**UNIT IV:**

**Information Security:** Threats in Networks, Network Security Controls–Architecture, Wireless Security,

Honey pots, Traffic Flow Security, Firewalls – Design and Types of Firewalls, Personal Firewalls,

IDS, **Email Security:** Services Security for Email Attacks Through Emails, Privacy-Authentication of

Source Message, Pretty Good Privacy(PGP), S-MIME. **IP Security**: Overview of IPSec, IP& IP version 6

Authentication, Encapsulation Security Payload ESP, Internet Key Exchange IKE, **Web**

**Security:** SSL/TLS, Basic protocols of security. Encoding –Secure Electronic Transaction SET.

**The most common network security threats**

**Here are the most common security threats examples:**

**1. Computer virus**

We’ve all heard about them, and we all have our fears. For everyday Internet users, computer viruses are one of the most common network threats in cybersecurity. Statistics show that approximately 33% of household computers are affected with some type of malware, more than half of which are viruses.

Computer viruses are pieces of software that are designed to be spread from one computer to another. They’re often sent as email attachments or downloaded from specific websites with the intent to infect your computer — and other computers on your contact list — by using systems on your network. Viruses are known to send spam, disable your security settings, corrupt and steal data from your computer including personal information such as passwords, even going as far as to delete everything on your hard drive.

**2. Rogue security software**

Leveraging the fear of computer viruses, scammers have a found a new way to commit Internet fraud.

Rogue security software is malicious software that mislead users to believe that they have network security issues, most commonly a computer virus installed on their computer or that their security measures are not up to date. Then they offer to install or update users’ security settings. They’ll either ask you to download their program to remove the alleged viruses, or to pay for a tool. Both cases lead to actual malware being installed on your computer.

**3. Trojan horse**

Metaphorically, a “Trojan horse” refers to tricking someone into inviting an attacker into a securely protected area. In computing, it holds a very similar meaning — a Trojan horse, or “Trojan,” is a malicious bit of attacking code or software that tricks users into running it willingly, by hiding behind a legitimate program.

They spread often by email; it may appear as an email from someone you know, and when you click on the email and its included attachment, you’ve immediately downloaded malware to your computer. Trojans also spread when you click on a false advertisement.

Once inside your computer, a Trojan horse can record your passwords by logging keystrokes, hijacking your webcam, and stealing any sensitive data you may have on your computer.

**Web threats**

**4. Adware and spyware**

By “adware” we consider any software that is designed to track data of your browsing habits and, based on that, show you advertisements and pop-ups. Adware collects data with your consent — and is even a legitimate source of income for companies that allow users to try their software for free, but with advertisements showing while using the software. The adware clause is often hidden in related User Agreement docs, but it can be checked by carefully reading anything you accept while installing software. The presence of adware on your computer is noticeable only in those pop-ups, and sometimes it can slow down your computer’s processor and internet connection speed.

When adware is downloaded without consent, it is considered malicious.

Spyware works similarly to adware, but is installed on your computer without your knowledge. It can contain keyloggers that record personal information including email addresses, passwords, even credit card numbers, making it dangerous because of the high risk of identity theft.

**5. Computer worm**

Computer worms are pieces of malware programs that replicate quickly and spread from one computer to another. A worm spreads from an infected computer by sending itself to all of the computer’s contacts, then immediately to the contacts of the other computers.

A worm spreads from an infected computer by sending itself to all of the computer’s contacts,, then immediately to the contacts of the other computers

Interestingly, they are not always designed to cause harm; there are worms that are made just to spread. Transmission of worms is also often done by exploiting software vulnerabilities. While we don’t hear about them much today, computer worm are one of the most common computer network threats.

**6. DOS and DDOS attack**

Have you ever found yourself waiting impatiently for the online release of a product, one that you’re eagerly waiting to purchase? You keep refreshing the page, waiting for that moment when the product will go live. Then, as you press F5 for the last time, the page shows an error: “Service Unavailable.” The server must be overloaded!

There are indeed cases like these where a website’s server gets overloaded with traffic and simply crashes, sometimes when a news story breaks. But more commonly, this is what happens to a website during a DoS attack, or denial-of-service, a malicious traffic overload that occurs when attackers overflood a website with traffic. When a website has too much traffic, it’s unable to serve its content to visitors.

A DoS attack is performed by one machine and its internet connection, by flooding a website with packets and making it impossible for legitimate users to access the content of flooded website. Fortunately, you can’t really overload a server with a single other server or a PC anymore. In the past years it hasn’t been that common if anything, then by flaws in the protocol.

A DDoS attack, or distributed denial-of-service attack, is similar to DoS, but is more forceful. It’s harder to overcome a DDoS attack. It’s launched from several computers, and the number of computers involved can range from just a couple of them to thousands or even more.

Since it’s likely that not all of those machines belong to the attacker, they are compromised and added to the attacker’s network by malware. These computers can be distributed around the entire globe, and that network of compromised computers is called botnet.

Since the attack comes from so many different IP addresses simultaneously, a DDoS attack is much more difficult for the victim to locate and defend against.

**7. Phishing**

Phishing is a method of a social engineering with the goal of obtaining sensitive data such as passwords, usernames, credit card numbers.

The attacks often come in the form of instant messages or phishing emails designed to appear legitimate. The recipient of the email is then tricked into opening a malicious link, which leads to the installation of malware on the recipient’s computer. It can also obtain personal information by sending an email that appears to be sent from a bank, asking to verify your identity by giving away your private information.

Uncovering phishing domains can be done easily with SecurityTrails.

**8. Rootkit**

Rootkit is a collection of software tools that enables remote control and administration-level access over a computer or computer networks. Once remote access is obtained, the rootkit can perform a number of malicious actions; they come equipped with keyloggers, password stealers and antivirus disablers.

Rootkits are installed by hiding in legitimate software: when you give permission to that software to make changes to your OS, the rootkit installs itself in your computer and waits for the hacker to activate it. Other ways of rootkit distribution include phishing emails, malicious links, files, and downloading software from suspicious websites.

**Web threats**

**9. SQL Injection attack**

We know today that many servers storing data for websites use SQL. As technology has progressed, network security threats have advanced, leading us to the threat of SQL injection attacks.

