# Security Analysis of the UBC Wireless Network

Li-Heng Lin, Chun Yue Gordon Wong, and Jeanette Sin Mei Tsang

***Abstract*—We have found that the UBC Wireless Network is extremely vulnerable due to the fact that UBC does not force users of the network to take important security measures such as connecting to the network by VPN. The users are left on their own to protect their computing safety but our survey of users have found that most user have little or no knowledge in computer security issues. Furthermore, vulnerability in the ARP protocol allows attackers to spoof as network gateways and intercept sensitive data. There is no implemental solution to this as the vulnerability of ARP is an inherent design flaw. To improve security, the only solution is to educate users so that users take security precautions and that users do not transmit confidential information through the wireless network.**

## I. Introduction

With the recent deployment of UBC's campus-wide wireless network, many students, and faculties are now able to enjoy the convenience of connecting to the Internet anywhere on the campus. However, wireless networks are inherently insecure as all wireless data transmission is transmitted over open air, and anyone with a wireless card can snoop the communications. Login names, passwords, confidential emails are often transmitted over open airwave without encryption and can be easily captured by attackers. With the number of users increasing monthly, to as many as 5000 users by October 2003 [1], the wireless network is becoming more attractive for malicious attacks as more confidential information become vulnerable. Yet, until now, there is still no security analysis determining the vulnerability and threats to this new wireless network. We are the first to do a Security Analysis of the UBC Wireless Network. We have found powerful tools that exploit the vulnerability in the network. Moreover, our survey of users of the network shows that many people are using the wireless networks without understanding the computing security issues.

## II. UBC Wireless Network Overview

The UBC Wireless Network's is a public network providing all students and faculties instant wireless access to the Internet anywhere at anytime within the UBC campus. The network consists of 1300 Access Points scattered across the whole campus to provide complete wireless coverage. The access points are connected together by switches and forms a large single LAN. Users need to authenticate before they can access the Internet from the wireless network.

The normal login is described as follow:

1) The user connects to an Access Point and receives a DHCP assigned IP address from the DHCP server (not shown). At this stage the user can communicate with other hosts in the network, but all traffic to the Internet is blocked by the gateway.

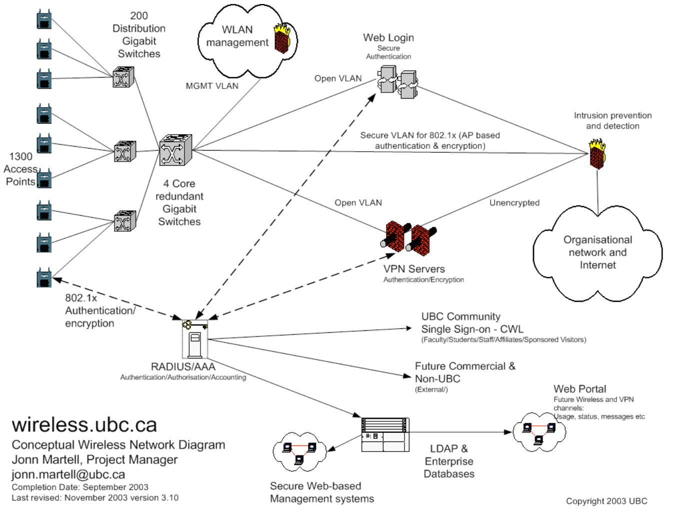


Fig. 1. Conceptual UBC Wireless Network Diagram. The 802.1X Authentication is not yet supported.

2) User opens Internet Explorer, and is automatically directed to a SSL-secured web login.

3) The user types in its login information into the web login page and the information is sent to the RADIUS/AAA server via the SSL protocol.

4) The RADIUS/AAA server obtains the corresponding entry in a SQL database and compares the information with that entered by the user. If they match, then login is allowed; otherwise, the login is refused.

5) After a successful login user is now able to communicate with the rest of the network and the Internet.

Since this is a campus area network, it is imperative that the network is available and accessible by new users with the least amount of effort (i.e. the open air-wave policy). As a result, the security policy is to have no encryption (such as WEP or WPA) on the network traffic because there is no optimum method in distributing the key. And, the only thing that new users are required to do in order to access the remaining part of the network is to login using their campus wide login (CWL) and password. More knowledgeable users can also use the VPN connection to establish a connection with the VPN server in order to gain access to the Internet.

