Security and privacy in public WLAN networks

Savio Lau

saviol@cs.sfu.ca

March 01, 2005

cnl communication networks laboratory

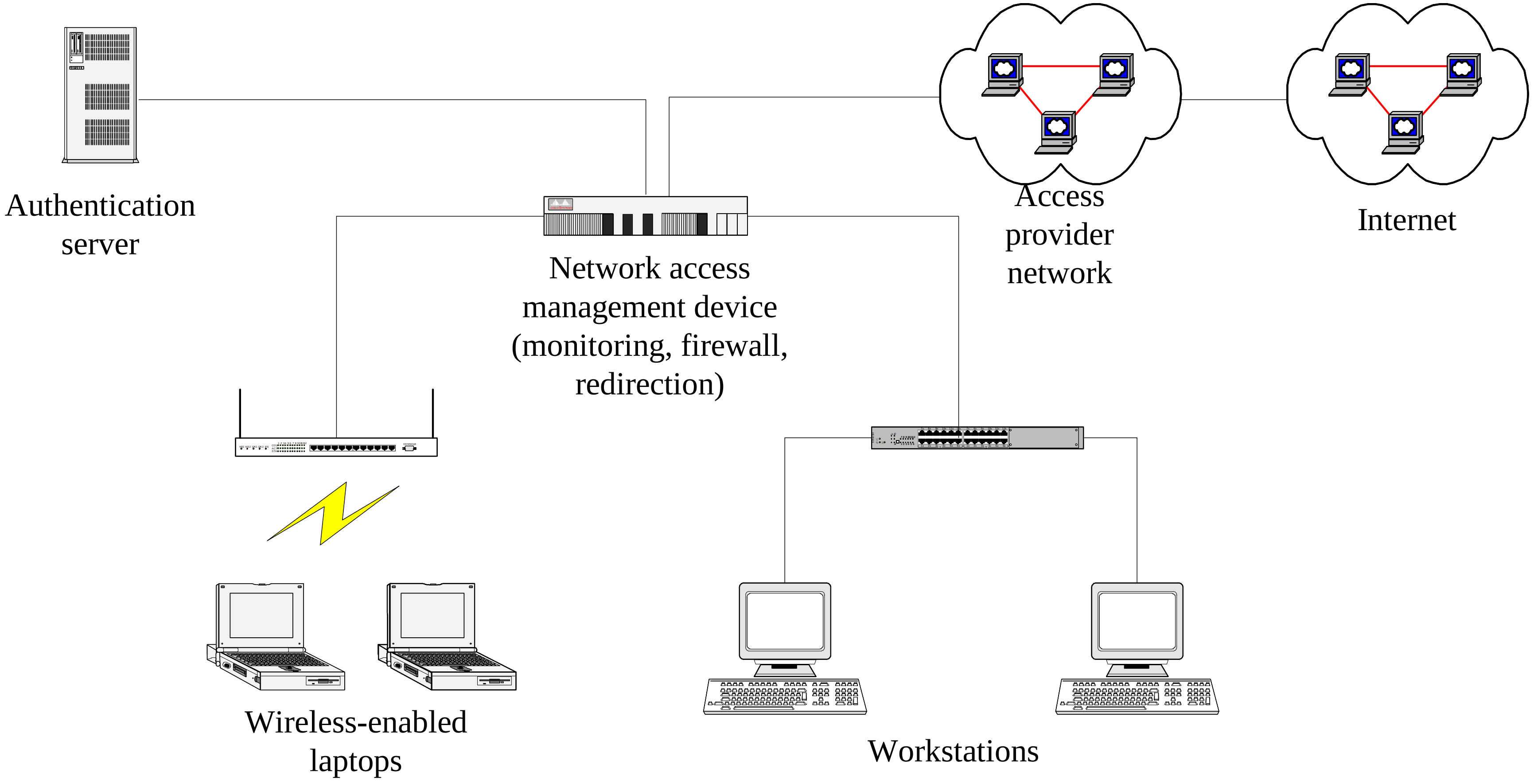
Roadmap

- Introduction of public WLAN networks
- Network security
- User privacy
- Experiments and analysis
- Conclusion

Public WLAN networks

- Refers to pay and non-pay networks that allows public to access limited services such as the Internet:
  - wireless access from coffee shops, Internet cafes
  - cellular companies operated networks: FatPort, T-mobile
  - campus networks: SFU, UBC

Layout of public WLAN networks



Layout of public WLAN networks

- 802.11a/b/g air link:
  - user WLAN devices
  - access provider WLAN routers
- Access provider network:
  - firewall
  - intrusion detection system
  - authentication services
- Internet

Difference between switched and wireless networks

- Switched networks prevents data snooping through neighboring ports:
  - redirection attacks through ARP cache poisoning and other means is possible, but easily detectable
- WLAN is by design a broadcast network:
  - signals can be received by multiple hosts within an area

