



The Art of Wireless War

KCCMG Impact Conference  
Fall 2004

"The general who wins a battle makes many calculations in his temple before the battle is fought." Sun Tzu, *The Art of War*

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle." Sun Tzu, *The Art of War*



## Wireless LAN Usage Is Growing

---

*"The percentage of companies spending more than \$10,000 annually [on WLAN deployments] will grow from 26 percent in 2003 to 35 percent in 2004."*

Julie Ask, Jupiter Research

*Although 84 percent of companies have not had their WLAN breached, "security is the top barrier, cited by nearly half of all companies" as the reason they are not deploying or expanding Wi-Fi networks.*

*Understanding Corporate WLAN Architecture Choices, Jupitermedia*

802.11a	5GHz OFDM PHY
802.11b	2.4GHz CCK PHY
802.11c	802.11 bridging
802.11d	International roaming
802.11e	QoS/efficiency enhancements
802.11F	Inter AP protocol
802.11g	2.4GHz OFDM PHY
802.11h	5GHz regulatory extensions
802.11i	Security enhancements
802.11j	Japan 5GHz band extensions
802.11k	Radio resource measurement
802.11l	Skipped (typographically unsound)
802.11m	Maintenance
802.11n	High throughput PHY

# Typical WLAN Configuration

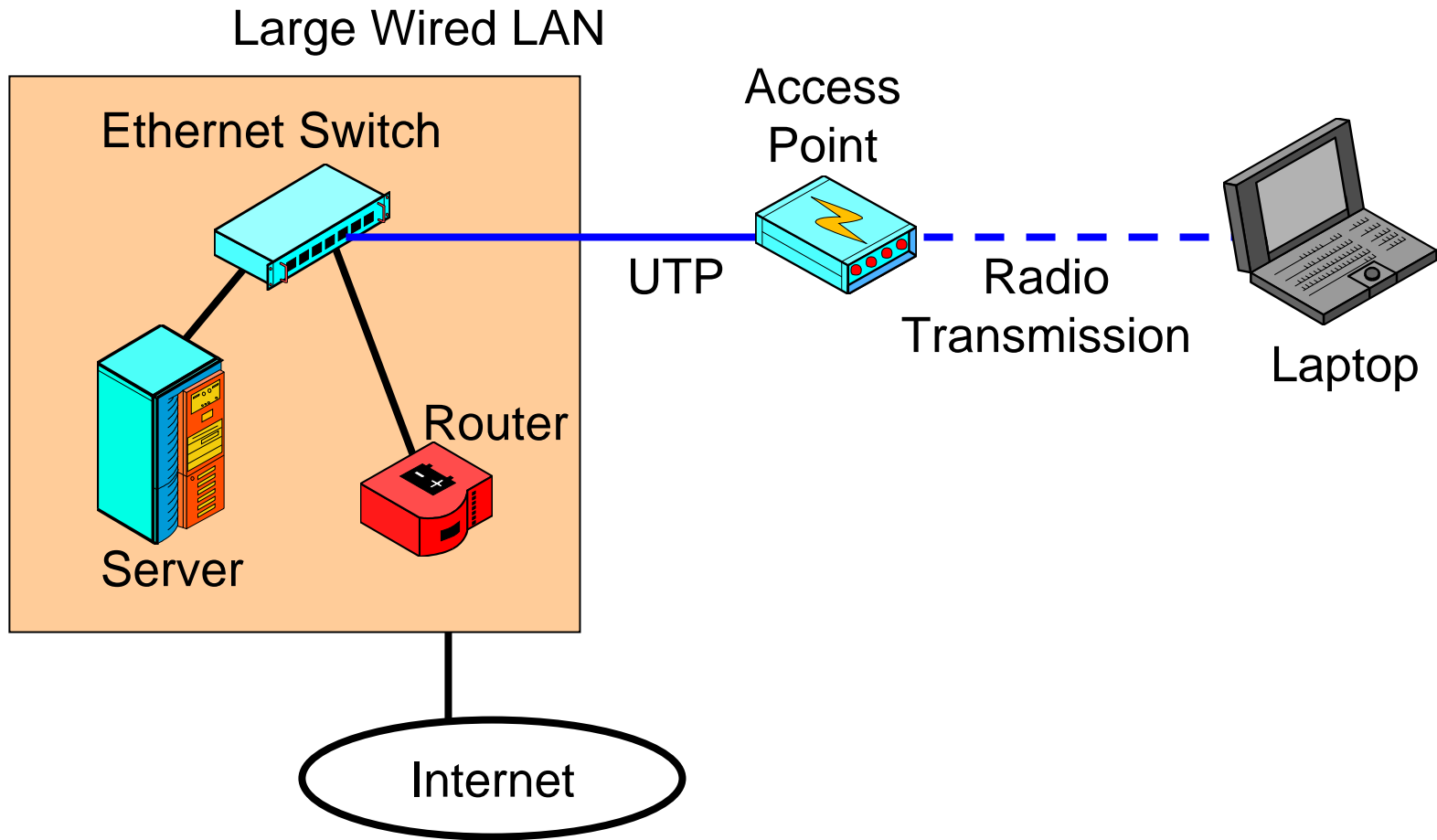


Diagram Courtesy of Intel Corp.

- Drive-By Insecurity
  - Traffic captured from outside the enterprise
  - Traffic “injected” into the enterprise

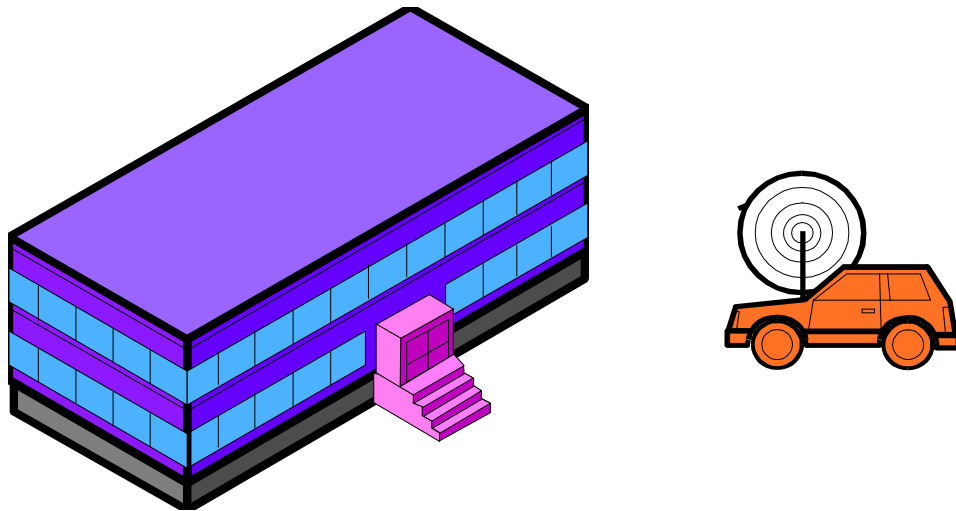


Diagram Courtesy of Intel Corp.

- **Wired Equivalent Privacy (WEP)**
  - **Initial security method for 802.11 devices**
  - **All stations share the same encryption key with the access point**
  - **This key is rarely changed**
  - **Shared static keys means that a large volume of traffic is encrypted with the same key**
  - **With so much traffic generated with one unchanging key, cryptanalysts were able to crack the key by collecting data for a few days**

- **Who**

- **Thrill Seekers - Access Thieves**
- **Identity Thieves**
- **Data Thieves**

- **How / Equipment**
  - **Laptop / PDA**
  - **Wireless card + Antenna**
  - **OS (sometimes Windows, usually Linux)**
  - **Software Tools**
    - **Netstumbler**
    - **Ethereal**
    - **WEPCrack**