SQL injection attacks are designed to target data-driven applications by exploiting security vulnerabilities in the application’s software. They use malicious code to obtain private data, change and even destroy that data, and can go as far as to void transactions on websites. It has quickly become one of the most dangerous privacy issues for data confidentiality. You can read more on the history of SQL injection attacks to better understand the threat it poses to cybersecurity.

**10. MIM attacks**

Man-in-the-middle attacks are cybersecurity attacks that allow the attacker to eavesdrop on communication between two targets. It can listen to a communication which should, in normal settings, be private.

As an example, a man-in-the-middle attack happens when the attacker wants to intercept a communication between person A and person B. Person A sends their public key to person B, but the attacker intercepts it and sends a forged message to person B, representing themselves as A, but instead it has the attackers public key. B believes that the message comes from person A and encrypts the message with the attackers public key, sends it back to A, but attacker again intercepts this message, opens the message with private key, possibly alters it, and re-encrypts it using the public key that was firstly provided by person A. Again, when the message is transferred back to person A, they believe it comes from person B, and this way, we have an attacker in the middle that eavesdrops the communication between two targets.

Here are just some of the types of MITM attacks:

DNS spoofing

HTTPS spoofing

IP spoofing

ARP spoofing

SSL hijacking

Wi-Fi hacking

Emerging threats in 2021

Fileless attacks

We’ve been hearing a lot about fileless attacks this year. Used to perform data breaches, this trending cyber attack method is—as its name implies—based not on new files or payloads, but on working with feature attributes present in the target system.

Most fileless attacks start with phishing attacks, which lead people to malicious campaigns. After executing social engineering attacks against the victim, they are able to perform memory-based setup for further execution. What’s worse is that most of the time these fileless attacks pass under the radar, and remain undetected until it’s too late.

**5G-based swarm attacks**

With the rise of new 5G technologies and networks, higher-speed transfers and large amounts of data can be retrieved and uploaded faster than ever. A new face of cybercrime is emerging.

High bandwidth-based attacks are more usual than ever too, affecting most technologies, but particularly focused on the Internet of Things and mobile devices. According to TechTarget, swarm attacks have increased more than 80% in the past few years, and will continue to grow.

The nature of swarm attacks involves multiple devices infected at the same time, which will later work on different attacking functions, depending on their role inside the bot-coordinated attack.

This type of attack also uses AI to discover new victims, switch attack strategy, and correlate and share data with the original attacker.

## What is Cybersecurity Architecture?

Cybersecurity architecture, also known as  “[network security architecture](https://blog.rsisecurity.com/enterprise-information-security-architecture-what-you-need-to-know/)”, is a framework that specifies the organizational structure, standards, policies and functional behavior of a computer network, including both security and network features. Cybersecurity architecture is also the manner in which various components of your cyber or computer system are organized, synced and integrated.

A [cybersecurity architecture framework](https://blog.rsisecurity.com/enterprise-information-security-architecture-what-you-need-to-know/)is one component of a system’s overall architecture. It’s designed and built to provide guidance during the design of an entire product/system.

Security architecture helps to position security controls and breach countermeasures and how they relate to the overall systems framework of your company. The main purpose of these controls is to maintain your critical system’s quality attributes such as confidentiality, integrity and availability. It’s also the synergy between hardware and software knowledge with programming proficiency, research skills and policy development.

The components listed below are part of an effective and carefully planned security architecture:

1. Direction in the area of incident response to threats, disaster recovery, systems configuration, account creation and management, and cybersecurity monitoring.
2. [Identity management.](https://www.rsisecurity.com/identity-access-management/)
3. Decided inclusion and exclusion of those subject to the domain of the security architecture.
4. Access and border control.
5. Validation and adjustment of the architecture.
6. Training.

## Features of Cyber security Architecture

The following are some of the features of cyber security architecture:

### Network Elements

* Network nodes like computers, NICs, repeaters, hubs, bridges, switches, routers, modems, gateways.
* Network communication protocols (TCP/IP, DHCP, DNS, FTP, HTTP, HTTPS, IMAP)
* Network connections between nodes using specific protocols
* Network topologies among nodes such as point-to-point, circular, chain, and hybrid

### Security Elements

* [Cyber security devices](https://cybersecurityforum.com/cybersecurity-faq/what-is-cybersecurity-architecture.html) like firewalls, Intrusion Detection/Protection Systems [IDS/IPS], encryption/decryption devices.
* Cyber security software (anti-virus software, spyware software, anti-malware software)
* Secure network communication protocols (TCP/IP, DHCP, DNS, FTP, HTTP, HTTPS, IMAP).
* Strong encryption techniques like end-to-end encryption, zero-knowledge privacy, blockchain.

### Security Frameworks & Standards

* Cybersecurity framework architecture standards like NIST Risk Management Framework (RMF) SP 800-37 and ISO IEC 27000-Series.
* Technology standards for cybersecurity software choices.

### Security Procedures & Policies

These are security procedures and policies directed towards your organization and enforced. According to [Cybersecurity Forum](https://cybersecurityforum.com/), a cybersecurity architecture should ideally be definable and simulatable using an industry-standard architecture modeling language (e.g., SysML, UML2).

## Key Phases in Security Architecture

These are the key phases in the security architecture framework and process:

1. **Architecture Risk Assessment**: Here, you evaluate the influence of vital business assets, the risks, and the effects of vulnerabilities and security threats to your organization.
2. **Security Architecture and Design:**At this phase, the design and architecture of security services are structured to aid the protection of your organization’s assets in order to facilitate business risk exposure objectives and goals.
3. **Implementation:** [Cybersecurity services](https://www.rsisecurity.com/services/) and processes are operated, implemented, monitored and controlled. The architecture is designed to ensure that the security policy and standards, security architecture decisions, and [risk management](https://www.rsisecurity.com/services/third-party-risk-management/) are fully implemented and effective for a long period.
4. **Operations and Monitoring:**Here, measures like [threat and vulnerability management](https://www.rsisecurity.com/threat-vulnerability-management/)and threat management are taken to monitor, supervise and handle the operational state in addition to examining the impact of the system’s security.

## Purpose of Cyber security Architecture

The [purpose of cyber security architecture](https://cybersecurityforum.com/cybersecurity-faq/cybersecurity-architecture-purpose.html) is simply to ensure that the main network architecture of your company including sensitive data and critical applications are fully protected against any present or [future threats and breaches.](https://blog.rsisecurity.com/is-your-company-being-reconnoitered-for-a-future-attack/) It’s important you fully understand the various weak points in your system in order to effectively and quickly proffer a solution.

