The Cryptographic Flaws in the TCP/IP Model

Felipe Marques Allevato
Michigan State University, East Lansing, MI, United States of America
Uploaded 10 December 2021

Abstract

In modern society, with the advancement of internet and a global usage of the tool, researchers have studied more about the main network models and their security breaches. From all of those, TCP/IP has been the most common model since its creation in 1983, and thus the most studied one. There have been found issues that allowed diverse types of attack reach the model's users. However, the most critical issue in the model was its Cryptographic design. To address this problem and propose different solutions, this paper has categorized and identified the most common design flaws and solutions regarding different algorithms and technologies (Including IPSec, Blowfish, AES, SF Block Cipher, and TLS/SSL). Firstly, the paper defined the most important concepts related to these flaws, then it explained the proposed solutions.
Keywords: Cryptographic Algorithm;TCP/IP model security; IPSec; Blowfish; AES; SF Block Cipher; Cryptographic attacks

1. Introduction

The 2020 Internet Crime Report [1] conducted by the Federal Bureau of Investigation's Internet Crime Complaint Center (FBI IC3) reports a continuous increase in the US internet crime complaint in the last years. The report received complaints in a structured way that could show the FBI specific attack trends and patterns. The following points highlight the most important results:

- In the last five years, it was discovered that there was a total of 2,211,396 complaints. This resulted in an aproximate total loss of 13.3 billion dolars.
- The 2020 Internet Crime Report reported 791,790 complaints on the year of 2020, an increase of more than 300,000 complaints from 2019, with losses exceeding $4.2 billion.
- The age of the victims has a huge correlation in the number of complaints and loss. Usually, victims in older ranges of age ($\geq$ 30) are more targeted and have the greatest financial losses, while younger victims (< 30) are less targeted and have the smallest financial losses.
- Some more common types of attacks were directly related to authentication and authorization breaches in 2020, such as Credit Card Fraud (17,614 victims), Personal Data Breach (45,330 victims), Ransomware (2,474 victims), Spoofing (28,218 victims), and BEC/EAC (19, 369 victims). These are directly related to issues on cryptographic systems and logistics. The total loss on these 5 categories was of $2.436.607.087, being the Business Email Compromise (BEC) / Email Account Compromise (EAC) the most impactful, with a total loss of $1,866,642,107.

To analyze attack trends and patterns, the statistics provided could be extremely useful. However, they do not solve all the issues in understanding and learning how to prevent and protect the users from them.

Additionally, as shown from the data, some of the most important attacks in the last years were correlated with some different breaches on authorization and authentication, both of which are mainly improved and secured by cryptographic algorithms.

In order to understand and improve the issues cited, few of the most common attacks and breaches used by attackers in modern TCP/IP networks [2] should be explained:

- *Brute-Force:* This tecnhique is known as an exhaustive search in iterations to bypass the user authentication. Sometimes it is a blind guess, but usually it uses some type of technique, such as a directory that uses discovered passwords from exploited databases. A case of brute-force attack happened in 2016 on the Alibaba website and compromised 20.6 million accounts. In this case they used a great database of 99 million usernames and passwords and were successful in exploiting the breaches.
- *Man in the Middle:* As the name might suggest, this happens in a type of "eavesdropping". It is when the attacker has access to an existing conversation or data transfer. The TCP/IP protocol suite does not have many mechanisms to avoid this type of attack, and that is why many technologies were introduced after its creation to solve this breach.
- *IP Spoofing:* This type of attack usually takes advantages from information contained in the IP packet header. For example, one of the most famous cases of IP Spoofing attack is the Mitnick attack against Tsutomu Shimomura in 2004. Since the TCP/IP handhsake was not built with cryptography in mind, Mitnick was able to determine the TCP sequence number and a trusted relationship between the terminal and the server. In the end, he was able to create a backdoor in Shimomura's computer and cleaned the footprints left at the logs.

The attacks cited are just few examples of the most common attacks in the TCP/IP model that are directly realted to cryptographic issues, also called as cryptographic attacks.

