Wireless Network Security

By:

Jose Rodriguez
# Table of Contents

- Wireless Network Security ................................................................. 1
- Table of Contents .................................................................................. 2
- Introduction ........................................................................................... 3
- Wireless Network Requirements .......................................................... 4
- Wireless Network Protocols ................................................................. 5
- Wireless Network Security ................................................................. 6
- Wireless Network Security Software .................................................. 7
- WarDriving ............................................................................................. 9
- Conclusion ............................................................................................. 10
- Acronyms and Abbreviations ............................................................... 11
- Definitions ............................................................................................. 11
- Reference ............................................................................................... 12
Introduction

Starting from the beginning, “the design of today’s Internet technology was guided by an Internet architecture that was developed in the 1970s, under the Internet research program of the Defense Advanced Research Projects Agency (DARPA) of the US Department of Defense. The objective was to develop communication protocols which would allow networked computers to communicate transparently across multiple, linked packet networks. This was called the Internetting project and the system of networks which emerged from the research was known as the "Internet." The system of protocols which was developed over the course of this research effort became known as the TCP/IP Protocol Suite, after the two initial protocols developed: Transmission Control Protocol (TCP) and Internet Protocol (IP”).

Moving forward from the basic of the development of the internet, we have come to a new era of communication. This form of communication is via wireless network, “going back to the 19th century, Guglielmo Marconi "the father of radio” made his mark in the world of wireless technology. When Marconi started experimenting with radio waves (Hertzian Waves) in 1894 his objective was to produce and detect radio waves over long distances. In 1896, Marconi was successful and obtained a patent and established the Wireless Telegraph and Signal Company Limited, the first radio factory in the world. In 1901, signals were received across the Atlantic and in 1905 the first wireless distress signal was sent using Morse Code. Wireless technology eventually progressed as an invaluable tool used by the U.S. Military. The Military configured wireless signals to transmit data over a medium that had complex encryption, which makes unauthorized access to network traffic almost impossible. This type of technology was first introduced during World War II when the Army began sending battle plans over enemy lines and when Navy ships instructed their fleets from shore to shore”.ii
Since the development of the radio wave, wireless networks have taken a toll towards the way that people setup and connect to a network. The beginning of WiFi devices has started to really emerge and the capabilities have become endless but with this capability we have now open a new form of hacking, which brings up the issue of security related to wireless networking. It is very simple to connect a WiFi access point to any current network topology, but the securing aspect is what a lot of novices have not completely implemented. This leaves open doors for anyone to access their systems, their wireless routers and performs malicious behavior which can lead to stolen information, locking or taking over the network, and even for the use of performing other malicious activities which will eventually end up hurting the incorrect individual(s).

**Wireless Network Requirements**

The basic requirement for a wireless network will include.

- **Wireless LAN cards** - One is required for each PC – These will go into a spare PCI slot inside your PC with the Antenna at the back of your PC.

- **Wireless Access cards** - these will be required if you have an older laptop that does not have WiFi capability.

- **Wireless USB adapters** - This is another form of wireless connectivity if for some reason you do not have a PCI slot available or your laptop does not accept and access card.

- **A wireless Router - This plugs into your Cable or ADSL Modem** - Depending on your connection. The Router enables you to both connect to your ADSL/Cable line as well as share the connection automatically between 4 to 16 computers, depending on the specification of the router purchased. Usually cable companies supply a cable modem; ADSL companies may require you to purchase an ADSL modem in which case an ADSL router is the option to pursue. Consult your ISP to see which will be available for purchase or given depending on the package.

Once you have obtained all the requirements, it will be time to connect and configure your wireless network. A basic configuration will include, connecting the
wireless access point to a ADSL/Cable modem, inserting the wireless access card on your laptop/pc, and configuring Windows/MAC/Linux to connect to your wireless access point. Below you will see a common wireless network configuration.

Wireless Network Protocols

Many protocols are available for a wireless network but choosing the best one will reduce the risks of being hacked. What are protocols? You may ask. Protocols are set of rules for communication as well as security. For example, if a device speaks English and the other one Spanish the communication will most likely fail due to the inability to communicate and exchange the correct information. Due to this we have protocol or rules that govern the way devices communicate, this gives it a standard way of communication.

