Types of Attacks That Can Be Carried Out on Wireless Networks

Westley Hansen

CS 4960

Dr. Martin

May 7, 2015

Abstract

Wireless Networks are very mainstream, it allows a way for computer devices to connect to the Internet, but open or closed, Wireless Networks have security issues leaving it vulnerable to a variety of attacks. Wireless Local Area Networks (WLANs) have been around for a while, but now the technology is being utilized in a variety of ways depending on locations like; homes, small businesses, hotels, conventions, restaurants, schools and more. Before getting to types of attack there will be a chance to get familiar with the technology by explaining some terms and ideas that will be needed to make the reading more useful. After getting acquainted with some terms, the next area that will be covered is what is lost in security from making a Wi-Fi network open. The types of attacks that are focused on the attacks section were pick to examine because the Wi-Fi network is somehow involved with creating vulnerabilities for these attacks to exploit. Finally the last section discussed is about the software application creating vulnerabilities because an error in code.

1. Introduction.

Wireless networks are useful and popular because it provides a way for multiple devices access the Internet without needing a wired connection. Data can be transmitted through the air as long as the computer is within the range of the Wi-Fi access point. Wi-Fi access points are not bounded by the walls of a business or home and depending on where the access point is positioned within the building the signal can easily go beyond the exterior walls.

These days there are more computer devices focused on being mobile; tablets, smartphones, and some laptops are designed to be extra light for the mobile user. All of those computer devices have Wi-Fi because Wi-Fi access is not the only home network solution; there are businesses offering and advertising free Wi-Fi. Businesses like Starbucks, McDonalds, Target, Best Western and many more offer free Wi-Fi because the technology is so mainstream right now.

2. Computer Networking Terms.

The type of wireless technology that will be the focus is the IEEE 802.11 WLAN also known as Wi-Fi. WLAN uses radio frequencies to transport data between the computer and Wireless Access Point. The IEEE set the standards for 802.11 in 1999 and as the technology improves standards the 802.11 if followed by a lower case letter indication stands being supported like 801.11a/b/g/n. (Comer, 2009) The figure below show that the different IEEE Standards for 802.11 are not the same.

IEEE Standard	Frequency Band	Data Rate	Modulation Technique	Multiplexing Technique
original 802.11	2.4 GHz	1 or 2 Mbps	FSK	DSSS
	2.4 GHz	1 or 2 Mbps	FSK	FHSS
	InfraRed	1 or 2 Mbps	PPM	–none–
802.11a	5.725 GHz	6 to 54 Mbps	PSK or QAM	OFDM
802.11b	2.4 GHz	5.5 and 11 Mbps	PSK	DSSS
802.11g	2.4 GHz	22 and 54 Mbps	various	OFDM

Figure 1 (Comer, 2009)

A packet is a block data that has be sent by sender to destination by way of the network or The Internet. Packets can vary in size. Packets are composed of two types of

information; first is the routing information and second is the data which also called the payload. (Comer, 2009)

The definition of a frame is a block of bits. A way to visualize a frame moving through a channel can be seen in the following figure.

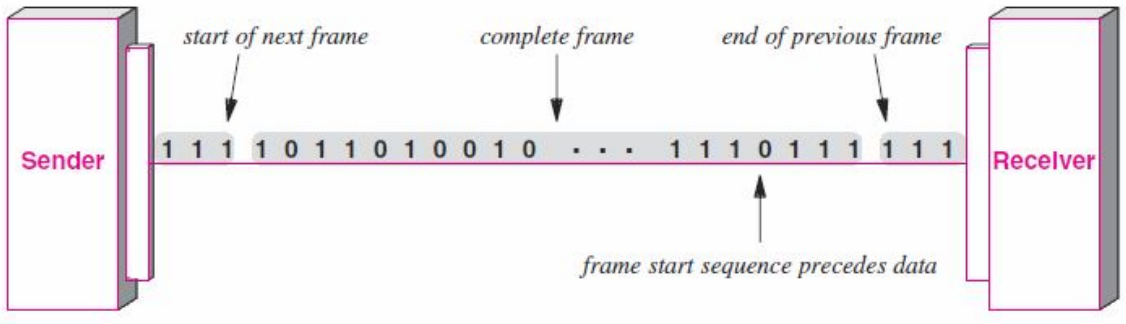


Figure 2 (Comer, 2009)

Handshake is a term to describe the act of setting up a connection between two endpoints. On a HTTPS website there would be a handshake to connect the Client and Server, also there would be a handshake to establish a secure connection where keys can be exchanged for encryption.

