***Research Findings***

***Author: Vineeth M***

***Date: 21,10,2025***

***1. Comparison of Encryption Protocols***

***What is Encryption?***

***Encryption*** *is the process of converting readable data, known as* plaintext*, into an unreadable form called* ciphertext *to protect it from unauthorized access. It ensures that sensitive information remains secure while being stored (*data-at-rest*) or transmitted (*data-in-transit*). Encryption works through mathematical algorithms that use keys to scramble and later unscramble the data. Only authorized users with the correct key can decrypt the ciphertext back into its original form. This process is essential for keeping online communications private and safeguarding data from hackers or other attackers.*

## ***What is an Encryption Protocol?***

***Encryption protocols*** *are sets of rules that determine how encryption algorithms are applied to protect data during communication or storage. These protocols use encryption algorithms, which perform cryptographic operations on plaintext using an encryption key, to secure information from unauthorized access. Each encryption protocol is designed to serve a specific purpose—for example,* ***TLS/SSL*** *is used to secure web communications,* ***SSH*** *is used for safe remote access to computers, and* ***IPsec*** *is used to protect data transmitted over virtual private networks (VPNs) by encrypting and authenticating each data packet. In short, encryption protocols ensure that data remains confidential, authentic, and protected while being transmitted or stored.*

***Secure Sockets Layer (SSL)***

***Secure Sockets Layer (SSL) is a security protocol developed by Netscape in 1995 to encrypt data and ensure secure communication between devices over a network. It provides privacy, authentication, and data integrity for online communications and is the predecessor of TLS, the modern standard. Websites using SSL/TLS display “HTTPS” in their URLs, showing that the communication is secure.***

*SSL secures communication through three main mechanisms.* ***Encryption*** *converts data into unreadable ciphertext to prevent unauthorized access.* ***Authentication*** *verifies the legitimacy of both client and server through the* ***handshake process****.* ***Data integrity*** *ensures that the transmitted information has not been altered, maintaining the accuracy and reliability of communication.*

*The* ***importance of SSL*** *lies in its ability to protect sensitive information like passwords and financial data, authenticate servers to prevent users from connecting to fake websites, and maintain the integrity of data during transit. By providing* ***confidentiality, authentication, and integrity****, SSL ensures secure and trustworthy online communication.*

***SSL certificates****, issued by trusted* ***Certificate Authorities (CAs)****, verify website identities and enable encryption. They are available in different types—****Single-Domain, Wildcard, and Multi-Domain****—and validation levels, including* ***Domain Validation (DV), Organization Validation (OV), and Extended Validation (EV)****, with EV offering the highest level of trust.*

***Transport Layer Security (TLS)***

***Transport Layer Security (TLS)*** *is a protocol that provides security at the* ***transport layer****, derived from* ***SSL****, ensuring that no third party can eavesdrop on or tamper with transmitted data. It secures internet communications by providing* ***encryption, authentication, and data integrity****.*

*TLS encrypts data using symmetric algorithms like* ***AES*** *and asymmetric algorithms like* ***RSA*** *and* ***Diffie-Hellman****, keeping transmitted information confidential. It supports various authentication, encryption, and hashing methods, and works with most web browsers, operating systems, and web servers. Operating beneath the application layer, TLS is largely invisible to users, making it* ***easy to deploy and use****.*

*The* ***TLS handshake*** *establishes a secure connection. The client sends supported TLS versions, cipher suites, and compression methods. The server selects compatible options, provides its* ***digital certificate****, and the client verifies it to confirm the server’s identity. Both parties then exchange keys to compute a* ***symmetric session key****, enabling secure communication.*

*TLS also includes* ***forward secrecy****, ensuring past sessions remain secure even if long-term keys are compromised. Hash functions like* ***SHA-256*** *guarantee* ***data integrity****, detecting any tampering during transmission.*

*Following* ***best practices****—updating configurations, disabling outdated algorithms, and keeping certificates current—is essential for TLS effectiveness. By providing* ***encryption, authentication, integrity, and forward secrecy****, TLS safeguards sensitive data such as passwords, financial transactions, and personal information, forming a cornerstone of modern network security.*

***IPSec (****Internet Protocol Security)*****

*IPSec, or Internet Protocol Security, is a set of rules that makes sending data over the internet safe. It works by* ***encrypting*** *your data so that no one else can read it and by* ***verifying*** *the sender to ensure the data is authentic. Think of it like a secure envelope that protects your message until it reaches the intended receiver. IPSec is commonly used in VPNs to create private connections and can work in different network setups, such as between two sites or for remote access. It also supports key management, tunneling, and is widely supported by different devices because it is an open standard.*

