# A Security Perspective on Wireless Networks

Aravindh SampathKumar[#1], Vignesh Selvakumar Sellamuthu[#2], Warren Clifford Evans[#3]

[#]*School of Computing, Clemson University*

[1]aravins@clemson.edu
[2]vsellam@clemson.edu
[3]warrene@clemson.edu

*Abstract*— **our objective in this project was to investigate how secure or insecure the Wi-Fi networks are in real-world usage today and provide a brief analysis of the methodologies available to penetrate into Wi-Fi networks and techniques used to attack users once a network has been penetrated. We also analyse the common vulnerabilities in public wireless hotspots and captive portals. By understanding the perspective of the attacker and the methodologies an attacker uses, one can better defend against those attacks.**

## I. Introduction

Due to open transmission nature of Wi-Fi, security is an obvious concern. The IEEE 802.11 standard, commonly referred as Wi-Fi networks were made available from the year 1997.Lot of advancements happened in the computing systems and new techniques were developed to penetrate or break the security of the Wi-Fi networks. On the other hand the standard also has had its share of advancements and is way improved now. But the early adopters still use the technology that was proven to be insecure.

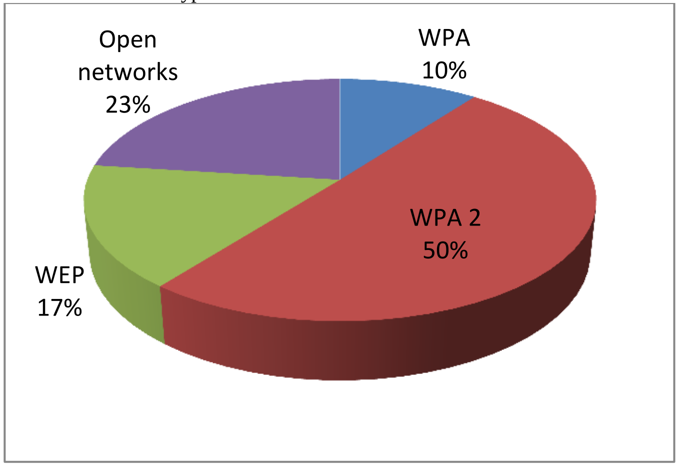
Our motivation in this project was to obtain a cross section of wireless networks around Clemson University and the city of Clemson, in order to see how many of them are vulnerable to common intrusion attacks. We also wanted to examine how insecure the local wireless access points are, and to attempt to determine ways to prevent common intrusion techniques by executing these techniques in a secure environment.

## II. WIRELESS NETWORKS – SECURITY

Today, there are only a handful of encryption mechanisms that can be used to secure a wireless network. The earliest implementation of the IEEE 802.11 standard was based on cryptographic implementation known as Wired Equivalent Privacy (WEP). The WEP encryption mechanism was proved to be insecure way back in 2001, but early adopters still utilize the mechanism in the wireless networks. A cryptographic mechanism named Wireless Protected Access (WPA) was developed as an interim solution to address the security concerns with WEP. The IEEE standard 802.11i brought the more sophisticated WPA2 that is based on AES cryptographic algorithm for enhanced security. Based on the needs for commercial users, there are two implementations of WPA/WPA2 namely WPA-PSK (Pre-Shared Key) for small scale networks and WPA-Enterprise for enterprise class networks. In case of Open networks for public access, they are often protected by a captive portal, which requires a user to sign into some kind of service hosted by whoever is providing the wireless access.

We collected data from the Clemson area with a python script written for and used on an Android phone, in order to make use of its API for Wi-Fi scanning and gathering GPS location coordinates. The GPS coordinates were used to create a map of the Clemson area. Once the data was collected, it was parsed to remove duplicate MAC addresses and the networks were then categorized according to their encryption techniques.