Roadmap

- Introduction of public WLAN networks
- Network security
- User privacy
- Experiments and analysis
- Conclusion

Network security

- Access providers establish network security for the following reasons:
  - metered access to services and accounting
  - protection of their own network from malicious attacks
  - prevention of viruses and worms from infecting their own network
  - prevention of unauthorized access to non-public services

Network security

- Network providers achieve network security through the following methods:
  - authentication for granting access
  - firewalls for limiting access to non-public services
  - rule-based monitoring of traffic for attacks, viruses, and worms
  - automatic preventive actions if malicious traffic is suspected

Example network: SFU

- Employs a Vernier Networks' product for access control:
  - endpoint screening
  - network access restriction
  - traffic inspection
  - remediation policy enforcement

Roadmap

- Introduction of public WLAN networks
- Network security
- User privacy
- Experiments and analysis
- Conclusion

User privacy

- User privacy includes:
  - controlled access to users' assets and data
  - safety of user traffic from eavesdropping
  - safety from malicious attacks
  - safety from viruses and worms

Achieving user privacy

- Access control can be achieved through the use of password-based sharing and firewalls
- Safety from attacks, viruses, and worms can be achieved through up-to-date anti-virus products and firewalls

Network security vs. user privacy

- Goals of network operators and users are not necessary identical
- Networks that are secure from providers' perspective may not guard users' privacy
- Network providers' task is to prevent malicious traffic from entering network
- How secure is network traffic over WLAN interfaces?

Roadmap

- Introduction of public WLAN networks
- Network security
- User privacy
- Experiments and analysis
- Conclusion