Due to the open air-wave policy, it is infeasible to restrain the kind of data being sent. This is because the cost of monitoring all the packets would be too high. As a result, all kinds of network traffic would be sent over the network, including possible malicious users who try to sniff packets. Therefore, the responsibility of securing the data being passed lies on the users themselves.

In essence, the UBC wireless network is an open network that allows individuals who have a valid CWL account to gain full access to the network resources. However, this also introduces vulnerabilities which are outlined in the next section.

## III. Vulnerability Analysis

### A. No Mandatory Encryption

Wireless networks are inherently vulnerable to sniffing as the data sent between the user and the access point is transmitted over open air; anyone in range can "listen" to the wireless traffic with his wireless card set in promiscuous mode. To protect the wireless communication, UBC provides VPN allowing users to encrypt the data sent between themselves and the gateway in the wired portion of the network. However, VPN is not mandatory in connecting to the network and it is the user's discretion whether he wants to use VPN or not. The concern is that a user may not be knowledgeable enough to use VPN when transmitting sensitive data thru the wireless network.

### B. Large Non-Segmented LAN

Furthermore, the whole wireless network is on a single LAN, connected with switches, and supports up to 4096 hosts. There is no segmentation of the network. A host on the network can send a packet directly to all other 4095 hosts without going through a router. This implies that a malicious host can perform ARP spoofing attacks on all 4095 hosts on the network.

ARP spoofing involves the malicious host sending a fake ARP reply packet to the victim host [2]. The fake ARP packet will contain a fake IP address/MAC address pairing. In the ARP protocol, a host gullibly updates its ARP cache with the content of a received ARP reply packet, without verifying the truthfulness of the content. This allows a malicious host to direct packets from the victim host to itself, even though the packets are not destined for the malicious host. One example is the malicious host sending an ARP packet to the victim, containing the gateway's IP address and its own MAC address. Upon receiving the ARP packet, the victim will associate the gateway's IP address with the attacker's MAC address. When the victim sends a packet to the gateway, the packet will contain the gateway's IP address, but with the attacker's MAC address. The switches, layer-2 devices, will only look at the MAC address and switch the packet to the attacker instead.

ARP spoofing enables a malicious host to direct packets from any host in the LAN to itself. It enables the attacker to sniff other hosts' packets or even perform Man-In-The-Middle attack on any host in the LAN. The UBC Wireless network, a non-segmented LAN with 4095 hosts open to attack, provides an attacker a wide selection of targets.

### C. Campus Wide Login

Users use their Campus Wide Login to authenticate to the UBC Wireless Network. However, Campus Wide Login is used to login to services such as WebCT, and MyUBC email accounts as well. If an attacker somehow obtains the user's CWL during user's login to the wireless network, then the user's WebCT and MyUBC accounts are compromised as well. Or in the other way, if an attacker captures the user's CWL while the user is accessing his MyUBC email account, then the attacker can gain unauthorized access to the UBC Wireless Network. This violates the *Least Common Mechanism Principe* which states that "Mechanisms used to access resources should not be shared [3]."

### D. Users

The UBC wireless network is intended for public use. Ease of Use is one of the primary goals and Usability is more important than Security [4]. As a result, users are only required to authenticate to the UBC wireless network to access the Internet. However, there are absolutely no security enforcements such as forcing students to use VPN or to install Virus Scanners on their computers. As a result, students are totally left on their own to protect themselves. Many students using the wireless network are students in the Arts or Science faculty who may not be aware of issues in computer security. UBC Wireless network becomes a large collection of vulnerable users, which can be very attractive for malicious intents. Professor Dave Michelson, one of the designer of the UBC Wireless Network justified the lack of security enforcement by saying that what most students do are protected anyways, since web pages that require the transmission of sensitive information all uses SSL. To understand how vulnerable the users really are, we surveyed wireless network users from a variety of backgrounds. Detail of the survey is discussed in next section.

## IV. Assessment of User Vulnerability by Survey

The purpose of the survey is to understand how users have been using the wireless network and to find out whether the users have taken basic steps to protect their computing privacy.

The survey was taken place in November 2004. The target group of the survey is student users of the UBC Wireless Network from the UBC's Main Library, Koerner's Library, Student Union Building (SUB), Woodward Building, Forestry Building, Macleod Building, and the Henry Angus Building. The survey was given out in form of paper questionnaire, consisting of twenty two questions in total. There were eighty four responses gathered.

