[[1]](#footnote-1)

Distributed Computing and Network Security

Cameron P. Tatum

*Abstract*—In this survey paper, I will be talking about distributed computing and the security of the network on which hosts are within. The first section of my paper will give a basic explanation of how transmission control protocol/internet protocol function, since the whole protocol plays a major role in networking and the exploits that come along. After that I will briefly explain a few exploits and vulnerabilities that networks are susceptible to. After a brief explanation of each I will propose my simple approach to prevent the attacks. I will also talk about secure communications and the use of cryptography and encryption to pass data on a network. In the next section I will review some of the existing research surrounding the topics I have discussed and what flaws may lie within their approach. Next I will talk about what future research may be ahead for continued study and examination of this topic. Lastly to end my survey paper, I will give a few concluding remarks with a list of my references I have used in this paper.

*Index Terms*—Cryptography, Cyber-attacks, Networks, Security

# INTRODUCTION

I

n a world where technology is ever-expanding and changing every day, it comes as no surprise that our lives are now dependent on technology. We expect technology to function for its intended purpose, and it can be very disheartening when it does not. Besides buggy, badly-written software, unsecure software is one of the major causes of failure in a technological system. Network security is a broad topic given that there are so many angles to cover. Why do you want to secure your network? Maybe because you are a business and unauthorized access to your network means an outsider could gain access to files within the system that only employees should be able to view. Or you could be in college trying to secure the router in your apartment so nobody else can sign in and run your data usage up. Whatever the reason may be, network security is an important aspect of the core of cyber security.

 I have taken courses in the networking field, an introductory course and an advanced distributed computing course, as well as introductory and advanced courses in cyber security, so I have a basic understanding of how communications over a network are ordered. Most of the topics and points in this paper are based off research I have done for this survey paper in scholarly files on Google. My research is mainly focused on the incoming and outgoing communications and packets on a network, and how wireless connectivity works on a network, and the security implications that are included with wireless devices.

# Approach

To begin talking about network security and attacks that can be carried out against a network, it is important to first understand how basic network protocols work.

## TCP/IP

TCP/IP, transmission control protocol/internet protocol is a standard for network communication that handles packets and controls where to send each packet to. The protocol is made of two separate protocols, the transmission control protocol (TCP), and the internet protocol (IP), which will be explained in greater depth in section “B” and section “C.” The TCP/IP structure is made up of four layers which make. The data-link layer, which is the physical hardware and network equipment. As its name suggests, it is used to link the different servers, nodes, and hosts of the network together. Next is the internet, or network layer which connects hosts of a network together. The next one up is the transport layer, which handles communication between hosts on a network. Then lastly, on top of the stack model, the application layer is utilized for communication between applications, or programs on a network.

## Transmission Control Protocol

Transmission Control Protocol (TCP) is a connection-oriented data delivery system. The common connection process used by the transmission control protocol is called a three-way handshake. A three-way handshake can be described in a physical example. For instance, if you walk up to somebody, shake their hand, and say “Hey how are you?” That person will acknowledge that you asked how they are doing, and reply, “I am well, how are you?” At which point you acknowledge that they asked how you are, and you reply with the appropriate acknowledgement, and now you have established a connection with that person. For a host to connect with a destination host, the source host will send out a SYN, or synchronize packet, to the destination host. The destination host will reply with an ACK, or acknowledge packet, letting the sender know that it received the request unharmed, and will send back a SYN packet. The sender will then send an ACK packet back to the destination to let them know the synchronization was received. An illustration of this can be seen below in Figure 1.



*Figure 1:* Photograph by Cisco [1]

## Denial-of-Service and Distributed-Denial of Service attacks

On a home wireless network, what is more aggravating than having to wait forever and a day to load websites, social media applications, and watch videos on YouTube? Not being able to access the network to do so and being denied the service you are paying for. A denial-of-service (DoS) attack and a distributed-denial-of-service (DDoS) is when “… an attacker attempts to prevent legitimate users from accessing information or services. By targeting your computer and its network connection, or the computers and network of the sites you are trying to use, an attacker may be able to prevent you from accessing email, websites, online accounts (banking, etc.), or other services that rely on the affected computer. [2].” The difference between denial-of-service attack and a distributed-denial-of-service is that a DoS is directed at you, the victim. A DDoS can be directed at you, if you are unfortunate enough to be on the receiving end, however more than likely, your computer will be used, along with many others, to carry out a DDoS attack on another computer or website. These attacks are carried out by flooding a specific IP address with multiple packets, or requests, until it cannot process all of them at the same time, causing it to crash and deny service to the user and others. For example, an attacker could get the IP address of a home router, then direct so many ping requests at it constantly, thus making it unusable to the family it belongs to. The legitimate packets that are supposed to be transmitted do not make it through to the network, and usually malware exploitation is used by the attacker. Unfortunately, there is no definite way to prevent such attack from happening, but there are measures that can be taken to attempt to rectify the situation. There are a few ways this can be resolved, such as resetting the modem and router to change IP addresses, blocking the IP address the requests are coming from, and setting up a stricter firewall to prevent such attack from happening again. However, calling your internet service provider is the only full-proof way of resolving that issue.