The best way to identify your system’s weak point is to employ the services of a cyber security architect. A cybersecurity architect will thoroughly evaluate surface vulnerabilities for different network topologies and [cyber-attacks](https://blog.rsisecurity.com/what-are-cyber-crimes/) to effectively defend your sensitive data and critical applications.

The primary goals of effective cybersecurity architecture are:

1. To ensure that all cyber-attacks are minimized, mitigated against, hidden or dynamic.
2. To ensure that cyber-attack surfaces should be relatively small in size, covertly stored, so that they are stealth in moving towards threat targets and difficult for [cyber threats](https://blog.rsisecurity.com/infographic-how-prepared-is-your-business-to-face-cyber-threats/) to detect and penetrate.
3. To make sure all your confidential and sensitive data is strongly encrypted, and be subject to end-to-end encryption techniques during transfer.
4. All cyber-attacks are aggressively detected, mitigated, and countered using countermeasures like Moving-Target Defenses (MTD).

**Wireless security is nothing but protecting computers, smartphones, tablets, laptops and other portable devices along with the networks they are connected to, from threats and vulnerabilities associated with wireless computing.**

**Wireless Communication**

Wireless communication refers to any type of data exchange between the parties that is performed wirelessly (over the air). This definition is extremely wide, since it may correspond to many types of wireless technologies, like −

**Wi-Fi Network Communication**

Bluetooth Communication

Satellite Communication

Mobile Communication

**Wi-Fi**

Wireless Fidelity (Wi-Fi) refers to wireless local area network, as we all know them. It is based on IEEE 802.11 standard. Wi-Fi is a type of wireless network you meet almost everywhere, at your home, workplace, in hotels, restaurants and even in taxis, trains or planes. These 802.11 communication standards operate on either 2.4 GHz or 5 GHz ISM radio bands.

These devices are easily available in the shops that are compatible with Wi-Fi standard, they have following image visible on the device itself. I bet you have seen it hundreds of times in various shops or other public places.

Due to the fact, that 802.11 based wireless network are so heavily used in all types of environments - they are also the biggest subject for various security researches across other 802.11 standards.

Wireless Clients

Wireless clients are considered to be any end-devices with a wireless card or wireless adapter installed. Now, in this 21st century, those devices can be almost anything −

Smartwatch

Modern Smartphones − These are one of the most universally used wireless devices you see in the market. They support multiple wireless standards on one box, for example, Bluetooth, Wi-Fi, GSM.

Laptops − These are a type of device which we all use every single day!

Smartwatch − An example of Sony based smartwatch is shown here. It can synchronize with your smartphone via a Bluetooth.

Smart-home Equipment − With the current progress of the technology, smart-home equipment might be for example a freezer that you can control over Wi-Fi or a temperature controller.

### What is a honeypot?

A honeypot is a network-attached system set up as a decoy to lure cyber attackers and detect, deflect and study hacking attempts to gain unauthorized access to information systems. The function of a honeypot is to represent itself on the internet as a potential target for attackers -- usually, a server or other high-value asset -- and to gather information and notify defenders of any attempts to access the honeypot by unauthorized users.

Honeypot systems often use hardened operating systems (OSes) where extra security measures have been taken to minimize their exposure to threats. They are usually configured so they appear to offer attackers exploitable vulnerabilities. For example, a honeypot system might appear to respond to Server Message Block (SMB) protocol requests used by the [WannaCry ransomware](https://searchsecurity.techtarget.com/definition/WannaCry-ransomware) attack and represent itself as an enterprise database server storing consumer information.

Large enterprises and companies involved in cybersecurity research are common users of honeypots to identify and defend against attacks from advanced persistent threat (APT) actors. Honeypots are an important tool that large organizations use to [mount an active defense against attackers](https://searchcloudsecurity.techtarget.com/tip/Active-cyber-deception-Can-it-improve-cloud-security) or for cybersecurity researchers who want to learn more about the tools and techniques attackers use.

The cost of maintaining a honeypot can be high, in part because of the specialized skills required to implement and administer a system that appears to expose an organization's network resources, while still preventing attackers from gaining access to any production systems.

### Honeypot placement How do honeypots work?

Generally, a honeypot operation consists of a computer, applications and data that [simulate the behavior of a real system](https://www.computerweekly.com/feature/Steal-a-march-on-cyber-criminals-through-security-by-deception) that would be attractive to attackers, such as a financial system, internet of things (IoT) devices, or a public utility or transportation network. It appears as part of a network but is actually isolated and closely monitored. Because there is no reason for legitimate users to access a honeypot, any attempts to communicate with it are considered hostile.

Honeypots are often placed in a demilitarized zone ([DMZ](https://searchsecurity.techtarget.com/definition/DMZ)) on the network. That approach keeps it isolated from the main production network, while still being a part of it. In the DMZ, a honeypot can be monitored from a distance while attackers access it, minimizing the risk of the main network being breached.

Honeypots may also be put outside the external firewall, facing the internet, to detect attempts to enter the internal network. The exact placement of the honeypot varies depending on how elaborate it is, the traffic it aims to attract and how close it is to sensitive resources inside the corporate network. No matter the placement, it will always have some degree of isolation from the production environment.

Viewing and logging activity in the honeypot provides insight into the level and types of threats a network infrastructure faces while distracting attackers from assets of real value. Cybercriminals can [hijack](https://searchsecurity.techtarget.com/definition/hijacking) honeypots and use them against the organization deploying them. Cybercriminals have also been known to use honeypots to gather intelligence about researchers or organizations, act as decoys and spread misinformation.

Virtual machines (VMs) are often used to host honeypots. That way, if they are compromised by malware, for example, the honeypot can be quickly restored. Two or more honeypots on a network form a [honeynet](https://searchsecurity.techtarget.com/definition/honeynet), while a honey farm is a centralized collection of honeypots and analysis tools.

Both open source and commercial offerings are available to help with deploying and administering honeypots. Products include standalone honeypot systems, as well as honeypots packaged with other security software and marketed as [deception technology](https://whatis.techtarget.com/definition/deception-technology). GitHub has an extensive [list of honeypot software](https://github.com/paralax/awesome-honeypots) that can help beginners get an idea of how honeypots are used.