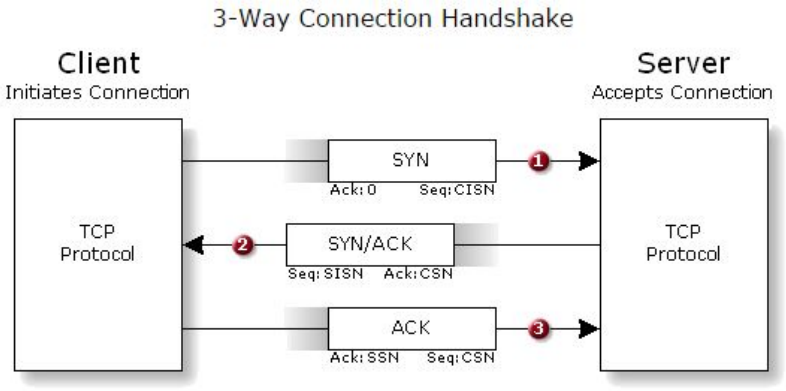


Figure 3 https://www.grc.com/r&d/nomoredos2.htm

The figure above shows a TCP handshake and the steps show exactly what is expected to happen. First the Client sends a Sync, than the Server responds with a Sync/Acknowledge finally ended with the Client Acknowledge.

3. Wireless Network Security.

Wi-Fi access points do not have to be open there are setting to close the network and require a password to join the network. When a Wi-Fi access point is closed the users of that closed network are safe from any type of packet sniffing because the packets are encrypted with either a WEP, WAP or WAP2. This kind of encryption is good for home user to setup so there won't be any outside eavesdropping. When Wi-Fi access points were in its early years an article notice that may home Wi-Fi were open because the consumer buying the product didn't know the full capabilities of Wi-Fi. So a home user setting up their Wi-Fi would click through the wizard following recommended setting and that is how Wi-Fi were left open because the company had that as the recommended setting. (Loo, 2008) These days the approach is that company default enables security on the W-Fi access point and therefore making the user responsible for turning off the security features if desired.

Large companies like Target are aware that there is a risk to offering open Wi-Fi for their customers. So the way companies have dealt with the problem, is that after connecting the Wi-Fi the first browser page the user sees will be of a terms of use agreement page. Which people usually just agree to so they can use the companies Wi-Fi. Here is what is in Target's Terms of Use agreement:

Quotes from Target Terms of Use for in Store Wi-Fi

Use of the Service is at your own risk.

The Service is not encrypted or secured in any way.

You assume full responsibility and risk for: (i) your own privacy and security; (ii) implementation any safeguards you deem to be appropriate to protect and secure your privacy and system; (iii) evaluating the stability, appropriateness or legality of any informational content.

Target has the right to monitor and screen your communications and activities.

(Target Brands, Inc., 2015)

The list goes on in the full Terms of Use page. It shows that the popularity of Wi-Fi because stores will to offer an insecure communication that leaves users at their own risk, while the company protects itself from lawsuits.

4. Types of Attacks.

The types of attacks that are going to be looked are going to be order by attack severity. First up will be packet sniffing, which is a network analysis tool and can be used to eavesdrop on open Wi-Fi networks, and could be considered a stepping stone for exploiting vulnerabilities of a network. Next the Session Hijacking will be covered, and followed by Man in the Middle.

