS)

- ➔ ○ Test the security of the basic operating system to ensure that the steps taken adequately address its security needs





Remove
Unnecessary
Services,
Applications,
Protocols

When performing the initial installation the supplied defaults should not be used

○ Default configuration is set to maximize ease of use and functionality rather than security

○ If additional packages are needed later they can be installed when they are required

→ If fewer software packages are available to run the risk is reduced

— System planning process should identify what is actually required for a given system



Configure Users, Groups, and Authentication

→ • System planning process should consider:

→ ○ Categories of users on the system

→ ○ Privileges they have

→ ○ Types of information they can access

→ ○ How and where they are defined and authenticated

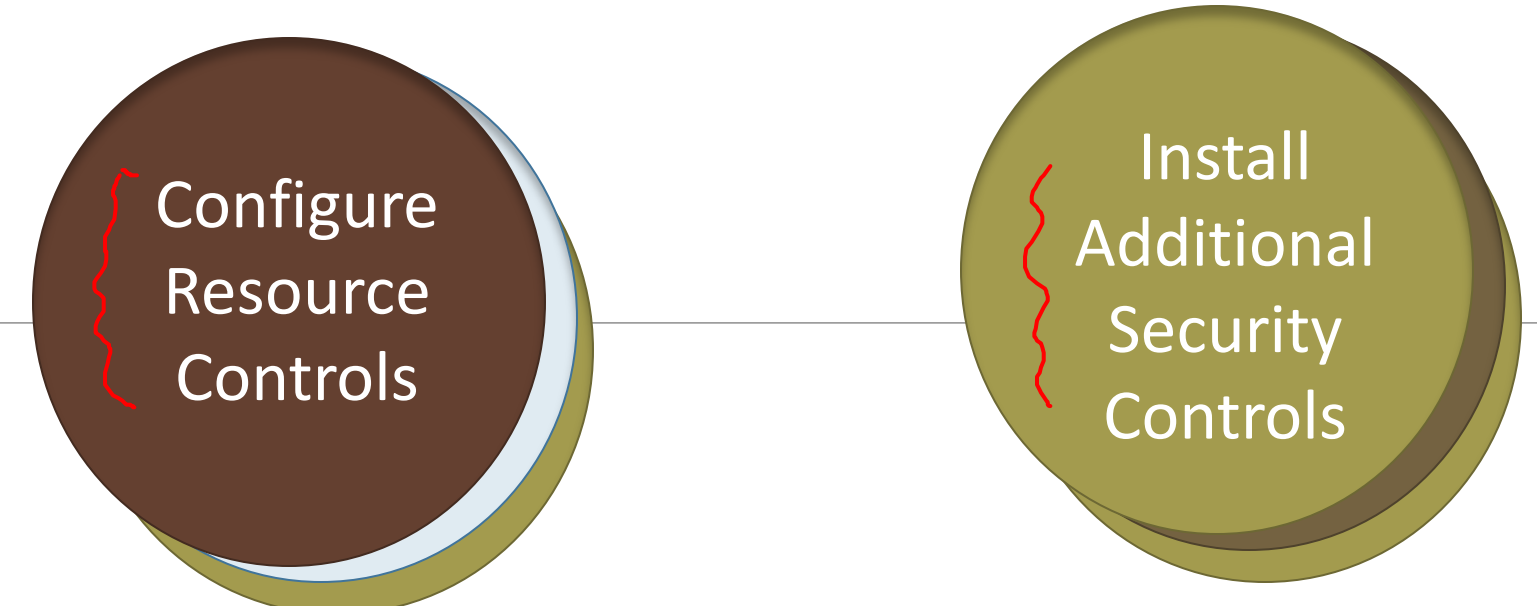
Not all users with access to a system will have the same access to all data and resources on that system

→ Elevated privileges should be restricted to only those users that require them, and then only when they are needed to perform a task

→ • Default accounts included as part of the system installation should be secured

○ Those that are not required should be either removed or disabled

○ Policies that apply to authentication credentials configured



Configure
Resource
Controls

Install
Additional
Security
Controls

Once the users and groups are defined, appropriate permissions can be set on data and resources

Many of the security hardening guides provide lists of recommended changes to the default access configuration

- Further security possible by installing and configuring additional security tools:

- Anti-virus software
- Host-based firewalls
- IDS or IPS software
- Application white-listing



Test the System Security

- There are programs specifically designed to:
 - ○ Review a system to ensure that a system meets the basic security requirements
 - Scan for known vulnerabilities and poor configuration practices
- • Should be done following the initial hardening of the system
- • Repeated periodically as part of the security maintenance process
- Final step in the process of initially securing the base operating system is security testing
- Goal:
 - Ensure the previous security configuration steps are correctly implemented
 - ○ Identify any possible vulnerabilities

Security Maintenance

Security Maintenance

Process of maintaining security is continuous

Security maintenance includes:

- Monitoring and analyzing logging information
- Performing regular backups
- Recovering from security compromises
- Regularly testing system security
- Using appropriate software maintenance processes to patch and update all critical software

Logging

Logging

Can only inform you about bad things that have already happened

In the event of a system breach or failure, system administrators can more quickly identify what happened

Key is to ensure you capture the correct data and then appropriately monitor and analyze this data