### What are honeypots used for?

Honeypots are used to capture information from unauthorized intruders that are tricked into accessing them because they appear to be a legitimate part of the network. Security teams deploy these traps as part of their network defense strategy. Honeypots are also used to research the behavior of cyber attackers and the ways they interact with networks.

[Spam traps](https://searchsecurity.techtarget.com/definition/spam-trap) are also similar to honeypots. They are email addresses or other network functions set up to attract spam web traffic. Spam traps are used in Project Honey Pot, which is a web-based network of honeypots embedded in website software. Its purpose is to harvest and collect the Internet Protocol (IP) addresses, email addresses and related information on spammers so web administrators can minimize the amount of spam on their sites. The group's findings are used for research as well and by law enforcement to combat unsolicited bulk mailing offenses.

### Types of honeypots

Based on design and deployment, there are two main types of honeypots: production and research.

1. **Research honeypots** perform close analysis of [hacker](https://searchsecurity.techtarget.com/definition/hacker) activity and aim to discover how hackers develop and progress in order to learn how to better protect systems against them. Data placed in a honeypot with unique identifying properties can also help analysts track stolen data and identify connections between different participants in an attack.
2. **Production honeypots** are usually deployed inside production networks alongside production servers; the honeypot acts as a decoy, drawing intruders away from the production network as part of the intrusion detection system ([IDS](https://searchsecurity.techtarget.com/definition/intrusion-detection-system)). A production honeypot is designed to appear as a real part of the production network and contains information to attract and occupy hackers to tie up their time and resources. This approach ultimately gives administrators time to assess the threat level and mitigate any vulnerabilities in their actual production systems.

Honeypots can be classified as pure, high-interaction or low-interaction:

1. **Pure honeypots** are full-fledged production systems that monitor a honeypot's link to the network. They are the most complex and difficult to maintain, but they also appear most realistic to attackers, complete with mock confidential files and user information.
2. **High-interaction honeypots** imitate the activities of the production systems, hosting a variety of services and capturing extensive information. The goal of a high-interaction honeypot is to entice an attacker to gain root -- or administrator-level -- access to the server and then monitor the attacker's activity.
3. **Low-interaction honeypots** simulate the most common attack vectors on the network: the ones services attackers frequently request. Therefore, they are less risky and easier to maintain. They do not point malicious users to the root system. The downside of this type of honeypot is that it is more likely to look fake to an attacker. Low-interaction honeypots are good for detecting attacks from bots and malware. Honeyd is an [open source virtual low-interaction honeypot](http://www.honeyd.org/).

There are several types of specialized honeypot technologies, such as the following:

* **Malware honeypots.** These are honeypots that mimic malware attack vectors -- places that malware attacks and replicates.
* **Spam honeypots.** These can detect the methods of spammers, monitor their activity and block spam.
* **Database honeypots.**These create decoy databases to mislead attackers using methods that are sometimes missed by firewalls, like [Structured Query Language (SQL) injections](https://searchsoftwarequality.techtarget.com/definition/SQL-injection).
* **Client honeypots.** These actively seek out malicious servers behind client attacks instead of passively waiting for connections. They use virtualization to establish themselves on the server and watch for suspicious modifications to the honeypot.

## What Does Traffic-Flow Security Mean?

Traffic-flow security is the use of various measures or methods to hide the presence of messages across a communicational medium, or to otherwise cloak messaging to prevent the observation of traffic levels across an IT infrastructure.  
  
The idea behind traffic-flow security is that even in highly protected systems, it might still be possible for outsiders to ascertain the amount of traffic over a system at any given time. The use of traffic-flow security tools makes it impossible for external observers to see whether traffic is changing in real time, or when any individual message goes from one location to another.

There are several methods for traffic-flow security. One involves the use of dummy traffic in addition to the encryption of actual messages, and sender and receiver addresses. This can make it look like a system is experiencing a consistently high level of traffic in order to obscure the actual volume of traffic in the network. Another option is to send a continuous encrypted signal even when a network is not being used.

The principle behind traffic-flow security shows how businesses and other parties may guard even seemingly basic data such as the date and time that someone accesses a platform, or when they send a message. In some situations, this data is not regarded as necessarily private; in other cases, it may be necessary to hide traffic on a platform where knowledge of access times and traffic levels could be used inappropriately by an outside observer.

**A firewall** is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

Firewalls have been a first line of defense in network security for over 25 years. They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet.

A firewall can be hardware, software, or both.

## Types of firewalls

### Proxy firewall

An early type of firewall device, a proxy firewall serves as the gateway from one network to another for a specific application. Proxy servers can provide additional functionality such as content caching and security by preventing direct connections from outside the network. However, this also may impact throughput capabilities and the applications they can support.

### Stateful inspection firewall

Now thought of as a “traditional” firewall, a stateful inspection firewall allows or blocks traffic based on state, port, and protocol. It monitors all activity from the opening of a connection until it is closed. Filtering decisions are made based on both administrator-defined rules as well as context, which refers to using information from previous connections and packets belonging to the same connection.

### Unified threat management (UTM) firewall

A UTM device typically combines, in a loosely coupled way, the functions of a stateful inspection firewall with intrusion prevention and [antivirus](https://www.cisco.com/c/en/us/products/security/amp-for-endpoints/best-antivirus-strategy.html). It may also include additional services and often cloud management. UTMs focus on simplicity and ease of use.

See our [UTM devices](https://meraki.cisco.com/products/appliances).

### Next-generation firewall (NGFW)

Firewalls have evolved beyond simple packet filtering and stateful inspection. Most companies are deploying [next-generation firewalls](https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-next-generation-firewall.html) to block modern threats such as advanced malware and application-layer attacks.

According to Gartner, Inc.’s definition, a next-generation firewall must include:

* Standard firewall capabilities like stateful inspection
* Integrated intrusion prevention
* Application awareness and control to see and block risky apps
* Upgrade paths to include future information feeds
* Techniques to address evolving security threats

While these capabilities are increasingly becoming the standard for most companies, NGFWs can do more.

### Threat-focused NGFW

These firewalls include all the capabilities of a traditional NGFW and also provide advanced threat detection and remediation. With a threat-focused NGFW you can:

* Know which assets are most at risk with complete context awareness
* Quickly react to attacks with intelligent security automation that sets policies and hardens your defenses dynamically
* Better detect evasive or suspicious activity with network and endpoint event correlation
* Greatly decrease the time from detection to cleanup with retrospective security that continuously monitors for suspicious activity and behavior even after initial inspection
* Ease administration and reduce complexity with [unified policies](https://www.cisco.com/c/en/us/products/security/what-is-network-security-policy-management.html) that protect across the entire attack continuum.