4.1 Packet Sniffer.

Packet sniffing tools are not a way to carry out attacks that would affect a user's computer. Packet sniffers are designed to be a tool to diagnose the networks flow and trouble shoot network problems. (Adrian, 2011) Another way to view packet sniffing is,

"It's a lot like eavesdropping… just listening in on the conversation your computer is having with the gateway." (Adrian, 2011) Packet sniffers work by catching all packets being sent or received on the network, it does not cause delays on the network nor does it interfere with users connections to the Internet. A packet sniffer can be used to detect malicious activity on a network. Packet sniffing tools can reconstruct files, images, and webpages from captured packets. (Wireshark Foundation, n.d.)

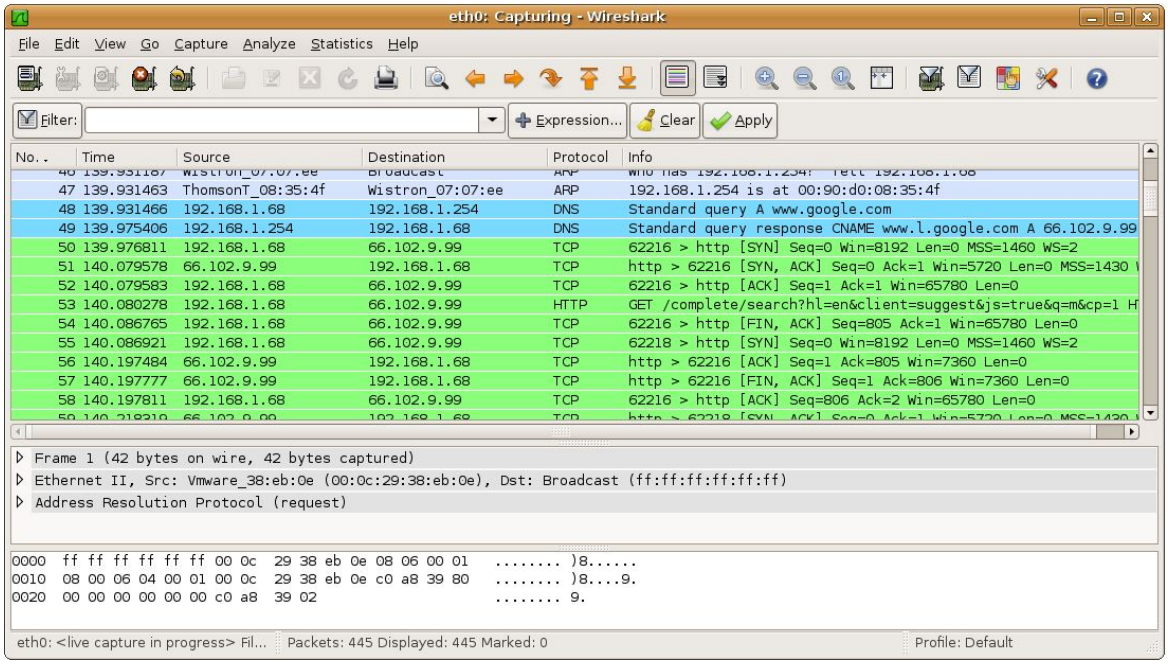


Figure 4 http://sectools.org/tool/wireshark/screenshot/0/

Packet sniffer can also give information about the type/brand of wireless router being used. This can allow attacker to gather information about an open Wi-Fi to explore vulnerabilities of the network. (Wireshark Foundation, n.d.)

Scenario: An attacker who finds an open Wi-Fi access point and joins the network than can start running a packet sniffer. After discovering the brand of Wi-Fi router being used the attacker can try logging into the router with the default user and password for the particular brand of router. If the attacker gets that level of access then the attacker basically owns that network.

4.2 Session Hijacking.

Session Hijacking involves capturing a cookie that has been used to authenticate a session on a server. Cookies are used to manage sessions between a Client and Server. If the user has requested to have the website to remember the sign password, then the cookie will add the user password to the cookie's data. Storing that kind of information in a cookie creates a weakness and something like packet sniffing (which is more eavesdropping, then an attack) can be used to capture to the cookie and possibly reveal log-in information. (Dacosta, Chakradeo, Ahamad, & Traynor, 2012) Even though there is HTTPS websites, packet sniffing tools like Wireshark, as stated on their website, can decrypt SSL/TLS (Secure Socket Link/ Transfer Layer Security) protocols and if a Key Exchange is found then it creates a possibility to decrypt cookies, and packets used on HTTPS websites. A Key Exchange is the way Client and Server decrypt each other's packets.