Information can be generated by the system, network and applications

Range of data acquired should be determined during the system planning stage

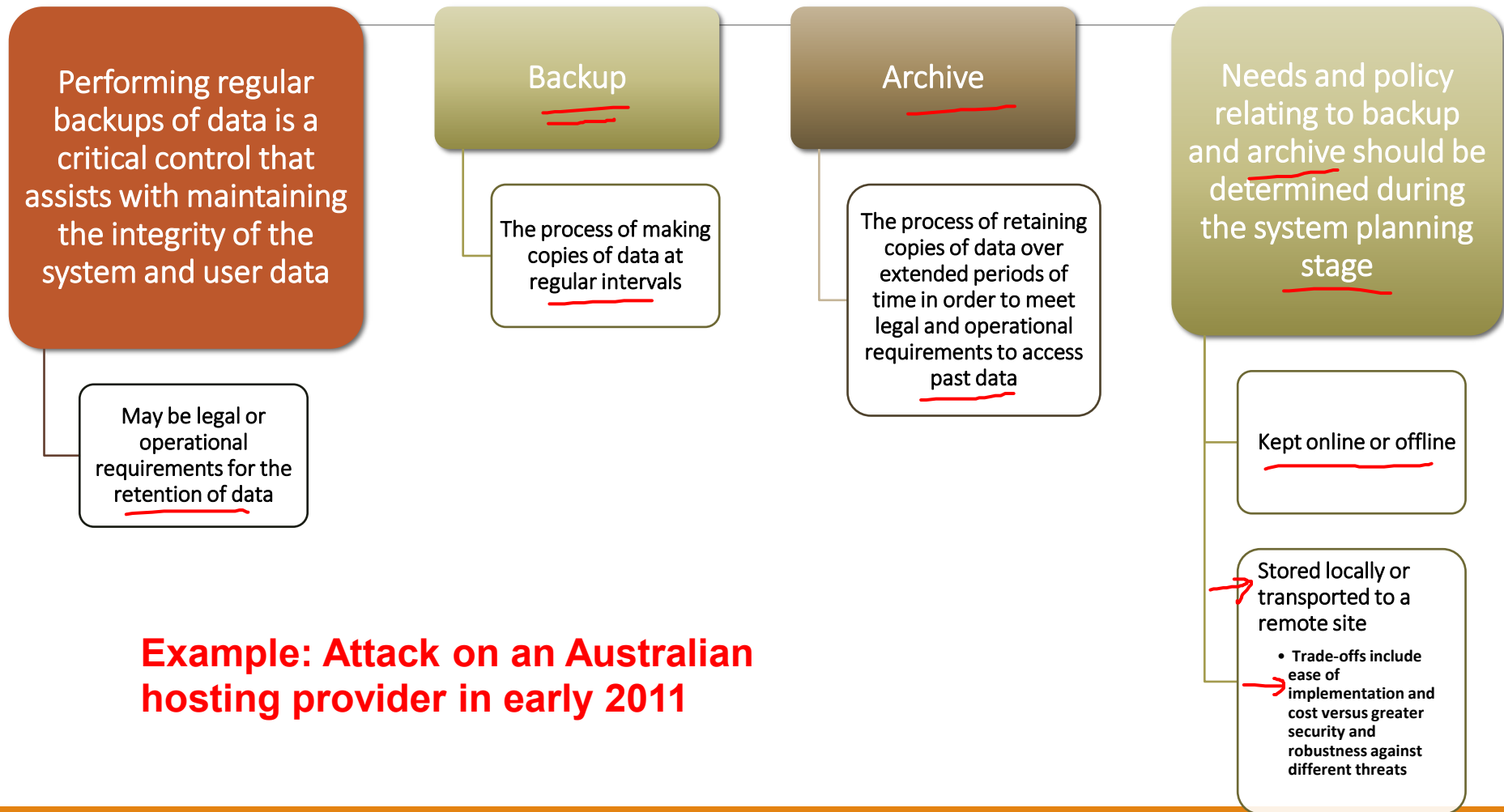
Generates significant volumes of information and it is important that sufficient space is allocated for them

- automatic log rotation

Automated analysis is preferred

Data Backup and Archive

Data Backup and Archive



Linux/Unix Security

Linux/Unix Security



.deb	64 bit	ARM	ARM 64
.rpm	64 bit	ARM	ARM 64
.tar.gz	64 bit	ARM	ARM 64

Patch Management

- Keeping security patches up to date is a widely recognized and critical control for maintaining security
 - Debian based distribution e.g. Ubuntu...include apt-get
 - RPM... Redhat based distribution e.g. Fedora...include up2date or yum
- Application and service configuration
 - Most commonly implemented using separate text files for each application and service
 - Generally located either in the /etc directory or in the installation tree for a specific application
- ○ Individual user configurations that can override the system defaults are located in hidden “dot” files in each user's home directory
- ○ Most important changes needed to improve system security are to disable services and applications that are not required

Linux/Unix Security

Users, groups, and permissions

- Access is specified as granting read, write, and execute permissions to each of owner, group, and others for each resource
- These are set using the chmod command.

Understanding The Linux File Permissions

Column: 1 2 3 4

- rwx rwx rwx

Directory/File/Link Information User Rights Group Rights Others Rights

While the first column defines a directory, file or link, the next 3 columns (2, 3, 4) define the permissions for the User, Group and Others (everyone else) groups.

Linux Permissions Made Easy

user group everyone

- rwx rwx rwx

decimal notification
binary notification

7 7 7

decimal notification: add each number to obtain the value (4 + 2 + 1 = 7)
binary notification: convert it to decimal then you should have the value (r-x = 101 base 2 = 5 base 10)

```
israr@israr-VirtualBox: ~/Desktop/CS627/Assignment2
israr@israr-VirtualBox:~/Desktop/CS627/Assignment2$ ls
AES aes-brute-force-master AES.c
israr@israr-VirtualBox:~/Desktop/CS627/Assignment2$ ls -l
total 32
-rwxrwxr-x 1 israr israr 17784 2021 31  سمير AES
drwxrwxr-x 4 israr israr 4096 2021 27  سمير aes-brute-force-master
-rw-rw-r-- 1 israr israr 5661 2021 27  سمير AES.c
israr@israr-VirtualBox:~/Desktop/CS627/Assignment2$
```

```
israr@israr-VirtualBox:~/Desktop/CS627/Assignment2$ chmod 777 AES.c
israr@israr-VirtualBox:~/Desktop/CS627/Assignment2$ ls -l
total 32
-rwxrwxr-x 1 israr israr 17784 2021 31  سمير AES
drwxrwxr-x 4 israr israr 4096 2021 27  سمير aes-brute-force-master
-rwxrwxrwx 1 israr israr 5661 2021 27  سمير AES.c
```

```
israr@israr-VirtualBox:~/Desktop/CS627/Assignment2$ chmod 700 AES.c
israr@israr-VirtualBox:~/Desktop/CS627/Assignment2$ ls -l
total 32
-rwxrwxr-x 1 israr israr 17784 2021 31  سمير AES
drwxrwxr-x 4 israr israr 4096 2021 27  سمير aes-brute-force-master
-rwx----- 1 israr israr 5661 2021 27  سمير AES.c
israr@israr-VirtualBox:~/Desktop/CS627/Assignment2$
```

