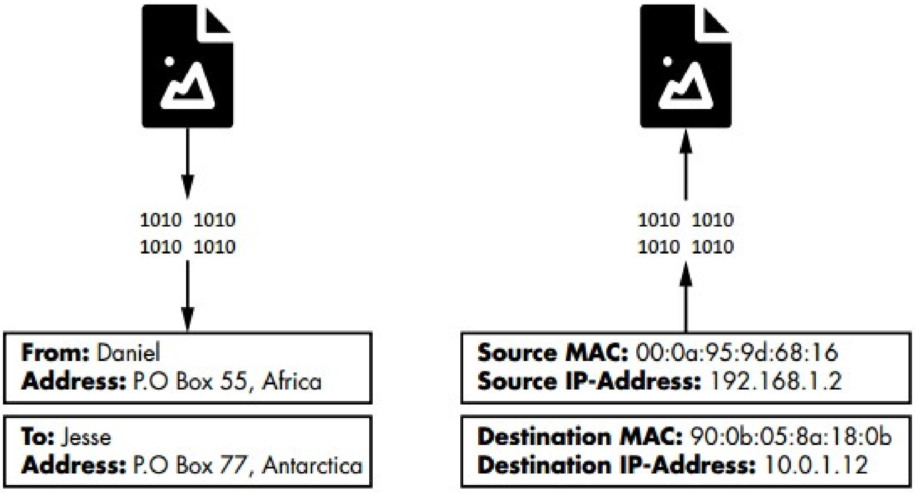
Introduction to Computer Network

How the Internet Transmits Data

Packets

All information on the internet is transmitted in packets. You can think of a packet as an envelope that contains the data that you want to send. As with the postal service, these packets are routed to their destinations based on a specified address.


1010 1010
1010 1010
From: Daniel
Address: P.O Box 55, Africa
To: Jesse
Address: P.O Box 77, Antarctica
1010 1010
1010 1010
Source MAC: 00:0a:95:9d:68:16
Source IP-Address: 192.168.1.2
Destination MAC: 90:0b:05:8a:18:0b
Destination IP-Address: 10.0.1.12

Parallels between envelopes and packets

The From Address section on an envelope contains two critical pieces of information: 1) the name of the person sending the letter, and 2) where they live. Similarly, packets have a source (*media access control [MAC] address*) that represents the machine sending the packet and a source (*IP address*) that represents where the packet came from. Other similar fields, known as packet headers, represent the packet's destination. The internet uses devices called *routers* to sort and forward packets.

