The Real Risks of Unencrypted Networks

Phil Peichel

12/12/2014

Abstract

Commercial wireless networking has become widely popular since the late 90's. They are used in a wide variety of locations such as airports, schools, and even households. Because of its widespread use and popularity, protection should be the number one priority for developers. While encryptions have provided users data protection, the use unencrypted networks have become widely popular due to its ease of access. This means that people are using a network which has the potential to expose very personal or critical data. So, how have people been able to protect themselves in the past? Virtual Private Networks (VPN's) and Hypertext Transfer Protocol Secure (HTTPS) have provided a ”protection on the go” service. But is this enough? Through these applications, as well as education the general public, the use of unencrypted networks can slowly become a safer environment to use.

Contents

A Introduction

When on the topic of network security, it is generally a good idea to at least have a breadth first insight of the characteristics, dangers, and uses of networks.This way of thinking is especially important for the general public who may not know the dangers that networks possess. These dangers increase even more when using unencrypted networks. This is because there is nothing standing between the user and the network. However, even with all of these dangers we should not just give up on unencrypted networks. These unprotected networks offer unique and useful environments, some of which end up being more efficient than encrypted networks. Even though they are potentially dangerous, unencrypted networks have become an important part of the modern wireless infrastructure.

B Background

Commercial wireless networks began to commercialize in the late 90's and early 2000's. This came paired with the 802.11 standards for wireless outlining two forms of authentication- Open System Association (OSA) and Shared Key Authentication (SKA). [11] OSA is an unencrypted network type that allows anyone to join.Its only credentials contain the name it broadcasts so users know which network to join. On the other hand, SKA led to an encryption based security known as Wired Equivalent Privacy (WEP). WEP configured a set amount of shared keys to be used across the network. Even with the addition of security credentials, this does not mean that they were safe. In fact, WEP contains numerous exploits. One example of an exploit actually comes from a potential solution to a problem WEP was trying to address. To solve synchronization issues, WEP used a per-packet exchange of keys instead of a per-session. This means that the master key is used much more frequently, meaning more chances of a leak. This system is almost counterintuitive in the sense that it is causing a higher chance of exposing sensitive information, instead of protecting it. Through some trial and error of a few different protocols we get to our most recent standard, Wi-Fi Protected Access II(WPA2). It is still quite similar to Wi-Fi Protected Access (WPA), "but it is widely accepted as the most secure wireless authentication currently available. Its secure key exchange, key rotation, master key protection and AES encryption are all best-of-breed in security technologies for now." [11]

C Issues

Wireless Network security issues have always revolved around two main points. The first is access. If there is no specified control as to who can use the network, then anyone near by would have the potential to join.The other point is privacy. This dictates who can and can not looks at the information that is being passed around. As stated earlier, unencrypted networks allow anyone to join the network. This means that "Your unencrypted network traffic is then clearly visible to everyone in range. People can see what unencrypted web pages you're visiting, what you're typing into unencrypted web forms, and even see which encrypted websites you're connected to so if you're connected to your bank's website, they'd know it, although they wouldn't know what you were doing."[12] This is exactly why unencrypted networks have the potential to be devastating. All of this data is just "floating through the air" unprotected. It's through this idea that potential flaws began to arise. A multitude of attacks have been developed that take advantage of this environment. Any device that is connected to an unencrypted network is at a potential risk of having its data leaked. We can see that, both in the past and even currently, wireless networks still contain security flaws that could lead to dangerous leaks of sensitive information.

C.1 Types of Attacks: Passive

A multitude of attacks have been developed that take advantage of unencrypted networks' characteristics. These attacks can be split into two categories: passive and active. A passive attack is "An attack in which an unauthorized party gains access to an asset and does not modify its content (i.e., eavesdropping). Passive attacks can be either eavesdropping or traffic analysis (sometimes called traffic flow analysis)" [12] Eavesdropping, or snooping, listens in on other devices that are sharing the unencrypted network. From there they can see what unencrypted sites people are using, the information users input into these unencrypted sites, and can even keep track of the encrypted sites people visit. With this sensitive information the snoopers can now input and hijack other's sessions, which could lead to even personal information. People don't even have to develop the code for these snooper programs. Wireshark and Firesheep are just two examples of free and easy to use snooper programs scattered across the Internet.[5] Traffic analysis works a little different than snooping. While both listen in on the packets that are being sent through the network, traffic analysis monitors the frequency and length of messages. This allows the receiver to guess the information whether or not it is encrypted. This isn't as popular since the process can turn into a brute force scenario. However, this brute force has the potential to work on both encrypted and unencrypted networks. Of course, if the information is correctly guessed, then the user would gain access to the (possibly) desired information.

