International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 7 (2018) pp. 4672-4671

Man in the Middle Attack: Prevention in Wireless LAN

Andrés Javier Pulido Bernal[1], Octavio José Salcedo Parra[1, 2], Roberto Albeiro Pava Díaz[2]

[1]*Faculty of Engineering - Universidad Distrital Francisco José de Caldas, Bogotá D.C., Colombia.*

[2]*Faculty of Engineering - Universidad Nacional de Colombia, Bogotá D.C., Colombia.*

Abstract

This document describes some strategies to prevent man in the middle attack on a network wireless LAN 802.11n , to do this, the man in the middle attack is implemented in a LAN domestic network and each proposed strategy has been validated in order to register the results. Man in the middle attack consists of ARP poisoning and DNS spooling which aims to redirect victim's HTTP requests to a web server installed on the machine of the attacker, in this way, the victim would always be re-directed to a site hosted on the web server of the attacker, disregarding to which domain the victim is pointing at; each strategy was validated and moderately successful results were found due to technical or administrative implications of each setting. Considering that for this article, an attack with particular characteristics was done, some strategies are expected not to work in all scenarios in which case it would be required to combine them or modify them.

Keywords: ARP, DNS, LAN, Packet, TCP.

INTRODUCTIÓN

For a computer to send data to another through a network, the compliance with some agreements at the hardware and software level is required, for handling, transporting, and ensuring the delivery of the traveler data to its specific destination, each data is fragmented into packages that have a low level structure that pass through thanks to a series of protocols that are stacked in a standardized model. Packets of information travel through a channel that can be wireline, fiber optic, or electromagnetic signals among others , this means that in any of these means is possible to intercept such messages and get to know part of the content of the message, its origin, its provenance and its structure.

There is an extensive documentation that describes the vulnerabilities on data networks and existing mechanisms to prevent various attacks, in the article "Man in the middle attack to the HTTPS protocol" [1] described the characteristics of a man in the middle attack on a wired network 802.3, in this attack the victim consulted a HTTPS site and the attacker intercepts the request, sends its own certificate and displays its own version of the site. In the article "Different Flavours of Man-In-The-Middle Attack, Consequences and Feasible Solutions"[7] some variations of this type of attack are arisen and also a possible effective solution in certain situations, in both texts, the two types of attack implemented in this article are mentioned, and some of the existing vulnerabilities that allow the execution of this type of attack are outlined.

BACKGROUND

Although there are few related works that exactly use open data sources to generate heat maps that show the occurrence of diseases in a given area, heat maps have been used to determine the occurrence of news generated in South Korea and are reported by Newscasts or portals worldwide, by Chen [1]. Keneshloo [2] uses GDELT (The Global Data on Events, Location and Tone) to predict an internal political crisis in a country of interest, is a very useful tool for social scientists and policy makers. It has a large amount of event data for historical analysis and thus generate a predictive utility. Santoso [3] in Design of a web-based Geographic Information Systems Spatial for Distribution of Historic Site and using the database of The National Archaeological Center of Indonesia offers a geographic information system on the distribution and location of historical sites in the region Of the island of Java. It is established that in terms of preservation, registration and the provision of information to the public on the importance of cultural heritage, for now, is very scarce, therefore the use of technology is especially needed in the topic of saving and consulting the Information related to historical sites. Chen [4] in Long Short-Term Memory Model for Traffic Congestion Prediction with Online Open Data is based on the increasing gravity of traffic congestion and making use of open data online, it creates an application that Can predict future traffic conditions to create immediate solution strategies.

OPERATION

To reproduce the MITM attack, there has been implemented two types of attacks: ARP Poisoning [2] and DNS spoofing [3] [4]. The first one consists of sending fake ARP messages containing manipulated MAC addresses to make a machine pass off as a different one, each machine maintains a cache with the translated addresses to reduce the delay and the load by which this attack aims to fix and maintain the false values in its cache. The second consists of generating false responses to the name resolution requests made by the victim host.