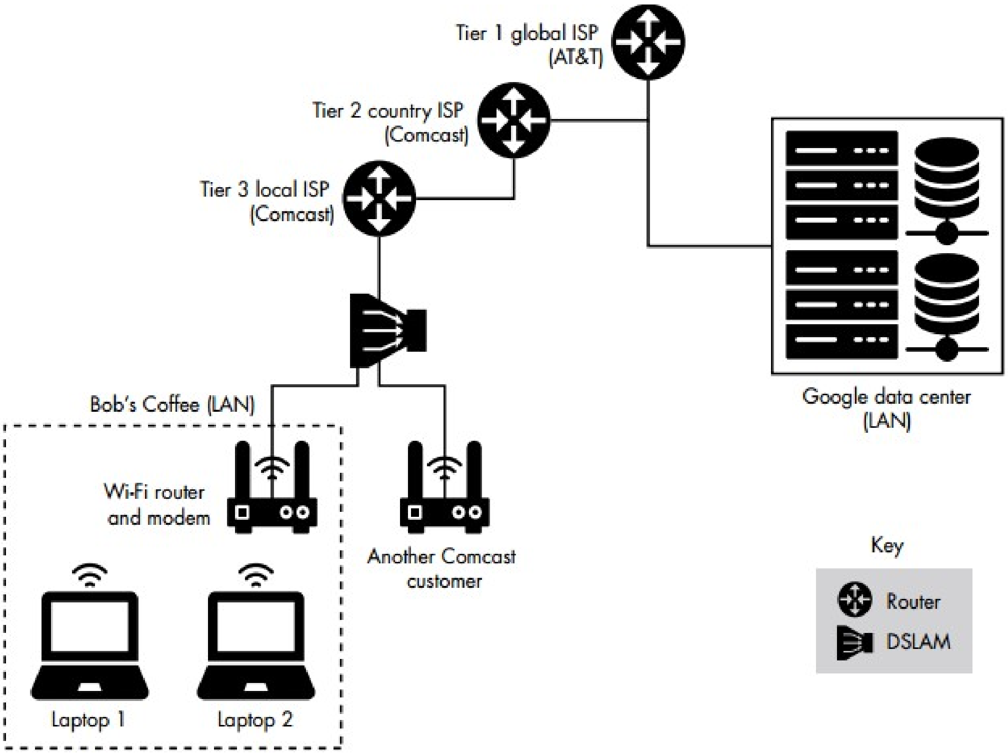
MAC Addresses

Your laptop contains a network interface card (**NIC**) that allows it to connect to WiFi routers. This card has a unique address, called a MAC address, that identifies your machine on the network. When the router wants to send your computer information, it labels that packet with your laptop's MAC address and then broadcasts it as a radio signal. All machines connected to that router receive this radio signal and check the packet's MAC address to see whether the packet is intended for them. MAC addresses are normally **48 bit numbers** written in hexadecimal (for example, **08:00:27:3b:8f:ed**)

IP Addresses

You probably already know that IP addresses also identify machines on a network. So why do we need both IP and MAC addresses? Well, networks consist of hierarchical regions similarly to how some countries are split into states, which themselves contain cities. IP addresses follow a structure that allows them to identify a device's place in the larger network. If you moved to another coffee shop, your laptop would be assigned a new IP address to reflect its new location; however, your MAC address would remain the same.

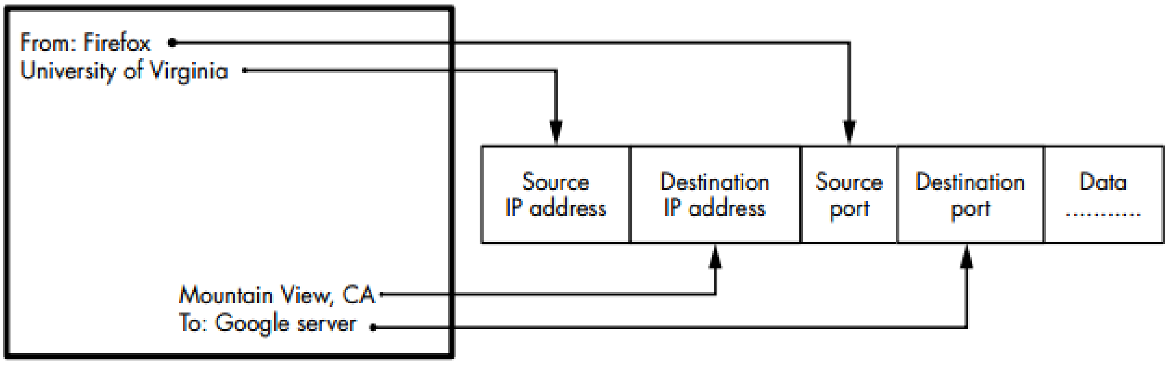
An IPv4 address encodes the network hierarchy information in a **32 - bit number.** This number is typically represented in four sections separated by dots (such as **192.168.3.1**). Each section represents an 8 - bit binary number. For example, the 3 in 192.168.3.1 actually represents the 8bit binary number 00000011.



A simplified view of the network hierarchy

Packets and the Internet Protocol Stack

A protocol is a set of rules that governs the communication between systems. In addition to governing communication rules, a protocol determines how information is laid out in a packet. They usually require the packet header to contain specific information.