TABLE 1
Distribution of Encryption Methods in Wireless Networks out of 2000 AP



Our data shows that half of all the networks identified were encrypted with WPA2, and almost one quarter of them were either open or not encrypted. Several of the WPA2 networks are maintained by Clemson University, as well as several of the open networks, which are protected with a captive portal (tigernet and clemsonguest respectively).

Examining the channels used by these wireless networks revealed that the majority of networks operated on one of three channels, either 1 6 or 11. The channel that the wireless networks operate on specifies the radio frequency that is used by the access point, or a specific band in the radio frequency. A channel who's numbers is separated by 5 or more are sufficiently far away from each other as to not generate interference.

WEP encryption is relatively less secure than WPA or WPA2. Using publicly available tools, a WEP encryption can be broken in a very short amount of time. Aircrack-ng is one of the most commonly used tools for cracking this encryption. The crack involves using airodump-ng to discover the network and capture passive traffic, and then using aireplay-ng to replay the gather traffic, and aircrack-ng which actually cracks the key by using collected IVs which are unique to the network, and is further explained in [1].

WPA encrypted networks are currently vulnerable to dictionary based attacks. In order to crack the network key, user is de-authenticated in order to capture their handshake with the router. The information gathered is then compared to a dictionary for matches. The key must be included within the dictionary in order for the crack to be successful. The dictionaries involved in these cracks can be very large, and the amount of time required to perform the crack depends on the size of the dictionary, and the length of the key used on the router. The exact method used is also further explained in [2].

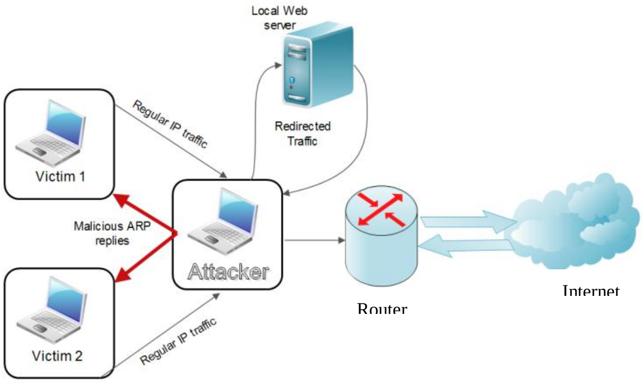
WPA utilizes an encryption mechanism called Temporal Key Integrity Protocol (TKIP) during the 4-way handshake for the data exchange between the access point (AP) and the station. The WPA encryption mechanism is considered to be relatively secured as against WEP because of the usage of TKIP.TKIP implements a more sophisticated key mixing function for mixing a session key with an initialization vector for each packet. This prevents all currently used key attacks because every byte of the packet key depends on every byte of the session key and the initialization vector. Additionally a 64 bit Message Integrity Check (MIC) is included in every packet to prevent the CRC32 based attacks. A sequence counter (TSC) is used so that packets are accepted only in order at the receiver thereby preventing the feasibility of simple replay attacks.

A recent research work has proven that the traffic encrypted using TKIP could be decrypted under certain conditions. Which means the WPA implementation is also not 100 percent secure as further explained in [3].

The IEEE 802.11i standard (referred to as WPA2) introduced CCMP, an AES based encryption protocol which is the only cryptographically sound protocol recognized by National Institute of Standards and Technologies (NIST). [4].

## III. MAN IN THE MIDDLE ATTACK ON A COMPROMISED NETWORK

A man-in-the-middle attack (MITM) intercepts communication between two systems by relaying messages between them. In this attack, the attacker makes an independent connection with both of the victim’ s machines. The attacker machine forces the traffic between the victim’s machines to route through his/her machine by sending a false ARP reply to both machines. The attacker can then create new connections and terminate existing connections, as well as view and replay anything that is private between the targets machines using tools like tcpdump or ettercap. This technique is also called as ARP cache poisoning or ARP Poison Routing (APR).



The following are some of the tools that an attacker could use to perform a successful MITM attack.