Linux/Unix Security

○ Guides recommend changing the access permissions for critical directories and files

○ Local exploit

- Software vulnerability that can be exploited by an attacker to gain elevated privileges

○ Remote exploit

- Software vulnerability in a network server that could be triggered by a remote attacker

Windows Security

Windows Security

Patch management

- “Windows Update” and “Windows Server Update Service” assist with regular maintenance and should be used
- Third party applications also provide automatic update support

Users administration and access controls

- Systems implement discretionary access controls resources
- Vista and later systems also include mandatory integrity controls (MIC)
- Objects are labeled as being of low, medium, high, or system integrity level
- System ensures the subject's integrity is equal or higher than the object's level

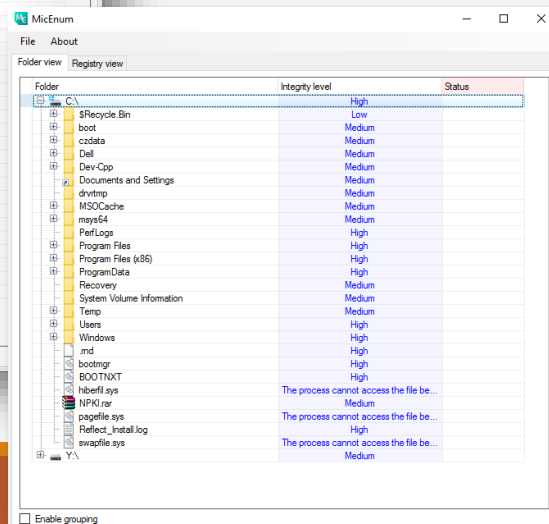
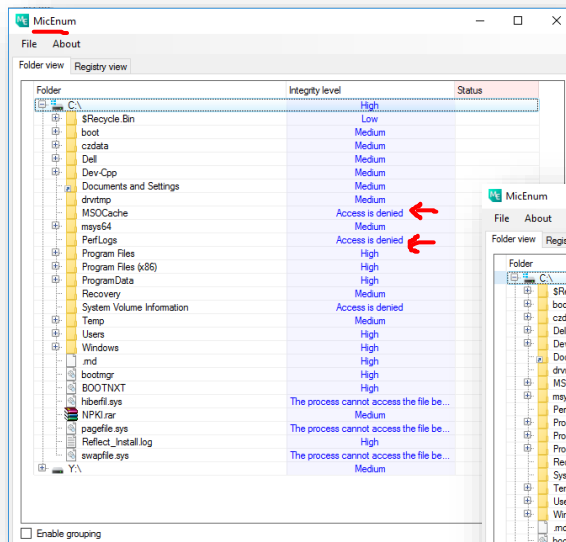
Mandatory Integrity Control (MIC) provides a mechanism for controlling access to securable objects. This mechanism is in addition to discretionary access control and evaluates access before access checks against an object's discretionary access control list (DACL) are evaluated

Windows Security

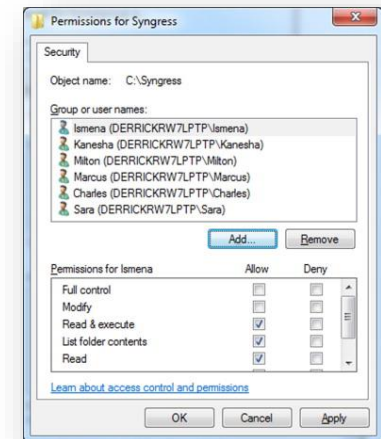
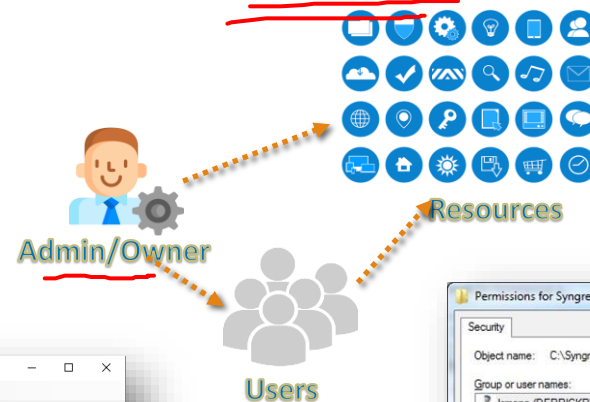
Mandatory Integrity Control (MIC) provides a mechanism for controlling access to securable objects. This mechanism is in addition to discretionary access control and evaluates access before access checks against an object's discretionary access control list (DACL) are evaluated

MANDATORY INTEGRITY CONTROL (MIC)

→ MicEnum Tool, Mandatory Integrity Control Enumerator



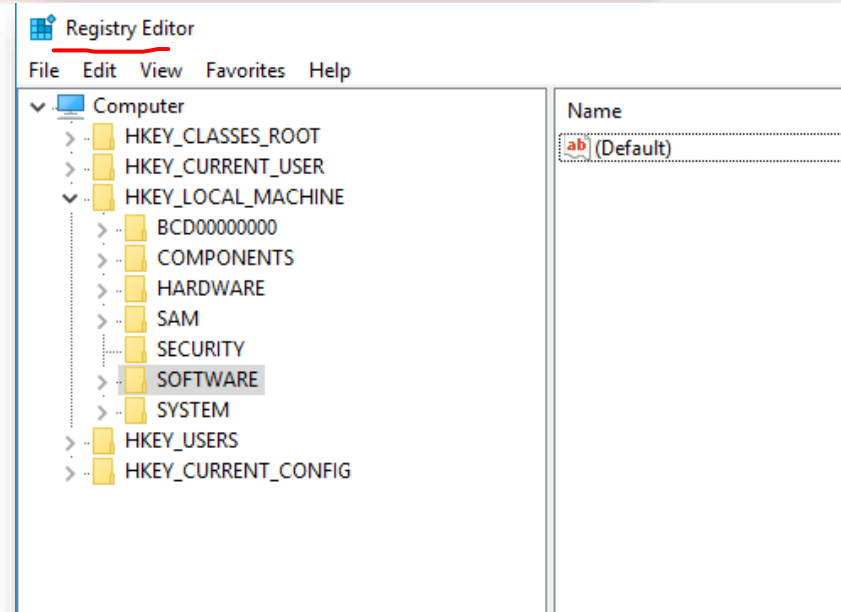
DISCRETIONARY ACCESS CONTROL LIST (DACL)