*IPSec works by securing data sent over the Internet, ensuring it remains private and unaltered. It protects information through* ***encryption*** *and* ***authentication****, creating a secure connection between devices. IPSec mainly operates in two modes:* ***Transport Mode****, which encrypts only the data portion of IP packets for end-to-end communication, and* ***Tunnel Mode****, which encrypts the entire IP packet, typically used in site-to-site VPNs.*

*To provide security, IPSec uses two main protocols:* ***AH (Authentication Header)*** *and* ***ESP (Encapsulating Security Payload)****. AH ensures the data comes from a trusted source and has not been modified, while ESP both authenticates and encrypts the data so it cannot be read by unauthorized parties. Encryption keys are exchanged securely using* ***IKE (Internet Key Exchange)****, allowing both devices to establish a safe connection.*

*The connection process happens in* ***two phases****.* ***Phase 1*** *establishes the IKE tunnel, a secure channel used for further negotiation. This can occur in* ***Main Mode****, which is more secure but slower, or* ***Aggressive Mode****, which is faster but less secure due to more exposed identity information.* ***Phase 2****, called Quick Mode, negotiates the IPSec Security Associations to create the actual secure tunnel. In this phase, devices choose between Tunnel Mode (encrypting the entire IP packet) or Transport Mode (encrypting only the data portion).*

*Once the IPSec tunnel is established, data can be transmitted safely between devices, protected from eavesdropping and tampering. After the communication ends, the devices close the secure connection, ensuring ongoing protection for future transmissions.*

## *How Does the IKE Protocol Work?*

*The paragraph explains that the Internet Key Exchange (IKE) protocol ensures secure communication over IP networks by automatically creating and regularly updating encryption keys. This continuous renewal of keys helps maintain strong data protection. In enterprise environments, where data security is crucial, IKE serves as the foundation for building Virtual Private Networks (VPNs) using IPsec. The protocol operates in two main stages: Phase 1 establishes a secure channel between devices, and Phase 2 sets up the actual encrypted tunnel for transmitting data safely.*

### *IKE Phase 1*

*Phase 1 is the stage where two devices, called IKE peers, build* ***trust*** *and set up a* ***secure communication channel****. During this stage, IKE decides which* ***encryption*** *and* ***authentication*** *methods will be used to protect the connection. The devices can confirm each other’s identity using a* ***shared secret key****,* ***public key encryption****, or a* ***digital signature****. One of the most important parts of this process is the* ***Diffie-Hellman key exchange algorithm****, which lets both devices create a* ***shared secret key*** *safely, even over an* ***unsecured network****, without needing to share any secret key beforehand. The type of encryption used and the strength of the keys are very important for keeping the data* ***private and safe from tampering****.*

*Phase 1 works in two modes:* ***Main Mode*** *and* ***Aggressive Mode****.* ***Main Mode*** *is more secure because it hides the identities of the two devices, but it takes longer since it uses six messages to finish the setup.* ***Aggressive Mode*** *is quicker, using only three messages, but it is less secure because it does not protect the identities of the devices during the negotiation.*

### *IKE Phase 2*

*Phase 2 begins by creating* ***Security Associations (SAs)*** *for IPsec. In this step, the two devices negotiate and agree on the exact settings for the IPsec tunnel, such as which* ***encryption*** *and* ***hashing algorithms*** *will be used to protect the data. The goal of Phase 2 is to make sure that all data sent through the IPsec tunnel is* ***encrypted*** *and* ***authenticated*** *according to the security policies agreed upon in Phase 1. Phase 2 always runs in* ***Quick Mode****, which quickly sets up the IPsec SAs using the secure foundation created earlier.*

*A key security option in Phase 2 is* ***Perfect Forward Secrecy (PFS)****. PFS ensures that each session uses a* ***new, unique key*** *that isn’t based on older keys. This means that even if a long-term key is stolen, past communication sessions cannot be decrypted. IKE also includes* ***replay protection****, which checks the order of incoming data packets to block* ***replay attacks****, where hackers try to resend captured packets to trick or disrupt the system.*

*During Phase 2 negotiation, the two devices exchange* ***proxy IDs****, which define what network traffic should be protected by the IPsec tunnel. A proxy ID includes the local and remote IP address ranges, and both peers must use matching IDs so that the correct traffic is secured between them.*

*Finally, Phase 2 decides whether to use* ***Encapsulating Security Payload (ESP)*** *or* ***Authentication Header (AH)*** *as the security protocol.* ***ESP*** *provides both encryption and authentication, while* ***AH*** *only provides authentication and integrity checking without encrypting the data.*