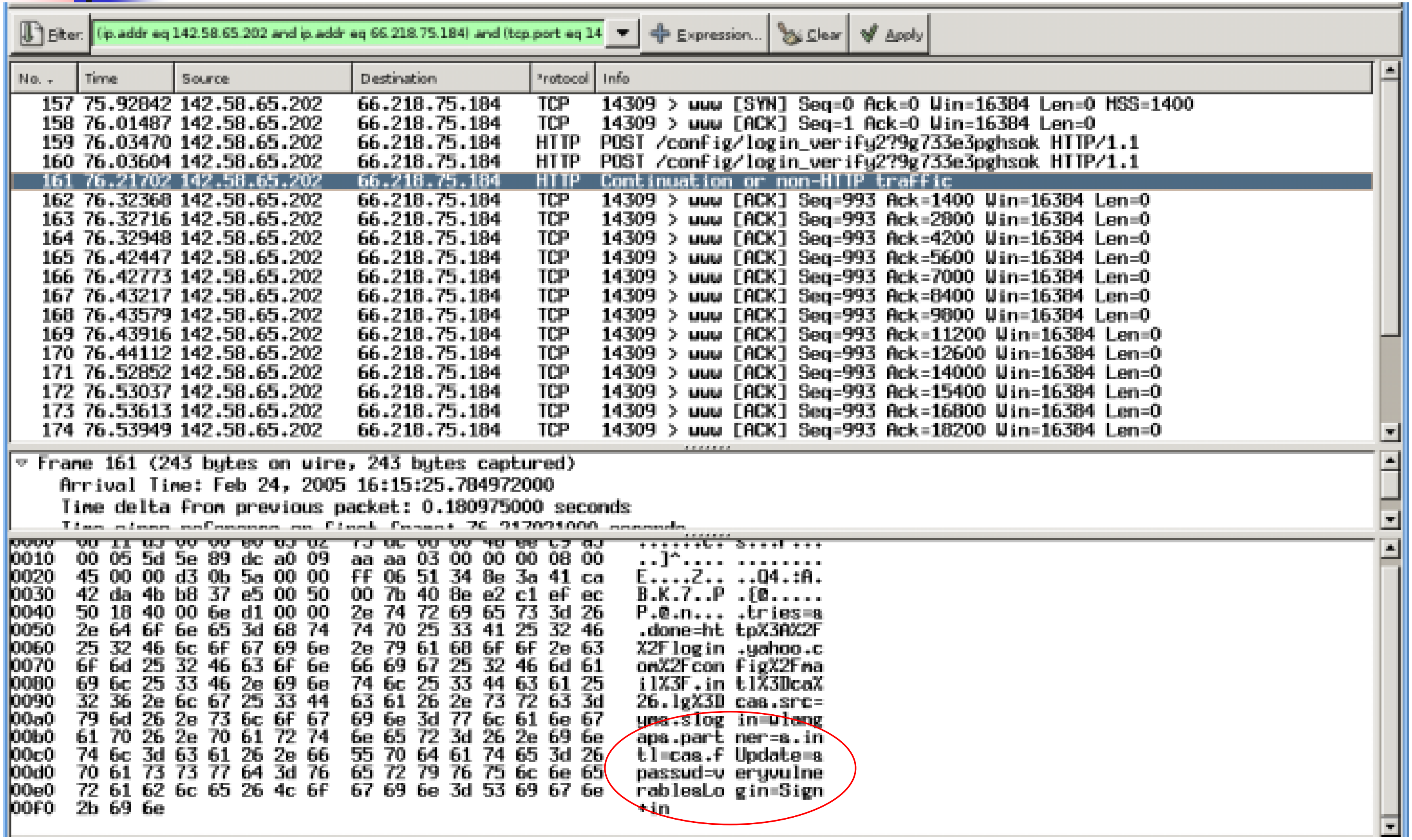
User privacy experiment

- Experiment was performed on SFU’s campus network
- Two laptops and a WLAN-enabled PDA were used
- One laptop was set to monitor/promiscuous mode to capture traffic from the PDA and the second laptop:
  - Ethereal under Linux was used to capture traffic
  - only traffic from the two laptops and the PDA were captured for privacy reasons

User privacy experiment

- The PDA and the second laptop attempt to access the following services:
  - Yahoo and Excite email services with newly created accounts
  - ICQ internet messaging
  - POP3 email retrieval
  - SMTP email transfer

Ethereal captures from PDA: Yahoo mail



Filter:
(ip.addr eq 142.58.65.202 and ip.addr eq 66.218.75.184) and (tcp.port eq 14
Expression...
Clear
Apply

```
No. -  Time     Source         Destination    Protocol Info
  157 75.92842 142.58.65.202  66.218.75.184  TCP      14309 > www [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1400
  158 76.01487 142.58.65.202  66.218.75.184  TCP      14309 > www [ACK] Seq=1 Ack=0 Win=16384 Len=0
  159 76.03470 142.58.65.202  66.218.75.184  HTTP     POST /config/login_verify2?9g733e3pghsok HTTP/1.1
  160 76.03604 142.58.65.202  66.218.75.184  HTTP     POST /config/login_verify2?9g733e3pghsok HTTP/1.1
  161 76.21702 142.58.65.202  66.218.75.184  HTTP     Continuation or non-HTTP traffic
  162 76.32368 142.58.65.202  66.218.75.184  TCP      14309 > www [ACK] Seq=993 Ack=1400 Win=16384 Len=0