C.2 Types of Attacks: Active

Active attacks directly attack the user in order to obtain their sensitive information or even hijack the session. There are several types of active attacks which include Masquerade, Replay, Modification, and Denial of Service (DOS). [12] Masquerade is where the attacker pretends to be something else. This could be it pretending to be a different device or wireless network. An unsuspected person might connect to Cafe xx wireless instead of Cafe Xx wireless, which is the official wireless of Cafe Xx. Instead of connecting directly to the wireless router, this victim has connected to an Ad Hoc network. This means that the person first connects to the hacker's computer and then receives Internet access through the attacker's wireless card. The victim will then unknowingly be passing information directly to the attacker before the call is sent out to the router. From there the information can be collected and abused. Modification of messages does exactly what its name states. It grabs packets and modifies part of it and either resends it or asks for another request. One of the main ways to approach this attack is through the use of email. The attacker sends an email that contains a hyper-link. The email itself does not contain any malware and the hyper-link looks legitimate (it may be a hyper-link that has a few characters changed, etc.). The hyper-link then redirects the victim to a malicious website and from there either asks for credentials or deposits the malware directly. This is what makes direct attacks hard to notice. Finally there is the Denial of Service attack (a.k.a DOS). A DOS attack can either inhibit or prevent the use of services. These attacks are usually aimed at specific websites or servers. The assailant attempts to overflow the site or server with requests (or pings) to the point where the server (or website) either slows down or stops functioning. This can essentially disable your computer, website, or network. It can also consume all of the target's resources with the possibility of having those resources work against the target.

D Why Take the Risk?

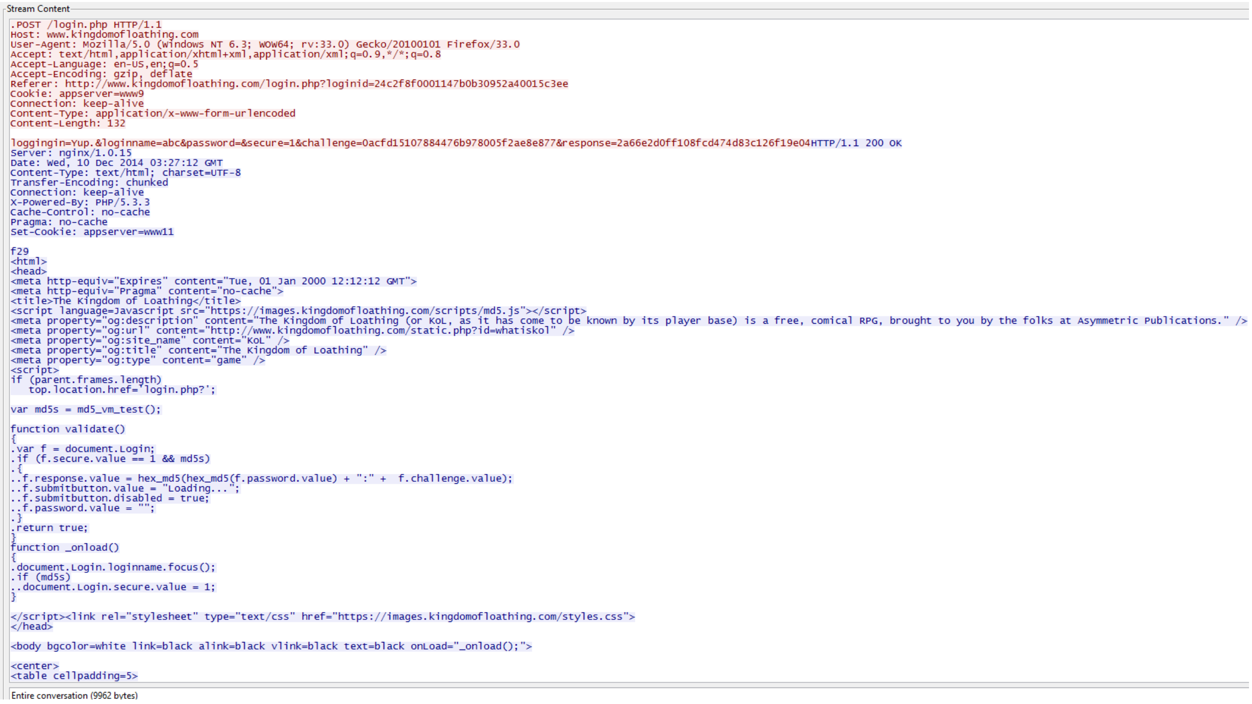
We have seen that unencrypted networks are vulnerable to two types of attacks. What these attacks have in common is that they actually end up making the captured packets into something that the hacker can use. These can be quite devastating since these captured packets can contain sensitive data. So out of the two, why would anyone want to choose the unsecured option? Is there any real reason to expose oneself to all of these potential dangers? Well it all boils down to a location and purpose outlook. Both home and business setting should probably be using some form of encryption. Be it provided security protocols, such as WPA or WPA2, or even their own personal VPN. On the other hand, having an open network provided as a service in libraries and coffee shops is very convenient. The desired content can also have an affect in choosing which network to use. While checking the weather may not warrant the use of encryption, accessing ones bank information (or other personal information) is highly recommended to be done through a secure network. Quick and easy access is not the only thing that unencrypted networks provide. They also can be used for fast and heavy downloads and file transfer. This is because it is not necessary for the data and router to continuously check each others' keys (i.e the correct information is going to the desired place from its proper owner). Keeping these two ideas in mind, we can see whether or not it is 'worth the risk' when using unencrypted networks.