There are a variety of protocols currently in use for wireless networking. One of the most used one is 802.11g. This standard is a huge improvement on the old standard
with was 802.11b which was only able to transmit at 11mbps. With 802.11g the transmission rate has been increased to 54mbps, but it still uses 2.4 GHz frequency range which unfortunately is also used by many other devices around the house. Another protocol is the 802.11a standard which runs in a whole different frequency range. 802.11a broadcasts in the 5 GHz range which allows for less interference from household devices. 802.11a standard is also capable of transmission rate up to 54 mbps like the 802.11g standard.

Wireless Network Security

Now in the 21st century, wireless communication is very prevalent and the need to keep the information safe which is traveling via wireless devices has become a very important topic. Many organizations, like schools, businesses, and others have in some form implemented the use of wireless connectivity. Even if the organization does not have a wireless access point they are still at risk if they have purchased new laptops for their employees. This is because now-a-days newer laptops have integrated wireless cards. Many wireless security requirements have been integrated on almost all wireless devices but the need for the individuals to setup and configure correctly is what has left a backdoor open for hackers. One of the most common and most simple to do this is to change the administrator password and even user name if possible to something that might not be so common. This will prevent unauthorized users to access the wireless access point or router and make configuration changes. A few forms of wireless network encryption can also be implemented, for example, a few of the most common ones are WEP, WPAv1, and WPAv2.

- **WEP** – This encryption is one of the most common encryption standards that comes with wireless LANs. It uses RC4 encryption which is the same as the one used for SSL web browser encryption. Anyone might think that this is a great form of encryption but when implemented on a wireless network it has flaws, which hackers have been able to discover and exploit.
- **WPAv1** – This form of encryption if a big improvement over WEP in that it used a pre-shared key (PSK) or passphrase to establish connectivity, but again it is
not a secure deal due to the fact that with a force dictionary attack a hacker can also gain access.

- **WPAv2** – “is a WiFi Alliance branded version of the final 802.11i standard. The primary enhancement over WPA is the inclusion of the AES-CCMP algorithm as a mandatory feature. Both WPA and WPA2 support EAP authentication methods using RADIUS servers and preshared key (PSK)”.

Even with these form of encryption added to a wireless network it is not an assurance that the network might not be compromise. Hackers have been able to exploit WEP and WPA encryption, so with time and patience one can discover the key to be able to access the network. Other steps that can be taken to secure a wireless network would be by using MAC filtering. With this, a router administrator can specify the computer with a certain MAC address to have access to the network, this ensure that only PC’s known to the administrator can have access. Again, this is not a huge improvement either because of the fact that hackers can still fake or mask a MAC address which will still provide them access to a secured wireless network. Another trick that can be used would be to disable DHCP and assign IP address to every pc on the network. This will prevent the router from assigning an IP address automatically to any pc that accesses the network. Again, this is not 100% safe because IP’s can also be masked.

**Wireless Network Security Software**

Many software are currently available that can be used for investigating and tracking the traffic on a network. A lot of these software are also available for free which allows for anyone to download them. Now is this a safe approach! Being that the software is advertised as a security probing software many hackers have been able to use them for their advantages. A few of these softwares are as follow;

- **BackTrack 3** – This software is a Linux Live CD which has all the tools that you would need to perform any type of network monitoring. The best part of this software is that it is all on a CD which can just be booted from, so there is no need to install or configure anything on a PC or laptop.
• **Airmon-ng** – This script can be used to enable monitor mode on wireless interfaces. It may also be used to go back from monitor mode to managed mode. What this means is that the wireless card will be capturing all packets it detects and not just the ones intended for its MAC address.

• **Airodump-ng** – “Airodump-ng is used for packet capturing of raw 802.11 frames and is particularly suitable for collecting WEP IVs (Initialization Vector) for the intent of using them with aircrack-ng. If you have a GPS receiver connected to the computer, airodump-ng is capable of logging the coordinates of the found access points. Additionally, airodump-ng writes out a text file containing the details of all access points and clients seen.”