These attacks are main components for attackers when trying to achieve certain goals. Some of them were cited in the Internet Crime Report of 2020. The following points will help udnerstanding these goals better and their relation to cryptographic attacks:

- *Information Theft:* With a great knowledge on cryptographic attacks, such as the *MITM* and *IP Spoofing*, and commonly used protocols, such as FTP and HTTP, attackers could steal some sensitive personal information by spoofing the host authentication mechanism. This could lead to common crimes reported by the FBI IC3, such as *Identity Theft* and *Personal Data Breach*, which caused $413.957.754 of loss on the year of 2020 and an increase of around 30.000 complaints in comparison to the last few years.
- *Extortion Attacks:* This type of crime is related to the threat of using or destroying sensitive information to obtain a financial gain. This includes typical attacks, such as Ransomwares and RATs. Usually the attacker will need to either bypass the authorization mechanisms of the system or exploit a breach found with MITM techniques.
- *Denial of Service (DoS):* The DoS class of attacks is related to the motivation of preventing some users to have access to a desired service. If the attacker has additional tools provided by previous attacks, such as having a botnet, they can perform even more dangerous attacks, such as *Distributed Denial of Service (DdoS)*. As shown by Cisco's Annual Internet Report (2018-2023) [3], it is one of the crimes with highest growth in the recent years and is expected to almost double the incidence from 2018 to 2023.

The following sections will be responsible to analyse the cryptographic breaches exploited by attackers in the TCP/IP protocol suite and its applitacions and recall some of the definitions made on this section.

2. The cryptographic threats to the TCP/IP model

This section goes into specific details on how some common attacks exploit the common cryptographic breaches existent in the TCP/IP protocol suite.

It will also be discoursed about common techniques that are used in order to sucessfully perform the attacks mentioned.

- *IP Spoofing*
- *TCP Authentication*
- *Session Hijacking*

These attacks were selected because they are the most common and easy to replicate in a controlled environment among the cryptographic category. Additionally, they are good to exemplify the common cryptographic concepts and flaws related to the TCP/IP model.

2.1 IP Spoofing

The IP Spoofing attack happens in the authentication and authorization pillars of security. It is described as when an attacker attempts to use a device or technology to trick other networks by masquerading as an authorized user.

In specific, this happens with the use of the Internet Protocol of the TCP/IP model, which largely uses the IPv4 technology. Additionally, this attack is commonly done with other specific TCP/IP technologies, such as DNS and ARP.

To comprehend this attack, it is important to understand the structure of the TCP/IP communications and the IP packet.

In computer networks based on the TCP/IP model, there are exchanges of network data packets, each containing multiple headers that orient the traffic .

The important header for the IP Spoofing attack is the source address, see Figure 1.

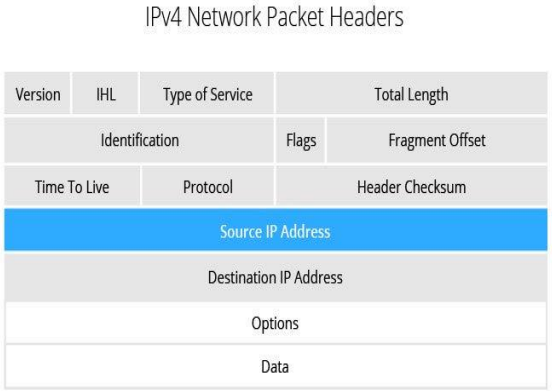

Figure 1: IPv4 network packet headers and focused on the Source IP Address

Then, the attack really begins when the attacker is able to identify, replicate, and falsify the content in the source IP header. This happens because of the clarity one might have when analysing the network logs of the target user, see Figure 2.

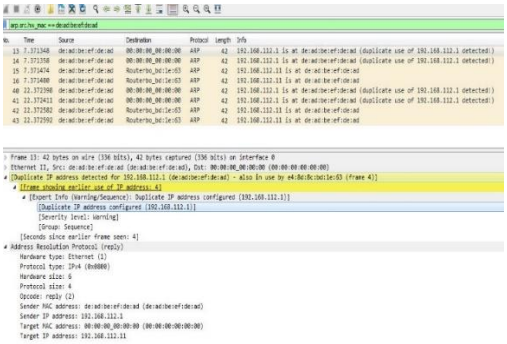

Figure 2: Network logs of an ARC network traffic having the IP Source header falsified by the attacker

Finally, the attacker may be able to send malicious data to the user indirectly, from a main server, for example. This can be done to achieve different abstract attacks, such as the DoS mentioned in the first section, as shown by the diagram in the Figure 3 bellow.