***Comparison of SSL/TLS and Ipsec***

|  |  |  |  |
| --- | --- | --- | --- |
| ***Feature*** | ***SSL*** | ***TLS*** | ***IPSec*** |
| *Operational Layer* | *Presentation layer & Transport layer* | *Presentation layer & Transport layer* | *Network layer* |
| *Primary Use Cases* | *web apps, email* | *Modern HTTPS, APIs, email, apps* | *VPNs, site-to-site, internal networks* |
| *Encryption Type* | *Uses Symmetric and asymmetric encryption* | *Uses stronger symmetric and asymmetric encryption* | *Uses AH for authentication and ESP for encryption/authentication* |
| *Authentication* | *Server authentication via digital certificate* | *Mutual authentication (server and optional client) via digital certificate* | *Uses pre-shared keys, digital certificate, or both* |
| *Encryption Algorithms* | *RC4, 3DES, weak RSA* | *AES-GCM, ChaCha20-Poly1305* | *AES-GCM, ChaCha20, 3DES* |
| *Common Vulnerabilities* | *POODLE, BEAST, CRIME, Logjam* | *Heartbleed, SWEET32* | *Replay attacks (if misconfigured)* |
| *Security Level* | *Very Low* | *Excellent (forward secrecy by default)* | *Excellent (packet-level protection)* |
| *Handshake Process* | *Basic handshake for key exchange and authentication* | *More secure handshake with added integrity checks* | *Uses IKE (Internet Key Exchange) for negotiation* |
| *Modes of Operation* | *Works over TCP (usually port 443)* | *Works over TCP (usually port 443)* | *Transport mode (end-to-end) and Tunnel mode (site-to-site)* |
| *Traffic Coverage* | *Protects web applications and emails* | *Protects web applications, APIs, and emails* | *Protects all IP packets (network-wide)* |
| *Forward Secrecy* | *No* | *Mandatory* | *Yes (with DH/IKE)* |
| *Current Status* | *Deprecated* | *Commonly used* | *Commonly used in VPNs and secure networks* |

***2.Intusion Detection System & Intrusion Prevention System***

# ***1.Intrusion Detection System (IDS)***

*An* ***Intrusion Detection System (IDS)*** *is a security mechanism designed to monitor network traffic and system activities for any signs of unauthorized access or malicious behavior. Intrusion happens when attackers gain access to systems or networks without permission, often using advanced methods to avoid detection. IDS acts as a vigilant observer that constantly watches over a network to detect such activities.*

*The IDS software analyzes data packets and identifies suspicious transactions or policy violations. When any malicious activity is detected, it immediately sends alerts to the system administrator for further investigation. All detected events are usually logged and can also be integrated with a* ***Security Information and Event Management (SIEM)*** *system for centralized analysis and management.*

*The main goal of IDS is to distinguish between normal and abnormal (attack) connections in a network. It builds a predictive model or classifier to detect potential intrusions. By doing this, IDS helps protect computer networks from both external cyber threats and internal misuse, ensuring that the network remains secure and reliable.*

***Common Methods of Intrusion***

***1.Address Spoofing:***

*Address spoofing is when an attacker hides their true origin by using fake IP addresses or unsecured proxy servers. This makes it difficult for defenders to trace or block the attacker, and can be used to impersonate trusted devices or bypass simple access controls.*

***2.*Fragmentation:**

*Fragmentation involves splitting malicious payloads into many small packets so that IDS engines or firewalls that inspect whole-packet patterns miss the attack. Because each piece looks harmless on its own, the full malicious intent only appears when fragments are reassembled—sometimes too late.*

*****3.Pattern Evasion:*****

***Pattern evasion means the attacker alters the form of their exploit so it no longer matches known signatures or rules used by IDS. Techniques include changing byte sequences, inserting harmless data, or varying timing; the result is that signature-based detectors fail to recognise the attack.***

*****4.*Coordinated Attack:****

***Coordinated attacks use multiple sources, ports, or steps at once (for example distributed scanning or simultaneous assaults) to overload or confuse the IDS. This can generate excessive alerts, hide the real attack among noise, or exploit timing gaps so defenders miss the true malicious activity.***

## ***Working of Intrusion Detection System(IDS)***

* *An IDS (Intrusion Detection System) monitors the traffic on a computer network to detect any suspicious activity.*
* *It analyzes the data flowing through the network to look for patterns and signs of abnormal behavior.*
* *The IDS compares the network activity to a set of predefined rules and patterns to identify any activity that might indicate an attack or intrusion.*
* *If the IDS detects something that matches one of these rules or patterns, it sends an alert to the system administrator.*
* *The system administrator can then investigate the alert and take action to prevent any damage or further intrusion.*

## *****Classification of Intrusion Detection System(IDS)*****

*****Network Intrusion Detection System (NIDS)*****

***A Network Intrusion Detection System (NIDS) is placed at a strategic point in the network to monitor traffic from all devices connected to it. It observes the data passing through a subnet and compares it with known attack patterns. If suspicious behavior is found, it sends alerts to the administrator. For example, a NIDS can be installed near a firewall to detect attempts to breach it.***