Windows Security

Application and service configuration

- Much of the configuration information is centralized in the Registry
- Forms a database of keys and values that may be queried and interpreted by applications
- Registry keys can be directly modified using the “Registry Editor”
- More useful for making bulk changes

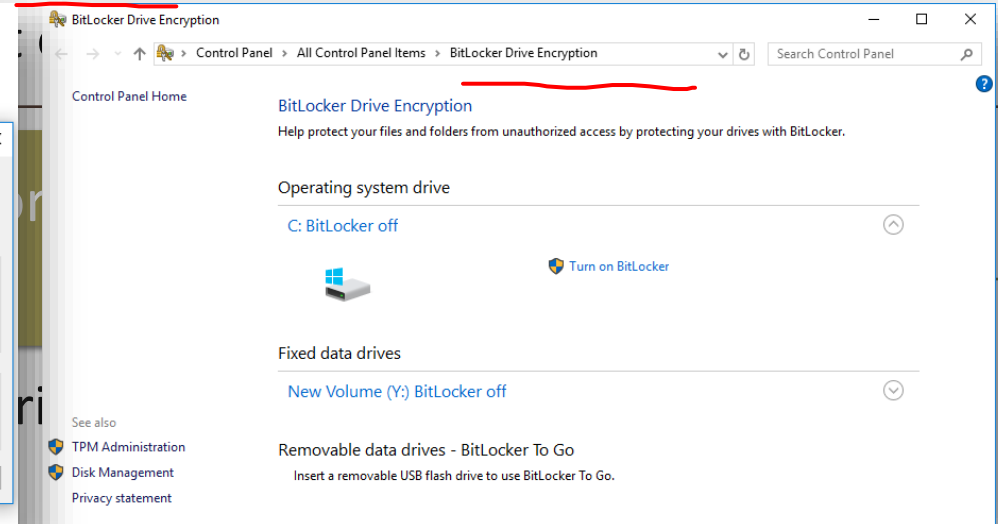
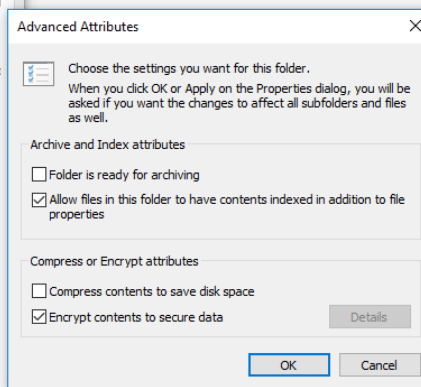
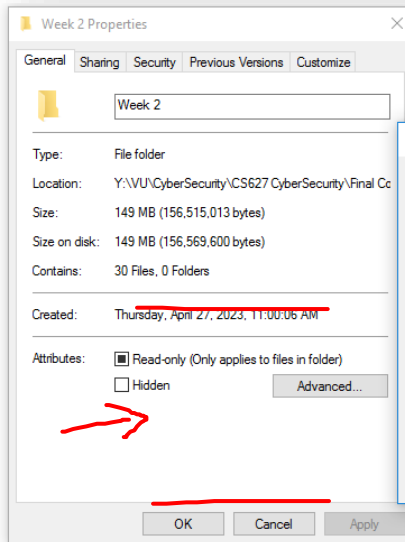
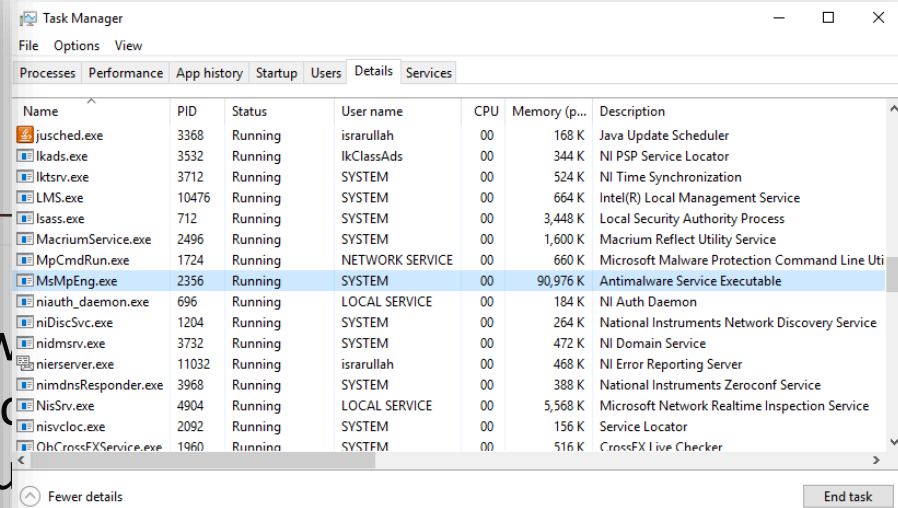
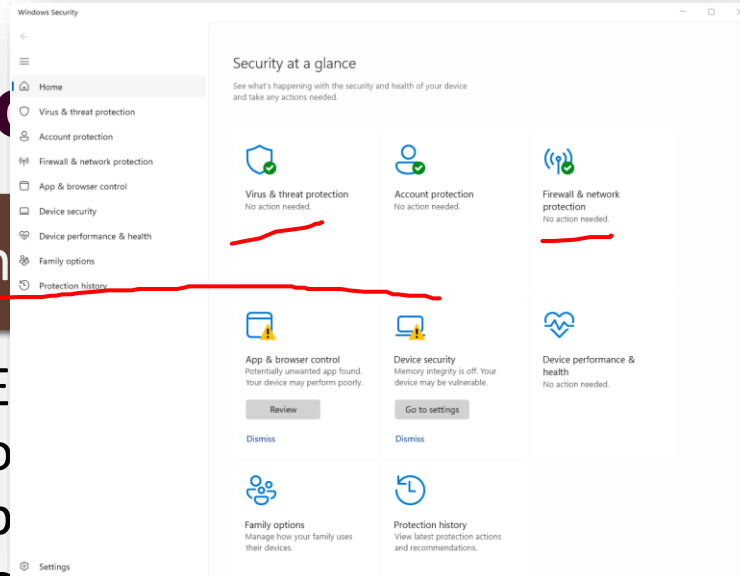


Windows

Other

- E
- o
- p

- Current generation windows systems include basic firewall and malware countermeasure capabilities



Full-disk encryption with AES using BitLocker

Cyber Crime

Cyber Crime

- Cybercrime is a type of crime involving a **computer** or a **computer network**.
- The computer may have been **used in committing the crime**, or it may be the **target**.
- Cybercrime may harm someone, someone's security or finances.