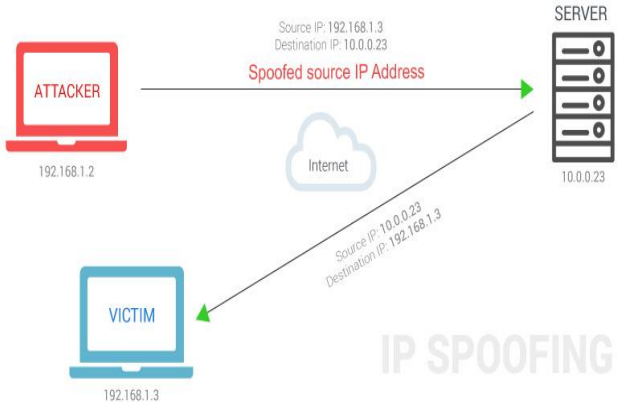

Figure 3: Diagram of an IP Spoofing attack as described

2.2 TCP Authentication

The TCP protocol is the base, together with UDP, of the TCP/IP model to higherprotocols. It has a simple handhsake structure.

This structure is called the “three-way handshake”. It begins by the client sending a request of synchronization, called SYN. Then, the server receives the synchronization process, SYN, accepts, and sends to the client another request of synchronization and a request of approvement of the first SYN, called ACK (acknowledgement). Finally, the client sends a final ACK request to the server and they estabilish a connection, see Figure 4.

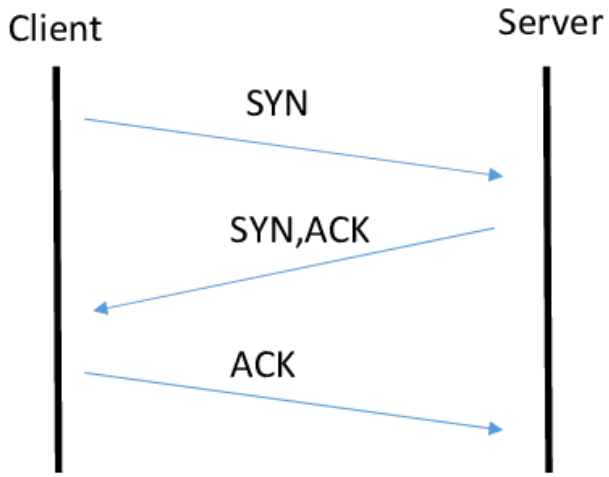

Figure 4: TCP 3-way handshake diagram

The issue on this handshake is simple: There is no authentication at all. The process is intended to create and estabilish a stable connection. However, as is possible to see in the whole TCP/IP system, there is no focus on a possible security, meaning that everyone on the network would be able to see the data transfer by itself.

After, some solutions were presented and will be cited in a future section. However, the original design did not consider any type of basic security.

2.3 Session Hijacking

The session hijacking attack can be caused by different vulnerabilities. Some of them have been mentioned before, such as the MITM and the TCP lack of Authentication.

This attack, as suggested by the name, happens when the attacker gets control of the session and session token of the victim.

Although there are multiple ways of doing this attack, all of them have something in common: The lack of cryptography. The lack of authentication and privacy provided by a cryptographic algorithm lets attackers manipulate an user’s session at their own will, see Figure 5.

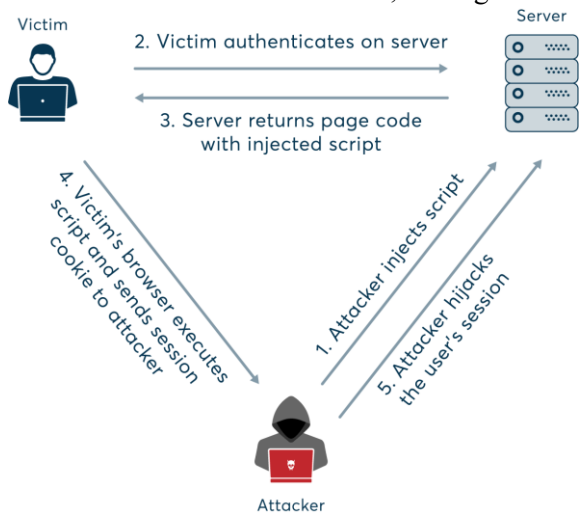

Figure 5: Diagram of the session hijacking attack in the TCP/IP model

3. TCP/IP Applications specific threats

In this section, it will be discussed the common attacks related to specific TCP/IP applications and their impacts in modern society.

- Telnet
- HTTP
- FTP
- ARP

It is important to remark that these specific applications, such as ARP, Telnet, and HTTP, are still commonly used nowadays and let diverse users vulnerable to a great variety of attacks.

3.1 Telnet

Telnet is a tool developed in 1969 and thoroughly implemented with the TCP/IP protocol suite. This tool works as a client-server based protocol that enables character-oriented data exchange through TCP connections. In other words, it enables an user to access and control another computer with text inputs, see Figure 6.

