Public Wi-Fi: Friend or Foe?

Dave Mancinelli

December 13, 2013

Abstract

Public wi-fi hotspots have become ubiquitous in coffee shops, airports, and other commercial venues where consumers have come to expect internet connectivity for their laptops, smart phones, and tablets. The traffic on public networks is largely unencrypted, but public wi-fi users, many of whom are unaware of the associated risks, continue to log in to email accounts, Facebook, bank accounts, or any other domains containing sensitive personal information. Such an environment – wherein a large base of users sends personal data across an unprotected network – could also be a hotspot for nefarious hacker activities. This paper examines the known hacker exploits of public wi-fi networks, such as man-in-the-middle attacks, packet sniffing, and ARP spoofing; analyzes the risks of using public networks; and provides recommendations for safer public wi-fi usage.

1 Introduction

Consumers have become to expect free, easy to use wi-fi in almost any public location, but are they aware of the dangers open public networks pose to their data? The risks have grown increasingly in the past few years, with many consumers engaging in online banking, shopping, and other communications over unencrypted public networks. Privacy has been a concern secondary to convenience for many users, but this may be a product of a lack of cyber security education. Public networks are among the easiest for attackers to exploit because of their open nature and the number of people who use them every day.

This paper aims to highlight some of the well-known attacks used on public networks and to analyze the balance between data protection and convenience.

2 Privacy and Data Leakage

The U.S. Census Bureau reports that retail e-commerce sales totaled $194 billion in 2011, an increase of sixteen percent from 2010 (U.S. Census Bureau, 2013). In 2011 sixty-eight percent of urban adults had ever performed some online banking (twenty-four as a typical daily activity), fifty-five percent had ever paid bills online, and seventy-three percent had ever bought a product online (U.S. Census Bureau, 2012a, b). Privacy loss is not limited to financial transactions, however, as forty-three percent of all users typically check a social networking site daily, and sixty-one percent send or read an email daily (U.S. Census Bureau, 2012a). The internet now provides a user easy access to many forms of personal information. The continuing rapid growth in e-commerce, online financial services, and social media suggests that consumers value convenience over the risk of online data theft. It is this preference for convenience that has driven the expansion of public-wi-fi hotspots into almost every public arena.

Users appreciate the benefits that public wi-fi offers them, but are they concerned, or even aware, of the dangers that an open public wi-fi network presents? The small survey conducted by (Attipoe, 2013) suggests not, as seventy-two percent of respondents were concerned with privacy loss, but sixty-two percent answered they were not aware of any security threats to a public network. In fact, seventy and thirty percent of users reported shopping online and banking online, respectively. Given the number of attacks that even a novice cracker could perform on an open network, there is a very real concern that personal data could become the property of a nefarious agent. This data includes, but is not limited to, bank account information, personal emails and contact lists, credit card numbers, passwords, and private communications. Once data is stolen, it cannot be recovered, and in most cases the users will never know who committed the theft, how it happened, or when it happened. The attacker could use the data in a number ways, for example, by selling credit card numbers, gaining access to a user's online accounts, or sending spam messages to contacts.

3 Attack Vectors

This section describes several attack strategies that can be used on open wi-fi networks. In many cases, it is very difficult, if not impossible, to detect that an attack is occurring. This is due to the open nature of public-wi-fi hotspot connections. Two main properties of public wi-fi provide attackers with relatively easy access to other users' data: (1) the unencrypted nature of public networks; and (2) the lack of a physical barrier to receiving all packets on the network. With neither of these security guards in place, an attacker can join the network anonymously, sniff packets intended for other users, redirect traffic to the attacker's computer, or otherwise disrupt network services. Further, these attacks are virtually untraceable, and in most cases very difficult to detect, making public wi-fi hotspots an even more attractive target to criminals.

The rest of this section details the most widely used attacks on public wi-fi networks, but certainly does not include all possible vulnerabilities.

3.1 Sniffing and Scanning

Sniffing By far the easiest and stealthiest method of intercepting other users' data is known as "packet sniffing." On an open, unswitched network such as most public wi-fi hotspots, data packets intended for a specific user are actually sent unencrypted to all other users connected to the network. There are several popular tools that will perform packet sniffing with the click of a button, like Wireshark, tcpdump, and Cain and Abel. Once sniffed, packets can be analyzed to find username/password pairs, files, instant messages, or any other unencrypted data sent over the network. Simply examining HTTP traffic can allow an attacker to infer patterns in another user's web browsing, which may facilitate other, more complicated attacks. Packets may also give away information on users' identities, for example from the device names sent from iPhones. There is very little protection against packet sniffing on an open network, because it is a completely passive action. The unintended recipient does not need to change network flow in any way but simply has to listen. This also makes it impossible for a sniffer to be identified by technological means.

