Report on cyberattacks

Chapter 1 : Whats is a cyberattack ?

Chapter 2 : Three computer attacks in practice

Chapter 3: Defences and solutions

Authors :

Boris ANODEAU
Flavien HANICOTTE
Marine HERVET

Supervisor:

Lyes KHOUKHI

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

GREYC

CONTENTS

FIGURES

CHAPTER 1: WHAT IS A CYBERATTACK?

1. Definition of a cyberattack

1.1. Definition, targets, interests and consequences

The term cyberattack has multiple definitions which may differ on certain points. We will here give a single definition with which we will stick throughout this report and develop around it. A cyberattack here designates an "attempt to expose, alter, disable, destroy, steal or gain unauthorized access to or make unauthorized use of an asset".

Cyberattacks can be conducted by a wide variety of attackers. These attackers can range from single individuals to entire organisations **[1]**. While single individuals will tend to conduct such attacks to gain money or to uncover some data, wider organisations can have other interests. As cybersecurity became a mandatory domain, nearly all governments created a cybersecurity division, and some even created specialized groups to conduct cyberattacks on foreign countries or organisations. The motivations of such groups can be economical, political or even military. While reasons differ, cyberattacks can target everyone : individuals, administrations, NGOs, companies, ranging from small start-up to multinationals.

All types of computer systems are exposed to cyberattacks, including servers, websites, networks, operating systems, routers, switches, etc. Each cyberattack exploits a certain type of flaw within the targeted computer system. As an example, malicious software can only be executed to gain access to the target on a system lacking antivirus software and proper access permissions. But it should also be reminded that successful cyberattacks, while taking advantage of machine flaws, usually involve inappropriate human behavior at a certain stage of the attack (Before : poor permissions, badly-configured firewall, etc. ; During : clicking on an unknown link sent by an unknown source, executing suspicious pieces of software, not alerting competent authorities, etc. ; After : still not contacting competent authorities, obeying the attackers' instructions, etc.). Such vulnerabilities have rendered cybersecurity measures and services indispensable, such as regular updates for both hardware and software in order to correct discovered flaws. While many flaws can be corrected, some attacks also make use of some specific system processing (regarding for example memory) that are mandatory for system functioning and that cannot be modified.

1.2. Active and passive attacks

Cyberattacks, while being specific to the type of system they are targeting, can be divided in two types : active and passive attacks.

1.2.1. Passive attacks

A passive attack designates an attack performed using only passive tools, i.e tools that do not tamper with the usual functioning of the targeted system **[2]**. Such passive attack can allow the attacker to steal or gain unauthorized access to the asset without extensive action. In such a situation, the attacker is only an observer. One of the main forms of passive attacks is *Traffic Analysis*, analysis of pieces of data exchanged on the network. It should be noted that communication encryption is a necessity in our current world. Another one would be *keylogging*, when the attacker recovers the keyboard inputs of a target in order to get relevant information such as passwords.

Passive attacks can also be a prelude to a following active one, the attacker taking advantage of the first phase to passively acquire data on the targeted system or individual.

1.2.2. Active attacks

Active attacks, as opposed to passive ones, will tamper with the targeted system **[3]**. This type of attack may weaken the integrity of the targeted asset, but such fact can be an advantage if the attacker's objective is to destroy, damage or make inaccessible the targeted asset. With this type of attack, the victim may become aware of the attack by noticing some modified or lost data, or an unusual behavior of the system.

1.3. Steps of an attack process : Kill Chain

Each cyberattack, either passive or active, either and inside or an outside one, follows a certain chain of events that only has small variations **[4]** : **The Kill Chain.**

The kill chain is divided in phases which describe the parts of the attack process.

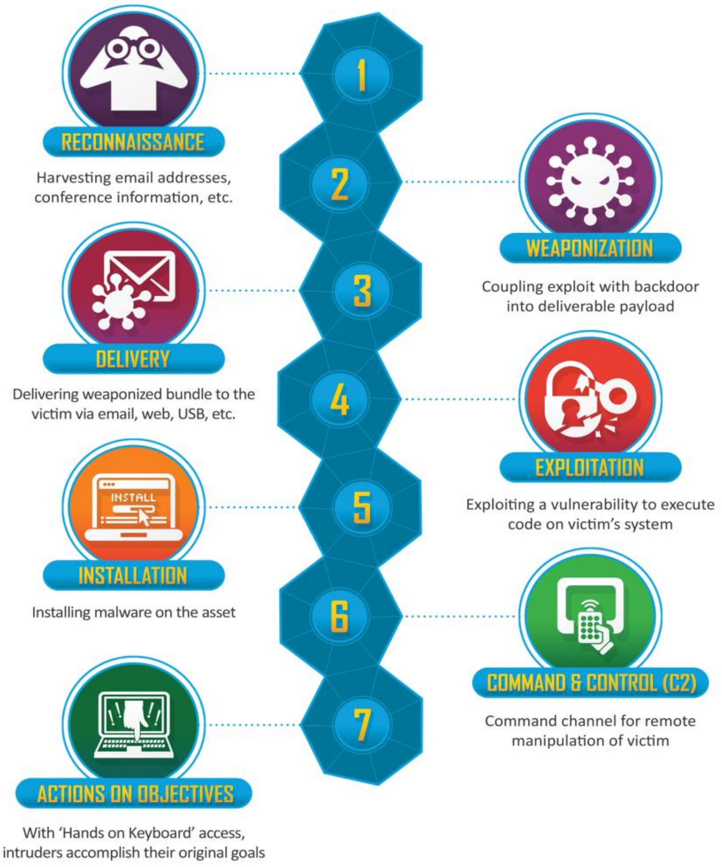

1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

Figure 1 Kill Chain **[5]**

1.3.1. Reconnaissance

The objective of this phase is to identify, learn and collect relevant data about the target. Multiple means can be used to achieve this first phase : social networks, online activity, technological and/or personal environment.

1.3.2. Weaponization

After acquiring the needed data to conduct the attack comes the development phase of the attack tools : the weapon. All relevant tools are created and settled up during this phase, including the needed pieces of software (viruses, trojans, malicious files, etc) related to the entry point chosen.

1.3.3. Delivery

The weapon is in this phase transmitted to the target, whether via files, emails, websites or trapped usb keys. At the end of this phase, the weapon can act on the targeted system.

1.3.4. Exploitation

During this critical phase, the weapon tries to exploit the chosen flaw and/or means of entry in order to access the target in the desired way. It either exploits a technological flaw or a human one. It is to be noted that if this phase fails, so does the overall attack.

1.3.5. Installation

Once access is obtained, the weapon will establish means to keep access to the target system.

1.3.6. C2-Command & Control

Once access is established and secured, the weapon will establish, through different means, “hands on keyboard access” to the remote attacker, in order for the latter to be able to finish the attack process.

1.3.7. Actions & Objectives

As all the six previous steps are completed, the attacker now has access to the asset within the targeted system and can perform the desired action with it : exfiltration, destruction, or another attack using the now controlled system.

2. Attackers

2.1. Black, grey and white hats

At first the term hacker designated an expert in computer sciences or a skilled computer programmer. For example Linus Torvald (the creator of Linux) can be considered, by some, as a hacker.

It now refers more to what is called a security hacker. Those ones use known or unreleased bugs and exploits to break into computer systems and access what is supposed to be private or restricted. That word includes experts but also "script kiddies", these are people that use known online malwares or exploits tools without knowing how they work. **[11], [12]**

We will here describe three types of expert hackers : black, white and grey.

Black hats are a part of the mainstream representation of the word "hacker" also known as "crackers", they are criminals that use their knowledge in order to get information or get access to a computer system for illegal purposes.**[6], [12]**

Grey hats are people between black and white hats. Their behavior is difficult to determine as they are not only malicious people: they can either fix and or exploit a security breach. The main difference between grey and black hats is that a grey hat will not use an exploit to make profits. They mainly hack for fun or for "troll" (which means making fun of or discrediting someone). **[6], [12]**

White hats are professional hackers that aim to keep data and computer systems safe from other hackers. They are hired by companies that want to protect their system (often insurance companies, banks or the government). **[6], [12]**

2.2. Goals for attackers

There are multiple reasons why black hats are hacking. The most common is personal accumulation of wealth. Money is often related to data, as a hacker is able to get access to restricted areas in a system, they can also access and get private data and sell it. Thus they can steal financial, credential or login information. **[11], [12]**

The target can be a normal person or a company depending on the hacker's abilities. There are also cases of spied companies: the hacker gets information from a company and sells it to its rival.

