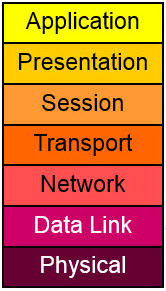
**Network Cybersecurity:**

**Understanding Standard Internet Protocols**

When most people hear the term “computer networking,” they immediately relate it to how to connect to the Internet, whether it be through the use of a wired or wireless connection. However, the actual definition encompasses much more than that. As defined by popular news site Techopedia, “a computer network is a group of computer systems and other computing hardware devices that are linked together through communication channels to facilitate communication and resource-sharing among a wide range of users.”[[1]](#footnote-2) In other words, networks are groups of devices that share information between another using various means of transport. These means of transport are known as “protocols,” and understanding them and their security properties is a core element to understanding cybersecurity.

  
The OSI Model

However, before diving into any specific protocols, it is helpful to think about computer networks in relation to a framework. Not only does this help us understand the pieces that make network communication possible, but it also helps us remember the roles of various protocols. While many frameworks have been created in order to describe computer networks, only one has survived the test of time: the Open Systems Interconnection model, or OSI model for short.

Read from the bottom up, the OSI model contains a series of “layers” that stack on top of one another to act as a bridge between our devices and the outside world. While we will eventually go deeper into each of these layers, having a brief overview makes deeper knowledge more easily digestible.

First, there is the physical layer, which includes network adapter cards, cables, and physical connections. Next is the data link layer, which includes device drivers and software used to make devices communicate with network adapter cards. Proceeding that is the network layer, which is where communications between devices are routed. After the data is routed, it reaches the transport layer, where the received data is formatted and error checked. Above the transport layer is the session layer, which allows network devices to interact with other devices, and further above that is the presentation layer, which controls the appearance of information on screens. Finally, there is the application layer, which supports tasks like e-mail or file transfer. It is also important to note that in the TCP/IP model (which is very similar to the OSI model), the application layer encompasses presentation and session, essentially making it one large layer.[[2]](#footnote-3)

Breaking up computer networks into pieces using the OSI model makes it clear that there is a lot of movement in a computer network, and completing this movement securely is of utmost importance. A common acronym in cybersecurity is CIA, which stands for confidentiality, integrity and availability. This is what protocols aim to achieve; movement that keeps information in the hands of the correct people, keeps information accurate, and keeps it accessible to the people who need it. Using the OSI model and CIA, we can effectively judge the security properties of various protocols, no matter what layer it works at.

The first group of protocols we must discuss is those that involve cabling, or the physical layer. The most common protocol we use when talking about how to connect to the Internet is UTP and STP, or *unshielded twisted pair* and *shielded twisted pair*. *T*wisted pair is a group of individual wires that are insulated together and used to connect from a computer to a “concentrator,” which include devices like bridges, network switches, hubs and more. There are several variations of twisted pair, but the most common by far is CAT5E, which allows transmissions of up to 1Gbps at a distance of 100 meters.

One may jump to the conclusion that shielded twisted pair is better than it’s unshielded counterpart, and from a security standpoint, they would be correct. Both types prevent crosstalk between wires, which maintains integrity in the CIA reference. Unshielded twisted pair is much cheaper and simpler to install, but is prone to radio frequency interference. Shielded twisted pair, on the other hand, can handle this interference much better, as it is covered by an outer covering, but as a result, it is more expensive and difficult to work with. As a result, unshielded is much more commonly used, but shielded is still used in token-ring topologies.[[3]](#footnote-4) Token-ring networks are much more susceptible to interference due to computers in the same network sending messages to each other at the same time, which warrants the extra cost.

Despite STP’s benefits, it’s important to note that both UTP and STP can be tapped, which allows attackers to eavesdrop on traffic. Thankfully, there are other protocols in the physical layer which aim to improve upon the shortcomings of twisted pair. A perfect example of this is coaxial. Coaxial cables contain a single wire that is protected by a metallic coat that reduces interference, which preserves integrity. It is also has a significantly higher transmission capacity, which preserves availability. However, confidentiality is where the coaxial cable struggles. Since the electrical signal is sent through a single wire, all an attacker has to do is bypass the metallic coat, and they will be able to tap the transmission completely undetected. It is much easier said than done, but the threat is still present and it is the primary flaw of the coaxial protocol.