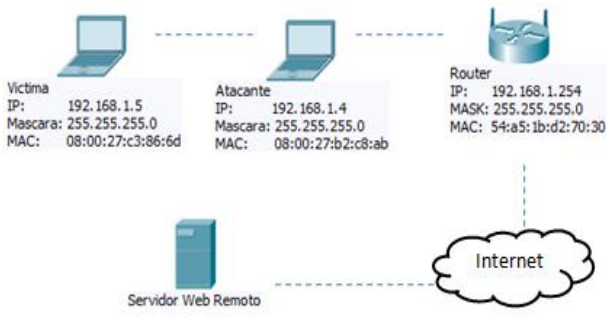

Figure 1. Network Configuration. Source: Authors

The Fig. 1 shows the typical configuration of a home network consists of a router that connects a couple of laptops to the internet, the attacking host has the IP address 192.168.1.4 and its goal is to intercept the communication between the victim host of the IP address 192.168.1.5 and the IP router address 192.168.1.254; This type of attack is known as MITM and consists of a host that is placed in the middle of two others to capture and modify the messages that are being transmitted [5]; In this implementation the objective is to generate a DNS false resolution when the host victim is trying to navigate anywhere on the internet through a router, so that it will be redirected to a web service that runs on the host of the attacker [6].

Used Equipment:

- Modem Router HG 530 with stand 802.11n.
- Laptop (attacker) with Intel ® network card Centrino ® Advanced-N 6205, with 2.4 GHz (802.11b/g/n) frequency modulation and Ubuntu operating system.
- Laptop (victim) with Qualcomm Atheros AR9485 network card, with 2.4 GHz frequency modulation (802.11b/g/n) and operating system Ubuntu Studio.

Sending ARP Requests to the Router

The customer sends ARP packets in a specific time interval to the Router in order to keep its ARP table updated, this prevents the attacker from overwriting it and from inserting a false reference of its MAC address. Initially the test is done by sending the request in a 60 seconds interval which comes configured by default in all Linux operating systems, then lower values were tested with a difference of 5 seconds more than used in the attack and then decreasing it in 5 seconds to obtain effective protection against man in the Middle attack implemented in this article. This is achieved with the following script running on the client (See Fig. 2).

```
#!/bin/bash
while true
do
echo lanzando ejecucion
arping -f 192.168.1.254
sleep 15
done
```

Figure 2. Script on the client for ARP requests. Source: Authors

As you can see this is a bash script that launches the ARPING command to the gateway of the network, this means that it sends an ARP message to host 192.168.1.254 to bring this record to be written to the local ARP table. Then the script pauses the execution for 15 seconds and then it goes back to repeat the cycle indefinitely since the instructions are contained in an infinite while loop. By Starting from setting 15 seconds or less in the script, the attack could not be conducted concluding that this range of values were effective to prevent the attack.

Monitoring the ARP Host Table

To run the script that runs on the client and that constantly checks if there is any change in the ARP table of the registration of the router's MAC address to launch an alert (See Fig. 3).

```
#!/bin/bash
while true
do
 a=`arp -a | awk '{print $4}' | grep 54:a5:1b:d2:70:33| wc -l`

 if [ $a = 0 ]
 then
   notify-send -t 0 'System is ARP hackeado'
 fi
sleep 0.5
done
```

Figure 3. Script for ARP Table Verification. Source: Authors

This script consists of a While sentence infinitely running, that contains a query to the ARP table in order to validate if there remains a record, in case that it does not remain any, it launches an informative window to the host victim user. The script uses the command AWK to filter the output of the command ARP - A and to get the column with the MAC address, in this way it is compared against to the previously existing address to know if it has been amended or not, if yes it launches a window which informs about the difference.

Configure Static Entries in the Table of the Customer

To set statically the MAC address of the Router on each client to avoid that it is updated in the man in the middle attack. In Linux the command to configure statically is ARP using the option i, the interface is identified and the static MAC address is sent (See Fig. 4).

```
arp -i wlan -s 182.168.1.254 54:a5:1b:d2:70:30
```

Fig. 4. Command to set a static MAC address reference. Source: Authors

Restrict Client ICMP Packets

This is achieved by some antivirus but it deprives the customer of accessing to certain services, perhaps the best-known is the ping command that is used to check if a computer is active in a network; Ping sends a message, calls an echo request to the target host and responds if the host is running. This tool is useful for administrators and technical support analysts but it is also used by hackers to analyze a computer on a network.