Aerosol	<a href="http://www.stolenshoes.net/sniph/aerosol.html">http://www.stolenshoes.net/sniph/aerosol.html</a>
Airfart	<a href="http://airfart.sourceforge.net/">http://airfart.sourceforge.net/</a>
AirJack	<a href="http://802.11ninja.net/airjack/">http://802.11ninja.net/airjack/</a>
Airscanner Mobile Sniffer	<a href="http://www.airscanner.com/downloads/sniffer/sniffer.html">http://www.airscanner.com/downloads/sniffer/sniffer.html</a>
AirSnarf	<a href="http://airsnarf.shmoo.com/">http://airsnarf.shmoo.com/</a>
AirSnort	<a href="http://airsnort.shmoo.com/">http://airsnort.shmoo.com/</a>
AirTraf	<a href="http://www.elixar.com/corporate/history/airtraf-1.0/">http://www.elixar.com/corporate/history/airtraf-1.0/</a>
anwrap	<a href="http://www.securiteam.com/tools/6O00P2060I.html">http://www.securiteam.com/tools/6O00P2060I.html</a>
AP Hopper	<a href="http://aphopper.sourceforge.net/">http://aphopper.sourceforge.net/</a>
AP Radar	<a href="http://apradar.sourceforge.net/">http://apradar.sourceforge.net/</a>
APHunter	<a href="http://www.math.ucla.edu/%7Ejimc/mathnet_d/download.html">http://www.math.ucla.edu/%7Ejimc/mathnet_d/download.html</a>
APSniff	<a href="http://www.bretmounet.com/ApSniff/">http://www.bretmounet.com/ApSniff/</a>
APTtools	<a href="http://winfingerprint.sourceforge.net/aptools.php">http://winfingerprint.sourceforge.net/aptools.php</a>
Asleap	<a href="http://asleap.sourceforge.net/">http://asleap.sourceforge.net/</a>
BSD-AirTools	<a href="http://www.dachb0den.com/projects/bsd-airtools.html">http://www.dachb0den.com/projects/bsd-airtools.html</a>
ClassicStumbler	<a href="http://homepage.mac.com/alk/classicstumbler.html">http://homepage.mac.com/alk/classicstumbler.html</a>
DMZS-Card	<a href="http://www.dmzs.com/tools/files/wireless.phtml">http://www.dmzs.com/tools/files/wireless.phtml</a>
dstumbler	<a href="http://www.dachb0den.com/projects/dstumbler.html">http://www.dachb0den.com/projects/dstumbler.html</a>
dweputils	<a href="http://www.dachb0den.com/projects/dweputils.html">http://www.dachb0den.com/projects/dweputils.html</a>
Ethereal	<a href="http://www.ethereal.com/">http://www.ethereal.com/</a>

FakeAP	<a href="http://www.blackalchemy.to/project/fakeap/">http://www.blackalchemy.to/project/fakeap/</a>
gpsd	<a href="http://freshmeat.net/projects/gpsd/">http://freshmeat.net/projects/gpsd/</a>
Hotspotter	<a href="http://www.remote-exploit.org/codes.html">http://www.remote-exploit.org/codes.html</a>
iStumbler	<a href="http://www.istumbler.net/">http://www.istumbler.net/</a>
KisMAC	<a href="http://www.binaervarianz.de/projekte/programmieren/kismac/">http://www.binaervarianz.de/projekte/programmieren/kismac/</a>
Kismet	<a href="http://www.kismetwireless.net/">http://www.kismetwireless.net/</a>
LibRadiate	<a href="http://www.packetfactory.net/projects/libradiate/">http://www.packetfactory.net/projects/libradiate/</a>
LibWnet	<a href="http://www.dachb0den.com/users/h1kari/work/.0-day/bat/">http://www.dachb0den.com/users/h1kari/work/.0-day/bat/</a>
Lucent/Orinoco Registry Encr./Decr.	<a href="http://www.cqure.net/tools.jsp?id=3">http://www.cqure.net/tools.jsp?id=3</a>
MacStumbler	<a href="http://www.macstumbler.com/">http://www.macstumbler.com/</a>
MiniStumbler	<a href="http://www.netstumbler.com/download.php?op=viewdownload&amp;cid=1">http://www.netstumbler.com/download.php?op=viewdownload&amp;cid=1</a>
Mognet	<a href="http://www.node99.org/projects/mognet/">http://www.node99.org/projects/mognet/</a>
NetChaser	<a href="http://www.bitsnbolts.com/netchaser.html">http://www.bitsnbolts.com/netchaser.html</a>
NetStumbler	<a href="http://www.netstumbler.com/download.php?op=viewdownload&amp;cid=1">http://www.netstumbler.com/download.php?op=viewdownload&amp;cid=1</a>
PocketWarrior	<a href="http://www.pocketwarrior.org/">http://www.pocketwarrior.org/</a> //Pong
PrismStumbler	<a href="http://prismstumbler.sourceforge.net/">http://prismstumbler.sourceforge.net/</a>
SSIDsniff	<a href="http://www.bastard.net/%7Ekos/wifi/">http://www.bastard.net/%7Ekos/wifi/</a>
StumVerter	<a href="http://www.sonar-security.com/">http://www.sonar-security.com/</a> //THC-LEAPcracker
void11	<a href="http://www.wlsec.net/void11/">http://www.wlsec.net/void11/</a>
WarGlue	<a href="http://sourceforge.net/projects/warglue">http://sourceforge.net/projects/warglue</a>