Fiber optics is the newest physical-layer protocol that aims to solve the problems of both twisted pair and coaxial. It has gained steam quickly over the past few years, and with good reason. It is completely immune to radio frequency interference, and it is nearly impossible to tap into fiber cable data without ending the data stream completely. The main shortcoming of fiber-optic cabling is it’s cost, which is significantly higher than both twisted pair and coaxial cables. In addition, it is a much less versatile cable, as it does not perform well under physical stress or bending.

All of these physical protocols have their purpose, as some are better at specific things than others. For example, while twisted pair is often used in Ethernet cables and connects devices to the Internet, coaxial cables are the go-to choice for transmitting video signals. Even clear “winners” like fiber are mostly reserved for telecoms or universities, due to how expensive it can get. This can change at the blink of an eye as technology improves and competition increases, but all of these protocols currently have a place in networking.

Data link protocols are next in the OSI model, and move data in and out of computer networks through the use of physical protocols. Having secure data link protocols in place is crucial, as insecure protocols can lead to bad data being sent across a network. All data link protocols work in a similar manner, as they take data and break it up into “frames” before transmitting it via physical connections.[[4]](#footnote-5) However, each protocol still has its place, as there are pros and cons to all options.

It’s also important to note that the data link layer is often divided into two sub-layers: Logical Link Control (or LLC) and Media Access Control (MAC). The LLC sublayer is responsible for establishing transmission paths between devices on a network, while the MAC sublayer is responsible for using unique hardware addresses to determine the source and destination for data. Many protocols in the data link layer fall into either the LLC or MAC sublayer, but there are also some protocols which overlap them both.

A perfect example of this is Ethernet, which is by far the most common data link protocol today. Ethernet is a common household name, as most people have heard of an Ethernet cable. However, while most people simply view it as a way to get internet connectivity to a device, Ethernet does much more than that. In addition to enabling devices to communicate with one another, Ethernet wraps frames in “packets” that other local devices can recognize and process, and contains error correction information that helps detect transmission problems

There are several types of Ethernet, with the main differentiator being speed. The entire family of Ethernet standards is called the Institute of Electrical and Electronics Engineers (IEEE) 802.3, and the first iteration of Ethernet was 10Base 5, which transmitted data at a speed of 10 megabits per second.[[5]](#footnote-6) Now, we have Ethernet cables that support over 10 *gigabits* per second, but despite the monumental speed upgrades, the underlying security mechanics via the use of packets have remained mostly the same.

802.3 has been the primary protocol used for household internet connections for a long time, but as time goes on, there is a new reliance on 802.11, or *wireless LAN*. Wireless LAN is a perfect example of a protocol which utilizes both LLC and MAC sublayers. It uses the same link control system as it’s 802.3 counterpart, but has a unique MAC system that identifies wireless connections differently than wired connections. The most common of these systems that gets used is called wireless fidelity, or as most people call it, Wi-Fi.

Wireless LAN also has a variety of security options that it uses in conjunction with systems like Wi-Fi. Wired Equivalent Privacy, or WEP, was the first popular security protocol used with 802.11 and encrypted data using the Rivest Cipher 4 (RC4) stream cipher.[[6]](#footnote-7) However, it was eventually deprecated due to it’s slew of weaknesses, such as a weak initialization vector and an ineffective integrity check value algorithm. WEP’s security flaws led to the emergence of Wi-Fi Protected Access, or WPA. Rather than RC4, WPA uses Temporal Key Integrity Protocol, or TKIP. This solved the issue of a weak initialization vector, as well as other issues like key management and replay attack protection.

However, just like WPA replaced WEP, WPA2 replaced WPA as the most current and secure security standard for wireless connectivity. WPA2 uses Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) and Advanced Encryption Standard (AES), both of which are far more secure than TKIP and RC4 respectively. Due to it’s constant key rotation and security properties, there is no reason to not use WPA2 whenever possible.

Other examples of protocols in the data link layer include Digital Subscriber Line (or DSL). which was a popular protocol to send data over telephone lines, and Asynchronous Transfer Mode (ATM), which was used over fiber before Ethernet became popular. It remains clear though that Ethernet and wireless LAN are the most common and relevant to our lives today.

Moving on in the OSI model, we have the network layer. The primary protocol used in the network layer is Internet Protocol, or IP. Similar to Ethernet, IP is an encapsulating protocol, but it goes a step deeper.[[7]](#footnote-8) Whereas Ethernet wraps packets in frames, IP actually wraps the data being sent into packets beforehand. In addition to encapsulation, IP is the protocol that is responsible for addressing. Every packet that gets created has a source address and destination address attached to it, and IP is the protocol that makes this happen. These addresses can be any combination of four numbers from 0 to 254, separated by dots (such as 123.45.67.89).