  163 76.32716 142.58.65.202  66.218.75.184  TCP      14309 > www [ACK] Seq=993 Ack=2800 Win=16384 Len=0
  164 76.32948 142.58.65.202  66.218.75.184  TCP      14309 > www [ACK] Seq=993 Ack=4200 Win=16384 Len=0
  165 76.42447 142.58.65.202  66.218.75.184  TCP      14309 > www [ACK] Seq=993 Ack=5600 Win=16384 Len=0
  166 76.42773 142.58.65.202  66.218.75.184  TCP      14309 > www [ACK] Seq=993 Ack=7000 Win=16384 Len=0
  167 76.43217 142.58.65.202  66.218.75.184  TCP      14309 > www [ACK] Seq=993 Ack=8400 Win=16384 Len=0
  168 76.43579 142.58.65.202  66.218.75.184  TCP      14309 > www [ACK] Seq=993 Ack=9800 Win=16384 Len=0
  169 76.43916 142.58.65.202  66.218.75.184  TCP      14309 > www [ACK] Seq=993 Ack=11200 Win=16384 Len=0
  170 76.44112 142.58.65.202  66.218.75.184  TCP      14309 > www [ACK] Seq=993 Ack=12600 Win=16384 Len=0
  171 76.52852 142.58.65.202  66.218.75.184  TCP      14309 > www [ACK] Seq=993 Ack=14000 Win=16384 Len=0
  172 76.53037 142.58.65.202  66.218.75.184  TCP      14309 > www [ACK] Seq=993 Ack=15400 Win=16384 Len=0
  173 76.53613 142.58.65.202  66.218.75.184  TCP      14309 > www [ACK] Seq=993 Ack=16800 Win=16384 Len=0
  174 76.53949 142.58.65.202  66.218.75.184  TCP      14309 > www [ACK] Seq=993 Ack=18200 Win=16384 Len=0
```

```
▽ Frame 161 (243 bytes on wire, 243 bytes captured)
    Arrival Time: Feb 24, 2005 16:15:25.784972000
    Time delta from previous packet: 0.180975000 seconds
    Time since reference or first frame: 76.217021000 seconds
```