*****Host Intrusion Detection System (HIDS)*****

***A Host Intrusion Detection System (HIDS) runs directly on individual hosts or devices. It monitors incoming and outgoing packets specific to that device and checks for changes in important system files by comparing current snapshots with earlier ones. If any unauthorized changes are detected, it alerts the administrator. HIDS is often used on critical machines that are not expected to change frequently.***

*****Hybrid Intrusion Detection System*****

***A Hybrid Intrusion Detection System combines the features of both network-based and host-based IDS. It merges information from host agents and network data to form a complete view of network activity. This approach increases detection accuracy and effectiveness. An example of a hybrid IDS is*** Prelude***.***

*****Application Protocol-Based Intrusion Detection System (APIDS)*****

***An Application Protocol-Based Intrusion Detection System (APIDS) monitors the communication within specific application protocols. It usually resides among servers and inspects application-level interactions, such as monitoring the SQL protocol to detect suspicious database transactions.***

*****Protocol-Based Intrusion Detection System (PIDS)*****

***A Protocol-Based Intrusion Detection System (PIDS) focuses on monitoring and analyzing the protocol communications between a user or device and a server. It helps protect web servers by examining protocols like HTTPS or HTTP to detect unusual activity at the application entry point.***

*****Signature-Based Detection*****

***a Signature-Based Detection System identifies attacks by comparing network traffic against a database of known threat signatures. When a match is found, it raises an alert. However, it requires frequent updates to stay effective, as it cannot detect new or unknown attacks that lack predefined signatures.***

# ***2.Intrusion Prevention System (IPS)***

*An* ***Intrusion Prevention System (IPS)****, sometimes called an* ***Intrusion Detection and Prevention System (IDPS)****, is a network security tool that* ***monitors network or system activities*** *to detect and stop malicious behavior. Its main functions include* ***identifying attacks, collecting information about them, reporting to administrators, and attempting to block or prevent the attack****.*

*IPS is considered an* ***enhancement of IDS (Intrusion Detection System)*** *because both monitor traffic and system activities for threats. Unlike a traditional IDS, which mainly* ***alerts administrators****, an IPS can* ***actively respond*** *to threats. This may include* ***blocking the attack, modifying system security settings, or altering malicious content*** *to prevent harm.*

***How Does an IPS Work?***

***1.Inline Deployment*** *An IPS is placed* ***directly in the path of network traffic****, either between the internal network and the internet or just behind a firewall. This allows it to* ***inspect every packet*** *and block malicious traffic instantly.*

****2.Traffic Preprocessing****

***Before analyzing the data deeply, the IPS first organizes all incoming network traffic. It normalizes the data to stop attackers from hiding threats using tricky encoding methods and reassembles fragmented packets so that every piece of information is complete and nothing is missed during inspection.***

****3. Layered Packet Inspection****

***The IPS performs deep packet inspection to fully understand the data passing through the network. It examines packets at different layers — checking where they come from and go at the network layer, observing the reliability or suspicious behavior at the transport layer, and identifying the type of data, such as logins or file transfers, at the application layer. This layered inspection helps the IPS detect hidden or complex threats that basic checks might miss.***

*****4. Detection Mechanisms*****

***After analyzing and organizing the packets, the IPS uses several detection methods to identify threats. It applies signature-based detection to compare network traffic with known attack patterns, much like matching fingerprints. Anomaly-based detection looks for unusual behavior, such as sudden spikes in traffic, while behavior-based detection monitors ongoing activities to spot suspicious actions like repeated failed logins. Finally, policy-based detection enforces administrator-defined rules, such as blocking certain file types or restricting access from specific countries.***

*****5. Automated Response Actions*****

*If the IPS detects any threat, it immediately takes action to protect the network. It can* ***drop malicious packets****,* ***block the attacker’s IP address****, or* ***end harmful sessions****. The IPS may also* ***send alerts or create logs*** *to inform administrators and can even* ***update firewall rules automatically*** *to prevent similar attacks in the future.*

*****6. Tuning and Maintenance*****

***An effective IPS requires regular updates and adjustments to stay reliable. It must be continuously tuned to keep up with new and evolving threats, reduce false positives that mistakenly block safe traffic, and maintain smooth performance even when the network is under heavy load.***

***Classification of Intrusion Prevention System (IPS)***

* ***Network-Based IPS (NIPS):*** *Monitors the entire network for suspicious traffic by analyzing protocol activity.*
* ***Wireless IPS (WIPS):*** *Focuses on wireless networks, inspecting wireless protocols to detect malicious or unauthorized activity.*
* ***Network Behavior Analysis (NBA):*** *Examines network traffic patterns to identify unusual behavior, such as distributed denial-of-service (DDoS) attacks, malware activity, or policy violations.*
* ***Host-Based IPS (HIPS):*** *Installed on individual hosts, it monitors events and activity on that host to detect suspicious or malicious behavior.*