Rogue Access Points and UBC's Wi-Fi Network

Arunkumar Chebium, Pawittar Dhillon, Kaveh Farshad, Farhan Masud
Department of Electrical and Computer Engineering, University of British Columbia
Vancouver, BC, Canada
{arun.chebium, peterdhillon, kfarshad, farhanmasud}@gmail.com

ABSTRACT

Rogue Access Points (RAPs) constitute arguably the biggest security threat to Wireless (Wi-Fi) networks today. In this term project, we have studied RAPs in UBC's Wi-Fi network. We have mined recently collected data about wireless access points on campus to extract information about RAPs, prepared scatter plots of this data, demonstrated some threats that a malicious hacker could give rise to by means of using a RAP (MAC address spoofing, phishing, snooping), and talked to a UBC IT network analyst to understand the countermeasures UBC has in place currently to counter the threat of RAPs. Based on this work, we develop a threat model and propose some additional countermeasures that could be employed by students, campus employees and UBC IT administrators to further reduce the threat posed by these RAPs.

INTRODUCTION

A RAP is, quite simply, *any* un-trusted or unknown access point in a wireless Local Area Network (WLAN) that could be used by hackers to gain backdoor access into an otherwise secure network and conduct malicious activity such as snooping, introducing worms and viruses, and launching Man-in-the-Middle (MiM) attacks. A common approach in the industry to detect RAPs is to use sniffer software such as AirMagnet, Airdefense, and NetStumbler and perform a walking audit with a portable device. These software programs can then capture the coordinates of the various Access Points (APs), their SSIDs (Service Set Identifiers), MAC addresses and signal strengths. However, this is a very time-consuming method; moreover, it only yields a snapshot at a certain point in time [1]. A more reliable - albeit expensive - approach involves the use of permanent antennas (probes) that continuously monitor the airwaves to obtain a full wireless footprint of the network [2]. Background probing may also be implemented for organizations that have established wireless network connectivity to augment the existing infrastructure [2].

Solutions proposed by academia to address this issue are few (see [3], [4], [5] for examples of major work). Also, because of their reliance on analyzing the content of actual network traffic, they seem a bit impractical to efficiently and quickly apply to an enterprise-strength network such as UBC's.

In this project, we begin by presenting data about the spread of RAPs in UBC's Wi-Fi coverage area. Then we demonstrate some threats that a hacker using a RAP can give rise to. This led us to conducting a security analysis and sketching out a threat model for the network. Then, based on an interview conducted with a UBC network analyst to understand the countermeasures currently employed by UBC to counter RAPs, we propose some additional countermeasures of our own which, in our opinion, will help further reduce the threats posed by RAPs.

ROGUE ACCESS POINTS IN UBC's Wi-Fi NETWORK

Our first task was to identify and map out the RAPs currently active in UBC's Wi-Fi network in order to get a grasp on the magnitude of the problem. In order to do this, we began with survey data pertaining to UBC's wireless coverage collected by a team member (Peter) as part of another course (EECE 496). The survey's primary intention was to obtain an estimate of the spread of wireless access points on campus so that a plan could be developed to introduce highly portable devices such as Wi-Fi equipped tablets, PDAs and VOIP-enabled devices into the wireless network. The survey was conducted by performing various walking audits that spanned the length and breadth of the UBC campus and resulted in comprehensive data about access points – legitimate and rogue – in the form of huge data files. Each data file consists of over 200,000 lines of data, with each line specifying information about an access point in terms of its GPS co-ordinates, SSID, and other parameters of interest.

Then, by means of a filtering program in MATLAB that we developed, we mined the data in these files and extracted information about those access points that have SSIDs other than 'ubc' and 'ubcsecure' (and are, therefore, unauthorized). We also used the program to prepare scatter plots of the extracted data in order to obtain visually intuitive representations. Here are some of these results:

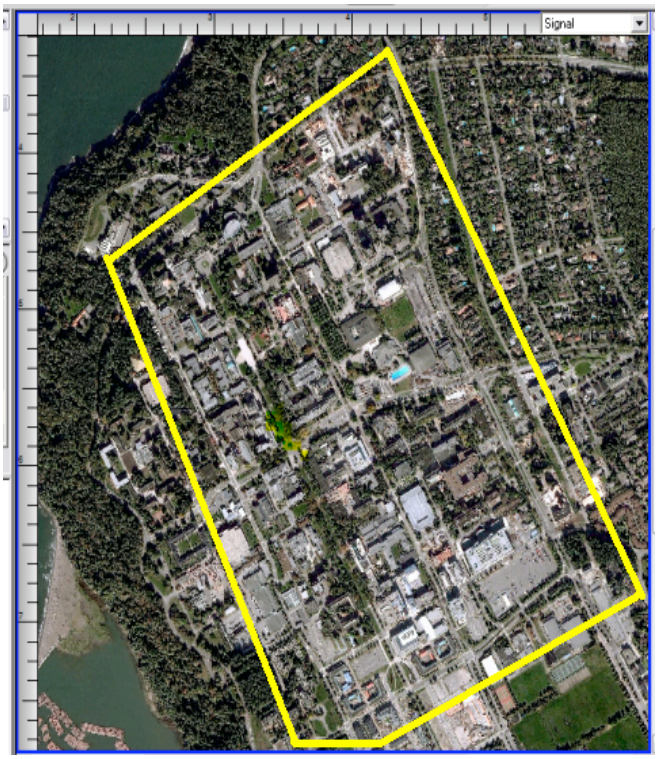

Fig 1: Area of campus that was surveyed

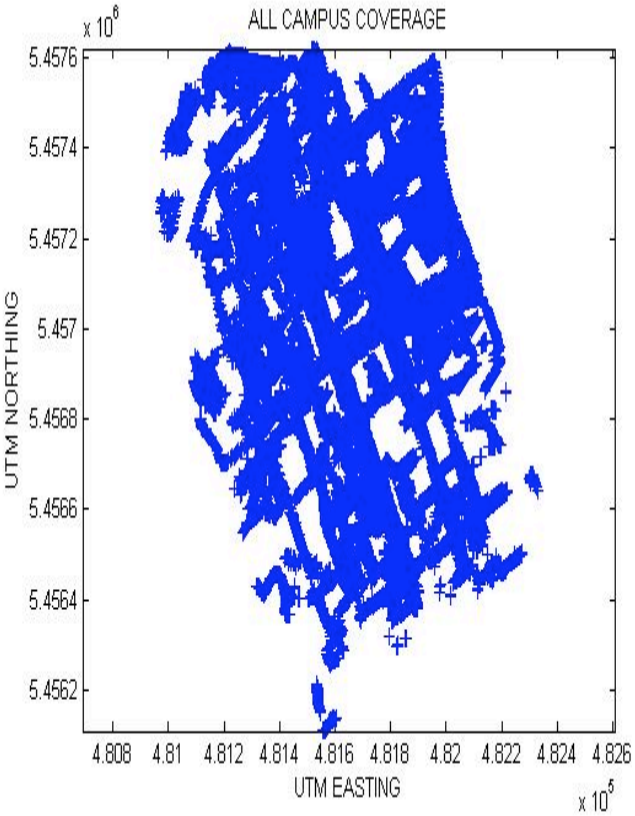

Fig 2: Map of legitimate access points across campus

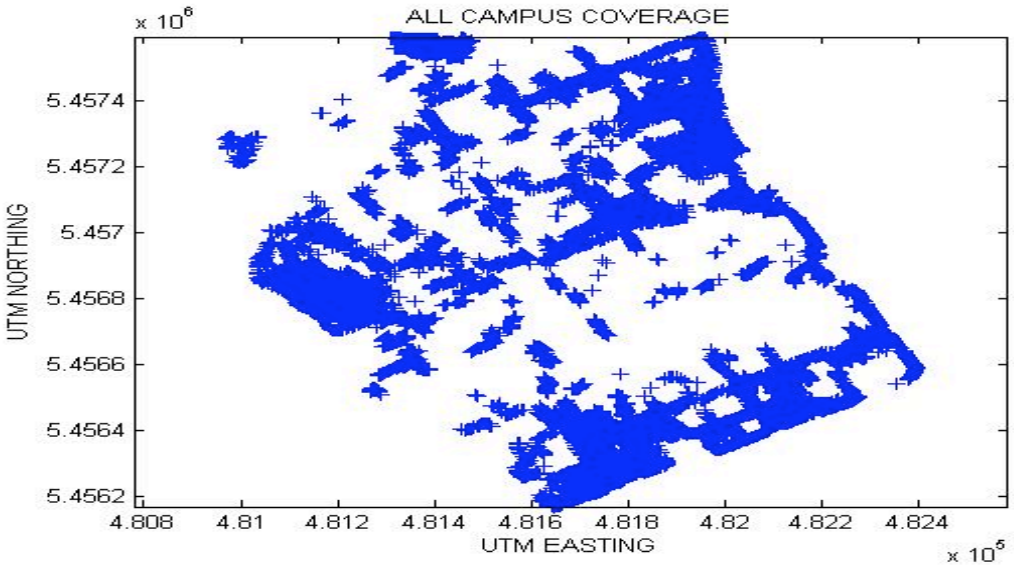

Fig 3: Map of Rogue Access Points across campus

Over 400 RAPs were found in the data that was mined to obtain RAP information.