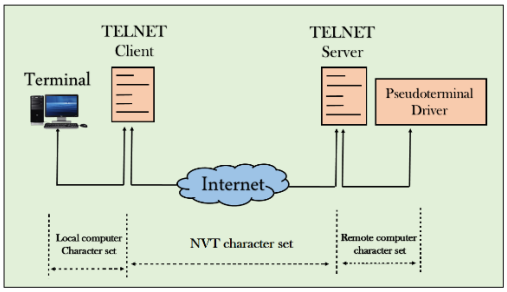

Figure 6: Telnet client-server protocol diagram

Additionally, because Telnet was implemented in the origins of TCP, it has its own low port number, the TCP 23.

3.1.1 Telnet Breaches

Telnet has some alarming flaws that have been found in the last years. First, it does not use any security mechanism of authentication, such as an RSA implementation. Second, and more important, the data is transferred through plain-text form.

In other words, any data, such as user and passsword, included in the protocol transfer is sent in plain-text through the connection. This means that anyone that is capable of viewing this data transfer, i.e. intercepts the message, will be able to take control over the other computer and quickly escalate the privileges, see Figure 7.

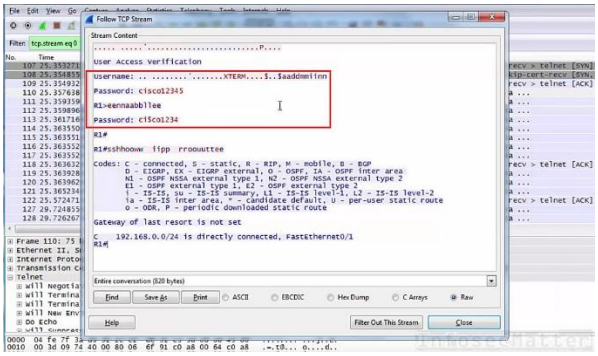

Figure 7: Network logs of a Telnet connection being sniffed

Additionally, a trojan or old application can open the ports and create a backdoor on telnet easily, putting the user in this great risk on the outdated protocol.

Because of these issues, one modern technology has been proposed and partially implemented, the Secure Shell (SSH).

3.1.2 Telnet V. SSH

The SSH was created with the idea of replacing the old Telnet protocol.

In order to address the issues of authentication and confidentiality, the SSH had a new tool added, called the PKI [4] (Public Key Infrastructure).

The way the PKI works is by performing a type of encryption based on two keys, a public and a private one. They, respectively, will encrypt or decrypt the respective data.

The infrastructure has the idea of making a trusted party sign the document associating the private key (that is the called certificate authority or CA). These documents are called certificates for the same reason. With these, the user can be sure that the message had complete integrity from the host, and the host can be sure that the user is legitimate, see Figure 8.

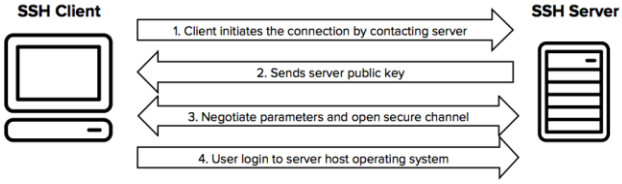

Figure 8: Diagram of the PKI implementation in the SSH protocol

The SSH then uses these certificates to authenticate the host and the users, making their connection confidential and authenticated, solving the issues of the Telnet.

3.2 Hypertext Transfer Protocol (HTTP)

The HTTP is one of the most used protocols of the last decade. With the advancement of the use of the internet, websites have been the core of the modern world.

The Hypertext Transfer Protocol was created in 1991 with the idea of advancing the World Wide Web project. It is, then, an application layer protocol that allows users to transfer data in the web.

As a request-response protocol [5], the HTTP works by sending hypertext messages between the client and servers. In this way, the protocol uses TCP connections to establish these connections and transfer the data in HTML, the language that used this new technology called the hypertext, see Figure 9.

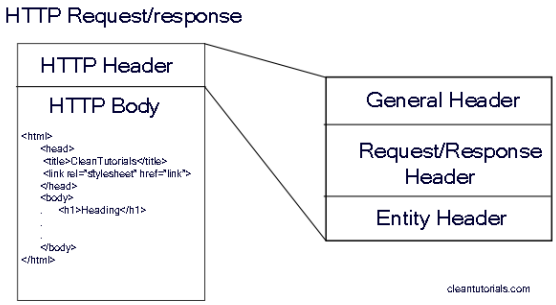

Figure 9: HTTP Hypertext message format in HTML

Additionally, the HTTP uses some request methods to perform specific tasks. Some of these methods are the “GET”, “POST”, and “DELETE”, which compose most of the HTTP connections, see Figure 10.

