Security Analysis on the Malicious Use of Public Wi-Fi (December 2010)

Moses Chan, Rob O'Dwyer, Marie Elise Desormeaux Leowski, and Steve Powell

[mochan@live.ca, odwyerrob@gmail.com, eleowski@gmail.com, powell.ivor@gmail.com]

***Abstract*— This report analyzes the vulnerability of users connected to unsecured public Wi-Fi. Data was collected by creating unsecured access points around UBC, public libraries and coffee shops. The collected data showed that 2528 different domains were visited by 270 different users. 213 websites used HTTPS strictly, while 105 websites used a combination of HTTPS and HTTP, suggesting that encryption was used only for login. The remainder of websites used no form of encryption. Successful attacks conducted through rogue access points were HTTP request and response modification and session hijacking; these attacks can be used against unencrypted traffic. The responses to a survey given to 36 individuals indicated that most users are aware of risks when using unsecured networks, but most do not take proper precautions when connected. Due to the locations of the access points and the survey respondents being mostly students, the results may be skewed towards university students. Though it is recommended that users take proper security precautions when using unsecured networks, websites can provide additional security for users by encrypting more traffic and making session cookies expire in a shorter time.**

***Index Terms*—Privacy, public Wi-Fi, unsecured networks, rogue access points.**

I. Introduction

LARGELY due to the prevalence of mobile devices in today's society, public Wi-Fi networks are an increasingly popular means of using the Internet. It has been reported that as of June 2009, there were 258,853 public Wi-Fi hotspots worldwide [1]. These networks are available in a broad range of places, from coffee shops and restaurants to university campuses and libraries; they provide quick and convenient access to email, online banking, and other services that may not otherwise be available while out in public. With the vast number of people connecting to unsecured Wi-Fi, this may seem like a safe practice; however, joining such networks can make your device and personal information vulnerable to attack.

For our project, we wanted to explore these vulnerabilities to see how critical they really were. We intended to find out what kind of data was being exposed over this type of connection, how easy it would be to exploit a public network to obtain such data, and how aware people were of the consequences. While connected to public networks, people check their email, visit social networking sites, and even make online purchases; all while potentially exposing their personal information. This problem is significant because such a large number of people use unsecured networks every day and their personal information may be at risk without their knowing.

We obtained our information by joining existing public networks as well as creating our own unsecured networks disguised as familiar ones. In analyzing the traffic over these connections, not only we were able to determine what sites people were visiting but also, in many cases, exactly what they were doing on them; this is even after they had logged in securely. Had these individuals been using a secure network, a firewall, a VPN, or sites that used only HTTPS, we would not have had the same access to their data or been able to monitor their activities.

It was found that people in the vicinity of our networks willingly joined and went about their business. Once connected, we were able to inspect the traffic as well as important data such as cookies being sent to and from the user and even the user's host name. We were also able to intercept and rewrite HTTP requests. Most of the traffic we observed involved social networking sites such as Facebook, but it also included users checking their email and possibly making online purchases.

This work was inspired by previous EECE 412 projects that forged the 'ubc' and 'ubcsecure' wireless networks in order to steal students' CWL credentials. We decided to take this a step further and use other public networks besides 'ubc'. We also wanted to see what was possible beyond just obtaining students' passwords by continuing to act as a legitimate network. This is certainly a problem worth investigating as the issue of the security of public Wi-Fi is a growing concern in our society as Internet scams are on the rise [2].

II. Analysis of Network Vulnerabilities

A. Rogue Access Points

The rogue access points (RAP) were set up using simple consumer wireless routers, and placed in areas where either a target unsecured Wi-Fi network was accessible and we could spoof it, or no unsecured or free access points were available as alternatives. The spoofing of existing wireless access points was simple to achieve; this only required using the same SSID (access point name) as the original and having a better signal strength in the surrounding area. After setting up our RAP, all clients currently on the target network and physically close enough to our router would typically switch to the new network automatically. When no network was available to spoof, an open access point was set up with an innocuous name, such as “Free Public Wi-Fi”. Both methods resulted in a network with no password, encryption, or signed certificate.