Actors and Stakeholders

- Internationally, both **state** and **non-state** actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes.
- Cybercrimes **crossing international borders** and involving the actions of at least one nation-state are sometimes referred to as **cyberwarfare**.
- Warren Buffett describes cybercrime as the "number one problem with mankind" and said that it "poses real risks to humanity".

- A 2014 report sponsored by McAfee estimated that cybercrime had resulted in \$445 billion USD in annual damage to the global economy.
- Approximately \$1.5 billion was lost in 2012 to online credit and debit card fraud in the US.
- In 2018, a study by the Center for Strategic and International Studies (CSIS), in partnership with McAfee, concluded that nearly 1 percent of global gross domestic product (GDP), close to \$600 billion, is lost to cybercrime each year.
- The World Economic Forum 2020 Global Risk Report confirmed that organized cybercrime groups are joining forces to commit criminal activities online, while estimating the likelihood of their detection and prosecution to be less than 1 percent in the US.

Privacy

- There are also many privacy concerns surrounding cybercrime when confidential information is intercepted or disclosed, legally or otherwise.

Cyber Crime Categories

- Computer Fraud
- Cyberterrorism
 - Ransomware
- Cybersex Trafficking
- Cyberwarfare
- Obscene / Offensive Content
- Ad-Fraud
- Online Harassment
 - Cyberbullying
 - Online predator
 - Cyberstalking
 - Cyber Racism
 - Internet troll
- Drug Trafficking
- Identity Theft
- Phishing

Computer Fraud

- Computer fraud is the act of using a computer to take or alter electronic data, or to gain unlawful use of a computer or system.
- If computer fraud involves the use of the internet, it can be considered **Internet fraud**.
- The legal definition of computer fraud varies by jurisdiction, but typically involves **accessing a computer without permission or authorization**.
- Forms of computer fraud include **hacking into computers to alter information, distributing malicious code** such as computer **worms or viruses, installing malware or spyware to steal data, phishing, and advance-fee scams**.
- Other forms of fraud may be committed using computer systems, including **bank fraud, carding, identity theft, extortion, and theft of classified information**.
- These types of crimes often result in the loss of personal or financial information.

Cyberterrorism

- Cyberterrorism are acts of terrorism committed through the use of cyberspace or computer resources.
- Acts of disruption of computer networks and personal computers through viruses, worms, phishing, malicious software, hardware, or programming scripts can all be forms of cyberterrorism.
- Government officials and information technology (IT) security specialists have documented a significant increase in network problems and server scams since early 2001.
- Within the United States, there is an increasing concern from agencies such as the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA).
- Such incidents are part of an organized effort by cyberterrorist foreign intelligence services or other groups to map potential security flaws in critical systems.

Cyberextortion (Ransomware)

- Ransomware is a type of malware used in cyberextortion to restrict access to files, sometimes threatening permanent data erasure unless a ransom is paid.
- The threat of ransomware is a global issue, with more than 300 million attacks worldwide in 2021.
- According to the 2022 Unit 42 Ransomware Threat Report, the average ransom demand in cases handled by Norton climbed 144 percent to \$2.2 million.
- This report included an 85 percent increase in the number of victims who had their personal information shown on dark web information dumps.
- A loss of nearly \$400 million in 2021 and 2022 is just one of the statistics showing the impact of ransomware attacks on everyday people.

Cybersex Trafficking

- Cybersex trafficking is the transportation of victims and then the live streaming of coerced sexual acts or rape on webcam.
- Victims are abducted, threatened, or deceived and transferred to "cybersex dens".
- The dens can be in any location where the cybersex traffickers have a computer, tablet, or phone with an internet connection.
- Perpetrators use social media networks, video conferences, dating pages, online chat rooms, apps, dark web sites, and other platforms.
- They use online payment systems and cryptocurrencies to hide their identities.
- Millions of reports of its occurrence are sent to authorities annually.
- New legislation and police procedures are needed to combat this type of cybercrime.
- There are an estimated 6.3 million victims of cybersex trafficking, according to a recent report by the International Labour Organization and IOM.
- This number includes about 1.7 million child victims.
- An example of cybersex trafficking is the 2018–2020 Nth room case in South Korea.

Cyberwarfare

- The U.S. Department of Defense notes that cyberspace has emerged as a national-level concern through several recent events of geostrategic importance, including the attack on Estonia's infrastructure in 2007, allegedly by Russian hackers.
- In August 2008, Russia again allegedly conducted cyberattacks, this time in a coordinated and synchronized kinetic and non-kinetic campaign against the country of Georgia.
- Fearing that such attacks may become normalized in future warfare among nation-states, the military commanders intend to adapt the concept of cyberspace operations impact in the future.

Obscene or offensive content

- The content of websites and other electronic communications may be distasteful, obscene, or offensive for a variety of reasons. In some instances, these communications may be illegal.
- The extent to which these communications are unlawful varies greatly between countries, and even within nations. It is a sensitive area in which the courts can become involved in arbitrating between groups with strong beliefs.
- One area of internet pornography that has been the target of the strongest efforts at curtailment is child pornography, which is illegal in most jurisdictions in the world.