### Definition

Email security is a term for describing different procedures and techniques for protecting email accounts, content, and communication against unauthorized access, loss or compromise. Email is often used to spread malware, spam and phishing attacks. Attackers use deceptive messages to entice recipients to part with sensitive information, open attachments or click on hyperlinks that install malware on the victim’s device. Email is also a common entry point for attackers looking to gain a foothold in an enterprise network and obtain valuable company data.

Email encryption involves encrypting, or disguising, the content of email messages to protect potentially sensitive information from being read by anyone other than intended recipients. Email encryption often includes authentication.

### How Secure Is Email?

Email was designed to be as open and accessible as possible. It allows people in organizations to communicate with each other and with people in other organizations. The problem is that email is not secure. This allows attackers to use email as a way to cause problems in attempt to profit. Whether through spam campaigns, malware and phishing attacks, sophisticated targeted attacks, or business email compromise (BEC), attackers try to take advantage of the lack of security of email to carry out their actions. Since most organizations rely on email to do business, attackers exploit email in an attempt to steal sensitive information.

Because email is an open format, it can be viewed by anyone who can intercept it, causing email security concerns. This became an issue as organizations began sending confidential or sensitive information through email. An attacker could easily read the contents of an email by intercepting it. Over the years, organizations have been increasing email security measures to make it harder for attackers to get their hands on sensitive or confidential information.

### Email Security Policies

Because email is so critical in today’s business world, organizations have established polices around how to handle this information flow. One of the first policies most organizations establish is around viewing the contents of emails flowing through their email servers. It’s important to understand what is in the entire email in order to act appropriately. After these baseline policies are put into effect, an organization can enact various security policies on those emails.

These email security policies can be as simple as removing all executable content from emails to more in-depth actions, like sending suspicious content to a sandboxing tool for detailed analysis. If security incidents are detected by these policies, the organization needs to have actionable intelligence about the scope of the attack. This will help determine what damage the attack may have caused. Once an organization has visibility into all the emails being sent, they can enforce email encryption policies to prevent sensitive email information from falling into the wrong hands.

### Email Security Best Practices

One of the first best practices that organizations should put into effect is implementing a secure email gateway. An email gateway scans and processes all incoming and outgoing email and makes sure that threats are not allowed in. Because attacks are increasingly sophisticated, standard security measures, such as blocking known bad file attachments, are no longer effective. A better solution is to deploy a secure email gateway that uses a multi-layered approach.

It’s also important to deploy an automated email encryption solution as a best practice. This solution should be able to analyze all outbound email traffic to determine whether the material is sensitive. If the content is sensitive, it needs to be encrypted before it is emailed to the intended recipient. This will prevent attackers from viewing emails, even if they were to intercept them.

### Email Security Tools

A [secure email gateway](https://www.proofpoint.com/us/glossary/email-gateway), deployed either on-premises or in the cloud, should offer multi-layered protection from unwanted, malicious and BEC email; granular visibility; and business continuity for organizations of all sizes. These controls enable security teams to have confidence that they can secure users from email threats and maintain email communications in the event of an outage.

An [email encryption solution](https://www.proofpoint.com/us/glossary/encryption) reduces the risks associated with regulatory violations, data loss and corporate policy violations while enabling essential business communications. The email security solution should work for any organization that needs to protect sensitive data, while still making it readily available to affiliates, business partners and users—on both desktops and mobile devices. An email encryption solution is especially important for organizations required to follow compliance regulations, like GDPR, HIPAA or SOX, or abide by security standards like PCI-DSS.

# Types of Email Attacks

* **Phishing:** Phishing is a form of fraud. Cyber criminals use email, instant messaging, or other social media to try to gather information such as login credentials by masquerading as a reputable person. Phishing occurs when a malicious party sends a fraudulent email disguised as being from an authorized, trusted source. The message intent is to trick the recipient into installing malware on his or her device or into sharing personal or financial information.

Spear phishing is a highly targeted phishing attack. While phishing and spear-phishing both use emails to reach the victims, spear-phishing sends customized emails to a specific person. The criminal researches the target’s interests before sending the email.

* **Vishing:** Vishing is phishing using voice communication technology. Criminals can spoof calls from authorized sources using voice-over IP technology. Victims may also receive a recorded message that appears authorized. Criminals want to obtain credit card numbers or other information to steal the victim’s identity. Vishing takes advantage of the fact that people trust the telephone network.
* **Smishing:** Smishing is phishing using text messaging on mobile phones. Criminals impersonate a legitimate source in an attempt to gain the trust of the victim. For example, a smishing attack might send the victim a website link. When the victim visits the website, malware is installed on the mobile phone.
* **Whaling:** Whaling is a phishing attack that targets high profile targets within an organization such as senior executives. Additional targets include politicians or celebrities.
* **Pharming:** Pharming is the impersonation of an authorized website in an effort to deceive users into entering their credentials. Pharming misdirects users to a fake website that appears to be official. Victims then enter their personal information thinking that they are connected to a legitimate site.
* **Spyware:** Spyware is software that enables a criminal to obtain information about a user’s computer activities. Spyware often includes activity trackers, keystroke collection, and data capture. In an attempt to overcome security measures, spyware often modifies security settings. Spyware often bundles itself with legitimate software or with Trojan horses. Many shareware websites are full of spyware.
* **Scareware:** Scareware persuades the user to take a specific action based on fear. Scareware forges pop-up windows that resemble operating system dialogue windows. These windows convey forged messages stating that the system is at risk or needs the execution of a specific program to return to normal operation. In reality, no problems exist, and if the user agrees and allows the mentioned program to execute, malware infects his or her system.
* **Adware:** Adware typically displays annoying pop-ups to generate revenue for its authors. The malware may analyze user interests by tracking the websites visited. It can then send pop-up advertising relevant to those sites. Some versions of software automatically install Adware.
* **Spam:** Spam (also known as junk mail) is unsolicited email. In most cases, spam is a method of advertising. However, spam can send harmful links, malware, or deceptive content. The end goal is to obtain sensitive information such as a social security number or bank account information. Most spam comes from multiple computers on networks infected by a virus or worm. These compromised computers send out as much bulk email as possible.