The wireless router was then connected to a laptop computer that would perform transparent forwarding of the traffic through another separate Internet connection (a secure wireless network). This would result in the network appearing to have a functional connection to the Internet, with slightly higher latency due to the intermediary computer.

The computer was set up to both forward the traffic and log it using Wireshark, a popular packet sniffing program. In addition, all data going to TCP port 80 (HTTP protocol) was forwarded to a local HTTP proxy server instead of directly to the Internet. This proxy server was used to test several possible attacks on the clients and their data, by means of parsing the insecure HTTP communication and modifying the requests and responses. This allowed us to test a variety of man-in-the-middle attacks since most web traffic was then passing through the proxy program.

B. *Established Public Access Points*

In addition to setting up our own networks, we joined preexisting unsecured public networks to get a better perspective on what kind of sites people were visiting and to see if it was possible to exploit these networks in the same manner as the ones we created. All of the unsecured networks encountered, in places such as coffee shops and libraries, were susceptible to packet sniffing using Wireshark, which allowed us to view all of the unencrypted traffic over the network. This proves that anyone connected to this kind of network with a packet sniffing utility installed would be have access to information such as the what sites users were viewing, what unencrypted data was being passed between them, and even users’ host names.

Since we did not create the network and were not routing traffic through our computer, we were not able to use an HTTP proxy and we could not carry out the attack that involved rewriting HTTP messages in transit. However, since cookies were sent in plaintext, we could still record and use them to create our own HTTP requests posing as the authenticated user.

C. *Attacks*

The four main attacks that we attempted were traffic monitoring with Wireshark, rewriting the parameters of an HTTP request, rewriting the response body of an HTTP response, and forging authenticated HTTP requests using session hijacking. The traffic monitoring consisted of running the packet capture program while traffic from wireless clients was passing through the network. All insecure HTTP requests and responses could be inspected and logged for later analysis, and the source and destination addresses could be logged for secure traffic (HTTPS). The request and response rewriting was done using the proxy server mentioned in II.A, and used simple pattern-matching and replacement with regular expressions to modify the client’s data. The last attack consisted of making fake requests on behalf of a client to a web server, using cookies we observed while monitoring traffic; this is known as session hijacking. Since the requests come from the same address and have the same session information in their cookies, it is difficult for the remote server to distinguish the difference between valid requests from the client and invalid ones [3]. Our version consisted of re-sending a request from the client after slightly modifying the contents.

The packet sniffing attack was successful, in the sense that a relatively large number of unsuspecting clients connected through our network, and the resulting traffic was logged. The two HTTP rewriting attacks were tested on simple local HTTP servers with example content, and on requests to the popular social networking site Facebook. Many similar requests to the domain www.facebook.com were observed while monitoring the network that appeared to be “status updates” - simple text messages that are posted to a user’s profile page. By rewriting a parameter in the HTTP request, we were able to change the user’s status to any given message. In addition, we were able to make simple modifications to response bodies, such as HTML content. However, this was less reliable as it required significantly more analysis of the original data to be able to modify it without damaging the integrity of the document or its encoding. The session hijacking attack was also successful against Facebook and several other authenticated sites, and worked as long as the clients’ session remained in effect, as expected.

The requirements for all of the attacks include physical proximity to the victim(s), as described in II.A, the necessary hardware to create the standalone access point and route traffic, and the credentials required to imitate a network. If imitating a secure network, the access point must have an identical security setup, including the same password so that clients will automatically connect. In addition, for the rewriting and session hijacking attacks to work, the web server being targeted must not be using SSL or TLS (e.g. HTTPS) for at least part of its communication. If these defenses are used, a man-in-the-middle attack using a transparent proxy is no longer as effective, as it is not feasible to provide a valid signed certificate with the content back to the client. Use of encryption technology will also render the data in the client’s requests unreadable to any packet sniffer.