Computer as a tool

- When the individual is the main target of cybercrime, the computer can be considered as the tool rather than the target.
- These crimes generally involve less technical expertise.
- Human weaknesses are generally exploited.
- The damage dealt is largely psychological and intangible, making legal action against the variants more difficult.
- These are the crimes which have existed for centuries in the offline world.
- Scams, theft, and the like existed before the development of computers and the internet.
- The same criminal has simply been given a tool which increases their potential pool of victims and makes them all the harder to trace and apprehend.

Computer as a tool

- Crimes that use computer networks or devices to advance other ends include:
 - Fraud and identity theft (although this increasingly uses malware, hacking or phishing, making it an example of both "computer as target" and "computer as tool" crime)
 - Information warfare
 - Phishing scams
 - Spam
 - Propagation of illegal obscene or offensive content, including harassment and threats
- The unsolicited sending of bulk email for commercial purposes (spam) is unlawful in some jurisdictions.
- Phishing is mostly propagated via email.
- Phishing emails may contain links to other websites that are affected by malware.
- Or they may contain links to fake online banking or other websites used to steal private account information.

Ad-fraud

- Ad-frauds are particularly popular among cybercriminals, as such frauds are lucrative and less likely to be prosecuted.
- Jean-Loup Richet, a professor at the Sorbonne Business School, classified the large variety of ad-fraud committed by cybercriminals into three categories:
 - identity fraud, attribution fraud, and ad-fraud services.

Ad-fraud

- **Identity fraud** aims to impersonate real users and inflate audience numbers.
- Several ad-fraud techniques relate to this category and include
 - traffic from bots (coming from a hosting company or a data center, or from compromised devices);
 - cookie stuffing;
 - falsifying user characteristics, such as location and browser type;
 - fake social traffic (misleading users on social networks into visiting the advertised website);
 - the creation of fake social media accounts to make the bot appear legitimate.

Ad-fraud

- **Attribution fraud** impersonates the activities of real users, such as clicks and conversations.
- Multiple ad-fraud techniques belong to this category:
 - hijacked devices and the use of infected users (through malware) as part of a botnet to participate in ad fraud campaigns;
 - click farms (companies where low-wage employees are paid to click or engage in conversations and affiliates' offers);
 - incentivized browsing;
 - video placement abuse (delivered in display banner slots);
 - hidden ads (which will never be viewed by real users);
 - domain spoofing (ads served on a website other than the advertised real-time bidding website);
 - clickjacking, in which the user is forced to click on an ad.

Ad-fraud

- **Ad fraud services** are related to all online infrastructure and hosting services that might be needed to undertake identity or attribution fraud.
- Services can involve
 - the creation of spam websites (fake networks of websites created to provide artificial backlinks);
 - link building services;
 - hosting services;
 - creation of fake and scam pages impersonating a famous brand and used as part of an ad fraud campaign.

Online harassment

- Cyberbullying
- Online predator
- Cyberstalking
- Cyber Racism
- Internet troll

- Whereas content may be offensive in a non-specific way, harassment directs **obscenities** and **derogatory comments** at specific individuals focusing, for example, on gender, race, religion, nationality, or sexual orientation.
- There are instances when committing a crime using a computer can lead to an enhanced sentence.
 - For example, in the case of United States v. Neil Scott Kramer, the defendant was given an enhanced sentence according to the **U.S. Sentencing Guidelines Manual §2G1.3(b)(3)** for his use of a cell phone to "persuade, induce, entice, coerce, or facilitate the travel of, the minor to engage in prohibited sexual conduct."
 - Kramer appealed the sentence on the grounds that there was insufficient evidence to convict him under this statute because his charge included persuading through a computer device and his cellular phone technically is not a computer.
 - Although Kramer tried to argue this point, the U.S. Sentencing Guidelines Manual states that the term "computer" means "an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

- In the **United States**, over 41 states have passed laws and regulations that regard extreme online harassment as a criminal act.
- These acts can be punished on a federal scale, such as **US Code 18 Section 2261A**, which states that using computers to threaten or harass can lead to a sentence of up to 20 years, depending on the action taken.
- Several countries outside the United States have also created laws to combat online harassment.
- In **China**, a country that supports over 20 percent of the world's internet users, the Legislative Affairs Office of the State Council passed a strict law against the bullying of young people through a bill in response to the Human Flesh Search Engine.
- The **United Kingdom** passed the **Malicious Communications Act**, among other acts from 1997 to 2013, which stated that sending messages or letters electronically that the government deemed "indecent or grossly offensive" and/or language intended to cause "distress and anxiety" can lead to a prison sentence of six months and a potentially large fine.
- **Australia**, while not directly addressing the issue of harassment, has grouped the majority of online harassment under the **Criminal Code Act of 1995**.
- Using telecommunication to send threats or harass and cause offense was a direct violation of this act.

- Freedom of Speech:
 - Although freedom of speech is protected by law in most democratic societies (in the US this is done by the First Amendment), it does not include all types of speech.
 - In fact, spoken or written "true threat" speech or text is criminalized because of "intent to harm or intimidate".
 - That also applies to online or network-related threats in written text or speech.

- 
- Cyberbullying:
 - Cyberbullying has increased drastically with the growing popularity of online social networking.
 - As of January 2020, 44 percent of adult internet users in the United States have "personally experienced online harassment".
 - Children who experience online harassment deal with negative and sometimes life-threatening side effects.
 - In 2021, reports displayed 41 percent of children developing social anxiety, 37 percent of children developing depression, and 26 percent of children having suicidal thoughts.

- Spying:

- The United Arab Emirates was named in a spying scandal where the Gulf nation along with other repressive governments purchased NSO Group's mobile spyware Pegasus for mass surveillance.
- Prominent activists and journalists were targeted as part of the campaign, including Ahmed Mansoor, Princess Latifa, Princess Haya, and more.
- Ghada Oueiss was one of the many high-profile female journalists and activists who became the target of online harassment.
- Oueiss filed a lawsuit against UAE ruler Mohamed bin Zayed Al Nahyan along with other defendants, accusing them of sharing her photos online.
- The defendants, including the UAE ruler, filed motions to dismiss the case of the hack-and-leak attack.