Scanning Scanning is method used to determine other hosts on the network. Though scanning can serve many legitimate purposes, an attacker can scan the network for exploitable weaknesses. Scans are generally difficult to detect, and most public hotspots do not have the resources to monitor such activity. There are several different types of scanning methods, though each follows the basic principle of sending certain types of packets to all possible IP addresses on the network and examining the responses. From those responses, an attacker may be able to identify, or "fingerprint", specific information about machines, such as operating system or open ports. Armed with this knowledge, an attacker may be able to propagate malware, use another host in a denial-of-service attack, or perform some other form of illicit behavior.

Man-In-The-Middle A man-in-the-middle attack (MITM) is a slightly more complicated form of attack, but it can allow for more . To describe this type of attack, it is best to start with an example. Consider Sally, who has connected to the public network at her local Starbucks and is searching for dogs on petfinder.com. She does not know that Dan, an attacker, is sniffing her packets and preparing a man-in-the-middle attack using her IP address. First, Dan tells Sally that he is the router, and then tells the router that he is Sally. When Sally tries to connect to petfinder, she is actually sending the request to Dan, who reads her request and forwards it on to the petfinder server. When the data returns, Dan replaces it with only cats, and sends it on to Sally, who thinks it is a legitimate response.

This attack relies on Dan's ability to manipulate the address resolution protocol (ARP), which links IP addresses to ethernet addresses. All hosts on the network communicate via ARP and keep a table with the link layer addresses of all other hosts. The vulnerability occurs because any host can announce that it is associated with any IP address, which allows a host to impersonate another. This strategy is know as ARP spoofing, and there are a number of tools that implement it.

A more serious MITM attack can even circumvent measures meant to keep data private, such sending data via the Secure Socket Layer (SSL) protocol. Acting as a tunnel from endpoint to endpoint, SSL provides a layer of encryption to HTTP traffic. However, an attacker can thwart this system by convincing another host that it is the intended recipient of the original data. In the example above, Dan would engage in Domain Name System (DNS) spoofing as well. When Sally makes her initial request, she asks a DNS server for petfinder's IP address. Since Dan sees that traffic first, he responds to Sally with his own IP. Now Sally initiates a secure connection with Dan, who is able to decrypt her data. He then re-encrypts that data, and sends it to the real website. To both parties, this looks like a secure connection.

There are safeguards to these attacks, but in many cases, they are not enough. Many SSL servers will use a certificate authority to verify the identity of the SSL connection. However, in many cases, the user is simply presented with an esoteric message about certificates, which is many users will unknowingly accept.

Rogue Access Points In this kind of attack, an attacker poses as an access point (AP) meant to look like a legitimate AP. A user may then connect to this AP, which in turn gives the attacker complete access to all network connections from that user (Brody, Gonzales, and Oldham, 2013). Rogue access points spawn from the newly established connectivity paradigm: users expect an internet connection wherever they are, and for free. Because of this demand, proving authenticity of an access point is a difficult challenge, as it can hamper a user's ability to connect to an AP quickly and transparently in any setting.

Dondyk and Zou (2013) point out a new attack via rogue access point, which they call "denial of convenience." The attack stems from the convenience offered to mobile device users, who benefit from public internet connections. In this attack, a user would connect to the fraudulent AP, but no requests for data would pass through. Since most smart phones will disable broadband connectivity in favor of a wi-fi connection, this renders the phone incapable of receiving data. This is just one of many attacks can be performed within the ever popular realm of mobile connectivity.

Denial of Service Like the denial of convenience attack described in the previous section, a denial of service (DoS) attack aims to disrupt service to a user's (or many users') device. A DoS attack can either make use of the spoofing and MITM tactics described earlier, or by means of network flooding.

Using spoofing, an attacker trick other users on the network into sending requests to the attacker. To execute the denial of service, the attacker need simply not pass the request packets through to the intended recipient. In a public wi-fi hotspot, a user would no longer have access to the router, and all network traffic would seem to cease.

One drawback of public wi-fi is the limited bandwidth it naturally imposes on users, especially at busy times (Noor, 2013). In this case, an attacker could flood the network with bogus packets, essentially eating up all of the allowable bandwidth. Users would notice either very slow or nonexistent network traffic entering and leaving their devices. It may seem that the attacker in this case would be easily identifiable, however, the attacker can spoof sender address on the bad packets. The attacker could also implement an attack wherein another user's machine is tricked into implementing the attack another user. This redirection makes it very difficult to pinpoint the actual perpetrator and prove guilt.

4 Protection Practices and Strategies

Why are public wi-fi hotspots so insecure? Unfortunately, there is a tradeoff between data privacy and user convenience. Finding the right balance between these two can prove difficult, and many public networks appeal to users' demands of easy, quick access by offering little to no protection. In fact, Starbucks specifically markets its wi-fi as being a "free, one-click" hotspot with "no password needed" (http://www.starbucks.com/coffeehouse/wireless-internet). This section provides some suggestions of preventative measures that can be taken by implementors and users of these networks alike.