**PGP (Pretty Good Privacy)**, is a popular program that is used to provide confidentiality and authentication services for electronic mail and file storage. It was designed by **Phil Zimmermann** way back in 1991. He designed it in such a way, that the best cryptographic algorithms such as RSA, Diffie-Hellman key exchange, DSS are used for the public-key encryption (or) asymmetric encryption; CAST-128, 3DES, IDEA are used for symmetric encryption and SHA-1 is used for hashing purposes. PGP software is an open source one and is not dependent on either of the OS (Operating System) or the processor. The application is based on a few commands which are very easy to use.

The following are the services offered by PGP:

**1.** Authentication

**2.** Confidentiality

**3.** Compression

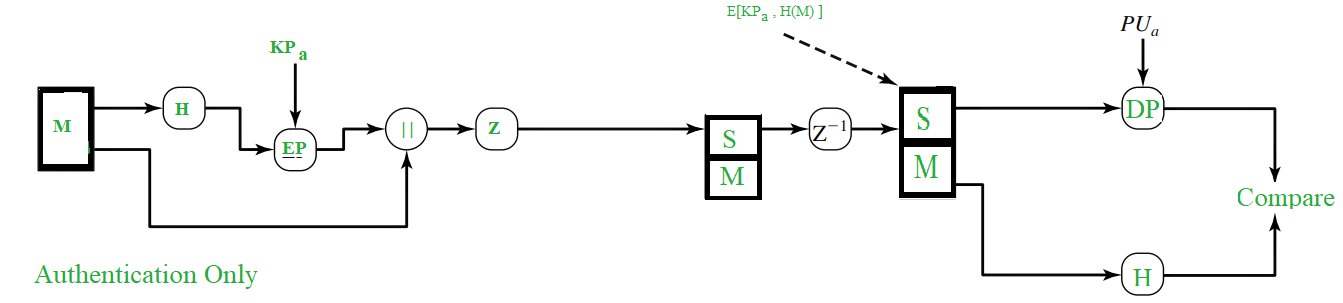
**4.** Email Compatibility

**5.** Segmentation

In this article, we will see about Authentication and Confidentiality.

**1. Authentication:**   
Authentication basically means something that is used to validate something as true or real. To login into some sites sometimes we give our account name and password, that is an authentication verification procedure.

In the email world, checking the authenticity of an email is nothing but to check *whether it actually came from the person it says*. In emails, authentication has to be checked as there are some people who spoof the emails or some spams and sometimes it can cause a lot of inconvenience. The Authentication service in PGP is provided as follows:



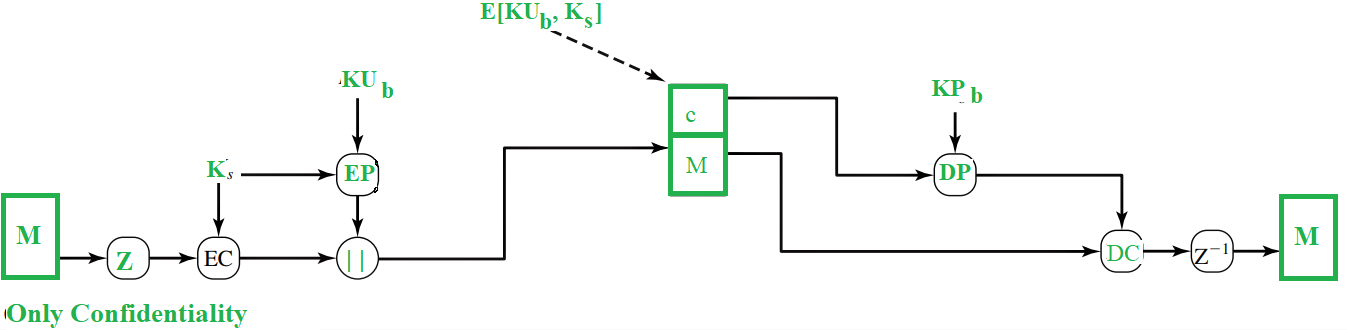
As shown in the above figure, the Hash Function (H) calculates the Hash Value of the message. For the hashing purpose, **SHA-1** is used and it produces a **160 bit** output hash value. Then, using the sender’s private key (KPa), it is encrypted and it’s called as **Digital Signature**. The Message is then appended to the signature. All the process happened till now, is sometimes described as *signing the message*. Then the message is compressed to reduce the transmission overhead and is sent over to the receiver.

At the receiver’s end, the data is decompressed and the message, signature are obtained. The signature is then decrypted using the sender’s public key(PUa) and the hash value is obtained. The message is again passed to hash function and it’s hash value is calculated and obtained.

Both the values, one from signature and another from the recent output of hash function are compared and if both are same, it means that the email is actually sent from a known one and is legit, else it means that it’s not a legit one.

**2. Confidentiality:**   
Sometimes we see some packages labelled as ‘Confidential’, which means that those packages are not meant for all the people and only selected persons can see them. The same applies to the email confidentiality as well. Here, in the email service, only the sender and the receiver should be able to read the message, that means the contents have to be kept secret from every other person, except for those two.

PGP provides that Confidentiality service in the following manner:



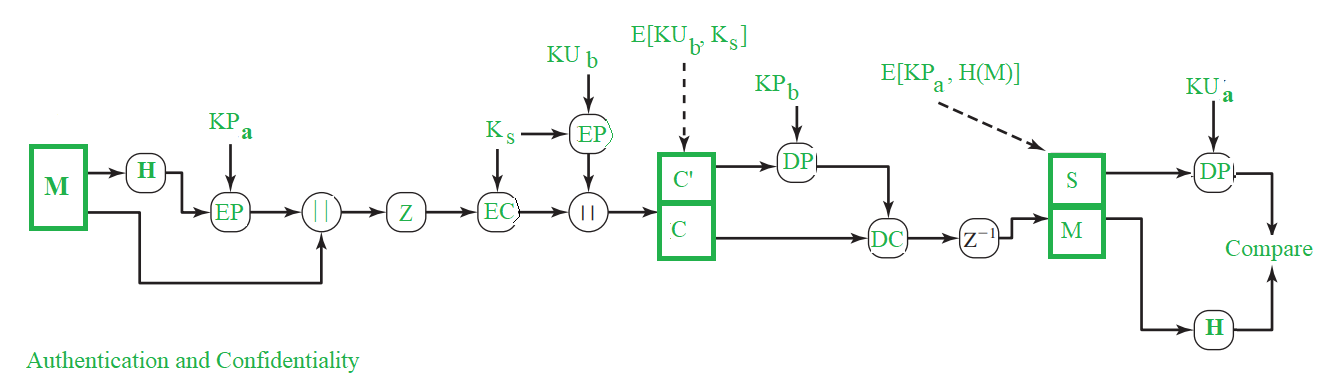
The message is first compressed and a 128 bit session key (Ks), generated by the PGP, is used to encrypt the message through symmetric encryption. Then, the session key (Ks) itself gets encrypted through public key encryption (EP) using receiver’s public key(KUb) . Both the encrypted entities are now concatenated and sent to the receiver.