The second goal of a hacker is to make someone lose money without earning direct benefits for himself, by attacking a company or a big website, disabling their website or data servers. An attacked company can lose millions of dollars because of a server or website down. For example in 2016 the DNS Dyn was attacked with a DDOS attack which disabled it for a day: the loss is estimated at 110 millions dollars. **[6], [8]**

2.3. Famous attackers

2.3.1. Black hats

As explained before, hackers can be groups or individuals. Although we often think they are shy guys coding alone in their garage, there are some very popular groups of hackers such as “Anonymous”, “GlobalHell”, “Bureau 121”, “Lizard squad”, “Lulzsec”.

One of the most famous former black hats is Kevin Mitnick.He is now an information technology consultant at Mitnick security consulting to advise on cybersecurity. **[7]**

Another famous black hat is Evgeniy Mikhailovich Bogachev, the author of the ransomware Gameover ZeuS. The FBI set a bounty of 3 millions dollars for whoever helped to arrest him. **[9]**

Figure 2 Anonymous Logo **[13]**

Figure 3 Kevin Mitnick **[14]**

2.3.2. White hats

On the opposing side, there are also some well-known names in white hats.

Dan Kaminski is the most famous white hat hacker: he found a big breach in DNS protocol Also, Charlie Miller has been able to break into a remotely controlled car’s system and control it entirely. His discovery led to the recall of 1.4 million cars. **[15]**

One should also note the name of Tsutomu Shimomura who helped the FBI to catch Kevin Mitnick. **[15]**

Figure 4 Charlie Miller **[16]**

Figure 5 Dan Kaminski **[17]**

3. Context of some major attacks

3.1. Most used attacks

3.1.1. DoS and DDoS

The DoS (Denial of Service) attack takes advantage of the limited capacity of the network or server. The goal for the attacker is to overload the server or channel to slow down or to render a service unavailable. Thus, the attacker sends a huge number of requests that the server cannot handle, or increase the number of packets in the channel to saturate it and render the server unreachable. Targets can be any entity with an online activity. **[18], [19]** A DDoS (Distributed Denial of Service) attack is based on the same principle, but here the attacker uses a network of "zombie machines", i.e. an arsenal of infected machines that he remotely controls to multiply the number of requests. This type of attack is constantly increasing, with millions of attempts every day worldwide, with volumes of hundreds of gigabits/second and rates of tens of millions of packets/second sent to the target. Nowadays, it is even easier to carry out these attacks because of online ready-to-use tools called booter or stresser. **[20]**

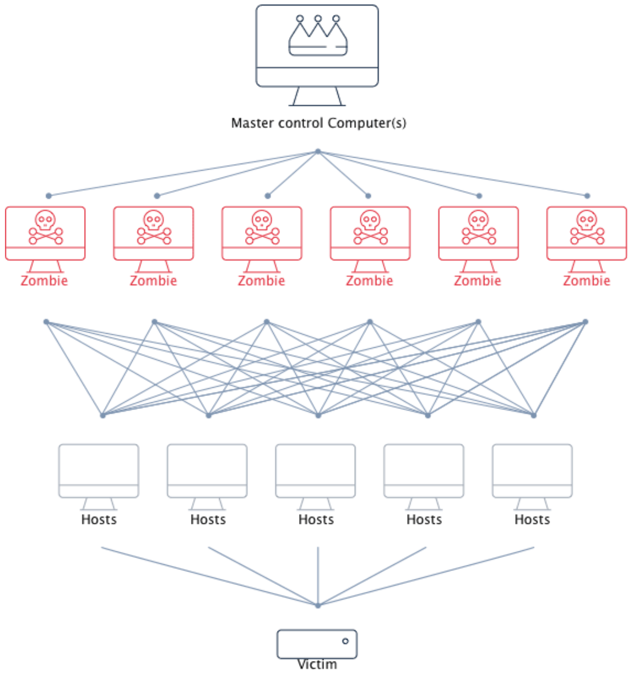


Figure 6 DDoS Attack **[21]**

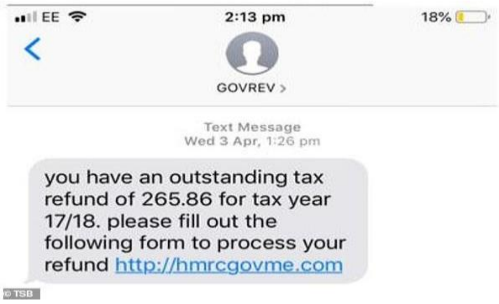
3.1.2. Man-in-the-middle

This hacking technique consists in intercepting communications between two individuals without them being aware that they are being spied on. This is a very effective attack for example for key exchanges without authentication. Once infiltrated into the network, the attacker can carry out passive or active attacks: he can read but also modify communications. **[18], [19]** The most commonly used attacks in this family of attacks are ARP Spoofing (the attacker pretends to be a router), DNS Poisoning (the attacker tampers with the DNS server to redirect communications to it) or network traffic analysis via a sniffer. **[22]**

These techniques will be discussed in more detail in Chapter 2.

3.1.3. Phishing & Spear Phishing

Phishing attacks use communication tools to spread links of malicious documents at large-scale. The attacker is hoping that the victims will fill out the fake form to recover their personal or login data, or that they will download an infected attachment. The Spear Phishing approach is similar but the attack is extremely targeted and aims at a specific person. Here, the attacker investigated his victim through social engineering (via web research, Linkedin, Facebook, etc.). to usurp the identity of someone the target knows. **[18], [19], [23]** Usually this is an immediate superior or a service the person subscribes. The message often mentions very short deadlines or serious consequences if this is not done quickly, urging the victim to act immediately. **[24]**



Text Message
Wed 3 Apr, 1:26 pm

you have an outstanding tax refund of 265.86 for tax year 17/18. please fill out the following form to process your refund http://hmrcgovme.com

Figure 7 Phishing Attack **[25]**

3.1.4. SQL Injection

SQL queries are used to manipulate and query a database to fetch information. A SQL injection attack consists of inserting malicious SQL queries into a web application to access or destroy data in the database. The most common way is to fill out a login form by providing an SQL condition that is always checked. **[26], [27], [28]**

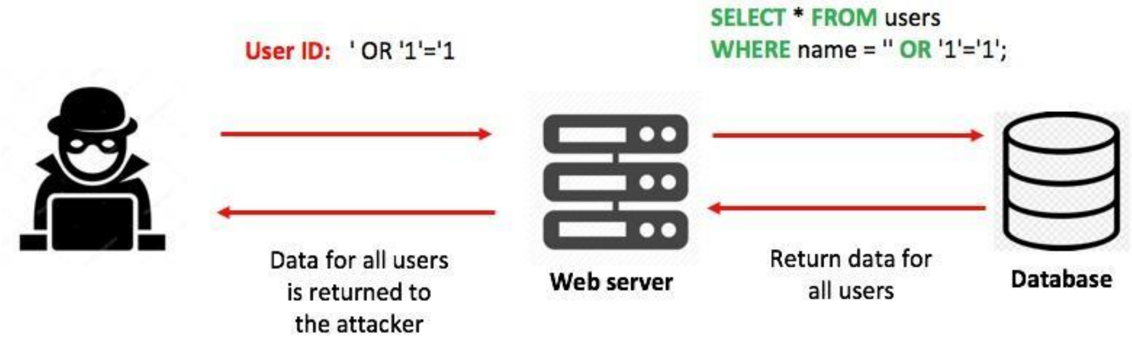

User ID: ' OR '1'='1
SELECT * FROM users
WHERE name = '' OR '1'='1';
Data for all users is returned to the attacker
Web server
Return data for all users
Database