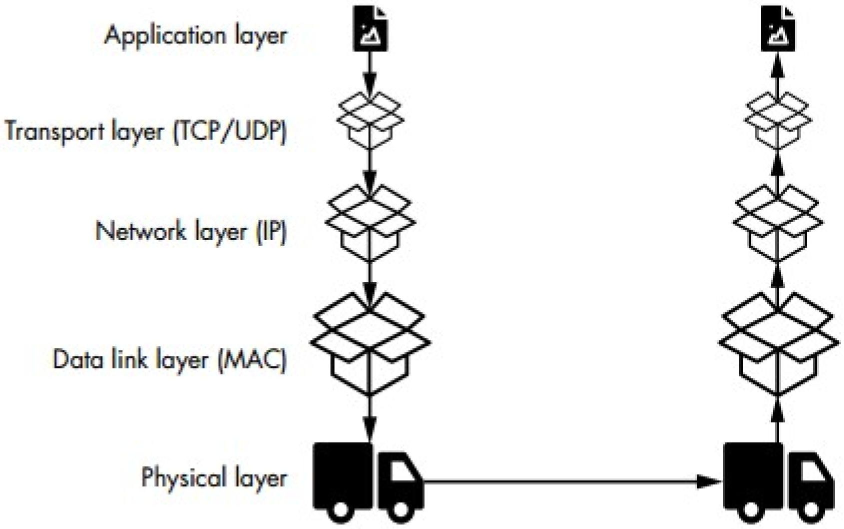
How header fields in a packet are like addresses on an envelope

In addition to IP addresses, this figure contains header fields for the source and destination port numbers, which are assigned by the operating system when it allows a process to communicate over the network. Port numbers are unique, meaning that no two processes on a machine can use the same port number. A process is an abstraction that represents a running program. Ports are necessary because they allow multiple processes on your computer to communicate with the internet simultaneously. When your operating system receives a packet from the network, it examines the port number to decide whether the packet is intended for your browser or messenger. However, ports also create a security risk because they open your computer to outside attackers. Often, one of the first things an attacker will do is scan a machine to discover open ports. A port is open if it accepts a connection from an external process. If the attacker finds an open port, they will attempt to infect your machine by sending it malicious packets.

The Five-Layer Internet Protocol Stack

To address the complexity of designing software for the internet, engineers decided to abstract the architecture into five independent layers. Each layer is responsible for managing the communication between specific components in the network.

Each layer is independent, meaning its actions aren't affected by the actions performed at the other layers. The protocol stack achieves this through a process called encapsulation, in which each layer treats information from the layers above it as generic data and does not try to interpret it.

