SECURITY RISKS OF USING WI-FI HOTSPOT:

SECURE SOCKET LAYER (SSL) UNDER BREACH ATTACK

Mentor: Ming Chow
Hao Wan
Hao.wan@tufts.edu

Table of Contents

Abstract

The last decade has witnessed a significant improvement of mobility of Wi-Fi enabled devices, including tablet computers and smart phones dominated by Android and iOS operating systems. What accompanies the aforementioned trend is the popularity of public hotspots offered by merchandises aiming to attract customers or collect statistics on their patrons. This act of “free-riding” on public hotspots exposes mobile device users to potential privacy and security risks, for their private data could be exposed to hackers or business owners through various attacks, especially Man-in-the-middle attack.

This paper explores of how techniques such as Secure Sockets Layer (SSL) can be employed reduce the risks of cyber-attacks at Wi-Fi hotspots. It will also focus on a new type of attack, the BREACH attack, that bypasses the security layer and retrieve secrets or other confidential information to expose the victims to additional attacks.

1. Introduction

1.1 Definition

Wi-Fi allows electronic device users to connect to the internet via radio waves. According to Wi-Fi Alliance, Wi-Fi is defined as the "wireless local area network (WLAN) product that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards".

On the other hand, hotspots are physical sites that offer Internet access using WLAN and Wi-Fi technology through the use of routers that are linked to Internet Service Providers (ISP). Nowadays, hotspots are easily found in modern societies. Many places such as airport, coffee shops, hotel lobby and restaurants offer charge-free and password-free access to their Wi-Fi.

1.2 Problems with Wi-Fi hotspot[i]

While it seems that Wi-Fi access at a local coffee shop or airport morning is free, hotspot users may not realize the significant cost they are paying in the form of jeopardizing their own privacy and financial wellbeing.

Since most hotspots offer unencrypted Internet access, at the moment of reaping the pleasure of connecting to login-free Wi-Fi networks, users are exposing themselves to many kinds of cyber-attacks.

One of the most basic thing crackers can do is to sniff on network traffic and extract private information from other people on the hotspot. Sniffing applications such as *Wireshark* can be employed to collect all chatting records, emails, online shopping and banking information away from or to the mobile devices on the public network. If the data is unencrypted, the cracker can

instantly get important information in plaintext (credit card numbers, for example) about the victims and exploit these leaked information for personal gains.

In addition to sniffing, crackers can also implement Address Resolution Protocol (ARP) Spoofing, which redirects network traffic to the crackers and modifies/blocks the packets sent to the victims; session hijacking can be done via the unsecure network such that the crackers can exploit victims' ongoing website sessions to transfer money or steal information; furthermore, Man-in-the-Middle attack can also be insidiously leveraged by the crackers to eavesdrop on the Internet traffic and steal login credentials for illegal purposes and deeds.

2. Service to the Community

Internet access becomes indispensable to many people today, due to the amount of work and communication done through online services. The prevalence of Wi-Fi access has greatly facilitate business people by providing convenient, fast and free access to Internet even when they are traveling abroad. At the same time, as cyber life becomes more common, more people enjoy spending more time surfing the Internet, shopping online, or chatting with friends on their mobile devices via free Wi-Fi. With the increasing adoption of Wi-Fi technology and people's urgent need for connectivity, the number of WIFI hotspots in the world is projected to reach 5.8 million by 2015, making it a 350% increase from 2011.[ii]

However, what complements the growing prevalence of hotspot is the increasing severity of security risks. The several types of common cyber-attacks mentioned in the previous section can be maliciously exploited to infringe on hotspot users' privacy and financial well beings. As Wi-Fi essentially uses radio wave for network communication, computers equipped with sniffers and connected to the same unsecure hotspot can receive almost any data sent through the radio waves. Login credentials sent through unsecure websites can be easily seen in plaintext by the crackers; even if information such as credit card number and security code is encrypted, the crackers may potentially use password crackers such as John the Ripper to crack the information. Due to the trouble of memorizing several well designed password, many people tend to either use simple passwords or use the same passwords for multiple accounts. This adds to their potential loss caused by cyber-attacks, since the successful crack of one user account may easily employed with the help of social engineering method to crack the same

user's other, potentially more important accounts. Critical information such as health records, business secrets, and personal messages could be leaked, causing great anxiety and loss to affected people (many people could be affect by just one leakage). Moreover, crackers may use the cracked financial accounts for illegal financial gains or cause other damages.