Another possible attack would be to set up a HTTPS proxy and redirect traffic going to port 443 to it. The proxy would be able to attempt a partial man-in-the-middle attack by self-signing its own certificate. This would allow us to do similar attacks on web servers that use secure traffic, except the client would receive a warning from their browser for each page load. This was decided to be beyond the scope of this project, and not worth the effort since it would most likely alert clients that something was amiss.

III. Results

A. Experimental Statistics

Out of the all the traffic logged in the analysis, traffic to 2528 unique domains was observed. This did not include IP addresses without domain names, as it is very difficult to determine the uniqueness of addresses due to the varied load balancing schemes in place on different sites. Out of these domains, only 213 of them used HTTPS communication exclusively, and 105 used a combination of HTTP and HTTPS. The majority used only insecure HTTP communication, with 1305 domains not appearing to do any secure communication. However, some of these statistics may be slightly skewed by websites and other services that use alternate domains for secure services, and by content distribution networks for static content that do not necessarily require secure communication. Most sites that implemented a combination of the two used secure communication exclusively for authentication of the user, and left all other traffic insecure.

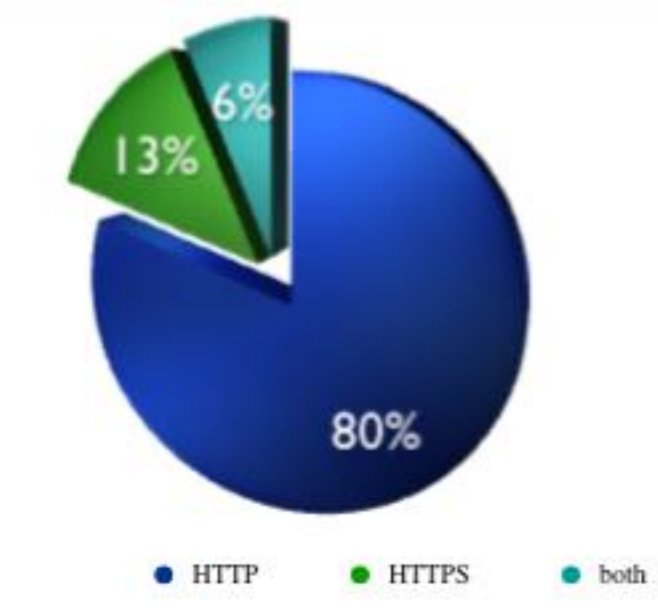

Figure 1. Website Encryption

Anonymous statistics were also collected about the users of the network. 270 different users connected in total, based on the number of unique local hostnames observed. Although this is actually the number of unique devices, it is unlikely that many users were using multiple devices on a public Wi-Fi network. In addition, many users hostnames included their first and last names, meaning that they could be identified and matched up to their browsing preferences and data. 35 users out of the total could be easily identified in this way. Although some traffic that could have related to financial data was observed, it was all encrypted securely, and thus no obvious analysis or attack was possible. This also made it difficult to determine whether people were actually doing financial transactions or just visiting sites that happened to do some form of business or e-commerce.

B. Network Exploitation

The attempted attacks were much more successful on sites that had partial security or none at all. Websites and domains that implemented HTTPS for all requests were immune to all of the attacks we attempted, with the exception of being able to track the user's browsing habits at the domain name level. However, the majority of domains that required authentication only implemented HTTPS for the login, which left users vulnerable to session hijacking and request rewriting. This places the integrity of the user's data and account at risk, as a hijacked session allows an attacker to act as the user temporarily. In addition, websites that do not implement layered security might be vulnerable to changing the account password or stealing valuable stored information like credit card numbers. The fact that these websites allow clients to make unencrypted requests also results in a permanent cross-site scripting vulnerability, because malicious scripts can be injected onto any page, and client requests can be modified to contain different parameters and data.