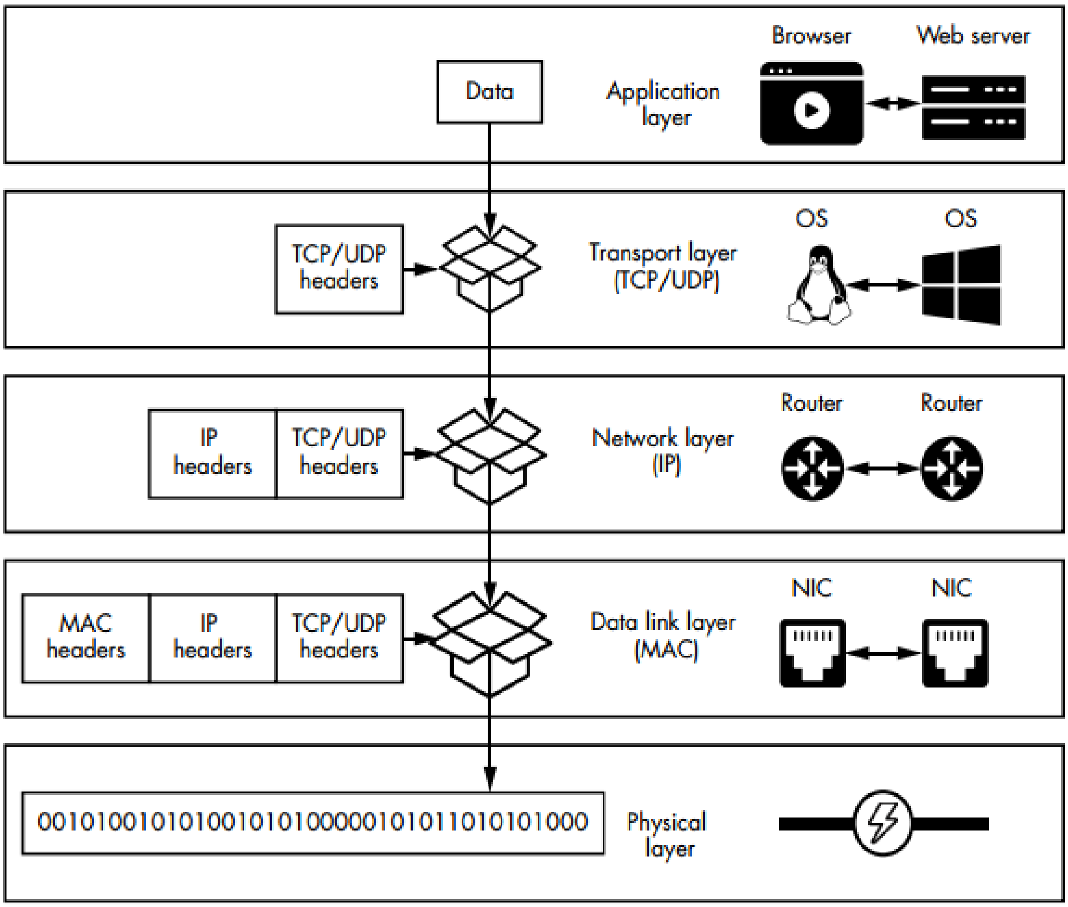


Five-layer internet protocol stack

Let's say a user composes an email. This happens at the application layer. As you can see, the messages associated with the email are then placed in transport layer packets. The transport layer does not read or alter the email in any way. It simply labels the packet with the information needed to process it. These transport layer packets are then placed into network layer packets and then data link layer packets before they are finally transmitted. By encapsulating and labeling each packet with its own headers, each layer can make decisions without depending on information from another layer.

The Application Layer

The application layer is responsible for communications between applications.There are several application layer protocols. The hypertext transfer protocol (**HTTP**) sends web pages to browsers, **Domain name system** (**DNS)** translate URL to ip address and the **file transfer protocol (FTP)** uploads files to a server. Email is sent using **SMTP.**



The network components that are communicating at each layer of the five-layer internet protocol stack

The Transport Layer

The transport layer is responsible for managing communication between processes communicating over the internet. This layer has two main protocols: the **transmission control protocol (TCP)**, which provides a guarantee that packets have reached their destination, and the **user datagram protocol (UDP)**, which is less complex and provides no guarantees.

The Network Layer

The network layer is responsible for controlling how packets flow between routers in the network. IP addresses are implemented at this layer.

The Data Link Layer

The data link layer is responsible for communication between NICs. It also detects errors that might have occurred during transmissions. The data link layer also implements the MAC protocol, which is responsible for sharing the transmission medium (for example, radio spectrum or wires).

The Physical Layer

The physical layer is responsible for converting the ones and zeros that represent data in a computer into a transmittable form. This could mean translating them into pulses of light, radio or electrical signals, or even sound.

Security Technology

Virus Scanners

A virus scanner is essentially software that tries to prevent a virus from infecting your system. In general, virus scanners work in two ways. The first method is that they contain a list of all known virus definitions. The virus definitions are simply files that list known viruses, their file size, properties, and behaviour. Generally, one of the services that vendors of virus scanners provide is a periodic update of this file. This list is typically in a small file, often called a .data file (short for data). When you update your virus definitions, what actually occurs is that your current file is replaced by the more recent one on the vendor's website. Any file on your PC or attached to an email is compared to the virus definition file to see whether there are matches. With emails, this can be done by looking for specific subject lines and content. The virus definitions often also include details on the file, file size, and more. This provides a complete signature of the virus. The second way a virus scanner can work is to look for virus-like behaviour. Essentially, the scanner is looking to see if the file in question is doing things that viruses typically do—things like manipulating the Registry or looking through your address book.