With regards to the aforementioned risks, this paper strives to raise people's awareness of the immense security concerns, which are more than often overlooked by people in front of the lure of "free" hotspot Internet access offered. At the same time, this paper explores and evaluates potential method to boost the security of Internet access at hotspots, making recommendations on how to minimize the risks associated. While the technical details mentioned in this paper aims to stimulate discussions among technology savvy people, the other parts of the paper is tailored towards the general public who sometimes or frequently use hotspots to do business or as a life style.

3. Action Item

To defend users of unsecure hotspot users, Secure Sockets Layer (SSL) protocols have been developed to improve the security of private data transmitted through the network. In following essay will dissect how SSL works, potential risks of attack even with the use of SSL, and further steps that could make the connection even more secure.

3.1 SSL

To better secure the mobile devices on unsecure hotspots, some mobile devices and websites use Secure Sockets Layer (SSL) protocols for Internet access. SSL is an enhanced version of Transmission Control Protocol (TCP) that aims to achieve confidentiality, data integrity and end-point authentication. Thus, it can be used to secure any applications that are based on TCP.

To understand how SSL improves security, we may find it helpful exploring the detailed steps of a pseudo SSL communication process. SSL has three main phrases, which are handshake, key derivation, and data transfer.[iii] To facilitate the explanation of the concepts, let us imagine a scenario in which Adam want to establish SSL connection with Bill.

Handshake

There are three steps involved in the handshake phrase. First, Adam need to establish a TCP connection with Bill. To achieve this, Adam shall first send a TCP SYN with a random sequence number N to Bill, who reply with a TCP SYN-ACK that has an acknowledgment number N+1 and a random sequence number B; then, Adam reply with a TCP ACK with a sequence number B+1 to establish the connection. Second, Adam sent a SSL hello message to Bill, who will then

respond with his certificate that contains his public key. Since the certificate has been certified by the Certificate Authority, Adam can be sure about the identity of Bill. In the final step, Adam sends the Encrypted Master Secret, a Master Secret encrypted with Bill's public key, to Bill. Bill will then use his private key to decrypt the Master Secret (MS), which will be used to generate session keys in the following phrases.

Key Derivation

Since both Adam and Bill now have the MS, they can use the MS to generate fours keys below by slicing MS into four parts for encryption and integrity checking:

1. E_a=session encryption key for data sent from Adam to Bill
2. M_a=session Message Authentication Code (MAC) key for data sent from Adam to Bill
3. E_b=session encryption key for data sent from Bill to Adam
4. M_b=session MAC key for data sent from Bill to Adam

The first and third key will be used for data encryption, while the second and fourth key will be used for integrity verification.

Data Transfer

Since both parties are sure about each other's identity and have the four set of keys, they can now sent secure data to each other over the established TCP connection. Data stream is broken into records, each of which is appended a MAC key for integrity checking. For messages sent from Adam, MAC is created by hashing the record data and the M_a. The package is encrypted by using session key E_a before being sent to Bill. For the data sent from Bill to Adam, similar

procedure applies. In addition, to avoid Man-in-the-Middle attack, each packet maintains a sequence number counter that is incorporated in the MAC calculation to ensure the right number of packets come in the right order.

With the aforementioned security procedures, the hotspot Internet access from mobile devices is definitely more secure, for crackers would have to crack the encryption before seeing the plaintext data. To ensure that SSL is used, Wi-Fi users should make sure that they are using *https* header, instead of *http*, when browsing the internet. For mobile phones, which are more commonly used in hotspots due to their compactness, users should check whether the mobile applications they use, be it iOS or Android applications, encrypt the communication data using SSL. If not, login credentials and other critical information can be easily obtained by attackers.

3.2 BREACH attack

While it seems that SSL does improve the security of Internet access at unsecure hotspots, new methods of serious attacks are invented recently. The rest of this section will be dedicated to expose the BREACH attack.[iv]

What is BREACH attack

BREACH attack is a compression side-channel attack against HTTPS traffic. Instead of attacking HTTP requests, it targets HTTP responses which often deliver secrets such as session cookies. It could compromise the secrets with a time frame of as short as 30 seconds by guessing the

secret (session cookie, for instance) one character at a time. Being agnostic to the version of SSL protection, it does not require Transport Layer Security (TLS) compression and can work against any cipher suite.