Figure 8 SQL Injection Attack **[29]**

3.2. Famous and historic attacks

3.2.1. Project Rivolta: Mafia Boy

Michael Calce, nicknamed Mafia Boy, was 15 years old when he carried out a DDoS attack in February 2000 and blocked the entire Internet. He has thus rendered the leading search engine Yahoo! (in these times) unavailable for an hour and also Amazon, CNN and Ebay. The teenager had just modified a script found online by adding the IP addresses of the sites he was targeting and created an arsenal of 200 zombie machines from an university network. The losses are estimated to be in billions of dollars. **[30]**

Figure 9 Michael Calce alias Mafia Boy **[31]**

3.2.2. Heartland Case: SQL Injection and Man-In-the-Middle attack

Heartland Payment Systems is a company managing online banking and payment transactions. During 2008, the hacker Albert Gonzalez, with the help of two Russian accomplices, infiltrated the network of Heartland and other financial services companies thanks to SQL injections. Once in the network, the attackers set up sniffers to detect and steal banking data circulating on the network. The group of hackers thus recovered more than 130 million bank numbers just from Heatland, before reselling them. **[30],[32]**

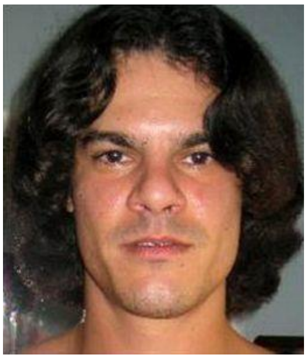


Figure 10 Albert Gonzalez **[33]**

3.2.3. Stuxnet

Stuxnet is a malware discovered in 2010 jointly designed by the United States and Israel to slow down the Iranian nuclear program. It was estimated that its development began between 2005 and 2006. Stuxnet exploited 4 new vulnerabilities on the Windows operating system, also called "0-day" vulnerabilities. The worm was designed to replicate itself and infect all the machines in the network. He then tries to detect whether software developed by Siemens controlling centrifuges for uranium enrichment was installed on the infected machine. In this case, the malware installs a rootkit in the machine's operating system to change the software's settings in order to destroy the centrifuges and thus slow down enrichment. It is estimated that this malware has destroyed about 1000 over 5000 centrifuges. The worm then spread to many countries but some removal tools were provided, including one from Siemens. **[34],[35]**

CHAPTER 2 : THREE COMPUTER ATTACKS IN PRACTICE

1. ARP Poisoning

1.1. Principle of the attack

ARP Poisoning (also known as ARP Spoofing or ARP Cache Poisoning) is a type of network cyberattack, that can be both active or passive depending on the attacker's intent. The attack, as the name implies, is based on ARP protocol, which is used inside a LAN in order to associate MAC addresses with matching IP addresses in order for the router to send traffic to the proper destination **[36]**, **[37]**, **[39]**.

This attack is a *Man in the Middle* attack, as the attack fools both the host and the target in order for data to transit through the attacker's machine by sending ARP response packets.

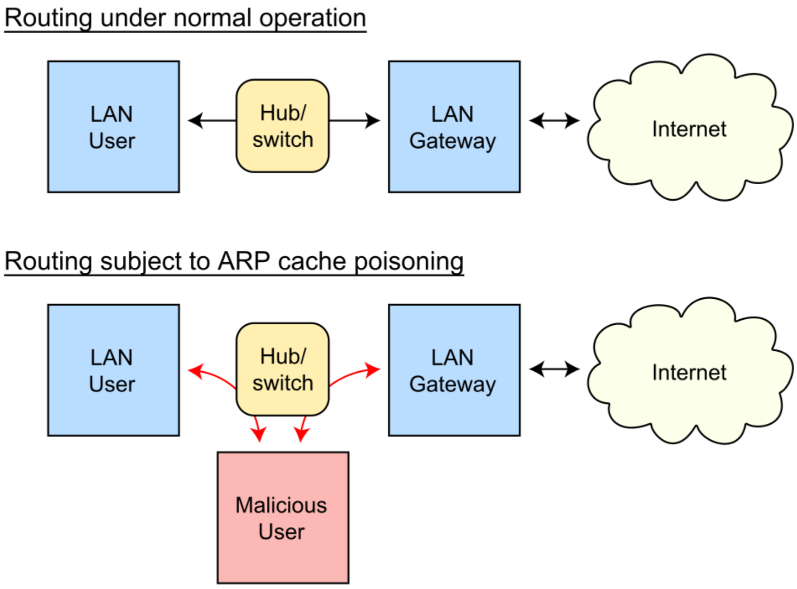


Figure 11 ARP Poisoning **[36]**

1.2. ARP Protocol

ARP (Address Resolution Protocol) is a telecommunications protocol used inside a LAN (Local Area Network) in order to associate IP addresses (Network layer) to MAC addresses (Data Link layer), in order to divert the right internet traffic to the designated machine inside the network. **[38]**

ARP protocol is generally used to contact the gateway or router used to connect to other networks and the internet. Such gateway or router (the Host) keeps a table (ARP cache) linking IP and MAC addresses, in order to forward traffic to the right target. When traffic to an unknown IP address is received, the Host sends an ARP request on the network, waiting for the answer of the machine with the right MAC address. As ARP has been designed for speed and not security, it does not natively integrate any form of authentication, making it a privileged attack point for attackers. Also, one of the critical flaws exploited by an ARP Spoofing attack is the fact that hosts will accept ARP response packets even though they have not sent any request.

1.3. Steps of the attack

1.3.1.Reconnaissance

As with every cyberattack, this phase consists in gathering as much intel as possible on the target in order to plan the proper attack on the system. As direct access to the targeted network is required to conduct the attack, it comes in handy to have knowledge about the router or gateway used, as well as the protective measures on the network and on the different systems **[39]**, **[40]**.

1.3.2. Weaponization

The attacker here has the choice to either conceive its own tools or to use already existing ones, such as Arpspoof or Driftnet.

1.3.3. Delivery

The means of delivery will here depend on the possibilities and choices of the attacker. He can either choose to access the network with a machine that is already in it (in the case of an attack on the company, a computer of the company connected to the right network will do), or use his own and connect it to the network.

1.3.4. Exploitation

Once connected to the target network, the attacker needs to bypass the defenses set in order to make his ARP response packets accepted by the targeted host.

1.3.5. Installation & C2C – Command and Control

When connexion is established, the attacker already has "hands on keyboard" access to the target system, making Installation process unnecessary. The C2C process will only consist in bypassing defenses in order to maintain connexion.

1.3.6. Actions & Objectives

Once the connexion is securised, the *Man in the Middle* phase of the attack is completed, as the attacker has access to all the data meant to be sent to the target. While it can be the end of the attack in itself, such phase can be followed by other phases, such as a DoS (Denial of Services) attack by dropping received packets, modify the data forwarded, or perform session hijacking if a session ID is received.

2. DHCP & DNS Spoofing

2.1. What is spoofing ?

The term spoofing is used in digital communications such as phone calls, email, ip related communications (DHCP, DNS and ARP). This term designates the fact of disguising yourself as a known and trusted source in order to get all the data traffic. As you replace the supposed known source, you gain access to the traffic and so, you are not only able to listen to it but also falsify datas and spread malwares. **[41]**

2.2. DHCP Spoofing

2.2.1. DHCP Protocol

Dynamic Host Configuration Protocol is a network management protocol. It is used in Internet Protocols (IP). DHCP's goal is to distribute dynamically IP addresses to each system of a network. For example, a network that has fifty machines but only ten ip addresses to distribute can use a DHCP server. That server will dynamically distribute IP addresses and allow the network to use all it's machines. **[42]**

2.2.2. DHCP Starvation

DHCP starvation is an attack that aims to create a "new" DHCP server that will respond to all the requests of the network instead of the original DHCP server. You can realize a DHCP starvation attack by sending a lot of fake DHCP requests to the DHCP server using a spoofed IP. If the DHCP server responds to them he will run out of IP addresses to distribute, at this point you can create a rogue server that will respond to the network's requests instead of the original server. **[43]**