The client's information that was transmitted over insecure channels was completely vulnerable, and could be logged and stored for later use by an attacker. In addition, all data sent insecurely from the server back to the client was now untrustworthy, because it could potentially be modified in transmit to contain almost anything.

C. Survey Results

A survey was conducted to sample the awareness of the vulnerabilities of using an unsecured Wi-Fi network. There were a total of 36 respondents; of which, only 3 claimed they never use an unsecured Wi-Fi network. The survey respondents were mostly students; a few professionals of a technical nature and non-technical nature had also responded. While this may skew the results since most respondents had some technical knowledge, it was observed that it was mostly students who connected to Wi-Fi networks while they were studying in coffee shops.

The following illustration and table summarizes the results of the survey.

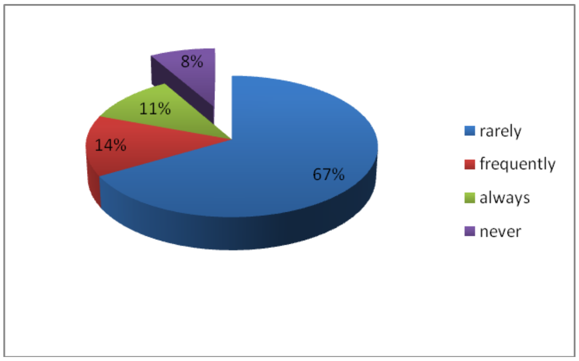

Figure 2. Unsecured Wi-Fi Usage

The pie chart above indicates that only 8% of the respondents claimed that they never used unsecured Wi-Fi networks. This illustrates the potential victim base of these attacks.

Question	Yes	No
Are you aware that others connected to the same unsecured networks can see your emails and the webpages you visit?	26	10
Are you aware that logins that don’t use HTTPS send your credentials in plain sight?	19	17
Are you aware that after login, many sites do not encrypt your messages and they can be intercepted and modified?	17	19
Do you run a personal firewall when connected to public networks?	16	20
Are you aware that people can make connections to and access your computer if no firewall is present?	32	4
Do you turn off file sharing when connected to public networks	29	7
Are you aware that others can access anything you’re sharing if you do not turn off file sharing?	33	3

Table 1. Awareness Level of Firewalls and File-Sharing

It can be seen that most respondents realize the potential risks of not using a firewall or turning off file sharing but do not seem to care. At least one respondent actually confirms this ideology. This individual, who has a technical background, had a different tendency dependent on whether or not a work machine or personal machine was used. More specifically, this individual employed a firewall on a work machine, but not a personal machine. While it cannot be conclusive due to one respondent’s answers, it should be noted that the survey did not ask for such details; this individual offered their comments of their own accord. To add on this, another individual stated that they did not care that their data can be accessed by others on the same network if they did not employ a firewall.

While the majority of people seem to be aware of the risks involved while not running a firewall or turning off file sharing, they were generally much less aware that their activities on the Internet could be viewed and potentially modified. Only 47% claimed that they were aware that their messages could be modified while 53% were aware that their login information is sent in clear text when authenticating to HTTP login pages. This compares to 89% who were aware that others could access their computer if they did not have a running firewall.

IV. Prior and Related Work

EECE 412 groups from previous years have analyzed various aspects of wireless network security, but with a much different focus from that of our project. The main difference between the previous studies and ours is that the other studies focused on vulnerabilities associated with connecting to networks, whereas our study focused primarily on analyzing the types of risks for users once they have knowingly logged in to an unsecured network.

One group spoofed the ‘ubcsecure’ network using self-signed certificates and used a survey to determine whether the average UBC student understood certificates [4]. Though both groups tricked users into joining a "malicious" network, our group's primary aim was not to steal passwords, but to observe users’ behaviours. Their report recommended teaching users to only use secure, trusted networks, which greatly limits options for users and is not always practical.