HTTPS compression (with gzip) involves two basic functionalities: deflate, which is to compress the data into smaller sized packets, and INFLATE, which is to restore such packets into the original data. To guess the secret characters, the BREACH attack zooms in on the DEFLATE process, which takes advantages of repeated strings to shrink the compressed payload.

If the secret string is repeated in the response body, DEFLATE will compress the body even further. If the attacker's guess on the token is right, then the compressed data will be a few bytes less in term of its size. In this way, the attack can brute force the first character of the secret or cookie, and proceed to the following characters once the previous character has been correctly identified.

How BREACH works

There are several premises for this attack to work: the web app is served from a server that uses HTTP-level compression; it reflects user input and a secret in HTTP response bodies.

On an unsecured Wi-Fi hotspot, the attacker can easily sniff on the victim's traffic (with or without ARP spoofing). By fooling the victim into visit an attacker-controlled site which contains invisible iframes pointing to the vulnerable server or by modifying any unsecure traffic, the

attacker can coerce the victim to send requests and measure the size of the resulting HTTP responses. In this way, the first and all subsequent characters of the secret can be cracked.

Mitigation Measures

While the BREACH attack is a powerful new attack against TLS/SSL, there are certain ways to mitigate, if not eliminate the risk.[v]

- *Length Hiding*

The BREACH attack works by firstly measuring the length of the cipher-text. By randomizing the length of the secrets with variable padding, we can hide the true length. While more requests and statistical analysis could be employed to infer the true length, length hiding with sophisticated padding can at least render the attack harder to implement.

- *Separating Secrets from User Input*

By delivering secrets in input-less servlets, we can completely eliminate the risk of BREACH attack as the attacker can no longer guess the secrets by analyzing the HTTP responses. However, this change may not be easily implemented by web applications due to the incumbent architecture.

- *Virtual Private Network (VPN)*[vi]

VPN uses tunneling protocols and security procedures including encryption to ensure that network traffic is confidential (even if the hotspot Wi-Fi is sniffed on, the sniffers can only obtain encrypted data) and authenticated (unauthorized users are denied access). Moreover,

integrity can be ensured to detect any message tampering. VPN also protects the mobile devices from many other attacks from the unsecure Wi-Fi networks. However, highly secured VPN services may incur some costs.

4. Conclusion

In this paper, we have examined the concepts and security problems involved in the Wi-Fi hotspots connections. Security measures and increasingly sophisticated attacks are continuously in a competition to counter each other. While complete security of Internet access at hotspots are not guaranteed, the awareness of the security loopholes is critical. With this awareness, the users can be more acquainted with the risks they are exposed to, and thus try to avoid communicating highly confidential information via unsecure Wi-Fi without taking any reliable security practices. On the other hand, more advanced Wi-Fi users can learn about techniques, such as VPN, to better encrypt the communication.

5. Supplementary Material

A supplementary video demonstrating the security risks of using Wi-Fi hotspot has been posted to the following link:

Security Risks of Internet Access at Wi-Fi hotspot exposed

http://www.youtube.com/watch?v=_huWju1Pbj8

6. References

[i] *Why Public WiFi Hotspots are Trouble Spots for Users,* Kent Lawson, March 10, 2013 http://blog.lifestore.aol.com/2013/03/10/public-wifi-hotspot-security/

[ii] *Wifi Hotspots set to more than triple by 2015,* informa, http://www.informa.com/Media-centre/Press-releases--news/Latest-News/Wifi-hotspots-set-to-more-than-triple-by-2015/

[iii] *Chapter Eight, Computer Networking: A Top-down Approach,* 2009, Kurose, James F., and Keith Ross W,.

[iv] *BREACH: Reviving the Crime Attack,* YOEL GLUCK, NEAL HARRIS, AND ANGELO (ANGEL) PRADO, July 12, 2013 http://breachattack.com/resources/BREACH%20-%20SSL,%20gone%20in%2030%20seconds.pdf

[v] *SSL, GONE in 30 SECONDS-A BREACH beyond CRIME*, YOEL GLUCK, NEAL HARRIS, AND ANGELO (ANGEL) http://breachattack.com/resources/BREACH%20-%20BH%202013%20-%20PRESENTATION.pdf

[vi] *Virtual Private Networking: An Overview, September 04, 2001* http://technet.microsoft.com/en-us/library/bb742566.aspx