Drug trafficking

- Darknet markets are used to buy and sell recreational drugs online.
- Some drug traffickers use encrypted messaging tools to communicate with drug mules or potential customers.
- The dark web site Silk Road was the first major online marketplace for drugs, starting operation in 2011.
- It was permanently shut down in 2014 by the FBI and Europol.
- After Silk Road 2.0 went down, Silk Road 3 Reloaded emerged.
- However, it was just an older marketplace named Diabolus Market, that used the name for more exposure from the brand's previous success.

- 
- Darknet markets have had a rise in traffic in recent years for many reasons, one of the biggest contributors being the anonymity offered in purchases, and often a seller-review system.
 - There are many ways in which darknet markets can financially drain individuals.
 - Vendors and customers alike go to great lengths to keep their identities a secret while online.
 - Commonly used tools are virtual private networks (VPN), Tails, and the Tor Browser to help hide their online presence.

- 
- Darknet markets entice customers by making them feel comfortable.
 - People can easily gain access to a Tor browser with DuckDuckGo browser that allows a user to explore much deeper than other browsers such as Google Chrome.
 - However, actually gaining access to an illicit market is not as simple as typing it in on a search engine like one would with Google.
 - Darknet markets have special links that change frequently, ending in .onion as opposed to the typical .com, .net, and .org domain extensions.

- 
- Digital/Virtual Currency:
 - To add to privacy, the most prevalent currency on these markets is Bitcoin.
 - Bitcoin allows transactions to be anonymous, with the only information available to the public being the record that a transaction occurred between two parties.

- 
- An issue marketplace users face is when vendors or the market itself are exit scamming.
 - This is when a vendor with a high rating will act as if they are selling on the market and have users pay for products they will not receive.
 - The vendor will then close off their account after receiving money from multiple buyers and never send what was purchased.
 - The vendors all being involved in illegal activities have a low chance of not exiting scamming when they no longer want to be a vendor.
 - In 2019, an entire market known as Wall Street Market had allegedly exit scammed, stealing \$30 million dollars from the vendors' and buyers' wallets in bitcoin.

- 
- FBI has cracked down on these markets.
 - In July 2017, FBI seized one of the biggest markets, commonly called Alphabay, which later re-opened in August 2021 under the control of DeSnake, one of the original administrators.
 - Investigators will pose as a buyer and order products from darknet vendors in the hopes that vendors leave a trail the investigators can follow.
 - One investigation had an investigator pose as a firearms seller and for six months people purchased from them and provided home addresses.
 - The FBI was able to make over a dozen arrests during this six-month investigation.

- 
- Another one of law enforcement's crackdowns was on vendors selling fentanyl and opiates.
 - With thousands of people dying each year due to drug overdose, investigators have made it a priority.
 - Many vendors do not realize the extra criminal charges that go along with selling drugs online.
 - Commonly they get charged with money laundering and charges for when the drugs are shipped in the mail on top of being a drug distributor.
 - In 2019, a vendor was sentenced to 10 years in prison after selling cocaine and methamphetamine under the name JetSetLife.
 - Although investigators spend large amounts of time tracking down people, in 2018, only 65 suspects who bought and sold illegal goods on some of the biggest markets were identified.
 - This is compared to the thousands of transactions taking place daily on these markets.

Famous Incidents:

- Data Leaks
- Celebrity Leaks
- Blackmailing
- Web Defacements
- Hacking / Spying
- Data Stealing
- Impersonation
- Superimposing / Fake Media
- ATM Fraud/Hacking
- Car Hacking
- Cryptocurrency / Forex

Identity Theft

- Identity theft occurs when someone uses another person's personal identifying information, like their name, identifying number, or credit card number, without their permission, to commit fraud or other crimes.
- The term identity theft was coined in 1964.
- Since that time, the definition of identity theft has been statutorily defined throughout both the U.K. and the U.S. as the theft of personally identifiable information [PII].
- Identity theft deliberately uses someone else's identity as a method to gain financial advantages or obtain credit and other benefits, and perhaps to cause other person's disadvantages or loss.
- The person whose identity has been stolen may suffer adverse consequences, especially if they are falsely held responsible for the perpetrator's actions.
- Personally identifiable information generally includes a person's name, date of birth, social security number, driver's license number, bank account or credit card numbers, PINs, electronic signatures, fingerprints, passwords, or any other information that can be used to access a person's financial resources.

Phishing

- Phishing is a form of social engineering where attackers deceive people into revealing sensitive information or installing malware such as ransomware.
- Phishing attacks have become increasingly sophisticated and often transparently mirror the site being targeted, allowing the attacker to observe everything while the victim is navigating the site, and transverse any additional security boundaries with the victim.
- As of 2020, it is the most common type of cybercrime, with the FBI's Internet Crime Complaint Centre reporting more incidents of phishing than any other type of computer crime.
- The term "phishing" was first recorded in 1995 in the cracking toolkit AOHell, but may have been used earlier in the hacker magazine 2600.
- It is a variation of fishing and refers to the use of lures to "fish" for sensitive information.
- Measures to prevent or reduce the impact of phishing attacks include legislation, user education, public awareness, and technical security measures.
- The importance of phishing awareness has increased in both personal and professional settings, with phishing attacks among businesses rising from 72% to 86% from 2017 to 2020.

Phishing Types

- Email phishing
- Spear phishing
- Whaling and CEO fraud
- Clone phishing
- Voice phishing
- SMS phishing
- Page hijacking
- Calendar phishing

Phishing Types

- **Email phishing**

- Phishing attacks, often delivered via email spam, attempt to trick individuals into giving away sensitive information or login credentials.
- Most attacks are "bulk attacks" that are not targeted and are instead sent in bulk to a wide audience.
- The goal of the attacker can vary, with common targets including financial institutions, email and cloud productivity providers, and streaming services.
- The stolen information or access may be used to steal money, install malware, or spear phish others within the target organization.
- Compromised streaming service accounts may also be sold on darknet markets.
- This method of social engineering attack involve sending fraud email or messages that appear to be from a trusted source, such as bank, amazon, or government agency.
- These messages will typically contain a link or attachment that, when you click, will install malware automatically on the targeted device or redirect them to fake login page of any trusted website where they will be promoted to enter their login credential.