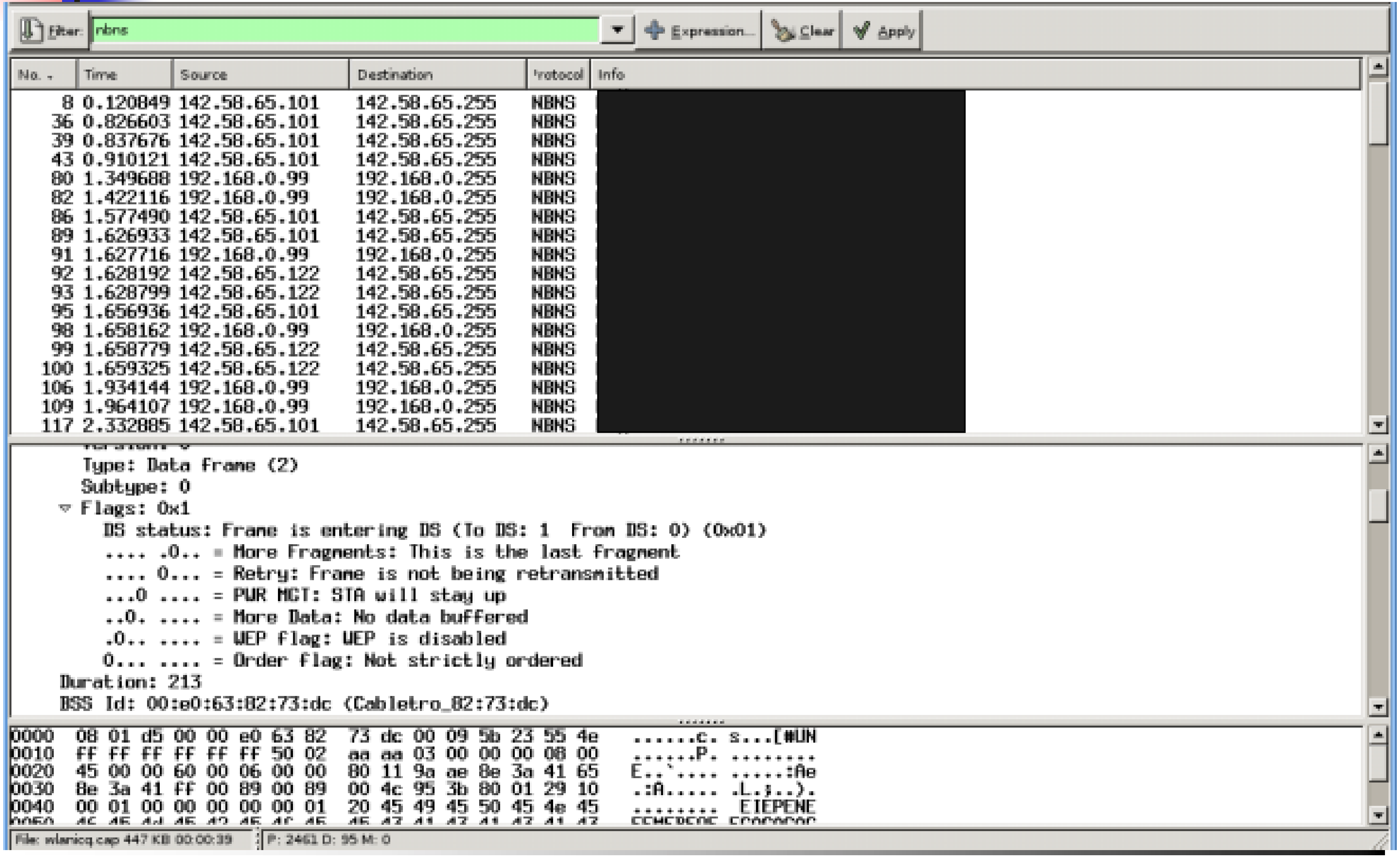
```
0010  00 05 5d 5e 89 dc a0 09  aa aa 03 00 00 00 08 00   ..]^.... ........
0020  45 00 00 d3 0b 5a 00 00  ff 06 51 34 8e 3a 41 ca   E....Z.. ..Q4.:A.
0030  42 da 4b b8 37 e5 00 50  00 7b 40 8e e2 c1 ef ec   B.K.7..P .{@.....
0040  50 18 40 00 6e d1 00 00  2e 74 72 69 65 73 3d 26   P.@.n... .tries=&
0050  2e 64 6f 6e 65 3d 68 74  74 70 25 33 41 25 32 46   .done=ht tp%3A%2F
0060  25 32 46 6c 6f 67 69 6e  2e 79 61 68 6f 6f 2e 63   %2Flogin .yahoo.c
0070  6f 6d 25 32 46 63 6f 6e  66 69 67 25 32 46 6d 61   om%2Fcon fig%2Fma
0080  69 6c 25 33 46 2e 69 6e  74 6c 25 33 44 63 61 25   il%3F.in tl%3Dca%
0090  32 36 2e 6c 67 25 33 44  63 61 26 2e 73 72 63 3d   26.lg%3D ca&.src=
00a0  79 6d 26 2e 73 6c 6f 67  69 6e 3d 77 6c 61 6e 67   ym&.slog in=wlang
00b0  61 70 26 2e 70 61 72 74  6e 65 72 3d 26 2e 69 6e   ap&.part ner=&.in
00c0  74 6c 3d 63 61 26 2e 66  55 70 64 61 74 65 3d 26   tl=ca&.f Update=&
00d0  70 61 73 73 77 64 3d 76  65 72 79 76 75 6c 6e 65   passwd=v eryvulne
00e0  72 61 62 6c 65 26 4c 6f  67 69 6e 3d 53 69 67 6e   rable&Lo gin=Sign
00f0  2b 69 6e                                           +in
```