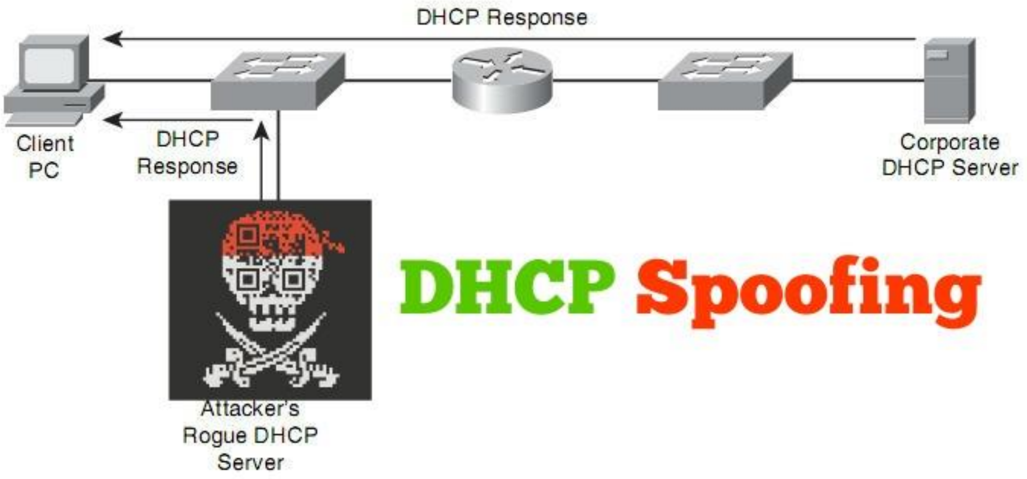


Figure 12 DHCP Spoofing **[44]**

2.2.3. DHCP Spoofing

Once that is done, we can begin the DHCP spoofing attack. As DHCP communicates with all the networks machines, it is kind of a hub of data. If someone can respond instead of the DHCP server, he can redirect the whole traffic and that is what we want to do in this attack. Once the rogue server is in place we can send requests and messages to the machines from the network to change their configuration, in particular their default gateway. Changing their default gateway will change the routing configuration and we can redirect the traffic to what we want (often the attacker's pc or a machine from outside of the network). We can now collect data, launch a man in the middle attack. For example broadcasting malwares in the network. **[43]**

2.3. DNS Spoofing

2.3.1. What is a DNS ?

DNS, Domain Name Server refers to the DNS server which is the internet phone book. Basically DNS will translate a site name (mostly URLs, for example http://google.com) into IP addresses. As machines can't communicate using URLs and humans can't memorize IP addresses, DNS links those two representations. As the servers make links between request and actual IP addresses you can think of a way to spoof it!

2.3.2. DNS Spoofing Attacks

DNS spoofing attack is the same as DHCP spoofing attack, you want to disguise yourself as a known source in order to redirect the traffic to you. There are multiple spoofing attacks: this following description is the DNS hijack attack. To perform DNS hijack attack , you need to access the DNS server and once that is done, you can change the DNS tables in order to redirect the traffic from a great website to a fake web site and gather data and credentials. **[45], [46]**

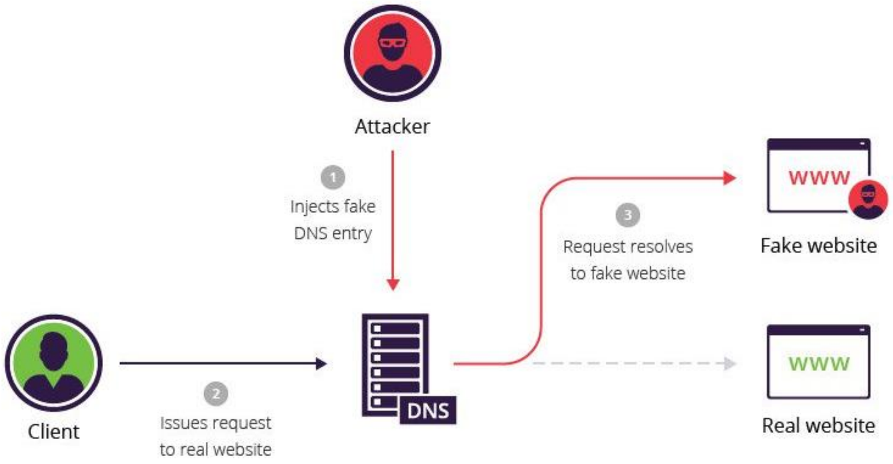


Figure 13 DNS Spoofing **[46]**

The second attack is the same but from the client side. This attack aims to redirect the traffic of the client only and make him think that he is on the real website. In order to do that you have to spoof the DNS server and communicate with the client instead of the DNS server. Once you spoof the DNS server, the client will communicate with you only and you are free to redirect him on a fake website. **[45], [46]**

3. VoIP Calls Listening

3.1. Difference between IP Telephony and VoIP

3.1.1. IP Telephony : a communication infrastructure

IP Telephony is a telephony infrastructure operating over IP thanks to an IPBX (Internet Private Branch Exchange). The IPBX connects the telephones and all terminals via the computer network. This infrastructure is mainly deployed in companies. This infrastructure enables unified communications by providing a collaborative platform with applications to communicate with voice, text and video (internal instant messaging app). **[47]**

3.1.2. VoIP: a protocol for voice transmission over the Internet Network

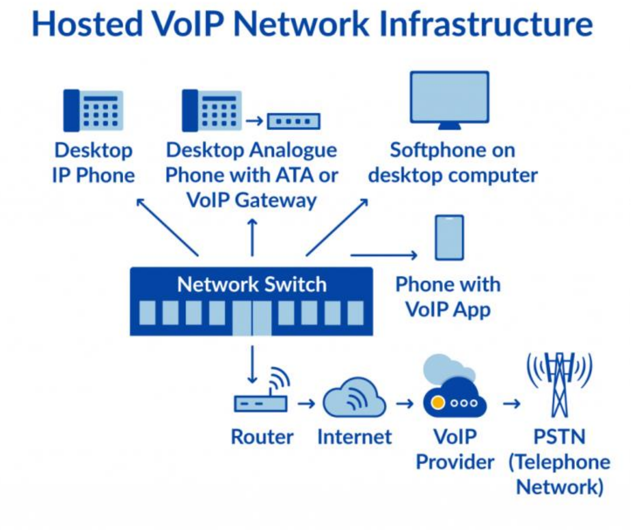

Hosted VoIP Network Infrastructure
Desktop IP Phone
Desktop Analogue Phone with ATA or VoIP Gateway
Softphone on desktop computer
Network Switch
Phone with VoIP App
Router
Internet
VoIP Provider
PSTN (Telephone Network)

Figure 14 VoIP Network Infrastructure **[48]**

VoIP (Voice over Internet Protocol) is a protocol used to transport voice streams over a data network. The voice is scanned to be converted into a decomposable digital signal. Then, the voice call is divided into data packets for transmission over the Internet network and will be brought together when it arrives. Thus, the voice is transferred by data packets like any data circulating on the web. This protocol was popularized by Skype in the 2000s. The difference with the conventional phone: the analog phone transforms air vibrations into an analog electric frequency and transmits them via the RTC network (Real-Time Communication) through analog lines via a phone socket. **[49]**

VoIP is only a change in routing protocol, it does not offer additional service, the tools used (landline) remain the same. It is the continuity of the analog telephone service that is going to disappear. The VoIP architecture is to be considered at the level of telephone subscriptions: VoIP subscriptions can be purchased from professional telecoms operators. Landline phones can therefore use VoIP via Internet Service Provider. VoIP relies on the

Internet connection to carry the voice, so the quality of the call will depend on the quality of the connection. For voice calls or video conferencing on a computer, one speaks of “softphone” for software phones, which involves the IP Telephony infrastructure. **[50]**

3.2. Protocols related to VoIP

The VoIP protocol uses 2 types of protocols:

- **Signaling**: SIP (mainly) -> management of exchanges between client/server
- **Media transport**: RTP -> routing media (voice or video)

3.2.1. SIP

SIP (Session Initiation Protocol) is a protocol used to initiate, maintain and terminate multimedia communication sessions. SIP packets can include voice or video data. It improves VoIP, supporting video conferencing, instant messaging and text. The SIP protocol can handle 4 roles: **[51][52]**

- **User Agent**: initiates and terminates sessions by transmitting requests and responses. This can be an UAC (User Agent Client) that launches requests or an UAS (User Agent Server) that contacts the users.
- **Proxy Server**: gateway that redirects requests between the UAC and the UAS.
- **Redirect Serve**r: in charge of redirecting calls when the physical location of an user has changed, is also useful to offload servers.
- **Registrar**: allows to save communication **[51]**

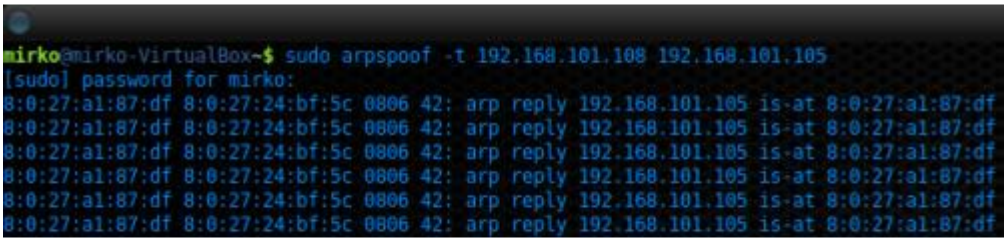
3.2.2. RTP & RCTP

RTP (Real-Time Transport Protocol) is a protocol considered as the standard for audio and video transport. This protocol is more suitable than TCP for example because it has a shorter transmission time because TCP promotes reliability to speed.