Two additional groups studied vulnerabilities with authentication on UBC's network, and vulnerabilities in key establishment using certain wireless security standards, respectively [5][6]. The latter group found that it was important for users to be educated on the principles of security to be safe. Though we agree, as will be mentioned in the discussion section, our findings suggest a different, more practical approach to protecting users.

A fourth report was conducted on the use of RAPs set up around the UBC campus, but with the aim of launching an attack to steal CWL login credentials using a fake CWL login page [7]. This report mentioned the possibility of packet sniffing using RAPs, but did not monitor any actual traffic or collect any data. Though we agree with this group on the issue of webpages with logins requiring the use of HTTPS to encrypt the transaction, based on our findings we believe that if a page requires a secure login, it should also encrypt all subsequent requests. Similar to the third group mentioned, this report recommended that users be educated in security and take extra precautions in protecting their data, such as by using a VPN. Though we agree, again we believe other actions are necessary.

V. Discussion and Recommendations

A. Analysis of Findings

Based on our results from both the unsecured networks we joined and our own RAPs, the vast majority of traffic we viewed did not use any form of encryption. Only 13% used HTTPS while 80% used HTTP. Additionally, 6% used a combination of HTTP and HTTPS. This usually indicated encryption of just the login process, while any successive transactions were sent without any form of security. These statistics demonstrate how vulnerable the majority of information sent over open connections is to interception by outside parties.

The tests were conducted in various areas of the UBC campus, as well as coffee shops such as Starbucks, and public libraries. Due to the fact that these areas are typically populated with students, our results reflect the kinds of websites this demographic visits as well as their level of awareness of Internet safety. Most users who connected to our networks did not appear to change their site viewing preferences or take any special precautions with the information they were sending although they were aware of the connection's lack of security. Since the attacks we carried out are equally viable in places such as hotels or airports, an attacker could easily gain access to much more sensitive data in the same manner and cause severe damage to the victim.

The notable strengths of our attacks include the simplicity with which they can be achieved; they don't require any special hardware or large amounts of time, just a basic router and packet sniffing program. This demonstrates the ease with which an attacker can gain access to personal information while connected to an unsecured network. This shows that our developments in this area could be a gateway to far more harmful activities.

B. CIA

1) *Confidentiality*: With the use of RAPs, users may think they are on a secure network, when in actuality they are not. Confidentiality is severely reduced due to the fact that while connected to a RAP, all Internet traffic can be captured with a tool such as Wireshark. With this captured traffic, one can determine what sites a user has visited and, to a degree, what they were doing on these sites. An even more concerning fact is that while a user is on an HTTP page the data they send and receive can be seen in plaintext. While most sites that require a login process do so using HTTPS, some do not; for these sites users' login credentials are also compromised. For the sites that do use HTTPS for their login process, the majority of them revert back to HTTP after the user has successfully logged in. In this case, while the user's login credentials are secured, the data they send and receive thereafter are not.

2) *Integrity*: With a transparent HTTP proxy running in tandem with a RAP, any HTTP request sent by the user connected to the RAP can be intercepted and re-written before it is received by the intended target. This can also work in reverse, where the data being received by the user can be re-written before it gets delivered to them. This man-in-the-middle attack reduces the integrity of the data being sent between the victim and their intended target.

3) *Availability*: Although this project's aim was not to specifically reduce accessibility, it most certainly can. While connected to a RAP, users can be redirected to any website an attacker wishes by using DNS redirects. Or, if the attacker wishes, they could simply block the request altogether and essentially be deploying a denial-of-service attack.

C. Recommendations for Users

Obvious recommendations for users that have been given by previous reports to mitigate risks include avoiding public networks when possible, using a wired connection when possible, and using a VPN to connect to public networks. Some additional tactics would be using an encrypted HTTPS proxy for connections, and connecting to public Wi-Fi hotspots that use a login. However, these precautions require specific actions by the user. Based on the findings of our survey – with the exception of awareness of request modification – the overwhelming majority of users who responded were well aware of the risks associated with using an unsecured public network. In particular, nearly all respondents were aware of the risks in not using a personal firewall, and yet fewer than half actually used one. These facts, along with our observations of network traffic, suggest that users are not concerned enough by the risks to bother performing any additional tasks to secure their data.