WarLinux	<a href="http://sourceforge.net/projects/warlinux/">http://sourceforge.net/projects/warlinux/</a>
Wavelan Tools	<a href="http://sourceforge.net/projects/wavelan-tools/">http://sourceforge.net/projects/wavelan-tools/</a>
WaveMon	<a href="http://freshmeat.net/projects/wavemon/">http://freshmeat.net/projects/wavemon/</a>
WaveStumbler	<a href="http://www.cqure.net/tools.jsp?id=08">http://www.cqure.net/tools.jsp?id=08</a>
WellenReiter	<a href="http://www.wellenreiter.net/ //WepAttack">http://www.wellenreiter.net/ //WepAttack</a>
WEPCrack	<a href="http://sourceforge.net/projects/wepcrack/">http://sourceforge.net/projects/wepcrack/</a>
Weplab	<a href="http://sourceforge.net/projects/weplab">http://sourceforge.net/projects/weplab</a>
WEPWedgie	<a href="http://sourceforge.net/projects/wepwedgie/">http://sourceforge.net/projects/wepwedgie/</a>
WEP_Tools (wep_crack/wep_decrypt)	<a href="http://www.lava.net/%7Enewsham/wlan/wep_tools.tgz">http://www.lava.net/%7Enewsham/wlan/wep_tools.tgz</a>
Wi-Find	<a href="http://evvl.rustedhalo.net/projects/wi-find/">http://evvl.rustedhalo.net/projects/wi-find/</a>
WifiScanner	<a href="http://wifiscanner.sourceforge.net/">http://wifiscanner.sourceforge.net/</a>
WinDump	<a href="http://windump.polito.it/">http://windump.polito.it/</a>
WiStumbler	<a href="http://www.gongon.com/persons/iseki/wistumbler/index.html">http://www.gongon.com/persons/iseki/wistumbler/index.html</a>
wscan	<a href="http://www.cs.pdx.edu/research/SMN/">http://www.cs.pdx.edu/research/SMN/</a>

The screenshot shows the 'Network Stumbler' application window titled 'Aspen\_Hills.ns1'. The interface includes a menu bar (File, Edit, View, Device, Window, Help) and a toolbar with various icons. The main area is divided into a left sidebar and a central table.

**Left Sidebar (Aspen\_Hills.ns1):**

- Channels
  - 6
  - 10
  - 11
- SSIDs
  - 2wIRE269
  - darnellhouse
  - default
  - joshnet
  - linksys
  - thieswlan
- Filters
  - Encryption Off
  - Encryption On
  - ESS (AP)
  - IBSS (Peer)
  - CF Pollable
  - Short Preamble
  - PBCC
  - Short Slot Time (11g)
  - Default SSID

**Central Table:**

MAC	SSID	Name	Chan	Speed	Vendor
000D88ECE376	default		6	54 Mbps	D-Link
000C41A4066C	Linksys		6	54 Mbps	Linksys
000124F2C964	darnellhouse		6	11 Mbps	Acer
00062564851A	linksys		6	11 Mbps	Linksys
0006258FBB43	linksys		10	11 Mbps	Linksys
000F3D4AFD04	joshnet		11	54 Mbps	
00D09EE30D71	2wIRE269		6	22 Mbps	2Wire
000F663893C4	linksys		6	54 Mbps	Linksys
000625A0EFB2	linksys		6	11 Mbps	Linksys
00062597827E	thieswlan		6	11 Mbps	Linksys

**Status Bar:** Ready | Not scanning | GPS: Disabled | 10 / 10

- **802.11i Security**
  - **802.11 Working Group introduced strong security**
    - **802.11i**
  - **Temporal Key Integrity Protocol (TKIP)**
    - **Each station gets a separate key for confidentiality**
    - **This key is changed frequently**

- **802.11i Security**
  - Products started becoming available in late 2003
- **Wireless Protected Access (WPA)**
  - Stopgap security method introduced before full 802.11i security could be developed
  - Introduced some parts of 802.11i in 2002 and 2003

- Locate the Router or Access Point Appropriately
- Change Default Administrator Passwords
- Change the Default SSID
- Disable SSID Broadcast
- Turn on Encryption
- Enable MAC Address Filtering
- Assign Static IP Addresses to Devices