It is used in conjunction with the RTCP (Real-Time Control Protocol) which collects traffic statistics and provides access to Quality of Service (QoS). It is this protocol that collects the information about the jig, the latency period and the loss of packets. **[52]**

3.3. Listening VoIP Calls

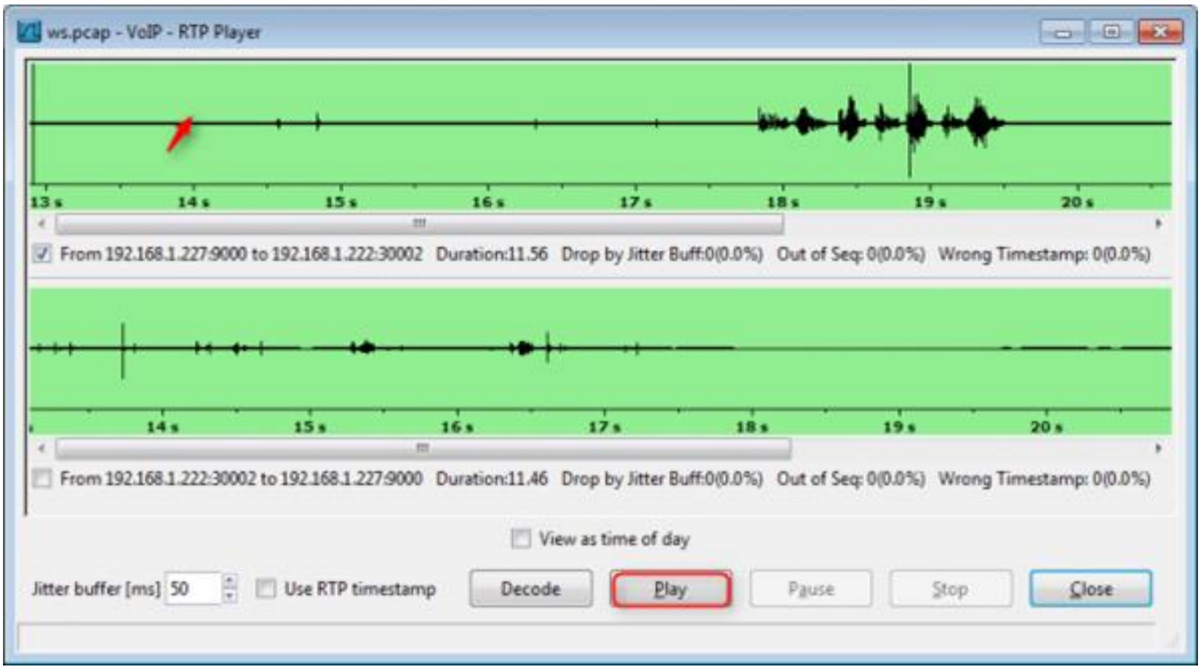
Eavesdropping consists in secretly listening to VoIP calls. The attacker captures SIP requests or the sent data through RTP protocol.
The first step of an Eavesdropping attack is a Man-In-the-middle attack. The attacker must redirect network traffic to him. It can use a spoofing ARP attack to associate its MAC address as the IP address of the PBX in order to receive all communications. **[53],[54]**



```
mirko@mirko-VirtualBox~$ sudo arpspoof -t 192.168.101.108 192.168.101.105
[sudo] password for mirko:
8:0:27:a1:87:df 8:0:27:24:bf:5c 0806 42: arp reply 192.168.101.105 is-at 8:0:27:a1:87:df
8:0:27:a1:87:df 8:0:27:24:bf:5c 0806 42: arp reply 192.168.101.105 is-at 8:0:27:a1:87:df
8:0:27:a1:87:df 8:0:27:24:bf:5c 0806 42: arp reply 192.168.101.105 is-at 8:0:27:a1:87:df
8:0:27:a1:87:df 8:0:27:24:bf:5c 0806 42: arp reply 192.168.101.105 is-at 8:0:27:a1:87:df
8:0:27:a1:87:df 8:0:27:24:bf:5c 0806 42: arp reply 192.168.101.105 is-at 8:0:27:a1:87:df
8:0:27:a1:87:df 8:0:27:24:bf:5c 0806 42: arp reply 192.168.101.105 is-at 8:0:27:a1:87:df
```

Figure 15 First Step Eavesdropping: Man-In-The-Middle Attack **[54]**

Then, the attacker will receive all the packets on his network, and he will be able to analyze them with a sniffer such as Wireshark. Indeed, Wireshark allows you to decode and play RTP voice packets. **[55],[56]**



☑ From 192.168.1.227:9000 to 192.168.1.222:30002 Duration:11.56 Drop by Jitter Buff:0(0.0%) Out of Seq: 0(0.0%) Wrong Timestamp: 0(0.0%)

□ From 192.168.1.222:30002 to 192.168.1.227:9000 Duration:11.46 Drop by Jitter Buff:0(0.0%) Out of Seq: 0(0.0%) Wrong Timestamp: 0(0.0%)

Jitter buffer [ms] 50 □ Use RTP timestamp

*Figure 16 Wireshark RTP Player***[55]**

CHAPTER 3 : DEFENCES AND SOLUTIONS

1. Countermeasures against ARP Poisoning attack

While ARP Poisoning attacks are relatively easy to conduct as long as the attacker has access to the targeted network, there are ways to prevent and defend against such attacks.

1.1. Static ARP Entries

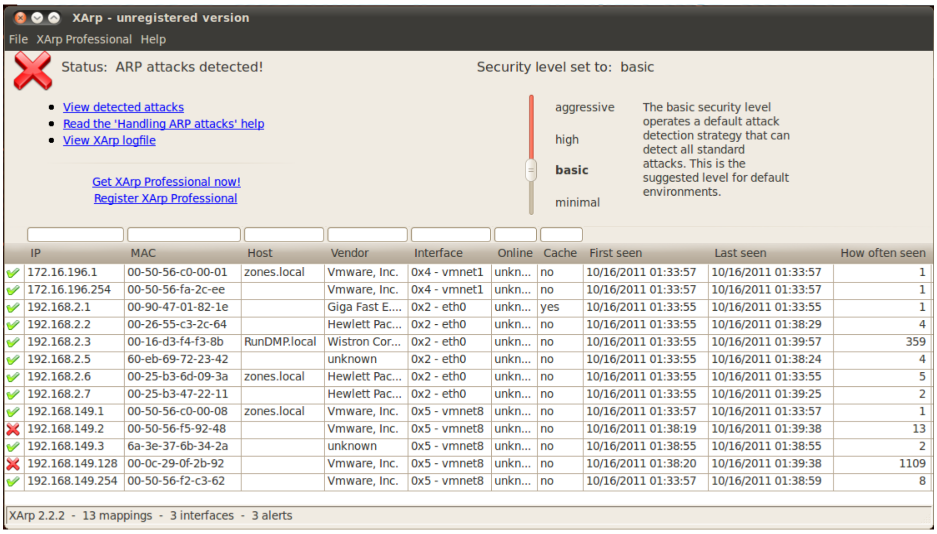
One of the basic ways to make ARP Poisoning inoperable inside a network is by using static read-only ARP entries set up manually **[57]**, **[59l]**. Such configuration will ignore any packet that would normally induce a modification in the mapping. While providing some security against ARP Poisoning attacks, such an option is nearly never used as it requires a lot of maintenance effort, as the generated mappings need to be manually transferred to all the hosts in the network in order for them to be able to communicate with one another. Any addition, deletion or modification in the mapping also requires manual maintenance, making such a solution relatively inoperable in most situations.