E Potential Solutions

Should unencrypted networks be avoided since they contain potential dangers? Well no, it's not as though everyone will be instantly attacked as soon as they connect to an unencrypted network. While unencrypted networks offer the least amount of protection, we have seen that encrypted networks aren't one hundred percent safe either. So how can people protect themselves when using unencrypted networks? First of all, the general populace needs a better understanding of the dangers that reside within using unencrypted networks. While it may be fine to connect to the coffee shop's wireless to check on the weather, using the same wireless to check one's bank balance would be ill advised. Second should be the continual development of more security protocols that would be available to those who wish to use them. VPNs and HTTPS are two of the most popular tools used for security on the go."A VPN, or Virtual Private Network, allows you to create a secure connection to another network over the Internet. VPNs can be used to access region-restricted websites, shield your browsing activity from prying eyes on public Wi-Fi, and more." [5] VPNs act as your personal security guard when connecting to the Internet. All traffic travels through a private channel which only you have access to. It also allows you to connect multiple personal devises and have them all act as though they were on the same local network. It also allows access to Geo-Blocked websites, bypass of Internet censorships, the downloading of files, as well as other useful tools.[5] VPNs are just one of the tools available to the public. However, VPNs do not guarantee safety. A VPN only secures the sending of the data from the user's computer to the desired website. Once the information reaches the website, it is up to the site's digression on the security of the data. If the site were to be corrupted, then the information would be in the hands of the attacker. This is just one of the examples of the flaws of VPNs. However, even with their flaws, the use of VPNs greatly reduces the risk of an attack. Being as safe as possible while using an unencrypted network is the best available option. If both the knowledge of wireless networks and the tools used to protect them grows, then wireless security should be able to grow at both a safer and quicker pace.