## Man-in-the-Middle Attack

A man-in-the-middle attack is exactly as it sounds, an attacker sits between you and the intended destination your packets are to go to. This attack is similar to eavesdropping, but the attacker not only listens to communications on a network, but can interfere with packets and alter data being transmitted. This type of attack is most commonly exploited on web communications, where data transmissions between two users run the gamut. A standard used to commonly ensure safety while surfing online is the hypertext transfer protocol secure, HTTPS, instead of HTTP. Although if this attack is to be carried out, it will be on a site where the margin of profit, if successful, is greater than the consequences of the action, such as banking websites, where money is in the mix. The HTTPS standard is accepted, and commonly used by default on sites, but if an attacker were to carry out this attack, he/she would forge a fake certificate in order to deprecate HTTPS to HTTP. As illustrated in an article about these attacks, “… a user on the *client host* (CH) wants to make a secure transaction on the *server host* (SH) using HTTPS. Given that CH and SH have to network exchange data, the attacker host (ATH) acts as a gateway for the traffic stream. The attacker [man in the middle] intercepts traffic from the source and forwards it to the destination, thus gaining the ability to modify messages and insert new ones without either party realizing it…. The CH and the SH see an apparently secure communication channel between them. In reality, the attacker has the ability to decrypt the entire communication because he or she possess the necessary keys [3].” A seemingly safe way to prevent this from happening is to use SSL/TLS certificates in adjunction with the HTTP Strict Transport Security (HSTS) protocol. This will activate the HTTPS protocol instead of HTTP, and ensure that every site the user connects to uses HTTPS, or else the browser will not navigate to it. In an extreme case, in 2015, a group in Europe stole over six million in Euros, close to seven million and seventy-thousand in U.S. currency. How did they do it? They infiltrated medium-sized firms and companies throughout Europe by gaining access to the email server. Once the hackers had control of the companies’ emails, it was a matter of waiting for clients to pay for services. Since the email were coming from “trusted” individuals in the company, the client did not hesitate to hand over banking information. The money was transferred into the hackers’ accounts, and they continued until they were arrested. First of all, this could have been easily prevented simply with an email certificate system, which would have required the hackers to also gain the private keys of all employees, but that was not the case.

## Cryptography and Encryption

In the growing world of technology, it is inevitable that, at some point, we must enter sensitive data in a form on a website somewhere, to be sent across a network, and into the wild, mysterious universe that is the world wide web. Since there is massive amount of gray area when it comes to, is a site secure, am I being sniffed, am I being watched, or is this being intercepted, there must be an added layer of protection. Data that is sent across a network, especially that of a large business with multiple hosts, the probability of your packets being sniffed is high. Packet sniffing is when a user connected to the same network is running a program, intercepts a data packet as it traverses the network, and prints out information and the contents of the packet. A username and password used to login to a social media account can be easily read to extract the username and password, if on an unsecure connection where there is no encryption and everything is sent in plain text. An example of what a sniffed packet looks like can be seen in Figure 2.



*Figure 2:* Photograph by Custom PC Review [4]

That is partially why it is important to use hypertext transfer protocol secure because it supports built-in encryption. There are two types of cryptography, symmetric key cryptography, and asymmetric key cryptography. With symmetric key cryptography, in order for the sender to be able to encrypt a message, and the receiver be able to decrypt the message, they both have to use the same public or private key. A few of the most popular ciphers that use symmetric key cryptography include AES, DES, and Blowfish. For asymmetric, a different key is used to encrypt the message than the one that is used to decrypt the message. The most popular algorithm used for asymmetric key cryptography is RSA.

Data Encryption Standard, or DES, cryptography uses sixty-four bits in the block size, fifty-six to be sent while using the other eight as parity bits. While not the most absolute encryption algorithm that could possibly be used, the final encrypted result could has multi-billions of possibilities, so the chance of someone decrypting the message are low. An overview of the DES algorithm can be seen in Figure 3.



*Figure 3:* Photograph by TutorialsPoint [5]

# Hardening

# Conclusion

In retrospect, setting up a secure network, and taking the extra time to maintain a secure network, is a sensible and often costless approach when being an administrator over a network. Copious amounts of money can be saved by taking the extra steps to ensure secure communications on a network. Not only can it save money in the future, but it can also save reputation, in the instance that you might be an administrator for a large and reputable company. Not many clients prefer to stick with a company that has multiple, or even one security breach, showing weakness in the system.

References

1. N. Pfeiffer, *What Is a Three-Way Handshake in TCP*. 2016
2. M. McDowell, “Understanding Denial-of-Service Attacks,” *US-CERT*, Nov. 04, 2009. [Online]. Available: <https://www.us-cert.gov/ncas/tips/ST04-015>. [Accessed Dec. 1, 2017]
3. F. Callegati, W. Cerroni, and M. Ramilli, “Man-in-the-Middle Attack to the HTTPS Protocol,” *Researchgate*, IEEE Computer Society, Feb. 03, 2009. Online. Available: <https://www.researchgate.net/profile/Walter_Cerroni/publication/224378197_Man-in-the-middle_attack_to_the_HTTPS_protocol/links/00b495231a356171f5000000.pdf>. [Accessed Dec. 1, 2017].
4. S. Chen, *Wireshark Tutorial: How to Use Wireshark for Network Analysis*. 2017
5. TutorialsPoint, *Data Encryption Standard*. 2017
1. [↑](#footnote-ref-1)