As you can see, the original message was compressed and then encrypted initially and hence even if any one could get hold of the traffic, he cannot read the contents as they are not in readable form and they can only read them if they had the session key (Ks). Even though session key is transmitted to the receiver and hence, is in the traffic, it is in encrypted form and only the receiver’s private key (KPb)can be used to decrypt that and thus our message would be completely safe.

At the receiver’s end, the encrypted session key is decrypted using receiver’s private key (KPb) and the message is decrypted with the obtained session key. Then, the message is decompressed to obtain the original message (M).

RSA algorithm is used for the public-key encryption and for the symmetric jey encryption, CAST-128(or IDEA or 3DES) is used.

Practically, **both**the Authentication and Confidentiality services are provided in parallel as follows :



.

# IP security (IPSec)

The **IP security (IPSec)** is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 communication points across the IP network that provide data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted and authenticated packets. The protocols needed for secure key exchange and key management are defined in it.

**Uses of IP Security –**  
IPsec can be used to do the following things:

Attention reader! Don’t stop learning now. Get hold of all the important CS Theory concepts for SDE interviews with the [**CS Theory Course**](https://practice.geeksforgeeks.org/courses/SDE-theory?vC=1) at a student-friendly price and become industry ready.

* To encrypt application layer data.
* To provide security for routers sending routing data across the public internet.
* To provide authentication without encryption, like to authenticate that the data originates from a known sender.
* To protect network data by setting up circuits using IPsec tunneling in which all data is being sent between the two endpoints is encrypted, as with a Virtual Private Network(VPN) connection.

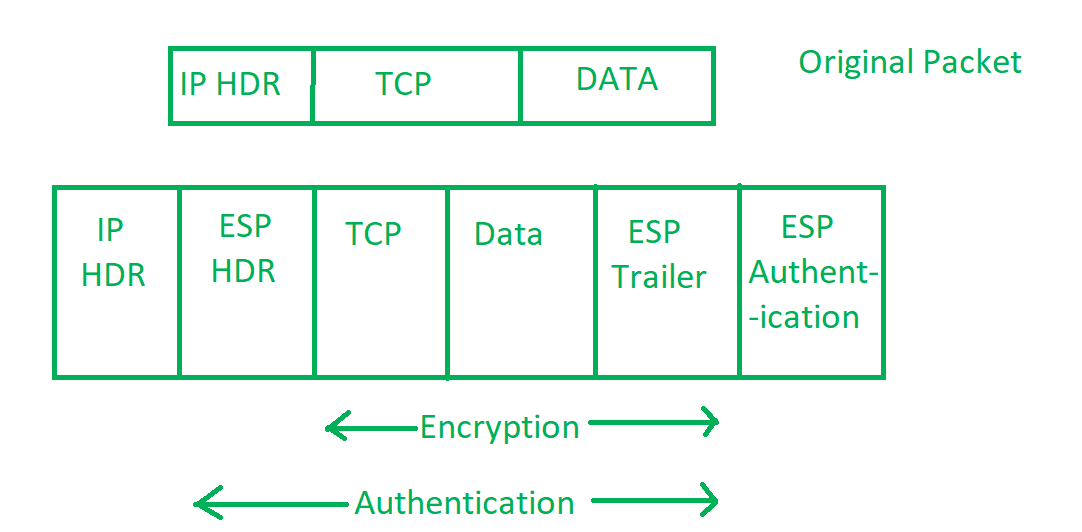
**Components of IP Security –**  
It has the following components:

1. **Encapsulating Security Payload (ESP) –**  
   It provides data integrity, encryption, authentication and anti replay. It also provides authentication for payload.
2. **Authentication Header (AH) –**  
   It also provides data integrity, authentication and anti replay and it does not provide encryption. The anti replay protection, protects against unauthorized transmission of packets. It does not protect data’s confidentiality.



1. **Internet Key Exchange (IKE) –**  
   It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices. The Security Association (SA) establishes shared security attributes between 2 network entities to support secure communication. The Key Management Protocol (ISAKMP) and Internet Security Association which provides a framework for authentication and key exchange. ISAKMP tells how the set up of the Security Associations (SAs) and how direct connections between two hosts that are using IPsec.

Internet Key Exchange (IKE) provides message content protection and also an open frame for implementing standard algorithms such as SHA and MD5. The algorithm’s IP sec users produces a unique identifier for each packet. This identifier then allows a device to determine whether a packet has been correct or not. Packets which are not authorized are discarded and not given to receiver.