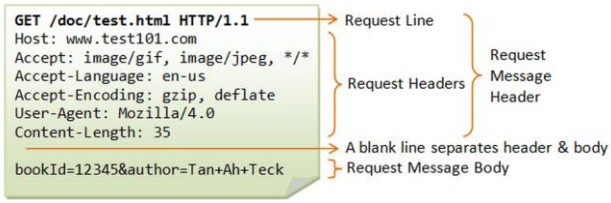

Figure 10: HTTP request message with specific “GET” method

3.2.1 HTTP Breaches

Although the protocol seemed like a savior and extremelly modern idea, the same is outdated and has a lot of security breaches that are still being addressed.

First, similar to Telnet, some of the breaches are related to the fact that HTTP was designed to send plain-text messages. This made any malicious individual have access to important data transferred between two users.

Second, the HTTP protocol is not encrypted in any sense. Not only it sends plain-text messages, but they are unveiled for any person to access and disturb its content, see Figure 11 for an example of attack.

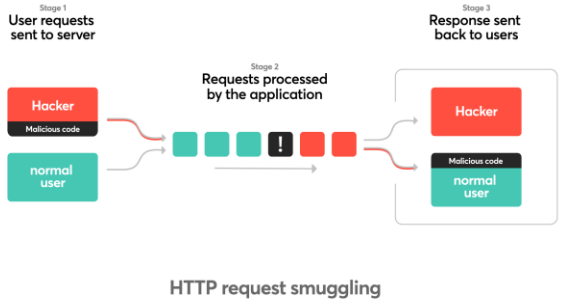

Figure 11: A diagram on the request smuggling attack on the HTTP

Because of all these breaches, the Open Web Application Security Project institution (OWASP) has highlighted the top 10 security risks [6] related to web development, being most of them derived from the HTTP issues.

3.2.2 Hypertext Transfer Protocol (HTTP) and the SSL/TLS

To solve the issues of the HTTP and other similar protocols, two technologies were developed in sequence, the SSL (Secure Socket Layer) and the TLS (Transport Layer Security).

The SSL was a cryptographic protocol that had the intention of increasing the security between user and server in explicit connections.

The TLS was created as a new version of the same, but focused on implicit connections (protocol oriented).

With the use of this new SSL/TLS cryptographic protocol, the HTTP was improved significantly. A new name was given to this new technology, called Hyper Text Transfer Protocol over Secure Socket Layer (HTTPS). This created a protocol that was better suited, although still with some issues, to modern society, see Figure 12.

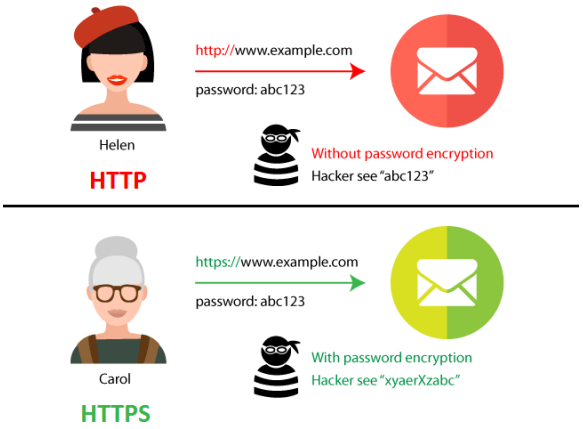

Figure 12: Diagram of a MITM attack on HTTP and HTTPS with the highlighted differences

3.3 File Transfer Protocol (FTP)

FTP is a client-server protocol that relies on two communication channels and has the intent of, as the name suggests, helping in the transfer of file type of data across a connection.

These two communication channels are the Control Connection and the Data Connection. The first is the client side of the protocol, where the user sends a request by an application to the server's port 21, while the server answers through the port 20. The second is the data side of the protocol, being a channel only used to transfer the file from one side to another, see Figure 13.

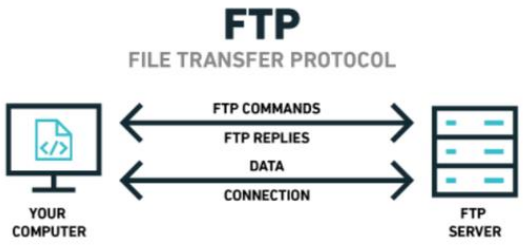

Figure 13: FTP diagram with the two different connection channels

3.3.1 FTP Breaches

Similar to the issues mentioned before, the FTP protocol was designed in an old time. Because of this, the same did not have any encryption in mind.