- Arpspoof (part of the DSniff suite of tools)
- Arpoison
- SSLStrip
- Ettercap

A. *Arpspoof:*

The principle of ARP spoofing is to send fake, or spoofed, ARP messages onto a LAN. Generally, the aim is to associate the attacker's MAC address with the IP address of another host (such as the default gateway). ARP spoofing attacks can be run from a compromised host on the Local Area Network (LAN) or from an attacker's machine that is connected directly to the target LAN.

B. *SSLStrip*:

This tool provides a demonstration of the HTTPS stripping attacks. It will transparently hijack HTTP traffic on a network, watch for HTTPS links and redirects, and then map those links into either look-alike HTTP links or homograph-similar HTTPS links.

C. *Ettercap:*

Ettercap can be used for computer network protocol analysis and security auditing. It is capable of intercepting traffic on a network segment, capturing passwords, and conducting active eavesdropping against a number of common protocols.

ARP Cache poisoning can be performed using the above mentioned arpspoof tool with sufficient knowledge of the victim and the target network.

In order to deceive the victim host that now the attacker’s MAC address is the one belonging to the IP of the gateway enter the following command:

```
# arpspoof -t <victim> <gateway>
```

In a separate session, the following command would deceive the gateway to believe the attacker is now the victim host.

```
# arpspoof -t <gateway> <victim>
```

Enabling IP forwarding on the host allows the traffic to go through. Otherwise victim will lose connectivity.

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

## IV. DNS CACHE POISONING ATTACK

After attacker get controls of the traffic. She/he can monitor all the activities of the both the victim's. Attacker can do DNS cache poisoning attack. Normally, a networked computer uses a DNS server provided by the computer user's organization or an Internet service provider (ISP). DNS servers are generally deployed in an organization's network to improve resolution response performance by caching previously obtained query results. Poisoning attacks on a single DNS server can affect the users serviced directly by the compromised server.

This technique can be used to direct victims to another site of the attacker's choosing. For example, an attacker spoofs the IP address DNS entries for a target website on a given DNS server, replacing them with the IP address of a server he controls. He then creates files on the server he controls with names matching those on the target server. A user whose computer has referenced the poisoned DNS server would be tricked into accepting content coming from a non-authentic server and unknowingly download malicious content.

## V. PUBLIC WIRELESS NETWORKS – SECURITY

A common use case for wireless networks are public access Wi-Fi networks(commonly referred as Hotspots).Hotspots are common in public facilities like Airports, restaurants etc. Public access networks are secured using a technique called "captive portal" in which all user traffic are trapped and redirected to a web-based authentication page which may require valid login credentials or agreement on terms and conditions before permitting the client to access the internet. Such architecture is expected to create a walled environment as intended by the owner of the hotspot.

Captive portals are generally based on one of the three following authentication mechanisms:

- Mac-Address based authentication, where a client is identified by their Mac-address. The portal at any time maintains a list of mac addresses that were authenticated already. The http traffic from authenticated mac addresses are not redirected whereas the requests from new mac addresses are redirected to the captive portal login page.
- IP address based authentication, where the http traffic from authenticated clients(identified by IP address) are not redirected whereas the https requests from new IP addresses are redirected to the captive portal login page.
- DNS Redirection - When a client requests a website, DNS is queried by the browser. The firewall will make sure that only the DNS server(s) provided by DHCP can be used by unauthenticated clients (or, alternatively, it will forward all DNS requests by unauthenticated clients to that DNS server). This DNS server will return the IP address of the Captive Portal page as a result of all DNS lookups.

The captive portals are generally circumvented in one of the following ways:

A. Evil-Twin Method - An Evil Twin is an access point offering a wireless connection to the Internet pretending to be a trusted wireless network. The unsuspecting user sees the Evil Twin hotspot which looks identical to the legitimate public network the user logs on to every day. By presenting the user with a familiar scenario, such as a login page to a hotspot, the user will readily provide his or her username and password. This attack exploits the lack of facility for users to identify a legitimate hotspot. There are several software tools that can turn a laptop with a capable wireless card into a wireless access point. One such tool we have tried is AirSnarf. [12]

B. Mac Spoofing - Mac address spoofing is a trivial technique used by attackers to assume the identity of another system that was already authenticated. This is accomplished by changing the wireless adapter's Mac address to that of an already connected system. To gather the Mac address of an already authenticated system, one can use a sniffer or monitor program like airodump-ng. Then, a program like macchanger could change the Mac address to the spoofed one.