It is important to differentiate between on-demand virus scanning and ongoing scanners. An ongoing virus scanner runs in the background and is constantly checking your PC for any sign of a virus. On-demand virus scanners run only when you launch them. Many modern antivirus scanners offer both options.

Keep in mind that any antivirus program will have some false positives and some false negatives. A false positive occurs when the virus scanner detects a given file as a virus, when in fact it is not. For example, a legitimate program may edit a Registry key or interact with your email address book. A false negative occurs when a virus is falsely believed to be a legitimate program.

Virus-Scanning Techniques

In general, there are five ways a virus scanner might scan for virus infections. Some of these are outlined and defined here:

- **Email and attachment scanning:** Since the primary propagation method for a virus is email, email and attachment scanning is the most important function of any virus scanner. Some virus scanners actually examine your email on the email server before downloading it to your machine. Other virus scanners work by scanning your emails and attachments on your computer before passing it to your email program.

- **Download scanning:** Anytime you download anything from the Internet, either via a web link or through some FTP program, there is a chance you might download an infected file.

- **File scanning:** This is the type of scanning in which files on your system are checked to see whether they match any known virus. This sort of scanning is generally done on an on-demand basis instead of an ongoing basis. It is a good idea to schedule your virus scanner to do a complete scan of the system periodically

- **Heuristic scanning:** Perhaps the most advanced form of virus scanning, this uses rules to determine whether a file or program is behaving like a virus and is one of the best ways to find a virus that is not a known virus. However, this process is not foolproof. Some actual virus infections will be missed, and some nonvirus files might be suspected of being a virus.

- **Sandbox:** Another approach is the sandbox approach. This basically means that you have a separate area, isolated from the operating system, in which a download or attachment is run. Then if it is infected, it won't infect the operating system.

Intrusion Detection System (IDS)

An Intrusion Detection System (IDS) is a security technology that monitors network or system activities for malicious or suspicious behavior and issues alerts or takes predefined actions when it detects such activity. The primary goal of an IDS is to identify potential security incidents and raise awareness about them so that appropriate measures can be taken to address the threat. IDS can be classified into different categories based on their deployment, detection methods, and functionality.

Deployment Categories:

1. **Network-based IDS (NIDS):** Monitors network traffic in real-time and analyzes packet headers or content to identify suspicious patterns or signatures indicative of known threats. NIDS are typically placed at strategic points within a network to monitor traffic.

2. **Host-based IDS (HIDS):** Operates on individual devices (hosts) and monitors activities such as log files, file integrity, system calls, and application behavior on the host. HIDS is effective at detecting attacks that may not be visible in network traffic.

3. **Hybrid IDS (H-IDS):** Combines features of both NIDS and HIDS, providing a more comprehensive approach to intrusion detection. Hybrid IDS can provide a more holistic view of security by analyzing both network and host-level events.

Detection Methods:

1. **Signature-Based Detection:** Relies on a database of known attack patterns, or signatures, to identify malicious activity. When the system detects a pattern that matches a known signature, it generates an alert. This method is effective against well-known and documented threats.

2. **Anomaly-Based Detection:** Establishes a baseline of normal behavior and alerts on deviations from that baseline. Anomaly-based detection is useful for identifying new, previously unknown threats or abnormal behavior that may indicate a security incident.

3. **Behavioral-Based Detection:** Focuses on the behavior of entities within the network or on a host. It looks for deviations from normal behavior, such as unusual patterns of data access or changes in user behavior, to detect potential threats.

Functionality:

1. **Network Intrusion Detection System (NIDS):** Specifically designed to monitor network traffic and identify suspicious patterns or signatures. NIDS can be placed at various points within a network to analyze traffic passing through.

2. **Host Intrusion Detection System (HIDS):** Installed on individual hosts (computers or servers) to monitor activities on that specific device. HIDS is particularly useful for detecting attacks that may originate from within the network.
3. **Signature-Based IDS:** Relies on a database of known attack signatures. It is effective against known threats but may struggle with detecting new or modified attacks that don't match existing signatures.
4. **Anomaly-Based IDS:** Focuses on detecting deviations from normal behavior. This approach is effective at identifying previously unknown threats but may generate false positives if the baseline is not accurately established.