Phishing Types

- **Spear phishing**

- Spear phishing is a targeted phishing attack that uses personalized emails to trick a specific individual or organization into believing they are legitimate.
- It often utilizes personal information about the target to increase the chances of success.
- These attacks often target executives or those in financial departments with access to sensitive financial data and services.
- Accountancy and audit firms are particularly vulnerable to spear phishing due to the value of the information their employees have access to.
- Threat Group-4127 (Fancy Bear) targeted Hillary Clinton's 2016 presidential campaign with spear phishing attacks on over 1,800 Google accounts, using the accounts-google.com domain to threaten targeted users.
- A study on spear phishing susceptibility among different age groups found that 43% of 100 young and 58 older users clicked on simulated phishing links in daily emails over 21 days.
- Older women had the highest susceptibility, while susceptibility in young users declined over the study, but remained stable in older users.

Phishing Types

- **Whaling and CEO fraud**
 - Whaling attacks use spear phishing techniques to target senior executives and other high-profile individuals[with customized content, often related to a subpoena or customer complaint.
 - CEO fraud involves sending fake emails from senior executives to trick employees into sending money to an offshore account.
 - It has a low success rate, but can result in organizations losing large sums of money.

Phishing Types

- **Clone phishing**
 - Clone phishing is a type of attack where a legitimate email with an attachment or link is copied and modified to contain malicious content.
 - The modified email is then sent from a fake address made to look like it's from the original sender.
 - The attack may appear to be a resend or update of the original email.
 - It often relies on the sender or recipient being previously hacked so the attacker can access the legitimate email.

Phishing Types

- **Voice phishing**
 - Voice over IP (VoIP) is used in vishing or voice phishing attacks, where attackers make automated phone calls to large numbers of people, often using text-to-speech synthesizers, claiming fraudulent activity on their accounts.
 - The attackers spoof the calling phone number to appear as if it is coming from a legitimate bank or institution.
 - The victim is then prompted to enter sensitive information or connected to a live person who uses social engineering tactics to obtain information.
 - Vishing takes advantage of the public's lower awareness and trust in voice telephony compared to email phishing.

Phishing Types

- **SMS phishing (Smishing)**

- SMS phishing or smishing is a type of phishing attack that uses text messages from a cell phone or smartphone to deliver a bait message.
- The victim is usually asked to click a link, call a phone number, or contact an email address provided by the attacker.
- They may then be asked to provide private information, such as login credentials for other websites.
- The difficulty in identifying illegitimate links can be compounded on mobile devices due to the limited display of URLs in mobile browsers.
- Smishing can be just as effective as email phishing, as many smartphones have fast internet connectivity. Smishing messages may also come from unusual phone numbers.

Phishing Types

- **Page hijacking**
 - Page hijacking involves redirecting users to malicious websites or exploit kits through the compromise of legitimate web pages, often using cross site scripting.
 - Hackers may insert exploit kits such as MPack into compromised websites to exploit legitimate users visiting the server.
 - Page hijacking can also involve the insertion of malicious inline frames, allowing exploit kits to load.
 - This tactic is often used in conjunction with watering hole attacks on corporate targets.

Phishing Types

- **Calendar phishing**
 - Calendar phishing involves sending fake calendar invitations with phishing links.
 - These invitations often mimic common event requests and can easily be added to calendars automatically.
 - To protect against this form of fraud, former Google click fraud czar Shuman Ghosemajumder recommends changing calendar settings to not automatically add new invitations.

Phishing Techniques

- Link manipulation
- Filter evasion
- Social engineering

Phishing Techniques

- **Link manipulation**

- Phishing attacks often involve creating fake links that appear to be from a legitimate organization.
- These links may use misspelled URLs or subdomains to deceive the user.
- Another tactic is to make the displayed text for a link appear trustworthy, while the actual link goes to the phisher's site.
- To check the destination of a link, many email clients and web browsers will show the URL in the status bar when the mouse is hovering over it.
- However, some phishers may be able to bypass this security measure.

Phishing Techniques

- **Filter evasion**
 - Phishers have sometimes used images instead of text to make it harder for anti-phishing filters to detect the text commonly used in phishing emails.
 - In response, more sophisticated anti-phishing filters are able to recover hidden text in images using optical character recognition (OCR).

Phishing Techniques

- **Social engineering**
 - Phishing often uses social engineering techniques to trick users into performing actions such as clicking a link or opening an attachment, or revealing sensitive information.
 - It often involves pretending to be a trusted entity and creating a sense of urgency, like threatening to close or seize a victim's bank or insurance account.
 - An alternative technique to impersonation-based phishing is the use of fake news articles to trick victims into clicking on a malicious link.
 - These links often lead to fake websites that appear legitimate, but are actually run by attackers who may try to install malware or present fake "virus" notifications to the victim.



Anti-phishing

Combating computer crime

- It is difficult to find and combat cybercrime perpetrators due to their use of the internet in support of cross-border attacks.
- Not only does the internet allow people to be targeted from various locations, but the scale of the harm done can be magnified.
- Cybercriminals can target more than one person at a time.
- The availability of virtual spaces to public and private sectors has allowed cybercrime to become an everyday occurrence.
- In 2018, The Internet Crime Complaint Center received 351,937 complaints of cybercrime, which lead to \$2.7 billion lost.

Combating computer crime

- Investigation
- Prevention
- Legislation
- Penalties
- Awareness
- Intelligence

Cyber Crime Jobs

- Government, Military, Law Enforcement Agencies
- Private sector companies
- Designations:
 - Cyber Crime Analyst / Forensic Examiner / Scientist / Specialist / Investigator
- Relevant Degree, Certifications and Experience



Cyber Crime Agencies and Organizations

- FIA – CCW
- Military
- Government Sector
- Private Companies
- CERTs

Cyber Crime Law in Pakistan

- PECA (2016)
 - Prevention of Electronic Crimes Act
- PPC (Pakistan Penal Code)
- CrPC (Criminal Procedure Code)
- FERA (Foreign Exchange Regulation Act, 1947)
- AMLA (Anti-Money Laundering Act, 2010)
- The Anti-Terrorism Act, 1997

Cyber Crime Reporting in Pakistan

- Modes:
 - Phone
 - Online
 - In-Person
- Required Documents
 - Application / Matter
 - CNIC
 - Proofs
- Process:
 - Application submission
 - Verification
 - Enquiry
 - FIR