Of all the respondents, 77% is undergraduate level, and 12% is graduate level. There is a fair breakdown of the faculty of which they are from: Arts (20%), Sciences (20%), Engineering (21%), Commerce (20%), other faculties (9.5%), and not stated (9.5%). The distribution on the types of operation system that the participants use are: Windows (65%), Mac (14.5%), and not stated (20.5%).

The most basic computing security measure includes the use of personal firewall and anti-virus software. According to the survey, 25% of respondents do not use anti-virus software and 48% of the respondents do not use firewall. The result suggests that a significant number of users are vulnerable to worms, and Trojans. Users' computers infected by Trojans may be hijacked and used by an attacker to launch attacks from the UBC Wireless Network. Of the users with Windows XP Operating System, 28% did not install Service Pack 2, which contains significant security enhancements.

Virtual Private Network (VPN) is the only way to prevent packets to be sniffed in open air. However, only 20% of the respondents are using VPN. For the remaining users who are not using VPN, 63% of them are not even aware of the VPN technology, 18% of them think the network is secure enough without using VPN, and 20% of them think that it is inconvenient to use. This suggests that the UBC IT department is not doing enough to inform users the security issues and not preaching the use of encryption.

We were interested in the main usage of the wireless network.

The table shows that the main usage of the network is Email, Browsing and Instant Messenger. From this, we were interested in determining how many users check their UBC email by Outlook or Eudora. We know that at the UBC Interchange website, instructions for setting up Outlook/Eudora did not teach users to use SSL encryption when accessing the UBC POP mail server. Since the POP mail server login/password is the CWL, this means many users are transmitting their CWL and emails in the open air. Forty percent of the respondents use Outlook/Eudora on the wireless network. Out of the 40%, only 32% ensured that Outlook connects to the mail server by SSL. The other 68% are transmitting their CWL in open air. One can probably obtain many CWL by sniffing packets in highly concentrated areas such as the Student Union Building. This underscores UBC IT department's failure to instruct users to setup their applications securely. Moreover, 9% of the user that uses Outlook/Eudora said they did not enable SSL but the email they access contains highly confidential information such as passwords, and credit card numbers. Forty-four percent of the user said that the email was private but not essential to be kept confidential.

TABLE I
USAGE CHART

| Main Usage | % Participants |
|---|---|
| Email | 83.3% |
| Browsing on non-UBC websites | 78.6% |
| Browsing on UBC's websites | 70.2% |
| Chat (instant messeger) | 61.9% |
| Streaming (for multimedia) | 31.0% |
| Online game | 17.9% |
| Others | 3.4% |

Next we wanted to determine the value of data that may be obtained from sniffing instant messenger conversations. Fortunately, only 7% of the respondents are having confidential conversations which contain personal information such as credit cared numbers and passwords, 58% are having private conversation which they would not like people to eavesdrop, and 35% are not concerned about any eavesdropping.

There is only a minority of users who are using FTP from the wireless connection. Of that group of user, about over half do not mind the transmitting data being stolen.

The UBC network is on at all time all year around (except for maintenance) and is providing services to over 1000 students daily according to Martell's work in 2003. It is shown in the survey that on average each student is connected to the network for 13.8 hours per week, which is about 2.76 hours per school day (Monday to Friday). For that about 50% of the users usually log onto the network at the same location and approximately the same time. To do a rough estimation, this means that daily about 500 students are vulnerable to attacks which are pin pointed to individual user.

In additional to the legitimate usages of the network, there also exist of downloading programs such as Bittorrrent, and Kazaa, which use peer-to-peer transmission. The information transmitted on these programs are not being patrolled or filtered in anyway, their contents are of low integrity. As an analogy, they are act like an open door to viruses and spy wares. Users who use these programs are at high risk of becoming the victims of malicious attacks. With excessive use of these programs would lead to congestion in the network traffic as well. The result of our survey shows that there are 64% of our survey participants who never use those programs. However, there are 12% who use them once or more daily, 4.8% who use them weekly, 4.8% who use them monthly, and 7.1% who use them once per term.

How secure is the UBC wireless network? About 30% of the participants think that wireless network is very secure that they would even send and receive confidential information such as back account information, and credit card information via the network. Then 51% think that it is not very secured in that they would send out non-sensitive yet personal data.