This is clearly a huge vulnerability, since the same does not encrypt the traffic of usernames, passwords, or any sensible data. As a conclusion, the plain FTP is vulnerable to packet caputre, MITM attacks, sniffing, etc., see Figure 14.

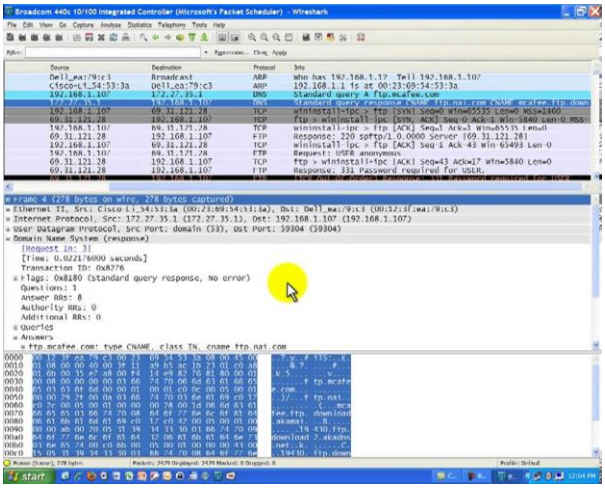

Figure 14: Network logs of FTP packet capture

3.3.2 The Secure FTP

The FTP, then, needed a secure connection between two parties. This was found at the mentioned SSH that solved most of the Telnet's issues.

With the combination of the SSH technology and the FTP protocol, the Secure File Transfer Procotol (SFTP) was created. The SFTP uses only the port 22, decreasing firewall holes, and is basically a data tunelling of an SSH connection in a server technology, see Figure 15.

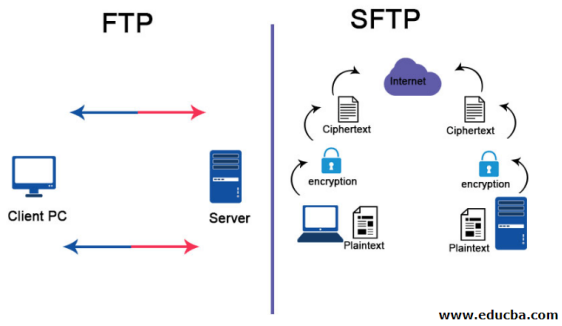

Figure 15: FTP and SFTP connection diagrams

3.4 Address Resolution Protocol (ARP)

The ARP was created with the introduction of the Internet Protocol. When the connections demanded an use of a dynamic protocol, the old MAC address needed a new tool to keep working. This was the Address Resolution Protocol (ARP).

This protocol was designed as a procedure that connected ever-changing IP addresses to their respective physical machine addresses (the MAC) in a local area network, see Figure 16.

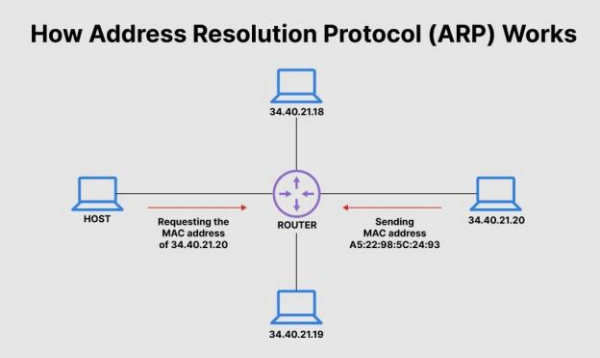

Figure 16: The ARP procedure diagram

3.4.1 ARP Breaches

The ARP was created in 1982 [7] and the creators did not have any type of authentication security method in mind. Because of this, any device can answer an ARP request, even if they are not the intended receiver.

This made a variety of attacks possible, such as ARP Poisoning, or ARP Spoofing, which is when an attacker intercepts the communication between two devices, disrupting, redirecting, or manipulating it at their own desire, see Figure 17.