However, while these are the types of addresses that most people will be familiar with, it is not the latest or most secure. These addresses are *IPv4* addresses, and the current version of IP is *IPv6*. The main difference between IPv4 and IPv6 is the number of available addresses. IPv4 has a total range of 2^32 possible addresses due to each address being a combination of 32 bits, whereas IPv6 has a total range of 2^128 possible addresses due to each address containing 128 bits.[[8]](#footnote-9)

One solution to the problem of running out of IP addresses on IPv4 is network address translation, or NAT. NAT is another protocol in the network layer that is responsible for turning source and destination addresses into actual usable addresses. Most IP addresses are actually private, and allocated under RFC1918. ISP’s do not route these private addresses, and instead they must be translated beforehand. Another similar protocol that does this is port address translation, or PAT. This does the same thing as NAT, but allows for even more addresses due to mapping multiple users to one address via port numbers. It is unlikely that the introduction of IPv6 will do away with NAT/PAT, as it still protects our private IP addresses despite the additional addresses that IPv6 provides us.

Even though IPv6 is the better option for the long term, transitioning has been slow for a number of reasons. Despite the naming convention, IPv6 is essentially a completely parallel network to IPv4, meaning that existing software and hardware have to be changed in order to support it. This will take a lot of time and money, as it is a protocol that is forcing us to adapt, rather than simply run an update.

After data packets are routed through the network layer, they enter the transport layer. In this layer, various protocols provide security for the packets through authentication, integrity checking, and more. The most notable of these protocols fall under the IPSec suite, which is short for Internet Protocol Security. These protocols are Authentication Header (AH) and Encapsulating Security Payload (ESP), and they are each vital in internet security. Authentication header allows the recipient of a message to verify the sender, and ESP ensures that the verified data remains private.[[9]](#footnote-10)

Both AH and ESP are extremely powerful and have multiple ways of implementation. One implementation is end-host implementation, which puts AH and IPSec into all host devices. With end-host implementation, security between two devices is confined to those two devices, which makes it (virtually) completely safe. The problem with end-host implementation is that most networks contain an innumerable amount of hosts, which makes it infeasible most of the time.

This is where router implementation comes into play. Router implementation is significantly easier to setup, as it secures connections between routers that thousands of clients can use, rather than implementing IPSec on the clients themselves. However, router implementation is still not perfect, as it only secures the connections between the routers; the connection between the routers and the local hosts are still insecure with IPSec alone.

Secure Sockets Layer (SSL) and it’s successor, Transport Layer Security (TLS) are two protocols that solve this issue.[[10]](#footnote-11)

.

Finally, we have the session, presentation, and application layers. As explained earlier, these layers are grouped into one large application layer in the TCP/IP model, as many of the protocols here overlap the three separate layers. This is where there are the most protocols, as it is the “endgame.” In other words, this is where data packets finally reach their destination, and as a result there are a lot of possible protocols to decide it’s behavior next. Some popular protocols include HTTP/HTTPS (which secures traffic to the world wide web), FTP (which secures traffic involving file transfers, and DNS (which translates names into network addresses).

.

While there are several protocols left out of this discussion, these are the standard internet protocols that we see in most computer networks today. Understanding the seven layers of the OSI model is extremely valuable when learning about computer networking, but understanding the ins and outs of every single protocol is arguably unnecessary. Instead, one can simply use the standard protocols as a baseline, then branch out and learn whatever is of interest to them. The standard protocols can also be used as a baseline when creating new, better protocols, which makes them even more important. Security will always be a primary concern in networking, so hopefully protocols continue to be improved upon.

1. https://www.techopedia.com/definition/25597/computer-network [↑](#footnote-ref-2)
2. s1 [↑](#footnote-ref-3)
3. s2 [↑](#footnote-ref-4)
4. s3 [↑](#footnote-ref-5)
5. s4 [↑](#footnote-ref-6)
6. s5 [↑](#footnote-ref-7)
7. S6 [↑](#footnote-ref-8)
8. S7 [↑](#footnote-ref-9)
9. S8 [↑](#footnote-ref-10)
10. s9 [↑](#footnote-ref-11)