THREATS DEMONSTRATED

Our second task was to demonstrate some of the threats that RAPs can give rise to. There are three threats that we demonstrated: (1) MAC Address Spoofing (2) Phishing (3) Snooping on sensitive data.

(1) MAC Address Spoofing: To demonstrate this threat, we brought in a 'rogue' desktop computer into UBC and, to allow it to log onto UBC's *wired* LAN, assigned it the MAC address of a trusted computer that was already authenticated and allowed to use the LAN. We then disconnected the trusted computer from the LAN and attempted to access the internet from the rogue computer instead. We were successful in our attempt.

(2) Phishing: Our second mode of attack was more involved. Our intention was to set up a wireless RAP on this rogue desktop computer and broadcast our SSID so that wireless-enabled laptops in the RAP's vicinity would automatically connect to our RAP instead of to UBC's regular wireless service (see [6] for an explanation of why laptops should automatically connect to our RAP). For this purpose, we purchased a commercially available wireless USB adapter that could easily be configured to also work as an access point (see [7]). Also, we gave our RAP an SSID of 'UBC' in order to make it seem as genuine as possible to a casual user who might happen to glance at our RAP's SSID.

We then created our own (fake) version of UBC's wireless login page. Using a freely available tool known as AirSnarf, we created the web-page such that, if a user attempts to log in at that page by typing his/her username and password, we would be able to capture those details in a file and direct the user to another web-page that would display the text "HACKERS.... Just so you know, your password has been obtained." Also, using another freely available tool known as TreeWalk, we poisoned the

cache of the rogue desktop computer so that all attempts to navigate to the URL www.ubc.com – on the rogue desktop computer as well as on any wireless laptops connected to our RAP – would load up our fake web-page (see [8] for a step-by-step explanation of this entire process). However, attempts to navigate to other URLs would work normally as intended, making it difficult for the victim to suspect any malicious activity. Finally, we brought in a wireless-enabled laptop in the vicinity of our RAP; immediately, the laptop *automatically connected* to our RAP and thus obtained wireless internet access through our RAP. Then, sure enough, when we navigated to www.ubc.com on the laptop, it brought up our fake web-page. When the user typed in his user name and password, the "HACKERS..." web-page was displayed, and the username and password were available on the rogue desktop computer for viewing. Thus we were able to demonstrate our version of phishing using a rogue desktop computer, a commercially-available wireless USB adapter, and freely available software tools.

(3) Snooping: The last threat that we were able to demonstrate was snooping. By running a freely available Ethernet sniffer application on the rogue desktop computer, we were able to observe all the internet traffic of the laptop that was connected to the wireless network through our RAP. One can very well imagine what a serious hacker might be able to do with this type of information: he could profile the victim's internet usage and activity, decrypt sensitive information and cause serious damage to the user.

SECURITY ANALYSIS

From our work in the previous section, we see that the victim is vulnerable in different ways. The first threat that we demonstrated – MAC address spoofing – is not only *disruptive* (by stealing someone's MAC address, we are denying them access to the internet and thereby causing a Denial of Service) but also *deceptive* (we are masquerading as an authenticated UBC user). Phishing, though, is more dangerous: the *confidentiality* of the victim's sensitive information is compromised, and by using the harvested username and password, the *integrity* of information that has been protected using this login data can also be compromised. Therefore, this threat is *usurpative* in nature.

Thus, we see that our work outlines the following *threat model*:

1. The *threat agents* here are hackers who would want to conduct malicious activity by using any one of the numerous RAPs available on campus/installing their own RAP (as we did, for example).

2. The threats that they could give rise to are deceptive, disruptive and usurpative in nature.

3. The *assets* at stake are: valid UBC network credentials (high-value), sensitive user login information (very high-value), and user internet profile and internet activity data (high-to-very-high value).

EXISITING COUNTERMEASURES

We talked to Mr. Geoff Armstrong, a Network Support Analyst in UBC's IT department[1], about existing countermeasures against RAPs. Here is a summary of what he had to say and our corresponding thoughts:

- UBC is aware of the presence of RAPs on campus (based on the data we collected, we could identify about 400 RAPs; however, according to Mr. Armstrong, there are about 800 of these currently).