Intrusion Detection Systems play a crucial role in a comprehensive cybersecurity strategy by providing real-time or near-real-time detection of potential security incidents, allowing organizations to respond promptly to mitigate risks.

Honey Pots

A honey pot is an interesting technology. Essentially, it assumes that an attacker is able to breach your network security. And it would be best to distract that attacker away from your valuable data. Therefore, one creates a server that has fake data—perhaps an SQL server or Oracle server loaded with fake data, and just a little less secure than your real servers. Then, since none of your actual users ever access this server, monitoring software is installed to alert you when someone does access this server.

A honey pot achieves two goals. First, it will take the attacker’s attention away from the data you wish to protect. Second, it will provide what appears to be interesting and valuable data, thus leading the attacker to stay connected to the fake server, giving you time to try to track them. There are commercial solutions, like Specter (www.specter.com). These solutions are usually quite easy to set up and include monitoring/tracking software.

Firewalls

A firewall is a crucial security technology that acts as a barrier between a trusted internal network and untrusted external networks, such as the internet. Its primary purpose is to monitor and control incoming and outgoing network traffic based on predetermined security rules. Firewalls play a fundamental role in enhancing the overall security posture of an organization by preventing unauthorized access, protecting against cyber attacks, and managing network traffic.

Importance of Firewalls:

1. **Access Control:** Firewalls control access to a network by examining the source, destination, and type of traffic. This helps in preventing unauthorized users or malicious entities from gaining access to sensitive systems and data.
2. **Network Security:** Firewalls act as a frontline defense against various cyber threats, including malware, viruses, and other malicious activities. They help block or filter malicious traffic before it can reach the internal network.

3. **Policy Enforcement:** Firewalls enforce security policies by allowing or blocking specific types of traffic based on predefined rules. This ensures that network users and devices adhere to the organization's security guidelines.
4. **Prevention of Unauthorized Communication:** Firewalls prevent unauthorized communication between internal and external networks, reducing the risk of data exfiltration and unauthorized access to sensitive information.
5. **Logging and Monitoring:** Firewalls log network traffic and events, allowing administrators to monitor and analyze activities. This aids in identifying potential security incidents, investigating breaches, and maintaining an audit trail.

How Firewalls Work:

Firewalls work by inspecting packets of data as they pass through the network and making decisions about whether to allow or block them based on predetermined rules. The key mechanisms used by firewalls include:

1. **Packet Filtering:** Examines the header information of packets, such as source and destination IP addresses, protocol type, and port numbers. It allows or denies packets based on specified rules.
2. **Stateful Inspection (Dynamic Packet Filtering):** Keeps track of the state of active connections and makes decisions based on the context of the traffic. This allows firewalls to understand the state of a connection and make more informed decisions.
3. **Proxy Filtering:** Acts as an intermediary between internal and external systems. It receives requests from internal users, forwards them to external servers, and then returns the results. This helps hide internal network details and provides an additional layer of security.
4. **Deep Packet Inspection (DPI):** Analyzes the content of data packets, not just the header information. DPI can identify and block specific types of content or applications, making it effective against certain advanced threats.

Categories of Firewalls:

1. **Packet Filtering Firewalls:** Examines packets based on predefined rules for source and destination addresses, ports, and protocols. It works at the network layer (Layer 3) of the OSI model.
2. **Stateful Inspection Firewalls:** Maintains a state table to track the state of active connections and makes decisions based on the context of the traffic. It provides a higher level of security compared to packet filtering.
3. **Proxy Firewalls (Application Layer Firewalls):** Acts as an intermediary between clients and servers, forwarding requests and responses. It can inspect and filter traffic at the application layer (Layer 7) and provides a higher level of control.
4. **Next-Generation Firewalls (NGFW):** Combine traditional firewall features with advanced security capabilities, such as intrusion prevention, application awareness, and deep packet inspection.

