# Public Wi-Fi Networks: Secure?

Ka Wai Charles Wan

12/14/2016

## Abstract

Public Wi-Fi networks are commonplace, frequently offered by outlets such as coffee shops, cafes, and airports as customer magnets. Commonly held to be insecure, the security community cautions against their use, but has been largely ineffective in impeding their proliferation. As providers have little incentive to secure their services and consumers remain largely unaware of how vulnerable they are, much work has been done to secure web traffic without user intervention. Yet, despite the rapid adoption of and improvements in HTTPS in recent years, web traffic remains quite vulnerable, particularly at the local level. Therefore, for consumers, the detriment of exposure still trumps the benefit of 'free' Internet access.

## 1 Introduction

Public Wi-Fi networks (or 'hotspots') are convenient services typically offered by outlets such as coffee shops, hotels, and airports as a way of attracting and retaining customers. It is not unusual for consumers to decide on an outlet based largely, if not entirely on whether or not it has 'free Wi-Fi'. As a reflection of this, major vendors such as Starbucks and McDonalds now advertise Wi-Fi in-store and on their websites. Furthermore, considering the fact that approximately 80% of smartphone data volume is over Wi-Fi, major providers such as Comcast and Orange have increasingly integrated access to public hotspots into their mobile data plans[8]. Despite frequent caution from the security community against the use of public hotspots, the allure of free Internet service to the general population means that it is here to stay.

Although it is in the interest of social welfare for providers to secure their services, they offer public hotspots for purely economic reasons. Of course, outlets generally do not, despite the name, offer public hotspots as public goods, but as club goods, excluding lingering customers and non-customers until a purchase is made. Beyond enforcing this exclusivity, there is little reason for outlets to front the extra costs to monitor and control congestion, or offer home or office level speeds, let alone implementing and upkeeping security systems. Indeed, it is not the provider's concern as to what consumers access over the network beyond that which is not permitted by law; but, the responsibiltiy of policing such content is written off to customers by way of 'Terms & Conditions' pages that few people read. As providers have little to lose, appealing to them is largely futile.

Ultimately, it falls to consumers to protect themselves. However, the general attitude is that service providers (both behind public hotspots and web services) are protecting them, and thus there is little need for caution. Until a few years ago, this was a very dangerous attitude to have, because the lack of provider attention

presented a low entry barrier for attackers, while consumers remained blissfully unaware of their stolen credentials. However, from around the early 2010s, major content providers such as Facebook and Youtube started enabling HTTPS as default[4], thereby accepting the consumers' lack of awareness as unavoidable. Still, despite HTTPS's relative effectiveness, the protocol still remains vulnerable to attack. As the battle between security researchers and attackers continues, the only constant is that consumers remain vulnerable, and should take steps to learn to protect themselves.

## 2 To the Community

Although significant progress has been made to defend people from attack, most websites today are not up-to-date with the latest developments in security. As attackers face little difficulty in gaining access to public Wi-Fi networks, users are already vulnerable at the local level. The result of a user's trust is exposure to exploitation at every level of Internet access, particular through man-in-the-middle attacks. In spite of providers being disincentivized from securing public hotspots, the security community has come a long way in securing the Internet; in fact, most web traffic is now encrypted. But, even with the latest fixes to HTTPS and other protocols commonly thought to be secure, users remain incredibly open to attack. There is only so much we can do protect users without their intervention. At the end of the day, there needs to be more education about security and personal intervention when it comes to the public.

## 3 WLAN Vulnerabilities

To service customers, outlets employ wireless local area networks (WLAN) typically accessible by via either a passphrase provided by employees on purchase of a good or a MAC-based user authentication system located on the access point (AP). Unfortunately, either method is highly insecure and presents a low barrier for an attacker, even a passive one, to snoop on customers.

Nowadays, outlets tend to host small, local HTTP servers on their APs, which redirect any initial DNS requests to said servers. During this initial step, consumers verify terms and conditions with the outlet, and the AP creates a temporary account based on the user's MAC address. The consumer is subsequently granted Internet access, while the AP tracks how long the user has been logged in. The latter allows outlets to limit how long a consumer is allowed to use the public hotspot. Although MAC authentication may work on the typical consumer, an attacker can easily circumvent this limit by spoofing or reconfiguring their MAC address, allowing uninterrupted sniffing and attacks on other users. APs that employ this model of authentication are typically unencrypted (no passphrase needed for access); still, according to WiGLE, only 6.56% of APs are not encrypted whatsoever, an all-time low. Though not as common as before, this model is still used and presents essentially no barrier to attackers.