F Project

For my project I wanted to see what I could attain from a unencrypted network while using a snooping method of attack. In order to do this I used a network analyzer called WireShark. It is a free program which, when connected to the desired network, will listen in on all the devices communicating on a network. This means that I am able to capture and decipher all of the traffic from the different users accessing the web. There were several things I noticed right away. First of all, I was able to track the host and destination of traffic. This means that I know exactly which device is communicating a website, and vice-versa, based on IP addresses. WireShark even gave the option to display device and website names instead of IP addresses in order to avoid confusion. The next thing I noticed was the sheer amount of different packets that were captured. It documents every single interaction between the device and destination. This includes requests, acknowledgments, certificates of authentication, password prompts, and so on. In order to not become overwhelmed by mass amounts of data, WireShark allows users to filter through the packets in order to find specific packet types. For my project, I was looking for unencrypted HTTP packets. With these packets I wanted to test to see whether or not I would be able to reconstruct objects with the information that was stored inside. This included both images as well as HTML web sites.



```
.POST /login.php HTTP/1.1
Host: www.kingdomofloathing.com
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:33.0) Gecko/20100101 Firefox/33.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.kingdomofloathing.com/login.php?loginid=24c2f8f0001147b0b30952a40015c3ee
Cookie: appserver=www9
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 132

loggingin=Yup.&loginname=abc&password=&secure=1&challenge=0acfd15107884476b978005f2ae8e877&response=2a66e2d0ff108fcd474d83c126f19e04HTTP/1.1 200 OK
Server: nginx/1.0.15
Date: Wed, 10 Dec 2014 03:27:12 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Cache-Control: no-cache
Pragma: no-cache
Set-Cookie: appserver=www11

f29
<html>
<head>
<meta http-equiv="Expires" content="Tue, 01 Jan 2000 12:12:12 GMT">
<meta http-equiv="Pragma" content="no-cache">
<title>The Kingdom of Loathing</title>
<script language=Javascript src="https://images.kingdomofloathing.com/scripts/md5.js"></script>
<meta property="og:description" content="The Kingdom of Loathing (or KoL, as it has come to be known by its player base) is a free, comical RPG, brought to you by the folks at Asymmetric Publications." />
<meta property="og:url" content="http://www.kingdomofloathing.com/static.php?id=whatiskol" />
<meta property="og:site_name" content="KoL" />
<meta property="og:title" content="The Kingdom of Loathing" />
<meta property="og:type" content="game" />
<script>
if (parent.frames.length)
   top.location.href='login.php?';

var md5s = md5_vm_test();

function validate()
{
.var f = document.Login;
.if (f.secure.value == 1 && md5s)
.{
..f.response.value = hex_md5(hex_md5(f.password.value) + ":" +  f.challenge.value);
..f.submitbutton.value = "Loading...";
..f.submitbutton.disabled = true;
..f.password.value = "";
.}
.return true;
}
function _onload()
{
.document.Login.loginname.focus();
.if (md5s)
..document.Login.secure.value = 1;
}

</script><link rel="stylesheet" type="text/css" href="https://images.kingdomofloathing.com/styles.css">
</head>

<body bgcolor=white link=black alink=black vlink=black text=black onLoad="_onload();">

<center>
<table cellpadding=5>
```

Figure 1: Unencrypted Packet

Figure 1 shows what an unencrypted packet may look like. It is one of the example HTTP packets I used for reconstruction demonstrations. If you look closely you can see that it contains the URL name, server information, and HTML code of the web site. This HTML code can be used in a complier in order to recreate a replica of the web site. With this information we can test and see that this site is capable of. One of my tests included whether or not I would be able to obtain the user name and password that the site requests on login. My findings showed that the packet had designated locations for both the user name and passwords I tested. The user names showed up every time, but the passwords were encrypted. This is because the website encrypts the password in a cookie once the user requests access. This is just one way websites can offer security, even without the use of HTTPS or an encrypted network. Now of course attackers have easy access to the user names, but this protection is still better than nothing while using an open network. After being able to find parts of critical information, I tested whether or not there was enough information necessary for recreation of objects. I was successful in duplicating both images and websites. This showed that unencrypted networks have the potential for information to be captured and interpreted in a some what easy manner.

G Future Trends

There have been a few trends in the past for the development in wireless networking. Speed has always been important. Over the past several years speed, both upload and download, has dramatically increased. We can see this even in the most recently approved networking standard. IEEE 802.11ac was just approved this past January. It has an expected throughput of at least 1 Gig per second. This will provide a much faster environment when being compared against previous standards. Since it was just approved, it will take a few years to fully implement this protocol. This trend of constantly trying to upgrade speed levels seems pretty straight forward. Faster speeds can benefit multiple work fields. It is an all around desired improvement as there is no foreseeable speed cap in the future. Protection has also had a few trends in the past. The encryption protocols of the past were always quickly noted of their flaws. Many different types of exploits were developed as a result of this. So the only thing left to do was create a more secure plan of action. WPA2, VPN's, and HTTPS are the results of these desires. The development of a secure protocol that doesn't hinder the user and others around him is necessary in order to feel safe when using wireless networks.