1.2. Packet Filtering

Another solution in order to prevent ARP Spoofing attacks is to set up some packet filtering on the network **[58]**, **[59]**. Such filtering will detect ARP poisoning trough the conflicting information contained inside the packets, and block such packets in order to maintain network integrity.

1.3. Software and configuration

There are some pieces of software that are able to detect and prevent ARP poisoning attacks, such Snort, X-ARP, ARP_Antidote, etc. They can use active, passive or both types of defences. While passive defences mainly consist in packet filtering, active defences usually involve some sort of certification in order to authenticate the machine responding to the ARP request, as the ARP protocol lacks native authentication check.


XArp - unregistered version
File XArp Professional Help
aggressive
high
basic
minimal
Get XArp Professional now!
Register XArp Professional

Status: ARP attacks detected!

Security level set to: basic

- View detected attacks
- Read the 'Handling ARP attacks' help
- View XArp logfile

The basic security level operates a default attack detection strategy that can detect all standard attacks. This is the suggested level for default environments.

	IP	MAC	Host	Vendor	Interface	Online	Cache	First seen	Last seen	How often seen
✓	172.16.196.1	00-50-56-c0-00-01	zones.local	Vmware, Inc.	0x4 - vmnet1	unkn...	no	10/16/2011 01:33:57	10/16/2011 01:33:57	1
✓	172.16.196.254	00-50-56-fa-2c-ee		Vmware, Inc.	0x4 - vmnet1	unkn...	no	10/16/2011 01:33:57	10/16/2011 01:33:57	1
✓	192.168.2.1	00-90-47-01-82-1e		Giga Fast E....	0x2 - eth0	unkn...	yes	10/16/2011 01:33:55	10/16/2011 01:33:55	1
✓	192.168.2.2	00-26-55-c3-2c-64		Hewlett Pac...	0x2 - eth0	unkn...	no	10/16/2011 01:33:55	10/16/2011 01:38:29	4
✓	192.168.2.3	00-16-d3-f4-f3-8b	RunDMP.local	Wistron Cor...	0x2 - eth0	unkn...	no	10/16/2011 01:33:55	10/16/2011 01:39:57	359
✓	192.168.2.5	60-eb-69-72-23-42		unknown	0x2 - eth0	unkn...	no	10/16/2011 01:33:55	10/16/2011 01:38:24	4
✓	192.168.2.6	00-25-b3-6d-09-3a	zones.local	Hewlett Pac...	0x2 - eth0	unkn...	no	10/16/2011 01:33:55	10/16/2011 01:33:55	5
✓	192.168.2.7	00-25-b3-47-22-11		Hewlett Pac...	0x2 - eth0	unkn...	no	10/16/2011 01:33:55	10/16/2011 01:39:25	2
✓	192.168.149.1	00-50-56-c0-00-08	zones.local	Vmware, Inc.	0x5 - vmnet8	unkn...	no	10/16/2011 01:33:57	10/16/2011 01:33:57	1
✗	192.168.149.2	00-50-56-f5-92-48		Vmware, Inc.	0x5 - vmnet8	unkn...	no	10/16/2011 01:38:19	10/16/2011 01:39:38	13
✓	192.168.149.3	6a-3e-37-6b-34-2a		unknown	0x5 - vmnet8	unkn...	no	10/16/2011 01:38:55	10/16/2011 01:38:55	2
✗	192.168.149.128	00-0c-29-0f-2b-92		Vmware, Inc.	0x5 - vmnet8	unkn...	no	10/16/2011 01:38:20	10/16/2011 01:39:38	1109
✓	192.168.149.254	00-50-56-f2-c3-62		Vmware, Inc.	0x5 - vmnet8	unkn...	no	10/16/2011 01:33:57	10/16/2011 01:38:59	8

XArp 2.2.2 - 13 mappings - 3 interfaces - 3 alerts

Figure 17 Xarp Linux main screen: Crosses indicate spoofing detection **[62]**

1.4. Operating System Level

It is to be noted that operating systems may have some sort of protection against ARP Poisoning attacks **[57]**. Linux distros ignores unsolicited ARP replies, while Solaris will only accept such replies after a preset timeout. On Microsoft Windows, the behaviour of the ARP Cache can be configured with a set of registry values.

1.5. Traffic Encryption

One of the options in order to protect a network against many types of attacks is traffic encryption **[58]**. As with all *Man in the Middle* attacks, traffic encryption makes the attacker unable to do anything with the packets he receives, as such packets are encrypted with keys the attacker does not have access to. In these cases, the attacker is able to conduct the attack, but the received information, that is encrypted, is pointless for him.

1.6. IPV6 NDP

Lastly, one of the most effective ways to protect a network from ARP Spoofing attacks is to use IPV6 instead of IPV4 and the associated Network Discovery Protocol (NDP) **[60]**, which includes native authentication check, and also provides an extension, Secure Neighbor Discovery (SEND) **[61]**, that can add a cryptographic layer to the communication, thus providing a way more secure infrastructure that cannot be targeted by ARP Poisoning attacks. However, the majority of the internet still uses IPV4 instead of IPV6, as the switch remains costly, relatively complex for large organisations, and is also still impacted by some software and hardware incompatibility. Enventually, while IPV6 is the best option in order to protect a network from ARP Poisoning attacks, companies usually do not consider it as a requirement.

2. To prevent DHCP & DNS Spoofing

2.1. DHCP Spoofing defences

2.1.1. DHCP spoofing protection

DHCP snooping is an option that you can enable. Once enabled the trusted switch ports of DHCP servers are memorized. For each DHCP request that goes through the switch, it checks if the port is trusted or untrusted. If it is untrusted it can just delete the request, that prevents fake DHCP servers to take over the network. **[63]**

2.1.2. IP Source Guard

IP source guard is based on IP address and subnet masks. It checks whether a request destination is in the subnet or not.

When a rogue DHCP server tries to spoof addresses, it can randomly take valid or invalid addresses. If a request asks for an IP destination that is not in the subnet then the request is deleted. But IP source guard is not that effective because the rogue server could take valid destination IP addresses and these would be forwarded. **[63]**

2.1.3. Dynamic ARP Inspection

Like DHCP snooping, trusted and untrusted sources are memorized in ARP tables. If a request with an untrusted source appears, it will be registered as an untrusted source, if it conflicts with an ARP table's entry it will send a log and drop the request. That way it prevents wrong sources from being added to trusted sources. **[63]**

2.2. DNS Spoofing defences

There are multiple ways to keep your DNS safe. The best way is to keep it inside your network and not open it to extern sources. But there are other ways, you could configure it safer. Using a random source port would prevent someone that isn't supposed to communicate with the DHCP server to send requests as they would not know the port. You can also randomize the outgoing requests. In order to do that one can for example randomize the query ID or randomize domain names. These randomizations will make it harder for hackers to spoof requests. **[64]**

3. To guard against VoIP Calls Listening

To avoid listening on VoIP, there are several recommendations to follow.