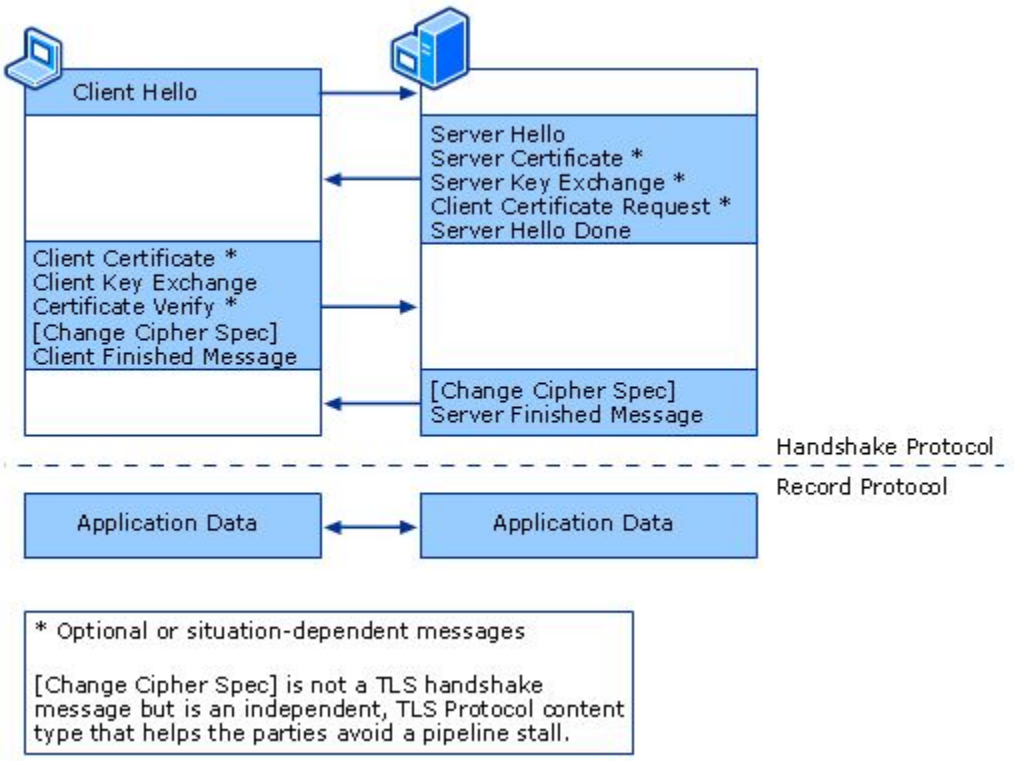
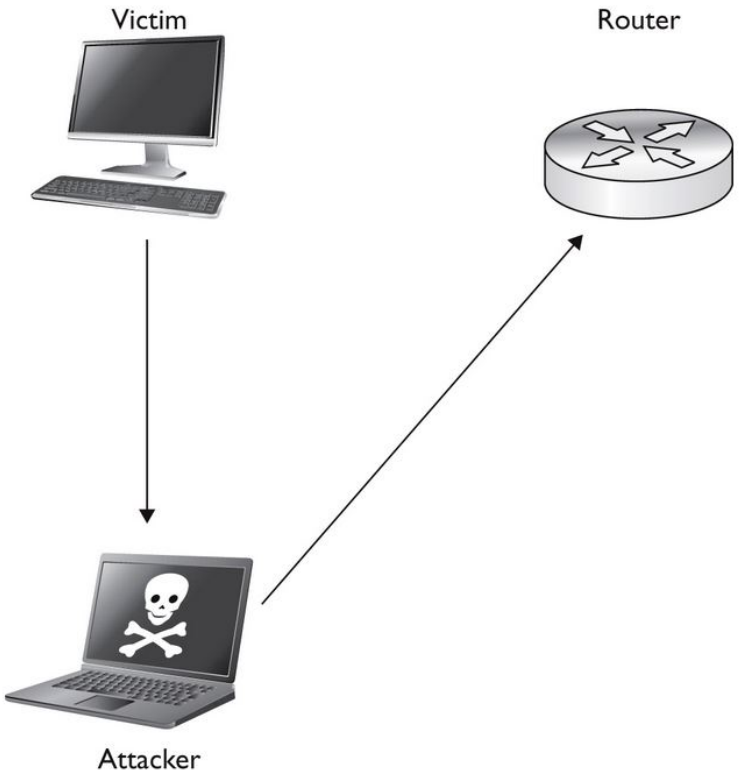