5. **Hardware Firewalls:** Physical devices that provide dedicated firewall functionality. They are often deployed at the network perimeter to protect an entire network.
6. **Software Firewalls:** Software-based solutions that can be installed on individual computers or servers. They are suitable for protecting specific devices or segments of a network.
7. **Cloud Firewalls:** Designed to protect cloud-based infrastructure and applications. They operate in cloud environments and provide security for virtual machines, containers, and other cloud resources.

Firewalls are a fundamental component of network security and are essential for safeguarding against a wide range of cyber threats. Their deployment and configuration should be part of a comprehensive cybersecurity strategy to ensure the protection of sensitive data and network resources.

SSL/TLS

SSL (Secure Sockets Layer) and its successor, TLS (Transport Layer Security), are cryptographic protocols that play a crucial role in ensuring secure communication over the internet. These protocols provide a secure channel between two devices, such as a web browser and a web server, to protect the confidentiality and integrity of data during transmission. Here are the key roles of SSL/TLS in cybersecurity:

1. Encryption:

- **Role:** SSL/TLS encrypts data during transit, preventing unauthorized parties from intercepting and reading sensitive information. Encryption ensures that even if intercepted, the data appears as unreadable gibberish without the appropriate decryption key.
- **Importance:** Protects user credentials, personal information, financial transactions, and other sensitive data from eavesdropping and interception by malicious actors.

2. Data Integrity:

- **Role:** SSL/TLS ensures the integrity of transmitted data by using cryptographic hash functions. This guarantees that the data has not been tampered with or altered during transit.
- **Importance:** Prevents attackers from modifying data in transit, providing assurance that the information received is the same as what was sent.

3. Authentication:

- **Role:** SSL/TLS supports mutual authentication, where both the client and the server can verify each other's identity using digital certificates. This helps users ensure they are interacting with legitimate websites.
- **Importance:** Mitigates the risk of man-in-the-middle attacks by confirming the authenticity of the communicating parties, enhancing trust in online interactions.

4. Securing Login Credentials:

- **Role:** SSL/TLS protects login credentials (username and password) during the authentication process. This is crucial for secure access to websites, online applications, and other services.
- **Importance:** Safeguards against credential theft and unauthorized access, ensuring the confidentiality of user accounts.

5. Secure Online Transactions:

- **Role:** SSL/TLS is widely used in securing e-commerce transactions and online banking. It protects financial information, such as credit card details, during the transfer between the user and the server.
- **Importance:** Establishes a secure environment for conducting online transactions, building trust among users and facilitating the growth of e-commerce.

6. Securing Web Browsing:

- **Role:** SSL/TLS is employed in HTTPS (HTTP Secure), which encrypts data exchanged between web browsers and servers. It secures the browsing experience and protects users from various cyber threats.
- **Importance:** Guards against man-in-the-middle attacks, session hijacking, and other forms of data interception that can compromise user privacy and security.

7. Compliance and Regulations:

- **Role:** SSL/TLS compliance is often a requirement for various industry standards and regulations, such as PCI DSS (Payment Card Industry Data Security Standard) for handling credit card information.
- **Importance:** Helps organizations meet legal and regulatory obligations related to the protection of sensitive data.

8. Protection Against POODLE, BEAST, and Other Attacks:

- **Role:** SSL/TLS protocols evolve to address vulnerabilities and weaknesses. For example, newer versions of TLS address vulnerabilities like BEAST (Browser Exploit Against SSL/TLS) and POODLE (Padding Oracle On Downgraded Legacy Encryption).
- **Importance:** Regular updates to SSL/TLS help mitigate emerging security threats and vulnerabilities.

In summary, SSL/TLS protocols are foundational to cybersecurity, providing a secure framework for data transmission, authenticating parties involved in communication, and safeguarding against a range of cyber threats. The adoption of SSL/TLS is essential for ensuring a secure and trustworthy online experience.

Virtual Private Networks

A VPN is a virtual private network. This is essentially a way to use the Internet to create a virtual connection between a remote user or site and a central location. The packets sent back and forth over this connection are encrypted, thus making it private. The VPN must emulate a direct network connection.