3.1. Use of VLANS

VLAN is a virtual local network that allows to group machines together according to logical criteria and to free from the boundaries of the physical network (localisation, addressing). These criteria may be for instance:

- MAC addresses
- Port number used
- Protocol used

In the context of VoIP, this logical segmentation is particularly useful against attacks, for example by separating data and voice streams. Thus, if an attacker succeeds in collecting the data streams, he will not have voice streams. **[65]**

3.2. Switchport Security Mac Addresses

In order to prevent a connection from an attacker to a port of the switch, it is possible to control/limit the MAC addresses that can connect to each port. It is both possible to limit the maximum number of MAC addresses for each port or to specify the list of allowed MAC addresses. **[66], [67]**

3.3. Use of IPSec Tunnels

IPSec (Internet Protocol Security) tunnels allow private, protected and authenticated communications over IP networks using cryptographic encryption algorithms. **[68]**

3.4. Use of TLS with SIP

SIP messages should be encrypted with the Transport Layer Security (TLS) protocol. This protocol allows authenticating the server (and sometimes the client), encrypting data and ensuring data integrity. TLS replaces SSL which has vulnerabilities, it should be used instead and SSL should be disabled on the servers. **[69]**

3.5. Use SRTP/SRTCP instead of RTP/RTCP

SRTP and SRTCP are the secure versions of RTP/RTCP. These protocols ensure the confidentiality of voice/video messages with 128-bit AES-CM encryption and message authentication with HMAC-SHA1 without reducing the quality of service (QoS). **[53], [70], [71]**

3.6. Use MiKEY for key exchange

MiKEY is a key management protocol for real-time applications. It can be used for VoIP in the SRTP protocol for necessary key exchanges for encryption of messages. MiKEY uses mainly 3 methods for key exchange: **[72]**

- Pre-Shared Key (PSK)
- Public Key (PK)
- Diffie-Hellman

SOURCES

[1] WikiPedia, 10/18/20, *"Cyberattack"*, Accessed : [10/13/2020], Available : https://en.wikipedia.org/wiki/Cyberattack

[2] GeeksforGeeks, 09/08/2019, *"Active and passive attacks in information security"*, Accessed : [10/14/2020], Available : https://www.geeksforgeeks.org/active-and-passive-attacks-in-information-security/

[3] WhatIs, 08/01/2020, *"Active attack"*, Accessed : [10/14/2020], Available : https://whatis.techtarget.com/definition/active-attack

[4] LockheedMartin, 02/13/2020, *"LM White Paper Intel Driven Defense"*, Accessed : [10/16/2020], Available : https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

[5] Medium. *The Cyber Kill Chain* [Online picture]. Accessed: October 6, 2020. Available: https://medium.com/cyberthreatintel/threat-intelligence-101-splendeurs-et-mis%C3%A8res-de-la-kill-chain-67869d5995e6

[6] Norton, 06/24/2017, *"What is the Difference Between Black, White and Grey Hat Hackers?"*, Accessed: [10/13/2020], Available: https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html

[7] Kaspersky, 10/17/2020, *"Top 10 Most Notorious Hackers of All Time",* Accessed: [10/13/2020], Available: https://www.kaspersky.com/resource-center/threats/top-ten-greatest-hackers

[8] MetaCompliance, 05/28/2019, *"10 Biggest DDoS Attacks and how your organisation can learn from them"*, Accessed: [10/13/2020], Available: https://www.metacompliance.com/blog/10-biggest-ddos-attacks-and-how-your-organisation-can-learn-from-them/

[9] Joseph Regan, 09/28/2019, *"The Most Dangerous & Famous Hackers Today"*, AVG, Accessed: [10/13/2020], Available: https://www.avg.com/en/signal/the-most-dangerous-hackers-today

[10] WikiPedia, 09/7/2020, *"Gameover ZeuS"*, Accessed: [10/13/2020], Available: https://en.wikipedia.org/wiki/Gameover_ZeuS

[11] WikiPedia, 09/4/2020, *"Hacker"*, Accessed: [10/13/2020], Available: https://en.wikipedia.org/wiki/Hacker

[12] WikiPedia, 06/10/2020, *"Security hacker"*, Accessed: [10/13/2020], Available: https://en.wikipedia.org/wiki/Security_hacker

[13] Wikipedia. *The emblem of Anonymous.* [Online picture]. Accessed: October 14, 2020. Available: https://en.wikipedia.org/wiki/Anonymous_(group)#/media/File:Anonymous_emblem.svg

[14] HealthcareITNews. *Kevin Mitnick.* [Online picture]. Accessed: October 14, 2020. Available: https://www.healthcareitnews.com/news/hacker-kevin-mitnick-dangers-human-factors-health-data-security

[15] King university, 06/23/2019, *"5 Famous White Hat Hackers You Should Know"*, Accessed: [10/13/2020], Available: https://online.king.edu/news/5-famous-white-hat-hackers-you-should-know/

[16] Wikipedia. *Picture of Charlie Miler speaking at Truman State University.* April 11, 2015. [Online picture]. Accessed: October 14, 2020. Available: https://commons.wikimedia.org/wiki/File:CharlieMillerHolmanSpeaker2015-20.jpg

[17] Wikipedia. *Dan Kaminsky2015portrait*. June 12, 2015. [Online picture] Accessed: October 14, 2020. Available: https://commons.wikimedia.org/wiki/File:Dan_Kaminsky2015portrait.jpg

[18] J. Melnick. *Top 10 Most Common Types of Cyber Attack*. Newrix Blog. May 15, 2018 (updated October 8, 2020). Accessed: October 11, 2020. [Online] Available: https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/

[19] A. Graham. *The 5 most common cyber attacks in 2020.* IT Governance. December 1, 2017 (updated May 9, 2019). Accessed: October 10, 2020. [Online] Available: https://www.itgovernance.co.uk/blog/different-types-of-cyber-attacks

[20] ANSSI. "Comprendre et anticiper les attaques DDoS ". Accessed : October 14, 2020. [Online] Available : https://www.ssi.gouv.fr/uploads/2015/03/NP_Guide_DDoS.pdf

[21] OVH. *What is anti-DDoS Protection?* Accessed: October 11, 2020. [Online] Available: https://www.ovh.com/world/anti-ddos/anti-ddos-principle.xml

[22] K. Chivers. *What is a man-in-the-middle attack ? March 26, 2020.* Accessed: October 14, 2020. [Online] Available: https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html

[23] Terranova Security. *Spear Phishing vs. Phishing*. September 27, 2019 (updated May 1, 2020). Accessed: October 12, 2020. [Online] Available: https://terranovasecurity.com/spear-phishing-vs-phishing/

[24] Terranova Security. *19 Examples of Common Phishing Emails*. July 17, 2020 (updated July 20, 2020). Accessed: October 12, 2020. [Online] Available: https://terranovasecurity.com/top-examples-of-phishing-emails/

[25]G. Nixon. *Just 18% could spot all of these fraud messages… could you do better?* This is money. July 11, 2020. Accessed : October 12, 2020. [Online] Available: https://www.thisismoney.co.uk/money/beatthescammers/article-8498297/Just-18-spot-fraud-messages-better.html

[26] S. Daityari. *SQL Injection: A Beginner's Guide for WordPress Users*. Kinsta. January 13, 2020 (updated March 6, 2020). Accessed: October 12, 2020. [Online] Available: https://kinsta.com/blog/sql-injection/

[27] W3school. *SQL Injection*. Accessed: October 12, 2020. [Online] Available: https://www.w3schools.com/sql/sql_injection.asp

[28] PortSwigger. *SQL Injection.* Accessed: October 12, 2020. [Online] Available: https://portswigger.net/web-security/sql-injection

[29] Whisperlab.org. *SQL Injection with sqlmap: a tutorial.* Accessed: October 12, 2020. [Online] Available: https://whisperlab.org/introduction-to-hacking/talks/sqlmap

[30] ARNnet from IDG. *Top 10 most notorious cyber attacks in history.* Accessed: October 5, 2020. [Online] Available: https://www.arnnet.com.au/slideshow/341113/top-10-most-notorious-cyber-attacks-history/

[31] *Mafiaboy, alias Michael Calce.* [Online picture] Accessed: October 14, 2020. Availablehttps://www.lapresse.ca/cinema/nouvelles/201207/17/01-4552597-abandon-du-projet-de-film-sur-mafiaboy.php

[32] J. Vijayan. *SQL Injection attacks led to Heartland, Hannaford breaches.* August 18, 2009. Accessed: October 12, 2020. [Online] Available: https://www.computerworld.com/article/2527185/sql-injection-attacks-led-to-heartland--hannaford-breaches.html

[33] U.S Secret Service. Albert-gonzalez. Wikipedia. August 19, 2009 [Online picture]. Accessed: October 14, 2020. Availablehttps://commons.wikimedia.org/wiki/File:Albert-gonzalez.jpg