WLAN encryption schemes are typically thought to be more secure; indeed, 56.42% of all wireless encryption use WPA2 (or RSN)[7], the latest WLAN encryption scheme yet. Although a passphrase is still used to gain initial access, WPA2 uses the Advanced Encryption Standard (AES), performing a 4-way handshake between clients and the AP to mutually authenticate and exchange unique keys, similar to TLS; the dynamic na-

ture of WPA2 permits regular updates to its encryption scheme[1]. WPA2 significantly improves over the original WEP and subsequent WPA because it dynamically creates relatively long keys for data exchange that are not easily obtained by attackers. WEP was and still remains notoriously easy to break because the user-selected 24-bit stream cypher is sent in plaintext with encrypted packets, and the static 40-bit secret key is not only shared across all devices, but must be changed on every device manually and is short enough to crack in a small amount of time[1]. WPA, on the other hand, uses a 128-bit secret key to scramble a different stream cypher per packet and includes checksums to ensure data integrity; unfortunately, the protocol generally requires passphrases to be 20 characters or more, which is difficult for human memory or sharing rapidly (as is typical in outlets), and thus unfavorable for both providers and consumers to employ[1]. Slightly better than unencrypted, 7.91% and 9.75% of wireless encryption are WPA and WEP, respectively[7].

WEP and WPA have long been considered to be insecure, with several well-known attack methods, as noted by Tews and Becks; tools that automate such attacks include the likes of Aircrack and Reaver, which are easily accessible and whose use are well-documented. This weakness has caused a sharp increase in WPA2 adoption in the last few years, though researchers at Brunel University, UK have examined WPA2's vulnerabilities and presented how the protocol can be fully exposed (Exposing WPA2 security protocol vulnerabilities), though not as easily[10]. Even without complex attacks, since short keys including words tend to be employed, attackers can more than likely launch brute-force attacks to learn passphrases with relative ease.

Essentially, no popular WLAN encryption scheme is sufficiently secure to protect something as attractive to attack as an outlet's customers. Any of the vulnerabilites mentioned above could be exploited to gain anonymous access to the system, but if an attacker did not want to take the time to do so, he or she could simply ask for the passphrase and outlet employees would likely be more than happy to oblige. In other words, hats off to the old adage that social engineering is the most successful form of hacking.

# 4 Provider Economics

Even WPA2 is now known to be insufficient encryption-wise, so it falls to providers to upgrade their systems. One option popular in corporate offices is WPA-Enterprise, which employs RADIUS servers to authenticate users, and authorizing each user via individual keys; even if an attacker is allowed into the system, there is simply not enough information about other users to successfully snoop[2]. Unfortunately, the cost of a WPA-Enterprise capable router is usually more than 10-times as expensive, and requires experienced IT administrators to setup and maintain. For profit-maximizing outlets, secure public networks represents an unfavorable investment. The sad reality is that in the world of networking, a significant driving force behind many decisions is not social welfare or security, but economic and political reasons.

Consider the average coffee shop. According to Payscale, a barista makes an average wage of $9.39 an hour, or an annual salary of $19,531.20 assuming a 40-hour work week. When it comes to public hotspots, their sole job is to provide the Wi-Fi password under a WEP or WPA system, or nothing if there is no encryption. IT network administrators, on the other had, make an average annual salary of $55,601. Even without factoring in additional capital costs, hiring even one person to overlook a

single outlet or even a cluster of outlet's adds greatly to a company's variable cost. Furthermore, the average network administrator is unlikely to be experienced enough in security to consistently defend against malicious activity. The security community is notorious for being low on talent; most tellingly, given the rise in cybersecurity attacks in recent years, the incoming Trump administration has been advised to train 100,000 specialists by 2020[5]. If governments have difficulty defending themselves, what hope do outlets have?

Besides the high expense of upgrading to and maintaining a secure system, it is economically advantageous to keep systems simple. Recall that the purpose behind public hotspots is to attract and retain customers. As long as an outlet can offer a service with sufficient speed and low enough congestion to keep customers satisfied, maintaining a public hotspot essentially becomes a fixed cost. Adding security would require that non-technical employees be trained to deal with some basic issues; especially considering the high turnover rate typical to unskilled workers at outlets, it is much cheaper to simply use a short static key that employees can share. Additionally, providers do not need to care about what content passes through their network beyond that which is unlawful; responsibility is written off to users by 'Terms & Conditions' they must agree to before access is granted. Thus, there is no need to front the costs to monitor network traffic. In effect, in the absence of significant customer dissatisfaction, providers essentially have no economic reason to upgrade; a simple system minimizes costs and keeps revenue high.