Ethereal captures from PDA: Yahoo mail

```
POST /config/login_verify2?9g733e3pghsok HTTP/1.1
...
Host: login.yahoo.com
...
User-Agent: Mozilla/4.08 (PDA; PalmOS/sony/model
    luke/Revision:2.0.22 (en)) NetFront/3.1

Referer:
    http://login.yahoo.com/config/exit?&.src=ym&.lg=ca&.intl=ca&.done
    =http%3a%2f%2flogin.yahoo.com%2fconfig%2fmail%3f.intl%3dca
    %26.lg%3dca
...
.tries=&.done=http%3A%2F%2Flogin.yahoo.com%2Fconfig%2Fmail%3
    F.intl%3Dca%26.lg%3Dca&.src=ym&.slogin=wlangap&.partner=&.in
    tl=ca&.fUpdate=&passwd=veryvulnerable&Login=Sign+in
```

Ethereal captures from 2nd laptop: NetBIOS (NBNS)



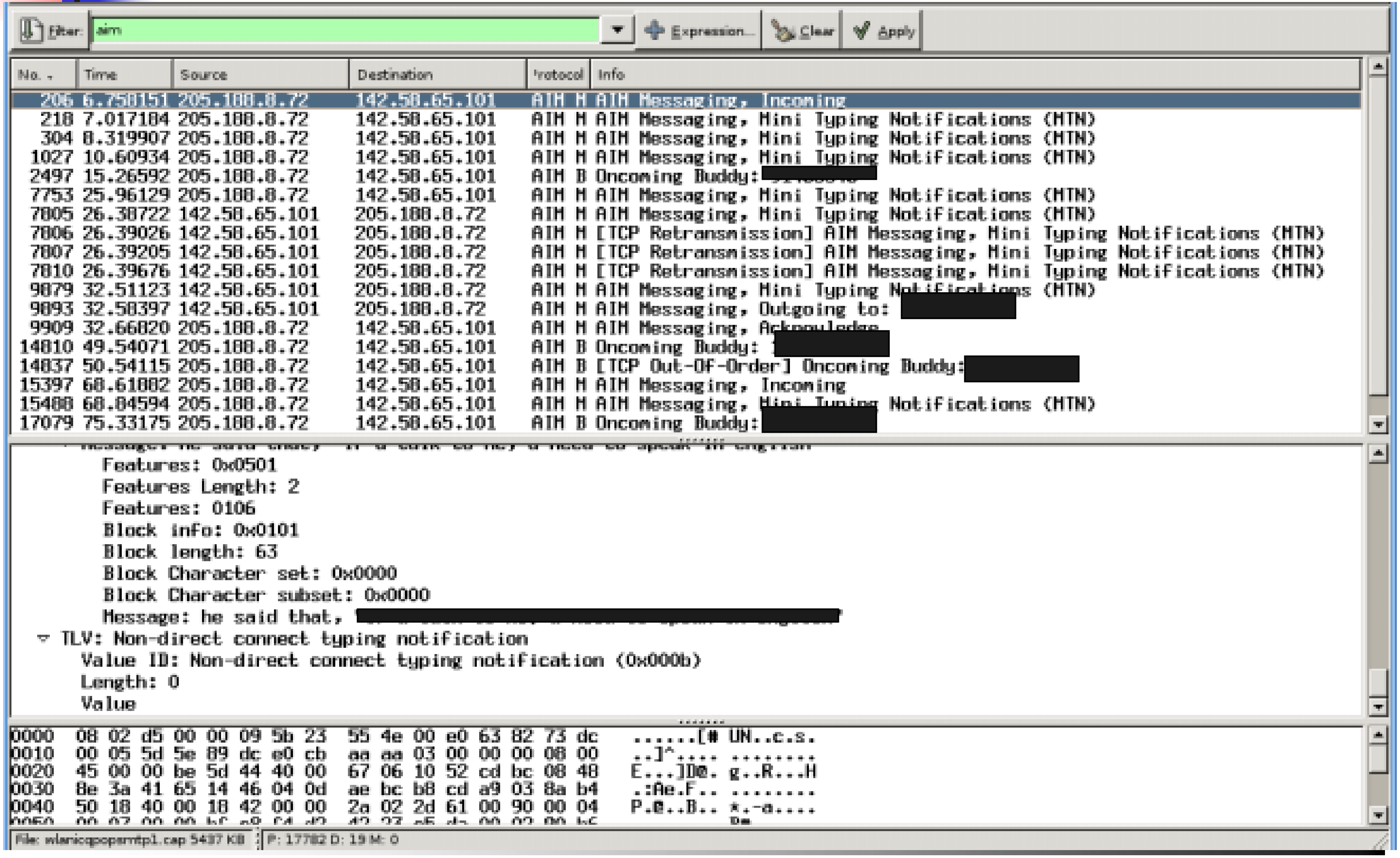
```
No. -  Time     Source          Destination     'rotocol Info
    8 0.120849 142.58.65.101   142.58.65.255   NBNS     [redacted]
   36 0.826603 142.58.65.101   142.58.65.255   NBNS
   39 0.837676 142.58.65.101   142.58.65.255   NBNS
   43 0.910121 142.58.65.101   142.58.65.255   NBNS
   80 1.349688 192.168.0.99    192.168.0.255   NBNS
   82 1.422116 192.168.0.99    192.168.0.255   NBNS
   86 1.577490 142.58.65.101   142.58.65.255   NBNS
   89 1.626933 142.58.65.101   142.58.65.255   NBNS
   91 1.627716 192.168.0.99    192.168.0.255   NBNS
   92 1.628192 142.58.65.122   142.58.65.255   NBNS
   93 1.628799 142.58.65.122   142.58.65.255   NBNS
   95 1.656936 142.58.65.101   142.58.65.255   NBNS
   98 1.658162 192.168.0.99    192.168.0.255   NBNS
   99 1.658779 142.58.65.122   142.58.65.255   NBNS
  100 1.659325 142.58.65.122   142.58.65.255   NBNS
  106 1.934144 192.168.0.99    192.168.0.255   NBNS
  109 1.964107 192.168.0.99    192.168.0.255   NBNS
  117 2.332885 142.58.65.101   142.58.65.255   NBNS
```

```
    Type: Data frame (2)
    Subtype: 0
  ▽ Flags: 0x1
      DS status: Frame is entering DS (To DS: 1  From DS: 0) (0x01)
      .... .0.. = More Fragments: This is the last fragment
      .... 0... = Retry: Frame is not being retransmitted
      ...0 .... = PWR MGT: STA will stay up
      ..0. .... = More Data: No data buffered
      .0.. .... = WEP flag: WEP is disabled
      0... .... = Order flag: Not strictly ordered
  Duration: 213
  BSS Id: 00:e0:63:82:73:dc (Cabletro_82:73:dc)
```

```
0000  08 01 d5 00 00 e0 63 82  73 dc 00 09 5b 23 55 4e   ......c. s...[#UN
0010  ff ff ff ff ff ff 50 02  aa aa 03 00 00 00 08 00   ......P. ........
0020  45 00 00 60 00 06 00 00  80 11 9a ae 8e 3a 41 65   E..`.... .....:Ae
0030  8e 3a 41 ff 00 89 00 89  00 4c 95 3b 80 01 29 10   .:A..... .L.;..).
0040  00 01 00 00 00 00 00 01  20 45 49 45 50 45 4e 45   ........  EIEPENE
```