[34] Kaspersky. *Top 5 most notorious cyberattacks.* November 6, 2018. Accessed: October 11, 2020. [Online] Available: https://www.kaspersky.com/blog/five-most-notorious-cyberattacks/24506/

[35] Kaspersky. *Stuxnet : Victims Zero*. November 18, 2014. Accessed : October 11, 2020. [Online] Available: https://www.kaspersky.com/blog/stuxnet-victims-zero/6775/

[36] Wikipedia, 10/13/2020, *"ARP Spoofing"*, Accessed : [10/16/2020], Available : https://en.wikipedia.org/wiki/ARP_spoofing

[37]Veracode, *"ARP Spoofing"*, Accessed : [10/16/2020], Available: https://www.veracode.com/security/arp-spoofing

[38] Wikipedia, 09/14/2020, *"Address Resolution Protocol"*, Accessed : [10/16/2020], Available :https://en.wikipedia.org/wiki/Address_Resolution_Protocol

[39] Imperva, *"ARP Spoofing"*, Accessed : [10/17/2020], Available: https://www.imperva.com/learn/application-security/arp-spoofing/

[40] International Journal of Advancements in Technology, 03/2014, *"A holistic approach to ARP poisoning and Countermeasures by using practical Examples and paradigm"*, Accessed : [10/19/2020], Available : https://www.longdom.org/open-access/a-holistic-approach-to-arp-poisoning-and-countermeasures-by-using-practical-examples-and-paradigm-0976-4860-5-82-95.pdf

[41] ForcePoint, "What is spooning", Accessed : [10/21/2020], Available: https://www.forcepoint.com/cyber-edu/spoofing

[42] WikiPedia, 10/1/20, "Dynamic Host Configuration Protocol", Accessed : [10/21/2020], Available: https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

[43] OmniSecu, "DHCP Starvation attacks and DHCP spoofing attacks", Accessed : [10/21/2020], Available: https://www.omnisecu.com/ccna-security/dhcp-starvation-attacks-and-dhcp-spoofing-attacks.php

[44] CCNP switch, Ideas Mag, "DHCP Snooping", Accessed : [10/21/2020], Available: http://ccnp300-115.blogspot.com/2016/08/dhcp-snooping.html

[45] Kaspersky, "What is DNS Cache Poisoning and DNS Spoofing", Accessed : [10/21/2020], Available: https://www.kaspersky.com/resource-center/definitions/dns

[46] Imperva, "DNS Spoofing", Accessed : [10/21/2020], Available: https://www.imperva.com/learn/application-security/dns-spoofing/

[47] J. Bai. *What is IP Telephony? How It Works & How It Helps Your Business.* Nextiva Blog. March 2, 2020. Accessed: October 22, 2020. [Online] Available: https://www.nextiva.com/blog/what-is-ip-telephony.html

[48] A. Kucharik. *What is the difference between IP Telephony and Voice over IP (VoIP)?* SearchNetworking. November, 2003. Accessed: October 22, 2020. [Online] Available: https://searchnetworking.techtarget.com/answer/What-is-the-difference-between-IP-telephony-and-voice-over-IP-VoIP

[49] C. Johnson. *How Does VoIP Work ? The 2020 Guide to VoIP Phone Systems.* Nextiva Blog. February 6, 2020. Accessed: October 22, 2020. [Online] Available: https://www.nextiva.com/blog/how-does-voip-work.html

[50] Wikipedia. *Voice over IP*. Accessed: October 22, 2020. [Online] Available: https://en.wikipedia.org/wiki/Voice_over_IP

[51] Wikipedia. *Session Initiation Protocol.* Accessed: October 22, 2020. [Online] Available: https://en.wikipedia.org/wiki/Session_Initiation_Protocol

[52] R. Kumar. What is the SIP Protocol ? Software Advice. April 15, 2020. Accessed: October 22, 2020. [Online] Available: https://www.softwareadvice.com/resources/what-is-sip/

[53] Penetration Testing Lab. *Eavesdropping VoIP Calls With Wireshark*. July 22, 2014. Accessed: October 22, 2020. [Online] Available: https://pentestlab.blog/2014/07/22/eavesdropping-voip-calls-with-wireshark/

[54] M. Raimondi. *VoIP Hacking Techniques*. Haking. May 22, 2014 (updated May 23, 2019). Accessed: October 22, 2020. [Online] Available: https://hakin9.org/voip-hacking-techniques/

[55] M. Mengel. *VoIP Call Playback & Other Wireshark Voice Tools.* Packet Pushers. November 20, 2012. Accessed: October 22, 2020. [Online] Available: https://packetpushers.net/voip-call-playback-other-wireshark-voice-tools/

[56] E. Jiang. *How to Analyze SIP Calls in Wireshark*. Yeastar. Accessed: October 22, 2020. [Online] Available: https://support.yeastar.com/hc/en-us/articles/360007606533-How-to-Analyze-SIP-Calls-in- Wireshark

[57] Wikipedia, 10/13/2020, *"ARP Spoofing"*, Accessed : [10/26/2020], Available: https://en.wikipedia.org/wiki/ARP_spoofing

[58] Veracode, *"ARP Spoofing"*, Accessed : [10/26/2020], Available: https://www.veracode.com/security/arp-spoofing

[59] Imperva, *"ARP Spoofing"*, Accessed : [10/17/2020], Available: https://www.imperva.com/learn/application-security/arp-spoofing/

[60] Wikipedia, 10/02/2020, *"Neighbor Discovery Protocol"*, Accessed : [10/26/2020], Available: https://en.wikipedia.org/wiki/Neighbor_Discovery_Protocol

[61] Wikipedia, 05/10/2018, *"Secure Neighbor Discovery"*, Accessed : [10/26/2020], Available: https://en.wikipedia.org/wiki/Secure_Neighbor_Discovery

[62] Téléchargement-pc, *"Télécharger XArp"*, Accessed : [10/26/2020], Available: http://www.telechargement-pc.fr/xarp/

[63] Tutorzine, 02/11/2019, *"How to prevent Spoofing attacks"*, Accessed: [10/27/2020], Available: https://tutorzine.com/prevent-spoofing-attacks/

[64] Paul Rubens, 10/18/2017, *"How to prevent DNS attacks"*, eSecurity Planet, Accessed: [10/27/2020], Available: https://www.esecurityplanet.com/network-security/how-to-prevent-dns-attacks.html

[65] GeeksForGeeks. *Types of Virtual Lan (VLAN)*. Updated: June 29, 2020. Accessed: November 1, 2020. [Online] Available: https://www.geeksforgeeks.org/types-of-virtual-lan-vlan/

[66] ComputerNetworkingNotes. *Swicthport Port Security With Examples*. Updated: August 6, 2018. Accessed : November 1, 2020. [Online] Available: https://www.computernetworkingnotes.com/ccna-study-guide/switchport-port-security-explained-with-examples.html

[67] S. Wilkins. *Switchport Security Concepts.* Pluralsight. February 22, 2012. Accessed: November 1, 2020. [Online] Available : https://www.pluralsight.com/blog/it-ops/switchport-security-concepts

[68] GeeksForGeeks. *IP security (IPSec).*Updated: February 4, 2020. Accessed: November 1, 2020. [Online] Available: https://www.geeksforgeeks.org/ip-security-ipsec/

[69] Kinsta. *TLS vs SSL: What's the difference? Which one should you use?* October 18, 2020. Accessed: November 1, 2020. [Online] Available: https://kinsta.com/knowledgebase/tls-vs-ssl

[70] M. Baugher, D. MacGrew, M. Shore. *Securing Internet Telephony Media with SRTP and SDP*. Cisco. November 10, 2014. Accessed: November 1, 2020. [Online] Available: https://tools.cisco.com/security/center/resources/securing_voip.html#12

[71] 3cx. *SRTP – Whats is Secure real-Time Transport Protocol ?* Updated: June 2, 2020. Accessed: November 1, 2020. [Online] Available: https://www.3cx.com/webrtc/srtp/

[72] G. Aghila, D. Chandirasekaran. *An analysis of VoIP Secure Key Exchange Protocols against Man-in-the-Middle Attack.* International Journal of Computer Applications. 2011.Accessed: November 1, 2020. [Online] Available: https://research.ijcaonline.org/volume34/number7/pxc3875930.pdf

Report on cyberattacks