What Hackers Know that you Don’t Know

Garry Drummond, CISSP, CWNA, CWSP,

Wireless Security Specialist - Motorola Solutions

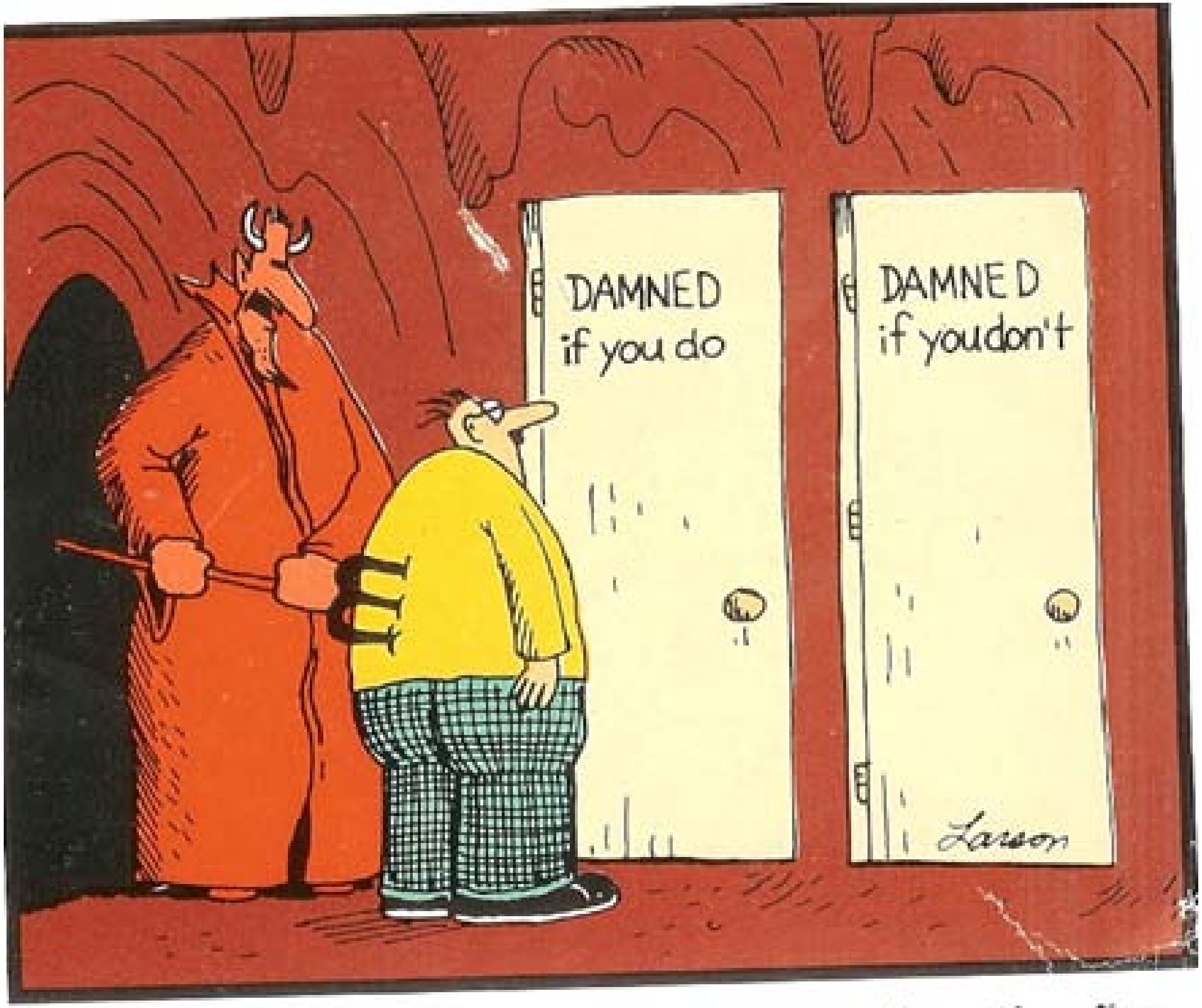
Wireless Hacking and

Hands On Workshop - Session D3

Agenda

- Overview Wireless Risk and Threats
- Live Exploit Demonstration (captive portals, phishing attacks, advanced tethered rogues)
- Mobile Platform Exploits (Smartphone attacks, IPad and Tablet attacks)
- Live Security Countermeasures and Containment – Air Termination
- Forensics Investigations
- Rogue Detection
- Technical Deep-dive of AirDefense Platform
- Hands on with Student - Security / Troubleshooting
- BackTrack - Training / Configurations