This measure is too restricting which makes it not so practical in most scenarios.

Use a Public Key System

The public key system is capable of providing digital signatures. By configuration, the parties should know previously the public key from each of them. Once they have been generated, the parties send digital signatures. The attacker fails to attack because is not capable of forging the signatures without knowing the private key used to generate these signatures.

ANALYSIS AND RESULTS

Sending ARP Requests to the Router

The effectiveness of the attack varies regarding the strategy employed, when a thread for ARP requests is created from the application, the client's ARP modification table remains unchanged with false data; When the attack is launched releasing ARP requests without the use of attack threads, is not effective against the mechanism that has been installed on the victim machine.

The interval of sending ARP requests also significantly affects the result of the test, when the attack is made by launching the ARP request in 30 seconds interval and the script on the victim runs every 15 seconds the attack is unsuccessful, but when is done in an interval of 5 seconds is an effective attack. A running time of 3 seconds on the script on the victim, avoided carrying out the attack when it generated ARP requests at 3 second intervals.

Monitoring the ARP Host Table

This strategy basically consisted of setting up a validation of the MAC of the gateway in the ARP table of the victim, this measure does not prevent the attack but it generates an indicator that our machine is being attacked. Establishing awareness levels of an attack of man in the middle, this strategy would be complementary as for example to the script settings mentioned in paragraph A.

Configure Static Entries in the ARP Table of the Customer

This strategy was effective in a 100% to prevent ARP Poisoning and it requires the registration of the MAC address of its gateway to be set in all computers in a network however, it is not effective to prevent DNS spoofing, recording manually the IP addresses of the sites visited by a customer is not a feasible option because it requires to add to the hosts files of the victim the resolution of the frequented servers and for an internet user, this is not a practical solution.

CONCLUSIONS

The Recurrent sending of ARP requests to the router from the victim is effective, depending on the refresh interval of the ARP table and the attacker code programming strategy, this result demonstrates the variety of solutions to the attack against the variety of ways to carry it out. For the test conditions the refresh every 15 seconds or less of the ARP table was effective to prevent man in the middle attack, this value can vary substantially depending on the characteristics of the attack. This defense was not effective when the attacker launches the attack at an interval of 1 second using threads. Another aspect to consider in this solution is the traffic that is generated on a network if all of your hosts are permanently launching requests to the router.

Some of the strategies proposed in this article are complementary, for instance, the script that runs on the client and maintains the ARP table updated, and the script that keeps monitoring the system by comparing the current record against one fixed

The static configuration of the MAC addresses of the computers can be a tedious task for a network administrator and this aspect should be considered when defining the set of measures that are to be planned in order to secure the network.

REFERENCES

[1] Cagellati Franco. Man in the middle attack to the HTTPS protocol (2009, January February). Security & Privacy, IEEE (Volumen 7) [On Line] http://ieeexplore.ieee.org. Páginas 78-81.

[2] DaleAthanasias (2014, April 19). [On Line] Available: https://wiki.python.org/moin/Documentation.

[3] DNS Spoofing .[On Line] Available: http://blog. vidasconcurrentes.com/seguridad/dns-spoofing

[4] Colasoft LLC (2014, September 20). [On Line] Available: http://www.colasoft.com/download/capsa-ent-whitepaper.pdf.

[5] Nayak Gopi Nath, Samaddar Shefalika Ghosh. "Different Flavours of Man-In-The-Middle Attack, Consequences and Feasible Solutions". Computer Science and Information Technology (ICCSIT) volumen 5, [On Line] Available: http://ieeexplore.ieee.org. Pages 491 - 495.

[6] SANS Institute. ICMP Attacks Illustrated (2001). [On Line] http://www.sans.org/reading-room/whitepapers/threats/icmp-attacks-illustrated-477

[7] Kumar, S., Tapaswi, S. A centralized detection and prevention technique against ARP poisoning. June 2012 [On Line] Available: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6246087&matchBoolean%3Dtrue%26queryText%3DARP+++Poisoning.