**Working of IP Security –**

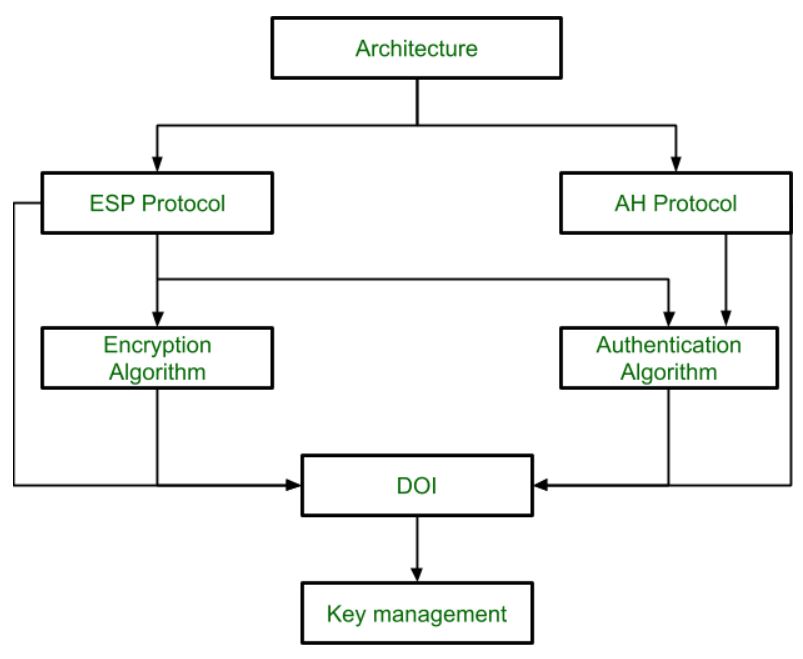
1. The host checks if the packet should be transmitted using IPsec or not. These packet traffic triggers the security policy for themselves. This is done when the system sending the packet apply an appropriate encryption. The incoming packets are also checked by the host that they are encrypted properly or not.
2. Then the **IKE Phase 1** starts in which the 2 hosts( using IPsec ) authenticate themselves to each other to start a secure channel. It has 2 modes. The **Main mode** which provides the greater security and the **Aggressive mode** which enables the host to establish an IPsec circuit more quickly.
3. The channel created in the last step is then used to securely negotiate the way the IP circuit will encrypt data across the IP circuit.
4. Now, the **IKE Phase 2** is conducted over the secure channel in which the two hosts negotiate the type of cryptographic algorithms to use on the session and agreeing on secret keying material to be used with those algorithms.
5. Then the data is exchanged across the newly created IPsec encrypted tunnel. These packets are encrypted and decrypted by the hosts using IPsec SAs.
6. When the communication between the hosts is completed or the session times out then the IPsec tunnel is terminated by discarding the keys by both the hosts.

**IPSec (IP Security) architecture** uses two protocols to secure the traffic or data flow. These protocols are ESP (Encapsulation Security Payload) and AH (Authentication Header). IPSec Architecture include protocols, algorithms, DOI, and Key Management. All these components are very important in order to provide the three main services:

* Confidentiality
* Authentication
* Integirity

**IP Security Architecture:**

Attention reader! Don’t stop learning now. Get hold of all the important CS Theory concepts for SDE interviews with the [**CS Theory Course**](https://practice.geeksforgeeks.org/courses/SDE-theory?vC=1) at a student-friendly price and become industry ready.

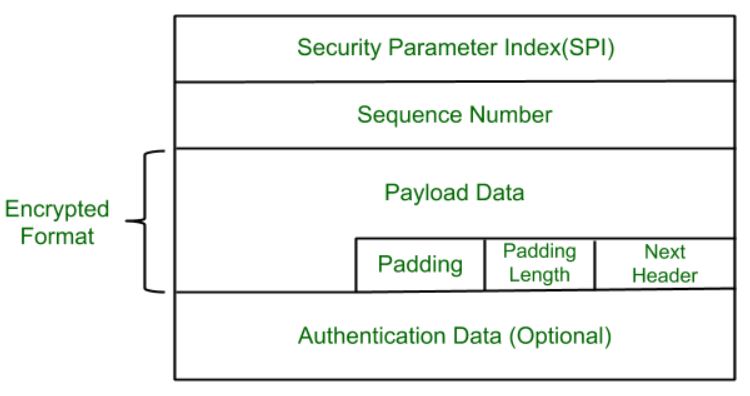


**1. Architecture:**  
Architecture or IP Security Architecture covers the general concepts, definitions, protocols, algorithms and security requirements of IP Security technology.

**2. ESP Protocol:**  
ESP(Encapsulation Security Payload) provide the confidentiality service. Encapsulation Security Payload is implemented in either two ways:

* ESP with optional Authentication.
* ESP with Authentication.

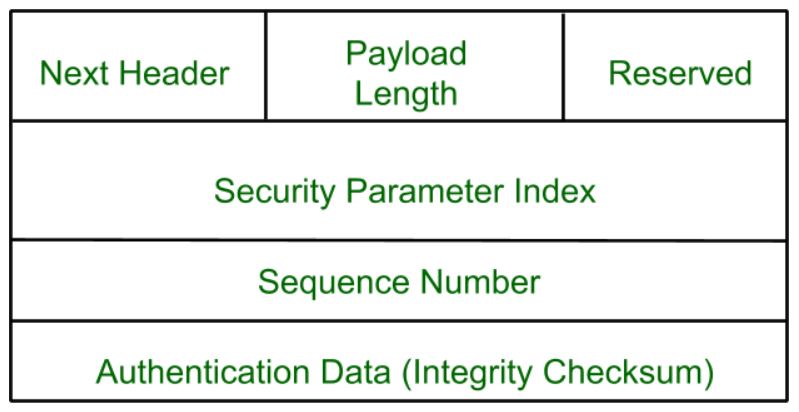
**Packet Format:**



* **Security Parameter Index(SPI):**  
  This parameter is used in Security Association. It is used to give a unique number to the connection build between Client and Server.
* **Sequence Number:**  
  Unique Sequence number are allotted to every packet so that at the receiver side packets can be arranged properly.
* **Payload Data:**  
  Payload data means the actual data or the actual message. The Payload data is in encrypted format to achieve confidentiality.
* **Padding:**  
  Extra bits or space added to the original message in order to ensure confidentiality. Padding length is the size of the added bits or space in the original message.
* **Next Header:**  
  Next header means the next payload or next actual data.
* **Authentication Data**  
  This field is optional in ESP protocol packet format.

**3. Encryption algorithm:**  
Encryption algorithm is the document that describes various encryption algorithm used for Encapsulation Security Payload.

**4. AH Protocol:**  
AH (Authentication Header) Protocol provides both Authentication and Integrity service. Authentication Header is implemented in one way only: Authentication along with Integrity.



Authentication Header covers the packet format and general issue related to the use of AH for packet authentication and integrity.

**5. Authentication Algorithm:**  
Authentication Algorithm contains the set of the documents that describe authentication algorithm used for AH and for the authentication option of ESP.

**6. DOI (Domain of Interpretation):**  
DOI is the identifier which support both AH and ESP protocols. It contains values needed for documentation related to each other.

**7. Key Management:**  
Key Management contains the document that describes how the keys are exchanged between sender and receiver.