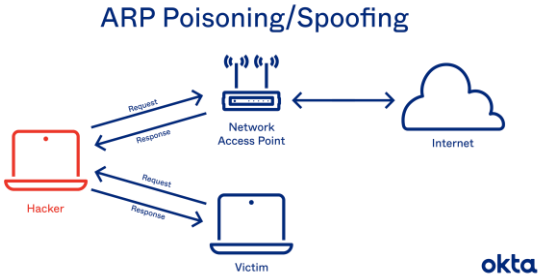

Figure 17: ARP Poisoning diagram

4. New technologies to improve the TCP/IP suite

In this section, other technologies that will probably be implemented or popularized in the future years will be mentioned, such as:

- IPSec/IPv6
- AES
- SF Block Cipher

Some of these tools, such as the IPv6 are in the beginning of the implementation, while others, such as the SF, were proposed in recent researches.

4.1 The revolution of the IP (IPSec/IPv6)

The first set of changes that are going to be discussed are the IPSec and the IPv6. These are clearly the most prominent and important changes on the TCP/IP model in the last decades.

First, one needs to understand the importance of the IPv6. Most devices in modern

society still use the outdated IPv4. As stated by Google [8], for example, an average between 32 and 37% of their users have IPv6 enabled. That means that around 63% of the other Google users, for example, are necessarily using IPv4.

This shows that the IPv4 is still the most used Internet Protocol version, and we should be afraid of it.

As shown in section 2.1, the IPv4 has some great vulnerabilities, mainly the IP Spoofing shown. This is because the IPv4 was designed without security in mind.

The IPv6 was designed with end-to-end encryption, making MITM attacks more difficult [9]. Additionally, the IPv6 supports more secure-name resolutions. As a comparisson to the section 2.1, the IPv6 header also makes IP Spoofing attacks improbable, with a great memory and specific separation and encryption to avoid the same, see Figure 18.

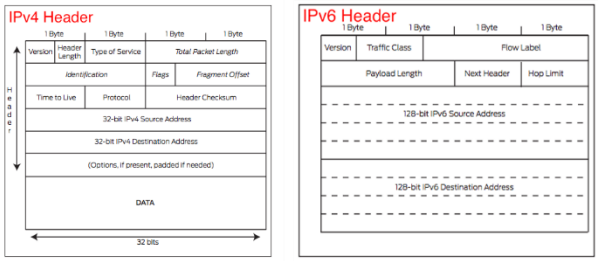

Figure 18: IPv4 and IPv6 headers comparisson

Finally, the IPv6 was included with native support to specific cryptographic algorithms, such as the famous IPSec.

4.1.1 The IPSec

The Internet Protocol Security (IPSec) is a secure network protocol suite that focus on specific authentication and encryption of data packets. It is used, for example, in the famous modern Virtual Private Networks (VPNs).

In its creation, the IPSec was a native protocol of the IPv6, working better in the same. It estabilishes a connection of end-to-end encryption for host-user, user-user, and host-host arquitectures, such as what a VPN does, see Figure 19.

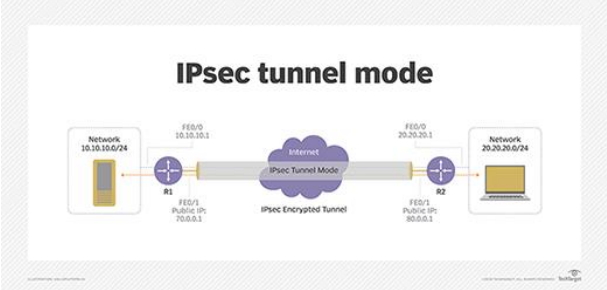

Figure 19: IPSec diagram of the end-to-end encryption in the "tunnel mode" (similar to VPNs)

4.2 The Advanced Encryption System (AES)

This technology is a standard symmetric block cipher that was first published in 1998 and is getting a wide adoption rate in the last years.

This standard was not specifically designed for TCP/IP but works with the suite properly. The same is used with modern APIs, VPNs, and XML transactions. It works, most of the times, with the RSA encryptions. While the AES is a symmetric key cipher, the RSA is an asymmetric one, meaning that both can work at the same time.

As a block cipher, the AES uses a secret key to encrypt data in an array. From there, a cipher is created in a block that includes the text and the key. After that, some shifting in the array's data rows are done, and a final cypher text block is created, see Figure 20.