• **Aireplay-ng** – “The primary function is to generate traffic for the later use in aircrack-ng for cracking the WEP and WPA-PSK keys. There are different attacks which can cause deauthentications for the purpose of capturing WPA handshake data, fake authentications, Interactive packet replay, hand-crafted ARP request injection and ARP-request reinjection.”

• **Aircrack-ng** – “Aircrack-ng can recover the WEP key once enough encrypted packets have been captured with airodump-ng. This part of the aircrack-ng suite determines the WEP key using two fundamental methods. The first method is via the PTW approach (Pyshkin, Tews, Weinmann). The main advantage of the PTW approach is that very few data packets are required to crack the WEP key. The second method is the FMS/KoreK method. The FMS/KoreK method incorporates various statistical attacks to discover the WEP key and uses these in combination with brute forcing.”

With these softwares that I have mentioned above, a hacker can gain access to a wireless network in a matter of minutes to a few days depending on how persistent the hacker is. This is also true depending on the current router encryption that is currently implemented for security purposes.
WarDriving

One of the most common ways that hackers try to access wireless networks is by the way of wardriving or driving around with the intention of accessing any open WLAN or easy to hack WLAN. With the softwares that I have mentioned above, an individual can drive around the neighborhood and try to capture as many packets needed to gain access to their targeted network. Once the hacker has gained access he/she can then try to take control over the network by accessing the router’s configurations. If the router is also protected with an administrator name and password, a hacker will most likely use brute force to try to gain access. Other ways that they can take over the network without the need to access the router is by becoming what is known as the man in the middle attack. With this the hacker is exactly that, man in the middle, where all the data from the wireless devices first passes through the hacker’s machine then on to the router. With this form of attack a hacker can capture all the information flowing throughout the network,
eventually being able to get password, usernames, and etc. Other form of attacks that a hacker can use would be DoS (Denial of Service) attack. With this form of attack a hacker overwhelsms the router by sending bogus requests and eventually drowning the router with messages and shutting down the network.

**Conclusion**

In conclusion, even though wireless networking has been increasing in what is now the most favorable form of networking, it is not very safe. From the experiment that I have performed in order to determine the weakness of wireless networking encryption, it really shows how individuals currently are still with the old format of wireless encryption, with this being WEP. This makes them very vulnerable to being hacked. As for the additional steps that I had explained previously for making a wireless network more secure, it is not 100% secure. Again for a persistent hacker they can find ways of masking and accessing a wireless network.

It is unbelievable how an individual with the use of a live cd can have access to software that can sniff, and break an encryption. Within this live cd there are also other tools for breaking password, as well as, other item that might be beneficial to anyone with a little more knowledge of what they are doing.
Acronyms and Abbreviations

- ISP: Internet Service Provider
- WIFI: Wireless Fidelity
- TCP/IP: Transmission Control Protocol and Internet Protocol
- HTTP: Hyper Text Transfer Protocol
- LAN: Local area network
- MAN: Metropolitan Area Network
- WAN: Wide-area network
- SSL: Secure Socket Layer
- IV: Initialization Vector

Definitions

Encryption: Any procedure used in cryptography to convert plaintext into cipher text in order to prevent anyone except the intended recipient from reading that data. There are many types of data encryption, and they are the basis of network security. Common types include Data Encryption Standard and public-key encryption.

Firewall: A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially Intranets. All messages entering or leaving the Intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Hacker: Unauthorized user who attempts to or gains access to an information system.

HTTP: the actual communications protocol that enables Web browsing.

LAN: It is a computer network covering a local area, like a home, office or small group of buildings such as a college.
Reference

ii http://www.jhsph.edu/wireless/history.html
iii http://www.dmccormick.org/pictures/WirelessHome.jpg
iv http://en.wikipedia.org/wiki/Wireless_security#WPAv1
v http://www.aircrack-ng.org/doku.php?id=airodump-ng
vi http://www.aircrack-ng.org/doku.php?id=aireplay-ng