Any secured website, such as the login page of UBC Wireless, is SSL-encrypted, and would have a golden padlock at the lower right corner along with "https://" at the front of the address. Normally, fake websites to these SSL-encrypted sites would not be able to present such features as the X509 certificate would need to be obtained through a governing body, and is hard to make up one. Yet, there are 42% of the participants who do not notice such safety features.

It is shown in the survey that only 60% of the participants actually check the name of the network (i.e. UBC) before they log onto the network. So if any illegitimate wireless network has been set up in the UBC campus area, and is giving out stronger signals than the UBC's access point, the computer may be in risk of being logged onto that non-UBC by default. User's data may be compromised by transmitting data to the illegitimate access point.

The above survey shows how vulnerable most users are due to lack of security knowledge. In fact, when told that users' instant messenger conversations and passwords are vulnerable for sniffing and other attacks, 82% of the participants are interested in learning more about how to be protected against security attacks. This shows that the users do care about their computing security, but they must be first educated about the dangers. UBC IT department should teach users about security issues more actively.

## V. Threat Analysis

### A. *Attack Tools*

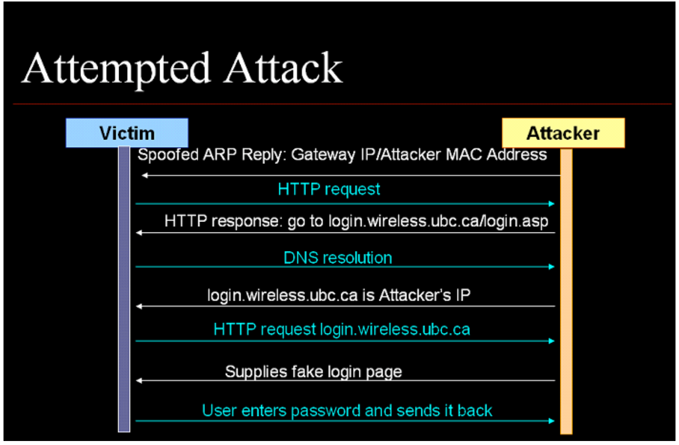
We have found a large list of tools that allow one to exploit different vulnerabilities in a network. These tools are free and available to download from the Internet. Below, we briefly describe each tool that we used.

1) Ethereal – This is a packet sniffer that supports dissection of many protocols. One of the most useful features that this program provides is the ability to follow a TCP stream; the user does not have to manually track down all the TCP packets involved in a TCP connection. We easily followed MSN messenger conversations that we have captured. We also used the program to filter out POP packets sent by users as they access their UBC email accounts by Outlook; and obtained unencrypted login/password information. This further underscores the Principle of Least Common Mechanism. Campus Wide Login is used to access UBC email accounts. It is also the same login to access the UBC Wireless Network. If we were malicious users we could use the captured Campus Wide Login to gain unauthorized access to the wireless network.

2) Cain, Ettercap - Cain and Ettercap are two separate tools but with very similar functionality. The tools allow the user to do Man-In-The-Middle attack through ARP spoofing. To become the Man-In-The-Middle between *Host A* and *Host C*, the tool sends to *Host A* an ARP packet containing [*Host C* IP Address / Attacker MAC address]. It then sends to *Host C* an ARP packet containing [*Host A* IP address / Attacker MAC address]. Packets from *Host C* to *Host A* will be first switched to the attacker's wireless card, and then the attacker forwards the packet to *Host A* and vice versa. The tools include SSL dissection support. When *Host A* wants to establish a SSL connection with *Host C*, the attacker will receive the request and respond with a fake SSL certificate. The attacker then establishes a separate SSL connection with Host C. The attacker will then forward the packets from A to C and C to A. The attacker can now see the communication between Host A and Host C in plaintext. We tried this attack on a normal user and the gateway of the network. We successfully poisoned the user's ARP cache, i.e. the user sent all his gateway traffic to our computer; however, we were not successful in spoofing the gateway's ARP cache. We suspected that the gateway updates its ARP cache only when it actually sends an ARP request. This result suggested that it will be difficult for an attacker to do the Man-In-The-Middle attack on a user connecting to a SSL encrypted website, which greatly increased our confidence in the Wireless Network's security.

### B. *Stealing Campus Wide Login*

Although we have failed to poison the gateway's ARP cache we were still able to poison a user's ARP cache. Leveraging this, we designed another attack aimed at obtaining a user's CWL.