G.1 Theoretical Limitations

Theoretical speed limitations is an interesting topic. 'The disparity between theoretical and practical Wi-Fi performance comes from network protocol overhead, radio interference, physical obstructions on the line of sight between devices, and distance between devices.' [9] All of these factors are incredibly important for wireless speed. So while we may develop the potential to reach incredible speeds, these factors will hinder it from reaching its maximum potential. However, when speeds of around 100 gigabytes per second have been successfully tested, the future of much faster wireless speed looks promising. Protection also has some key limitations.'Taking advantage of network-based security features is difficult in that geography and topology are major factors. They dictate ownership boundaries and legal jurisdictions, and it's hard to establish a set of choke points from which all network traffic can be monitored or controlled.'[7] How do we make a security protocol that completely protects the user while not impeding on those nearby. Since wireless networks can span over such large areas, it is hard to say who should have authority over security type, allowed content, bandwidth control, etc. Until these key points are figured out, it will be hard to expand upon our current security protocols.

H Conclusion

While networks an incredibly useful way to access the web and transfer data, we have also seen the dangers that lurk within it's us. Both passive and active attacks give the potential for loss of sensitive data. Options do exist that allow for a 'safer' browsing experience, but a one hundred percent secure option does not exist. However, just because unencrypted networks may not be the safest way to browse the Internet, it does not mean that they should not be used. If users become more informed on the whens, wheres, and whys of networking, then users can fear less about potential loss.The future of wireless networks security should push towards two ideas. First should be the development of a more secure protocol then the standards which are being used currently. The second idea is teaching the general populous about wireless networks, what to watch out for, and the countermeasures used to better protect themselves. Its these steps that will make both encrypted and unencrypted wireless networks safer places.

References

[1] Eric Butler. Firesheep. http://codebutler.com/firesheep/.

[2] Eric Escobar. The dangers of unsecured wifi hotspots. http://www.quickanddirtytips.com/tech/mobile/the-dangers-of-unsecured-wifi-hotspots?page=1.

[3] Eric Geier. Here's what an eavesdropper sees when you use an unsecured wi-fi hotspot. http://www.pcworld.com/article/2043095/heres-what-an-eavesdropper-sees-when-you-use-an-unsecured-wi-fi-hotspot.html.

[4] Eric Geier. What wi-fi eavesdroppers see on unsecured networks. http://www.nowiressecurity.com/articles/.

[5] Chris Hoffman. Htg explains: What is a vpn? (and why you might want to use one). http://www.howtogeek.com/133680/htg-explains-what-is-a-vpn/.

[6] Michael Kassner. Convenience or security: You can't have both when it comes to wi-fi. http://www.techrepublic.com/blog/it-security/convenience-or-security-you-cant-have-both-when-it-comes-to-wi-fi/.

[7] David Lacey. The future of network security. http://www.computerworld.com/article/2537015/networking/the-future-of-network-security.html.

[8] Michael Miller. The future of wireless networks. http://forwardthinking.pcmag.com/show-reports/303730-the-future-of-wireless-networks.

[9] Bradley Mitchell. How fast is a wi-fi network. http://compnetworking.about.com/cs/wireless/f/wirelessspeed.htm.

[10] Keith Morris. Wireless security: Past, present, future. http://www.giac.org/paper/gsec/3229/wireless-security-past-present-future/105346.

[11] null. A brief history of wireless security. http://securityuncorked.com/2008/08/history-of-wireless-security/.

[12] Madhavi Dhingra Deepika Srivastava and Vipul Sharma. Wireless network security threats and their solutions: A short study. http://www.techrepublic.com/resource-library/whitepapers/wireless-network-security-threats-and-their-solutions-a-short-study/.

I felt that there was a lot that I learned in this class over the last semester. I transfered into the Computer Science major quite later into my college education. Because of this, I feel as though there has been a huge influx of new information being thrown at me constantly. I felt that this course really allowed me to focus in on one area of interest since there are many topic areas which are unknown to me. Of course this doesn't mean that the other courses have had no affect on me. Learning how to program has greatly changed even just the way I think and approach problems. I feel as though my thesis would have been quite different without a programming background. Networking was also a very influential class. It was very helpful to both get information from a class as well as from my own independent research. Having both opportunities side by side made understanding some of the new information easier. Operating Systems was also helpful in that it gave me a background in encryption methodology. Understanding this made the how's and why's of encrypted networking easier. In return, these factors helped make a much stronger thesis presentation. I felt that having this class truly did bring in different elements of my past and present computer science classes.