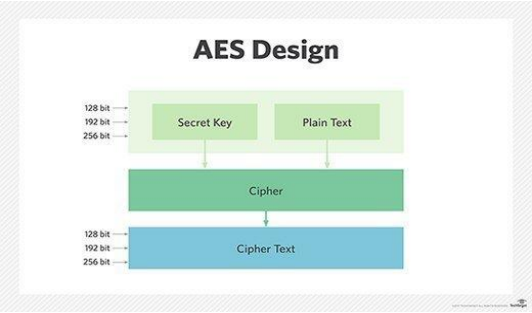

Figure 20: AES Cipher design diagram

4.2.1 The SF Block Cipher

Based on the old Blowfish and the new AES block ciphers, researchers have been trying to create a new and better block encryption standard.

The most prominent one in the recent years has been the SF block cipher [10], published by Annand Kumar and Dr. Karthikeyan in 2011.

This cipher worked in a similar way as the AES and Blowfish ciphers. However, the specific choice of shifting 512 bits and additional changes made in the project made the SF block cipher more adaptated to a great amount of data used in some situations (also future tendencies). This included a better throughput analysis the bigger the data size was, see Figure 21.

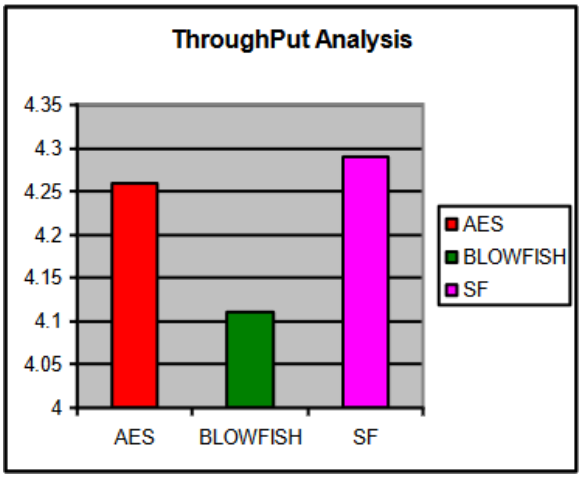

Figure 21: Throughput analysis of the encryption of the SF, AES, and Blowfish algorithms

5. Conclusion

It is clear that the most used protocol suite of modern times, the TCP/IP, has not been designed with any type of security in mind. However, some changes and new protocols have been done, proposed, or are in the middle of the change by the time this paper was written.

Furthermore, it is expected that modern connections will get safer in the future decades and the algorithms cited in this paper will be commonly used. An adhesion to the IPv6 protocol and a greater switch from the FTP to the SFTP are extremly important for this improvement in internet connections.

Finally, the TCP/IP model is in a constant change and is achieving a safer state. It is also important to remark that, maybe, in the future, a new protocol suite might be proposed and some of the modern issues corrected.

References

[1] IC3, “2020 Internet Crime Report,” FBI NationalPress Office, Washington, D.C., USA, Mar. 17 2021[Online]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

[2] Steven M. Bellovin, “A look back at ‘SecurityProblems in the TCP/IP Protocol Suite’”. AnnualComp. Sec. App. Conference, Dec. 2004. [Online].Available: https://www.cs.columbia.edu/~smb/papers/acsac-ipext.pdf

[3] “Cisco Annual Internet Report (2018–2023) WhitePpaer”, Cisco Systems, Inc. , San Jose, CA, USA. Accessed: Oct. 27, 2021. [Online]. Available:https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

[4] “What is PKI (Public Key Infrastructure)?”, SSH Academy, Accessed: Dec. 6, 2021. [Online]. Available: https://www.ssh.com/academy/pki

[5] “Hypertext Transfer Protocol (HTTP)”, ExtraHop protocol support library, Accessed: Dec. 6, 2021. [Online]. Available: https://www.extrahop.com/resources/protocols/http/

[6] “OWASP Top 10:2021”, Open Web Application Security Project Foundation

(OWASP), Sept 24, 2021 [Online]. Available: https://owasp.org/www-project-top-ten/

[7] Robert Grimmick, “ARP Poisoning: What it is & How to prevent ARP Spoofing attacks”, Varonis, Accessed: Dec. 7, 2021. [Online]. Available:https://www.varonis.com/blog/arp-poisoning/

[8] “Google IPv6”, Google LLC, Accessed: Dec. 9, 2021. [Online]/ Available: https://www.google.com /intl/en/ipv6/statistics.html#tab=ipv6-adoption

[9] Jason Andress, “IPV6: the next internet protocol”, April 2005. [Online]. Available:www.usenix.org /system/files/login/articles/1027-andress0504.p

[10] Anand Kumar.M and Dr. S. Karthikeyan, “A New 512 Bit Cipher - SF Block Cipher”, International Journal of Computer Network and Information Security, Vol. 4[11], 2011, pp. 55-6