From a customer's point of view, there appears to be benefit as the cost for a good offered by outlets comes with free access to a public hotspot. However, there tends to be little consideration for the provider's motivations, which in turn opens up customers to attack. Ultimately, the prevalence of low-security public hotspots offer significant producer surplus and little consumer benefit.

# 5 HTTP Security

With both weak WLAN security and providers unwilling to secure their hotspots, hackers consistently have had more or less unfettered access to public hotspots. Although there has been much work to secure network traffic over the Internet, users are most vulnerable at the source, giving rise to the popularity of man-in-the-midlde (MITM) attacks. Because HTTP traffic represents 75% of TCP traffic[4], HTTP has served as a constant target for attack and security research for both blackhats and whitehats alike.

Practically, the common layperson does not have enough knowlege or awareness to protect themselves against cyberattack, such that the security community has moved towards securing the Internet without user intervention. With HTTP, the SSL/TLS encryption scheme has been incorporated to develop HTTPS, a secure equivalent, which has been increasingly adopted since its inception. According to Naylor et al., the presence of HTTPS doubled in two years at the time of writing, with Facebook and Youtube contributing greatly when they enabled HTTPS as default for users in late 2013 and early 2014[4]. Furthermore, despite the common conception regarding high infrastructure costs needed to support HTTPS (to accommodate computational, memory, and network overhead), in addition to certificate costs, 50% of web traffic was encrypted by 2014, including large content such as videos[4]. The growing presence of HTTPS is simultaneously a response to greater public awareness of the need for security, and an acknowledgment that the public lacks the tools to effectively defend itself in an increasingly complex

cybersecurity landscape.

HTTPS has since made it much more difficult for attackers to perform MITM attacks. For one, attackers cannot normally sniff HTTPS traffic, because they lack the secret encryption keys shared between client and server. Indeed, even if a public hotspot does nothing to impede attackers, they would be much less likely to acquire sensitive information if traffic is HTTPS-protected. This would justify a user's trust in 'the system' had a disruptive tool called sslstrip not been released in 2009. Created by Moxie Marlinspike and presented at BlackHat DC 2009, the tool permits MITM attacks that transparently downgrade user traffic from HTTPS to HTTP, while the attacker maintains a secure connection with the server on the client's behalf; because the tool generates certificates from the requested site and forwards them back to the client, browsers are fooled into believing they have connected with the intended secure site[3]. Though there are easy ways to check for a secure connection, most people only encounter HTTPS via links or 302 errors[3]. So, even if a loaded site shows signs of being compromised, most users would likely remain oblivious. Used with ARP spoofing, attackers can easily circumvent HTTPS and gain access to a plethora of sensitive data from a public hotspot.

HTTP Strict Transport Security (HSTS) is a policy published in 2012 that specified a new header "Strict-Transport-Security", whose value indicates how long the user(-agent) should use HTTPS only for a given site, such as for a year. The fix was the industry response to SSL-stripping attacks[6]. In the event of a forced downgrade, if a time value has already been received, a user would enforce HTTPS even if a response were HTTP; but, if it is the user's first time visiting a site, HSTS can still be stripped away. Still, the latter is unlikely to occur for popular sites such as Facebook or Google. Unfortunately, the general weakness of HSTS is that it is time-sensitive; if an attacker could force a victim's clock to advance until HSTS expires, then the victim would once again be vulnerable to SSL-stripping[6]. A tool called DeLorean has been created to exploit Network Time Protocol (NTP), which operating systems use to synchronize time; by blasting users wtih custom NTP packets, HSTS can be rendered useless. Still, many operating systems only synchronize at specific intervals, impeding NTP attacks somewhat.

Despite the widespread belief in HTTPS, it is far from secure. In a public hotspot setting, HSTS, as the most up-to-date defense against SSL-strip attacks, would deter most passive efforts, though a persistent hacker could certainly break through. Unfortunately, as with the slow adoption of HTTPS, HSTS has not yet seen widespread adoption; thus many 'secure' websites remain vulnerable to MITM attacks.