File: wlanicq.cap 447 KB 00:00:39   P: 2461 D: 95 M: 0

Ethereal captures from 2nd laptop: ICQ



```
No. -  Time       Source          Destination     'rotocol  Info
  206 6.750151   205.188.8.72    142.58.65.101   AIM M AIM Messaging, Incoming
  218 7.017184   205.188.8.72    142.58.65.101   AIM M AIM Messaging, Mini Typing Notifications (MTN)
  304 8.319907   205.188.8.72    142.58.65.101   AIM M AIM Messaging, Mini Typing Notifications (MTN)
 1027 10.60934   205.188.8.72    142.58.65.101   AIM M AIM Messaging, Mini Typing Notifications (MTN)
 2497 15.26592   205.188.8.72    142.58.65.101   AIM B Oncoming Buddy: [redacted]
 7753 25.96129   205.188.8.72    142.58.65.101   AIM M AIM Messaging, Mini Typing Notifications (MTN)
 7805 26.38722   142.58.65.101   205.188.8.72    AIM M AIM Messaging, Mini Typing Notifications (MTN)
 7806 26.39026   142.58.65.101   205.188.8.72    AIM M [TCP Retransmission] AIM Messaging, Mini Typing Notifications (MTN)
 7807 26.39205   142.58.65.101   205.188.8.72    AIM M [TCP Retransmission] AIM Messaging, Mini Typing Notifications (MTN)
 7810 26.39676   142.58.65.101   205.188.8.72    AIM M [TCP Retransmission] AIM Messaging, Mini Typing Notifications (MTN)
 9079 32.51123   142.58.65.101   205.188.8.72    AIM M AIM Messaging, Mini Typing Notifications (MTN)
 9093 32.58397   142.58.65.101   205.188.8.72    AIM M AIM Messaging, Outgoing to: [redacted]
 9909 32.66820   205.188.8.72    142.58.65.101   AIM M AIM Messaging, Acknowledge
14810 49.54071   205.188.8.72    142.58.65.101   AIM B Oncoming Buddy: [redacted]
14837 50.54115   205.188.8.72    142.58.65.101   AIM B [TCP Out-Of-Order] Oncoming Buddy: [redacted]
15397 68.61882   205.188.8.72    142.58.65.101   AIM M AIM Messaging, Incoming
15488 68.84594   205.188.8.72    142.58.65.101   AIM M AIM Messaging, Mini Typing Notifications (MTN)
17079 75.33175   205.188.8.72    142.58.65.101   AIM B Oncoming Buddy: [redacted]
```

```
        Features: 0x0501
        Features Length: 2
        Features: 0106
        Block info: 0x0101
        Block length: 63
        Block Character set: 0x0000
        Block Character subset: 0x0000
        Message: he said that, [redacted]
  ▽ TLV: Non-direct connect typing notification
      Value ID: Non-direct connect typing notification (0x000b)
      Length: 0
      Value
```

```
0000  08 02 d5 00 00 09 5b 23  55 4e 00 e0 63 82 73 dc   .......[# UN..c.s.
0010  00 05 5d 5e 89 dc e0 cb  aa aa 03 00 00 00 08 00   ..]^.... ........
0020  45 00 00 be 5d 44 40 00  67 06 10 52 cd bc 08 48   E...]D@. g..R...H
0030  8e 3a 41 65 14 46 04 0d  ae bc b8 cd a9 03 8a b4   .:Ae.F.. ........
0040  50 18 40 00 18 42 00 00  2a 02 2d 61 00 90 00 04   P.@..B.. *.-a....
```

File: wlanicqpopsmtp1.cap 5437 KB   P: 17782 D: 19 M: 0

Ethereal captures from 2nd laptop: Yahoo mail

```
GET
    /config/login?.tries=1&.src=www&.md5=&.hash=&.js=1&.last=&promo=&.intl=us&.bypass=&.partner=&.u=1spon6t127e88&.v=0&.challenge=9gMkEIGtJaAhGmqnTlT_Rmp2KfNW&.yplus=&.emailCode=&pkg=&stepid=&.ev=&hasMsgr=0&.chkP=Y&.done=http%3A//www.yahoo.com&login=wlangap&passwd=d161f26c355df6ae13ba0ff8f82d4f0a&.persistent=&.save=1&.hash=1&.md5=1 HTTP/1.1

Host: login.yahoo.com
...
```

The password is protected with an md5 hash

Ethereal captures from 2nd laptop: Excite mail

```
POST /excitereg/login_process.jsp HTTP/1.1

Host: registration.excite.com
...
Referer: http://registration.excite.com/excitereg/login.jsp
...
snonce=FmX0EuFFsgEH1OEdvSBMAw%3D%3D&stime=4223b948&timeskew=13&crep=OeSHuHThQr9nmg%3D%3D&jerror=none&membername=wlangap&password=xxxxxxx&gofer=Sign+In%21&perm=0
HTTP/1.1 302 Found

Date: Tue, 01 Mar 2005 00:37:49 GMT

Server: Apache/1.3.29 (Unix) Resin/2.0.5 mod_ssl/2.8.16 OpenSSL/0.9.7c
```

Password is encrypted: note that it shows the password is 7-letters long

Ethereal captures from 2nd laptop: POP3 mail

```
+OK Qpopper (version 4.0.5) at rm-rstar.sfu.ca starting.
...
X-LOCALTIME Mon, 28 Feb 2005 17:31:05 -0800

IMPLEMENTATION Qpopper-version-4.0.5
...

USER somebody (name replaced)

+OK Password required for somebody.

PASS abcdef (visible password replaced)

+OK somebody has 583 visible messages (0 hidden) in 27739618 octets.
```

Ethereal captures from 2nd laptop: SMTP mail

```
220 rm-rstar.sfu.ca ESMTP Sendmail 8.12.10/8.12.5/SFU-5.0H; Mon, 28 Feb 2005 17:32:16 -
      0800 (PST)
...
MAIL FROM:<somebody@sfu.ca> SIZE=374 (name replaced with somebody)
...
Message-ID: <4223C632.6050605@sfu.ca>
Date: Mon, 28 Feb 2005 17:32:34 -0800
From: Somebody <somebody@sfu.ca>
User-Agent: Mozilla Thunderbird 1.0 (Windows/20041206)
X-Accept-Language: en-us, en
MIME-Version: 1.0
To:  somebody@sfu.ca
Subject: smtptest
Content-Type: text/plain; charset=ISO-8859-1; format=flowed
Content-Transfer-Encoding: 7bit
testing smtp messages
250 2.0.0 j211WGCk006855 Message accepted for delivery
QUIT
221 2.0.0 rm-rstar.sfu.ca closing connection
```