Attempted Attack

Victim

Attacker

Spoofed ARP Reply: Gateway IP/Attacker MAC Address

HTTP request

HTTP response: go to login.wireless.ubc.ca/login.asp

DNS resolution

login.wireless.ubc.ca is Attacker's IP

HTTP request login.wireless.ubc.ca

Supplies fake login page

User enters password and sends it back

Fig. 2. Sequence Diagram of our attempted attack.

1) We poison the victim's ARP cache with the ARP reply packet [Gateway IP Address / Our MAC address]. The victim will now send all his gateway traffic, including HTTP and DNS requests to our machine.

2) We run a proxy server on our computer that handles HTTP requests and DNS requests.

3) When the user attempts to browse the Internet, his computer will send a HTTP request to our computer. Our computer then redirects the user to our own webpage with the address "login.wireless.ubc.ca". Since our computer handles the user's DNS requests as well, we can spoof the domain name of our computer. The browser on the user's computer will be fooled into thinking that it is actually displaying a webpage at "login.wireless.ubc.ca" and displays this on the URL field of the browser.

4) By making our webpage identical to that of UBC Wireless Network login page, we can lure the users entering their CWL into our webpage. We will then have the user's CWL. After this we update the user's ARP cache with the correct entries and he can then browse normally.

We successfully performed this attack at the UBC Wireless Network. This is a serious implication as this attack was not too difficult to perform. We didn't have to write any code and the attack was performed with free existing tools. It is a matter of time before a keen attacker will perform such type of attacks, obtaining Campus Wide Login of students, professors. Professors' Campus Wide Logins are especially valuable as it may lead to the ability to change students' grades.

## VI. Suggested Solutions

According to the literatures, ARP spoofing utilizes the flaw in the ARP protocol in which the victim accepts any ARP replies from the attacker, thus any crafted ARP replies can easily make their way into the victim's ARP table. As a result, forged ARP entries are used, causing the victim's computer to talk to the attacker's computer rather than a legitimate host, such as the real network gateway.

Solution to the ARP attacks include:

1) Intrusion Detection System – an intrusion detection system is a system that can collect metrics data and based on the statistics, determine if an attack is or has occurred, and it comprises of the following modules:

Network Monitor – it is located either on a host computer or on another independent machine promiscuously watching all the traffics. It monitors the network packets to identify patterns that belong to any known attacks. Upon detection, it can either report to the network administrator or performs other actions to minimize the impact of the attack.

System Integrity Verifier – it is a component used to evaluate the integrity of the system, for example, if any system files have been modified in an unauthorized manner (which may potentially mean that a backdoor has been planted into the system).

Log File Monitor – this component monitors and analyzes log files in order to detect other offline attacks.

Deception System – some intrusion detection system includes a component that can emulate holes in a system, thus trapping attackers.

Basically, an intrusion detection system tries to implement the Clark-Wilson security model. Although it may be a rather costly solution, it is one of the more accepted solutions due to its effectiveness. Duffy [5] also describes a handling process for when an ARP attack occurs.

Use of intrusion detection system will allow on going attacks to be detected. The network administrators can then take appropriate action.

2) Static ARP entries – let users make static entries in the ARP table for important addresses such as the gateway, and the VPN server. These entries would not be changed by incoming ARP reply packets and ARP spoofing cannot take place. The attacker will not be able to pretend to be the gateway.

Solutions to sniffing:

1) IPSEC Based VPN – mandatory use of VPN for all wireless network users. This will prevent sensitive wireless data from being sniffed.

Lastly, it cannot be emphasized less that users need to be more educated. When users are aware of the risks involved using the wireless network, they will more likely to take security precautions and not transmit sensitive information across the network. The IT department could post postures regarding wireless security on campus, provide free seminars, put different security "hints" regularly on the actual login page so that users can be informed every time they log onto the network.

## References

[1] John Martell, "Deploying the World's Largest Campus IEEE 802.11b Network," November 2003.

[2] Sean Whalen. (2001, April). An Introduction to ARP Spoofing [Online]. Available: http://node99.org/projects/arpspoof

[3] Matt Bishop, *Introduction to Computer Security*. Toronto, ON: Addison-Wesley, 2005, pp. 206.

[4] John Martell, "Deploying the World's Largest Campus IEEE 802.11b Network," November 2003.

[5] Shawn P. Duffy, CISSP, Wireless Vulnerability: ARP Poisoning, GCIH Certification in Advanced Incident Handling & Hacker Exploits, 2002E.