Figure 5 https://technet.microsoft.com/en-us/library/cc783349%28v=ws.10%29.aspx

Scenario: A possible environment where this type of attack could happen is at a hotel. Hotels offer free Wi-Fi to the guests so if an attacker was a guest at a hotel, there may be more of an opportunity to find high value victims. Guests may be more inclined to use the hotel Wi-Fi to make online purchases, travel arrangement, and send work documents.

4.3 Man in the Middle.

The idea to a Man in the Middle attack is not too hard to understand. The idea of a Man in the Middle attack is for the attacker to get in between the victim and the Wi-Fi router. Which will set a new path of data flow, where data between the victim and Wi-Fi router is flowing between the attacker's computer, who is in the middle. The following figure shows the new path that is created from a successful Man in the Middle attack.



Ways to carry out Man in the Middle attacks:

- ARP Spoofing
- DNS Spoofing
- Setting computer as a Hotspot with an inviting name

One way to carry out a Man in the Middle attack is to use ARP (Address Resolution Protocol) spoofing. First it is important to know what ARP does. The ARP is responsible for getting an IP address to the computer MAC address. (Regalado, et al., 2015) Continuing with the attack, the attacker will use an ARP spoofing tool to send an ARP message to the Victim to associate the attacker's MAC address with the victim's IP address resulting with the Victim's ARP cache to be updated by the attacker. So now any packets coming to the Victim's computer will first goto the Attacker's computer which

will then be forwarded to the Victim there by completing the Man in the Middle connection. At this point the Attacker will be able to see all packet info even if the website is encrypting its packets. (Regalado, et al., 2015) Also the attacker may be able to manipulate the data of the packets.

5. Denial of Service

Denial of Service attack also called DOS attack. A DOS attack is intended to deny victims from a network service (CERT Carnegie Mellon University, n.d.). The most common way to carry out an attack is by flooding. The specific case that will be looked at is a Sync flood; although a DOS SYN flood is an old way to carry out a DOS attack, it still works well when targeting smaller Wi-Fi networks.

A SYN flood is exploiting the networks method of establishing a connection. When a computer want to connect to a Wi-Fi access point the connecting computer sends a SYN then the Wi-Fi will send a SYN, ACK the Wi-Fi waits for the computer to finish the connection similar to a handshake. So in a SYN flood DOS attack the attacker's computer will use a tool to send a lot of SYN request to the Wi-Fi then the Wi-Fi will respond and wait, but the attacker never responds to finish the connection. That result is a lot of in filling up the waiting queue since each spot will be waiting for the connection to time out. This denies people who what to actually connect to Wi-Fi access because the Wi-Fi queue if full and waiting for fake connections.