C. DNS Tunneling - Simply put, the idea is to tunnel all outgoing traffic through Domain Name System (DNS).A client program encapsulates all the TCP packets into the DNS packets destined to a domain/subdomain pointing to a custom name server .The encapsulated packets passes through the network (secured by captive portal) and the network relays the packets as they seem to be legitimate DNS packets. The custom name server resolves the DNS packets and replies back by the same mechanism of encapsulating TCP packets into the DNS packets as DNS response. The said technique though achieves circumventing the captive portal is still unencrypted. Hence adding the sophistication of ssh before encapsulating the TCP packets and running an ssh server would yield a slow but stealthy way of bypassing the captive portal. [13].

## VI. FUTURE WORK

We would like to make a detailed analysis of the Wi-Fi networks with a larger sampling of wireless networks and further categorize the open networks into unsecured ones and the ones that are secured by captive portal. Also we would research for alternative methods to cracking WPA.

We would like to explore effective firewall/router configurations to protect against ARP/DNS spoofing techniques.

## VII. CONCLUSION

WEP is known to be insecure since 2001, but as shown from the analysis, there are still several networks that use the WEP mechanism. They need to be changed to use WPA2.

Though WPA is relatively better secured than WEP, WPA is still not 100 percent secure due to the usage of TKIP. Hence CCMP based WPA2 need to be used instead.

Due to the possibility of replay attacks in WPA networks using the TKIP, password should be complex enough and cross-checked with existing dictionaries to prevent dictionary based guesses.

To defend against the ARP spoofing and DNS Spoofing, a firewall could be configured in the network that watches over and detects unusual ARP replies and discard them.

Public Wireless hotspots could use the "DNS Redirection" and also maintain a whitelist of urls to be resolved by the DNS and not relay DNS packets of non-authenticated systems.

## REFERENCES

[1] Simple WEP crack - http://aircrack-ng.org/doku.php?id=simple_wep_crack&DokuWiki=3ef7232eb17e33aaa8694f68fd18dc84

[2] How to crack WPA/WPA2 - http://aircrack-ng.org/doku.php?id=cracking_wpa&DokuWiki=3ef7232eb17e33aaa8694f68fd18dc84

[3] Paper “Practical attacks against WEP and WPA” – Martin Beck and Erik Tews - http://dl.aircrack-ng.org/breakingwepandwpa.pdf

[4] Brad Antoniewicz, “802.11Attacks” - http://www.mcafee.com/us/resources/white-papers/foundstone/wp-80211-attacks.pdf

[5] Tool used in cracking TKIP - http://www.aircrack-ng.org/doku.php?id=tkiptun-ng

[6] A Whitepaper on MITM attack - http://globalthreatcenter.com/wp-content/uploads/2009/11/MIMT-Whitepaper031.pdf

[7] ARPSpoof - http://su2.info/doc/arpspoof.php

[8] SSLStrip - http://www.thoughtcrime.org/software/sslstrip/

[9] Ettercap - http://en.wikipedia.org/wiki/Ettercap_(computing)

[10] http://www.ab9il.net/wlan-projects/wifi-security2.html

[11] Tool used in Evil-Twin Method - AirSnarf - Airsnarf - http://airsnarf.shmoo.com/

[12] Evil-Twin method - https://www.cirosec.de/fileadmin/pdf/veroeffentlichungen/ADWi-PhishingPaper0605.pdf

[13] DNSTunneling - http://dnstunnel.de/

[14] Captive portal - http://coova.org/CoovaAP