Providers Providers of public wi-fi hotspots take a "use at your own risk" approach to network security. Most public wi-fi vendors will redirect a user's browser to a "terms of service" page, which must be agreed upon before the user can connect. This redirection is known as a "captive portal," and may also be used to check user authenticity or charge for connectivity (Spaulding, 2012). While this strategy provides the user with some indication that the portal is insecure, it does not do enough to warn users about the potential dangers. Instead, this page often presents a lengthy legal document that protects the vendor from data loss liability, which most users will likely dismiss without reading. In the case of Starbucks, the captive portal does not offer any indication that the user is connecting to an insecure network (http://www.starbucks.com/coffeehouse/wi-fi-auth). In the small survey conducted by Attipoe (2013), eighty-six percent of respondents answered yes to having connected to public wi-fi, twenty-one percent thought that public networks were secure, and forty-four percent were not sure about the security of public networks. These numbers indicate that users are largely uneducated about the potential for personal data loss when they are at their local coffee shop. Therefore, education campaigns and precise, clear warnings about public networks are the first step towards a more secure public internet.

Although public vendors may not be willing to sacrifice ease of use for confidentiality, adding encryption to their networks would greatly decrease the possibility for data loss. Though encryption would not completely secure data on a network (e.g., an attacker with the network password could still decrypt the information), it does add a layer of complexity that could persuade an attacker to look elsewhere.

Users Users can take several steps to ensure that their own data is reasonably protected when accessing public wi-fi hotspots. Of course, the best security measure is to not send any data that the user would not want intercepted. However, this means the user must sacrifice some convenience, such as paying a bill at the coffee shop, for security. If sensitive data must be sent via HTTP from a public network, a user should ensure that all traffic is encrypted using a secure socket layer (SSL) or transport layer security (TLS) for the duration of the remote connection. Though an attacker may still be able to subvert secure protocols in some cases, the time and complexity involved may dissuade the attacker from trying.

The next option for users is to send all transmission through a virtual private network, or VPN. A VPN works as a "benign man-in-the-middle," allowing a user to communicate via an encrypted channel to any other point on the internet. One drawback of using a VPN is the added cost, as most VPN providers charge a recurring fee for their services. In addition, users must know in advance to use VPN technologies, and then take steps to install software and set up the service. To get around this issue, Radenkovic, Howard, and Greiffenhagen (2013) propose deploying dedicated routers to home-based hotspots that would handle VPN connections transparently. Perhaps a similar system could also be devised for other types of public networks.

5 Conclusions

Public wi-fi hotspots are not going anywhere. As more mobile devices enter the marketplace, consumers will regard public wi-fi as the norm, rather than the exception. If a venue cannot offer internet connectivity, the modern consumer will be likely to choose an establishment that does. Therefore, public wi-fi vendors have as much to gain from securing public networks as do users, and an increased role from vendors would help to make a more secure internet for all users. Whether through stronger encryption methods, VPN tunneling, or simple informational campaigns, there are many steps that vendors should consider in the future for securing their networks. This is not to say, however, that users are not as responsible for the data they send over public networks. The rapidly expanding number of online financial, medical, and commercial transactions begs the need for more secure public networks. The only question is if public wi-fi security will stem from preventative foresight, or reactionary woe.

6 References

Attipoe, Elliot Kojo. End Users Perception about Security of the Public Wireless Network. International Journal of Societal Applications of Computer Science, vol. 2, issue 8, august 2013.

Brody, R.G, K. Gonzales, and D. Oldham. Wi-fi hotspots: secure or ripe for fraud? Journal of Forensic Investigative Accounting, 5(2):27 47, december 2013.

Dondyk, Erich, and Zou, Cliff C. (2013). Denial of Convenience Attack to Smartphones Using a Fake Wi-Fi Access Point. In The 10th Annual IEEE CCNC- Mobile Device Platform Applications.

Elliot, A. K. Users perception about security of the public wireless network. International Journal of Societal Applications of Computer Science, 2(8):434438, august 2013. ACM 978-1-4503-2365-9/13/09.

Noor, M.M., and W. H. Hassan. Current threats of wireless networks. In The Third International Conference on Digital Information Processing and Communications, pages 704713, 2013.

Radenkovic, Milena, and Heidi Howard, and Greiffenhagen, Christian. (2013). Providing Security for Wireless Community Networks. In LCD-Net13, September 30, 2013, Miami, Florida, USA.

Spaulding, J., A. Krauss, and A. Srinivasan. Exploring an open wifi detection vulnerability as a malware attack vector on ios devices. In Malicious and Unwanted Software (MALWARE), 2012 7th International Confer- ence on, pages 8793, 2012.

U.S. Census Bureau. (2013). E-Stats.

U.S. Census Bureau. (2012, a). Typical Daily Internet Activities of Adult Internet Users: 2011. Information Communications: Internet Publishing and Broadcasting and Internet Usage. Table 1160.

U.S. Census Bureau. (2012, b). Internet Activities of Adults by Geographic Community Type: 2011. Information Communications: Internet Publishing and Broadcasting and Internet Usage. Table 1159.