- UBC has a wireless control board that constantly monitors all activity on the UBC wireless network using full-time probes and detects the emergence of RAPs. Indeed, when a RAP appears, analysts such as Mr. Armstrong receive notification alerts via the wireless control board. They can then monitor these APs and, in case any RAP engages in malicious activity, analysts can use valid APs surrounding the rogue to *contain* it (using a standard industry technique such as four-point or eight-point containment where the legitimate APs surrounding the RAP broadcast higher-power signals than the rogue, ensuring that users only connect to these legitimate APs). *However, we were able to conduct malicious activity using our RAP; thus, even though there are system-level techniques available for containment, vulnerabilities and vulnerable time-frames when attackers can operate still exist in UBC's Wi-Fi network.*

- Also, UBC's IT mostly uses due diligence to eliminate RAPs; in most cases, according to Mr. Armstrong, they go 'knocking on the doors' of people running RAPs and ask them to dismantle them. However, this is considerably low-tech, and, based on our work, we argue that this approach cannot provide a quick-enough solution against an attacker who runs, say, a phishing operation from within UBC, especially since he/she can move quickly within UBC and 'hide' his/her RAP behind the considerable number of RAPs already on campus.

Thus, our opinion is that though there are counter-measures in place currently, they need strengthening, especially in the light of the number of RAPs currently on campus and the surprisingly malicious activity that can be conducted – in a very short time-frame – using a RAP.

PROPOSED COUNTERMEASURES

The countermeasures that we propose advocate the principle of *Defense in Depth* by ensuring that there are multiple layers in the defense paradigm employed. These measures recommend that students, campus employees and UBC IT administrators employ some basic safeguards in order to reduce the threats due to RAPs. These are grouped into two categories: 'victim-centric' countermeasures and 'system-centric' countermeasures.

1. 'Victim-centric' countermeasures

The following are some easy safeguards that can be employed by students and campus employees that can prevent them from becoming victims:

- Ensure that all pages which require logging in operate under the "https" protocol. Change browser settings so as to demand certificates from the login website and only login when certificates are valid and unexpired and reflect web-site and issuing

[1] He can be reached at geoff.armstrong@ubc.ca

authority names correctly. (This may be thought of as a variation of *The Principle of Complete Mediation*, in that every access to an asset (login data) is mediated by the user himself/herself.)

- Use VPN whenever possible to log onto campus wireless networks.

2. *'System-centric' countermeasures*

   The following are some simple, additional measures that could be employed by UBC's IT department:

   - Regularize the removal of RAPs; establish strict time-intervals within which every RAP must be dismantled.
   - Quarantine systems that create and operate RAPs and maintain revocation lists of offending MAC addresses and SSIDs.
   - Publish this list on prominent web-sites in the UBC network so that users are better educated about the risks involved with RAPs.

CONCLUSION

Rogue Access Points pose big security threats to enterprise-strength networks but they can be neutralized with due diligence and decisive action. It is our hope that, by demonstrating some of the threats involved, detailing a threat model, and proposing easily-implemented countermeasures, we have been able to increase reader awareness of this important security problem and educate the reader about how best to avoid some of the risks involved and safeguard the confidentiality and integrity of their sensitive information.

REFERENCES

[1] "*Identifying Rogue Access Points*". URL: http://www.wifiplanet.com/tutorials/article.php/1564431.

[2] "*Rogue Access Point Detection: Automatically Detect and Manage Wireless Threats to your Network*". URL: www.espireit.com.au/assets/107/files/RogueAccessPointDetection.pdf

[3] W. Wei, K. Suh, Y. Gu, B. Wang, J. Kurose, "*Passive online rogue access point detection using sequential hypothesis testing with TCP ACK-pairs*", accepted to appear in ACM Internet Measurement Conference (IMC) 2007.

[4] R. Beyah, S. Kangude, G. Yu, B. Strickland, J. Copeland, "*Rogue Access Point Detection using Temporal Traffic Characterstics*", GLOBECOM 2004.

[5] J. Hall, M. Barbeau and E. Kranakis, "*Enhancing Intrusion Detection in Wireless Networks using Radio Frequency Fingerprinting*", Communications, Internet and Internet Technology, 2004.

[6] "*Your computer connects to an access point that broadcasts its SSID instead of an access point that does not broadcast its SSID*".URL: http://support.microsoft.com/kb/811427

[7] "*ZyXEL ZyAIR G-220 - USB 2.0 802.11G Wireless Adapter & Soft-AP - G220*". URL: http://www.buy.com/prod/zyxel-zyair-g-220-usb-2-0-802-11g-wireless-adapter-soft-ap/q/loc/101/10381071.html

[8] "*Evil Twin Access Points for Dummies*". URL: http://airsnarf.shmoo.com/airsnarf4win.html