There are three different protocols that are used to create VPNs:

1. **Point-to-Point Tunneling Protocol (PPTP)**
   Point-to-Point Tunneling Protocol (PPTP) is the oldest of the three protocols used in VPNs. It was originally designed as a secure extension to Point-to-Point Protocol (PPP). It adds the features of encrypting packets and authenticating users to the older PPP protocol. PPTP works at the data link layer of the OSI model. PPTP offers two different methods of authenticating the user: Extensible Authentication Protocol (EAP) and Challenge Handshake Authentication Protocol (CHAP). EAP was actually designed specifically for PPTP and is not proprietary. CHAP is a three-way process whereby the client sends a code to the server, the server authenticates it, and then the server responds to the client. CHAP also periodically reauthenticates a remote client, even after the connection is established.
2. **Layer 2 Tunneling Protocol (L2TP)**
   Layer 2 Tunneling Protocol (L2TP) was explicitly designed as an enhancement to PPTP. Like PPTP, it works at the data link layer of the OSI model. It has several improvements to PPTP. First, it offers more and varied methods for authentication—PPTP offers two, whereas L2TP offers five. In addition to CHAP and EAP, L2TP offers PAP, SPAP, and MS-CHAP. PPTP will only work over standard IP networks, whereas L2TP will work over X.25 networks (a common protocol in phone systems) and ATM (asynchronous transfer mode, a high-speed networking technology) systems. L2TP also uses IPsec for its encryption .
3. **Internet Protocol Security (Ipsec)**
   IPsec is the latest of the three VPN protocols. One of the differences between IPsec and the other two methods is that it encrypts not only the packet data (recall the discussion of packets in Chapter 2), but also the header information. It also has protection against unauthorized retransmission of packets. This is important because one trick that a hacker can use is to simply grab the first packet from a transmission and use it to get their own transmissions to go through. Essentially, the first packet (or packets) has to contain the login data. If you simply resend that packet (even if you cannot crack its encryption), you will be sending a valid logon and password that can then be followed with additional packets. Preventing unauthorized retransmission of packets prevents this from happening. IPsec operates in one of two modes: Transport mode, in which only the payload is encrypted, and Tunnel mode, in which both data and IP headers are encrypted.

Authentication and Authorization

Authentication and authorization are fundamental components of cybersecurity that work together to ensure the security and integrity of systems, networks, and data. These two processes play distinct but interconnected roles in controlling access to resources and protecting against unauthorized activities.

Authentication:

Definition: Authentication is the process of verifying the identity of a user, device, or system. It ensures that the entity attempting to access a system is who or what it claims to be.

Key Aspects:

1. **Identification:** Users or entities provide a unique identifier, such as a username, email address, or digital certificate, to assert their identity.

2. **Verification:** The system validates the provided identifier by comparing it with stored credentials, such as passwords, biometric data, or cryptographic keys.

3. **Authentication Factors:**

   - **Knowledge Factor:** Something the user knows (e.g., passwords, PINs).
   - **Possession Factor:** Something the user possesses (e.g., smart cards, security tokens).
   - **Biometric Factor:** Something inherent to the user's physiology (e.g., fingerprints, facial recognition).

4. **Multi-Factor Authentication (MFA):** Involves using two or more authentication factors to enhance security. For example, combining a password with a fingerprint scan.

Importance:

- Authentication ensures that only authorized users or entities can access systems, applications, or data.
- It helps prevent unauthorized access, identity theft, and protects against various cyber threats.

Authorization:

Definition: Authorization is the process of granting or denying access rights and permissions to authenticated users or systems based on their identity and level of trust.

Key Aspects:

1. **Access Control:** Determines what resources (files, databases, applications) a user or system is allowed to access and what actions they can perform.

2. **Permission Levels:** Assigns specific permissions or privileges to users based on their roles, responsibilities, and the principle of least privilege.

3. **Policy Enforcement:** Enforces security policies by controlling the actions users can take within a system or network.

Importance:

- Authorization ensures that authenticated users have the appropriate level of access to resources, minimizing the risk of unauthorized activities.
- It helps maintain data integrity, confidentiality, and overall system security.