6. Software Having Vulnerabilities.

Software can have vulnerabilities that are not seen immediately and vulnerabilities can go more unnoticed if the software is working correctly. Apple's operating system for OS X, iOS and Apple TV had a problem that effected the Safari web browser. The bug is in the following section of code:

The handshake algorithm containing the goto fail bug

```
if ((err = ReadyHash(&SSLHashSHA1, &hashCtx)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &clientRandom)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
        goto fail;
        goto fail;
    if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
        goto fail;
```

Figure 6 (Bland, 2014)

In the figure above is the code segment where the error occurs; there is an extra line of code in the end of the If statement:

If ((err = SSLHashSHA1.update(&hashCtx, &signedPrams)) !=0)
goto fail;
goto fail;

that causes the code to end prematurely. The extra 'goto fail;' caused to code to jump to the end without completing the SSL/TSL handshake. (Bland, 2014) Which means that the secured website the user connected to didn't establish a secure link. The code in the figure was copied six times though out Apple's system. Apple's website states, "An

attacker with a privilege network position may capture and modify data sessions protected by SSL/TSL." (Apple Inc., 2015) This error creates the opportunity for a Man in the Middle attack. All bugs were fixed in February 2014. (Bland, 2014) This example really stands out because it wasn't the customer or the potential attacker who created this vulnerability, it was a programmer who made a big error in the coding. The snippet of code could of easily been missed by the programmer since the code causing the big error was only two words long, 'goto fail;.'

7. Conclusion.

Wi-Fi access points continue to grow because it gives businesses an edge when they offer a way to connect multiple devices to the Internet without the need of many messy wires, but offering open Wi-Fi can make users vulnerable to a degree of attacks. Attacks like Packet Sniffing, Session Hijacking, Man in the Middle, and Denial of Service attacks can be carried out on open Wi-Fi creating security issues. Even software can create a weakness in a device with buggy coding. Researching the information for this paper sheds light how complex networks are and there are many areas of networking that people are trying to exploit and do some harm.

Future

Observing attacks at this level of the Internet was fun and gained a lot of factual knowledge. It would be interesting to see how attacks are carried out against large companies like Target, Sony Playstation, Sony Entertainment, and other big companies. While searching for information for this paper a term also showed up often in the

search; Intrusion Detection System (IDS). These systems are expensive and help aid the network authority find anomalies in the network. It would be interesting to see how the IDS algorithms worked, whether the algorithms are capable of learning.

References

Adrian, H. (2011, November 14). *Packet Sniffing Basics*. Retrieved from Linux Journal: http://www.linuxjournal.com/content/packet-sniffing-basics

Apple Inc. (2015, April 6). *About the security content of iOS 7.0.6*. Retrieved from Apple Support: https://support.apple.com/en-us/HT202934

Bland, M. (2014). Finding More Than One Worm in the Apple. *Queue - Security, 12*(5), 1-12. Retrieved from http://doi.acm.org.ezproxy.lib.csustan.edu:2048/10.1145/2620660.2620662

Bulbul, H., Batmaz, I., & Ozel, M. (2008). Wireless Network Security: Comparison of WEP (Wired Equivalent Privacy) Mechanism, WPA (Wi-Fi Portected Access) and RSN (Robust Security Network) Security Protocols. *e-Forensics '08* (pp. 1-6). Adelaide, Australia: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering.

Comer, D. E. (2009). *Computer Networks and Internets* (5th ed.). Upper Saddle River, NJ: Pearson Prentice Hall.

Dacosta, I., Chakradeo, S., Ahamad, M., & Traynor, P. (2012). One-time cookies: Preventing session hijacking attacks with stateless authentication tokens. *ACM Transactions on Internet Technology, 12*(1), 24. Retrieved from http://dl.acm.org.ezproxy.lib.csustan.edu:2048/citation.cfm?id=2220352.2220353&coll=DL&dl=ACM&CFID=509702246&CFTOKEN=89471183

Haidong, X., & José, C. B. (2005). Hardening Web browsers against man-in-the-middle and eavesdropping attacks. *Proceedings of the 14th international conference on World Wide Web (WWW '05)* (pp. 489-498). New York: ACM. Retrieved from http://doi.acm.org.ezproxy.lib.csustan.edu:2048/10.1145/1060745.1060817

Wireshark Foundation. (n.d.). *Wireshark Frequently Asked Questions*. Retrieved from Wireshark: https://www.wireshark.org/faq.html