# 6 Defenses

The best defense is to abolish public Wi-Fi networks; there are simply too many avenues for attack. But, pursuing this draconian path would likely cause massive outcry from both customers and outlets. Alternatively, the first step would be to mandate and enforce a basic level of encryption for public hotspots, at least WPA-Enterprise. If an outlet wishes to offer network services, then it should be required to register with an authority, which will police these public hotspots to ensure compliance. This approach is similar with policies regarding food production, construction, and so on. The next step would be to require websites to comply with up-to-date policies such as HTTPS and HSTS. This is a little more difficult because the Internet is decentralized and is therefore unregulated; as such, site administrators are free to adopt any level of

technology they want, possibly at the expense of users. Ideally, all websites should enable HTTPS-level security by default.

Still, it is impossible to defend people effectively without their intervention. Users should be educated about the basic dangers regarding public Wi-Fi access - that attackers can very easily intercept their traffic and recover credentials, encrypted or not. The illusion of 'the system' protecting them should be quashed and a sense of caution should be instilled. On a slightly more advanced level, some basic user-oriented tools should be offered that can be easily setup and ran to detect and shutdown attacks like ARP spoofing. Most of the Internet-aware population already know about antivirus software, as outdated as they are; why not basic security tools too? It should not be the case that these tools live solely in the realm of the security community; security concerns everyone.

# 7 Conclusion

At all levels of a public Wi-Fi network, users are vulnerable to having their information stolen. Due to weak to nonexistent WLAN encryption schemes employed by outlets, there is essentially nothing stopping attackers from breaking in and initiating MITM attacks; in fact, providers often are more than willing to provide any 'customer' with the necessary passphrase, so attackers can figuratively walk right in. Although HTTPS and HSTS deter some passive efforts, a knowledgeable and persistent attacker can easily circumvent these defenses, downgrade security protocols in an SSL-strip attack, and steal sensitive information. As providers have little reason to secure their systems as it would increase their variable costs, it falls to users to protect themselves. Barring greater education, users can defend against attack on a public hotspot by not using it for anything that requires security, which includes emails, social media, banking, and so on. People should keep those activities on private networks that are not as accessible to attackers, and only use public hotspots for basic web-browsing.We have come a long way since the days of WEP and pure HTTP, but we still have a long way to go.

## References


[1] Bulbul, Halil Ibrahim, Ihsan Batmaz, and Mesut Ozel. "Wireless Network Security: Comparison of WEP (Wired Equivalent Privacy) Mechanism, WPA (Wi-Fi Protected Access) and RSN (Robust Security Network) Security Protocols." Proceedings of the 1st International ICST Conference on Forensic Applications and Techniques in Telecommunications, Information and Multimedia (2008). ACM. Web. 10 Dec. 2016.

[2] Hoffman, Chriss. "Warning: Encrypted WPA2 Wi-Fi Networks Are Still Vulnerable to Snooping." How-To Geek. 8 Dec. 2014. Web. 11 Dec. 2016.

[3] Marlinspike, Moxie. "New Techniques for Defeating SSL in Practice." BlackHat DC 2009. Washington DC. BlackHat. Web. 12 Dec. 2016.

[4] Naylor, David, Alessandro Finamore, Ilias Leontiadis, Yan Grunenberger, Marco Mellia, Maurizio Munafò, Konstantina Papagiannaki, and Peter Steenkiste. "The Cost of the "S" in HTTPS." CoNEXT '14 Proceedings of the 10th ACM International on Conference on Emerging Networking Experiments and Technologies (2014): 133-40. ACM. Web. 12 Dec. 2016.

[5] Pagliery, Jose. "Panel to Trump: Train 100,000 Hackers." CNNMoney. Cable News Network, 2 Dec. 2016. Web. 10 Dec. 2016.

[6] Selvi, Jose. "Bypassing HTTP Strict Transport Security." BlackHat Europe 2014. BlackHat. Web. 12 Sept. 2016.

[7] "Statistics." WiGLE. Web. 11 Dec. 2016.

[8] Tefficient AB. Using Public Wi-Fi as Customer Magnet. Industry Analysis. 24 Sept. 2016. Web. 12 Dec. 2016.

[9] Tews, Erik, and Martin Beck. "Practical Attacks against WEP and WPA." Proceedings of the Second ACM Conference on Wireless Network Security - WiSec '09 (2009). ACM. Web. 11 Dec. 2016.

[10] Tsitroulis, Achilleas, Dimitris Lampoudis, and Emmanuel Tsekleves. "Exposing WPA2 Security Protocol Vulnerabilities." International Journal of Information and Computer Security 6.1 (2014): 93. InderScience Online. Web. 11 Dec. 2016.