D. Recommendations for Websites/Services

Though everyone is ultimately responsible for securing their own data, there are actions that we believe web services should undertake to make security as easy as possible for users. Firstly, webpages that use a secure login should maintain that encryption over the entire session. Encrypting only the login prevents attackers from sniffing login credentials, but the confidentiality of all data sent afterward is still vulnerable. Additionally, by giving session cookies a short lifetime, the threat of session hijacking is lessened.

VI. Conclusion

The general findings of the report can be broken down into two parts. Firstly, when using unsecured public Wi-Fi networks, users are susceptible to several easy-to-conduct attacks: traffic sniffing, HTTP request modification, and session hijacking. Most of the traffic observed was of little value, such as personal email, but these data were susceptible to sniffing. High value information, such as financial transactions, however, appeared to be secure even when conducted on unsecure networks. Secondly, the surveyed users generally seem to be aware of the aforementioned threats, yet many do not seem to believe that they are of a serious enough nature to take action in securing their information on the Internet.

Though security is ultimately the user’s responsibility, and there are ways for users to mitigate vulnerabilities on an unsecured network, such as by using a firewall, a VPN or an HTTPS proxy, websites can provide additional security for the convenience of users. Web services using secure login should encrypt all subsequent requests to protect the confidentiality and integrity of the data that requires a password to access. Additionally, creating session cookies with a shorter lifetime reduces the threat of session hijacking being conducted.

The results were based on observing and surveying what were mostly university students. If the study were done on a broader range of people, the results could possibly differ, both in terms of the value of the data at risk and the level of user knowledge.

REFERENCES

[1] C. Ainsworth-Vince. "The Coffee Shop Hackers - Business - Macleans.ca." Editorial.*Maclean's* 29 Nov. 2010: 34. *Macleans.ca - Canada News, World News, Politics, Business, Culture, Health, Environment, Education*. Web. 30 Nov. 2010. Available: http://www2.macleans.ca/2010/11/25/the-coffee-shop-hackers/.

[2]JiWire. "Public Wi-Fi Hotspots Grow 400% Worldwide." *Marketing Charts: Charts and Data for Marketers in Web and Excel Format*. Web. 04 Nov. 2010. Available: http://www.marketingcharts.com/interactive/public-wi-fi-hotspots-grow-400-worldwide-10263/

[3]Babur, Bhaskari, Rao. "A Survey on Session Hijacking" (IJCSIS) International Journal of Computer Science and Information Security, Vol. 8, No. 7, October 2010.

[4]N. Gentleman, I. Kwon, W. Wong and K. Kam. (2009, December). Attack on WPA-PEAP. [Online]. Available: http://courses.ece.ubc.ca/412/term_project/reports/2009/WPA-PEAP_analysis.pdf

[5] W. K. Woo, Q. Wei, J. H. Y. Chiang and J. M. C. Tsai. (2004, November). A Security Analysis of UBC Wireless Network. [Online]. Available: http://courses.ece.ubc.ca/412/term_project/reports/2004/A%20Security%20Analysis%20of%20UBC%20Wireless%20Network.pdf

[6] S. Chang, B. Huang, V. Lam and H. Yen. (2004, November). Security Analysis of Public Wireless Internet Access Points. [Online]. Available: http://courses.ece.ubc.ca/412/term_project/reports/2004/Security%20Analysis%20of%20Public%20Wireless%20Internet%20Access%20Points.pdf

[7] A. Chebium, P. Dhillon, K. Farshad and F. Maud. (2007, November). Rogue Access Points and UBS’s Wi-Fi Network. [Online]. Available: http://courses.ece.ubc.ca/412/term_project/reports/2007-fall/Rogue_Access_Points_and_UBC_Wi-Fi_Network.pdf