Experimental results

- User privacy is not preserved because traffic is not encrypted
- Email services such as Yahoo and Excite encrypt passwords but received email contents and sent email messages are in plain text
- Captured user's data and passwords appear as plain text if simple browsers are used:
  - Netfront 3.1 for PalmOS

Experimental results

- Instant Messaging (IM) messages such as MSN or ICQ are captured in plain text
- POP3 and SMTP messages are sent in plain text by default:
  - SSL and TLS options are available but are hidden from view
  - access providers do not always provide encrypted email transfers

Experimental results

- Windows NetBIOS services automatically broadcast workgroup and ID to network:
  - windows shared folders could be accessed by others in the network

Vulnerability prevention

- Is WLAN traffic encryption possible?
- Only if access providers choose to provide it:
  - may require newer equipment
  - difficulty in setup results in increased support calls
  - degradation of WLAN performance
  - Not the access provider’s problem:
    - “We strongly recommend that our customers be aware of the security concerns of wireless networking and ensure the security of their Internet connections... It is your responsibility to adopt security measures which are best suited to your situation.”

Vulnerability prevention

- Is WLAN traffic encryption possible?
  - WEP is supported by all 802.11 devices:
    - anyone with the WEP key can decode traffic:
    - WEP usage is not useful in public networks
    - WEP is also vulnerable to cryptography attacks [2]
  - WPA uses temporal keys: not all 802.11 devices support this encryption type

[2] S. Fluhrer, I. Mantin, and A. Shamir, “Weakness in the key scheduling algorithm in RC4,” *Lecture Notes in Computer Science*, vol. 2259, pp. 1-24, 2001.

Vulnerability prevention

- End-to-end encryption protocols prevent data shown in plain text:
  - HTTP or HTTPS with SSL
  - POP3 and SMTP with SSL/TLS
  - encrypted terminal access using SSH
  - VNC using cryptographic APIs
  - virtual private networks (VPN)

Network security

- Testing network security requires both providers' and users' consent
- We analyzed Vernier Network's white paper for deployment setup
- Focus of our analysis was to examine if the SFU network is secure

“Evil twin” attacks

- “Evil twin” is a rogue access point using identical Service Set Identifier (SSID) as the WLAN provider [3]
- If the provider network such as SFU employs authentication, a redirection server using an identical login page could be used in an attack:
  - poses as the access provider’s authentication sequence
  - login page captures the access provider’s user logins and other logins and passwords

[3] C. Klaus, “Wireless LAN Security FAQ,” Internet Security Systems, Oct 6th, 2002 [Online]. Available: http://www.iss.net/wireless/WLAN_FAQ.php.

“Evil twin” attacks

- Aside from security audits, no known detection method for “evil twin” exists
- Users may be able to detect rogue access points after login by examining the IP address given by the access point
- Users cannot detect rogue access points prior to access:
  - security professionals at the RSA security conference in Feb, 2005 had their logins compromised [5]

[5] Press Release “AirDefense Monitors Wireless Airwaves at RSA 2005 Conference,” Feb 17th, 2005 [Online]. Available: http://airdefense.net/newsandpress/02_07_05.shtm.

“Evil twin” attacks

- From access provider perspective:
  - “Evil twin” attacks compromise user credentials
  - may compromise network security if other services are provided besides Internet access
  - thanks to monitoring, attackers may be unable to use the network for malicious means or to spread viruses and worms

Conclusion

- Public WLAN networks may be convenient to use but are insecure from a user's perspective
- Privacy concerns may be partially mitigated by using encrypted protocols
- Future WLAN protocols may provide required level of user privacy

References

[1] Vernier Networks, "Network access management: stopping intruders and worms before they get on the network" (white paper) [Online]. Available: http://www.verniernetworks.com/library/pdfs/wp_stopping_intruders_and_worms.pdf.

[2] S. Fluhrer, I. Mantin, and A. Shamir, "Weakness in the key scheduling algorithm in RC4," *Lecture Notes in Computer Science*, vol. 2259, pp. 1-24, 2001.

[3] C. Klaus, "Wireless LAN Security FAQ," Internet Security Systems, Oct. 6th, 2002 [Online]. Available: http://www.iss.net/wireless/WLAN_FAQ.php.

[4] Ethereal [Online]. Available: http://www.ethereal.com.

[5] AirDefense "AirDefense Monitors Wireless Airwaves at RSA 2005 Conference," (press release), Feb. 17th, 2005 [Online]. Available: http://airdefense.net/newsandpress/02_07_05.shtm.