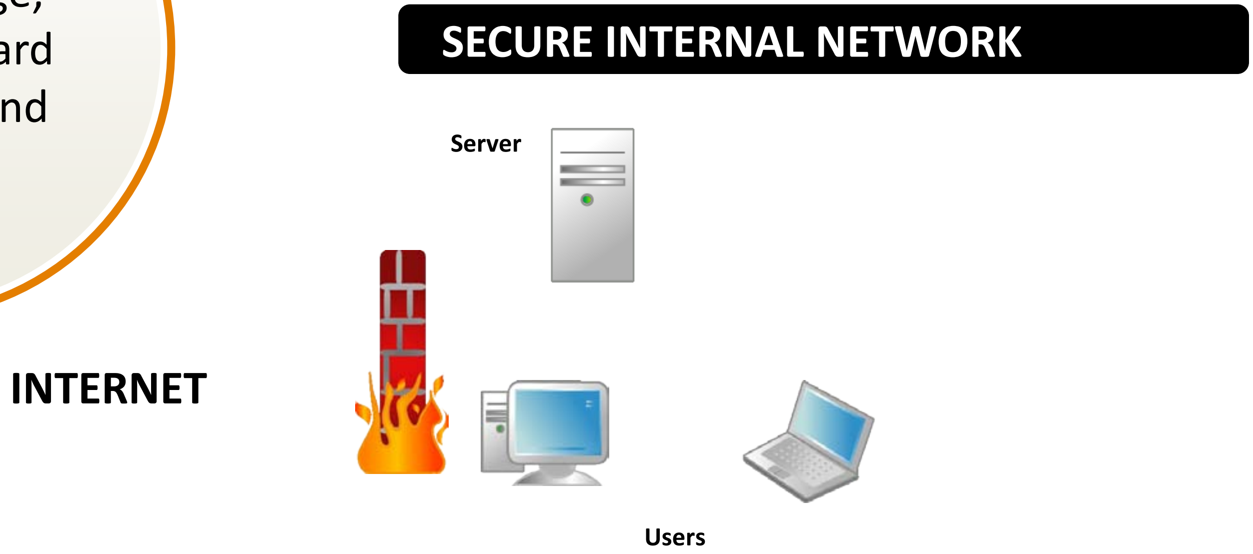
Get Ready for the Untethered World!



"C'mon, c'mon — It's either one or the other."

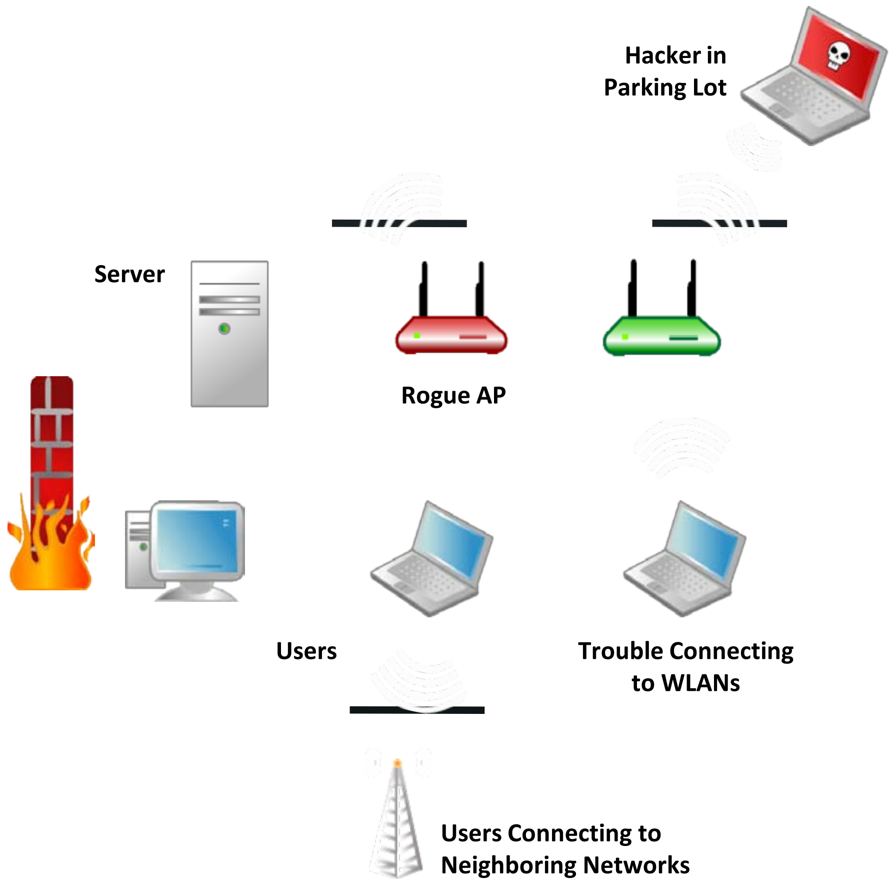
Traditional Wired Network

Well-Defined Network Edge, Straightforward to Manage and Secure

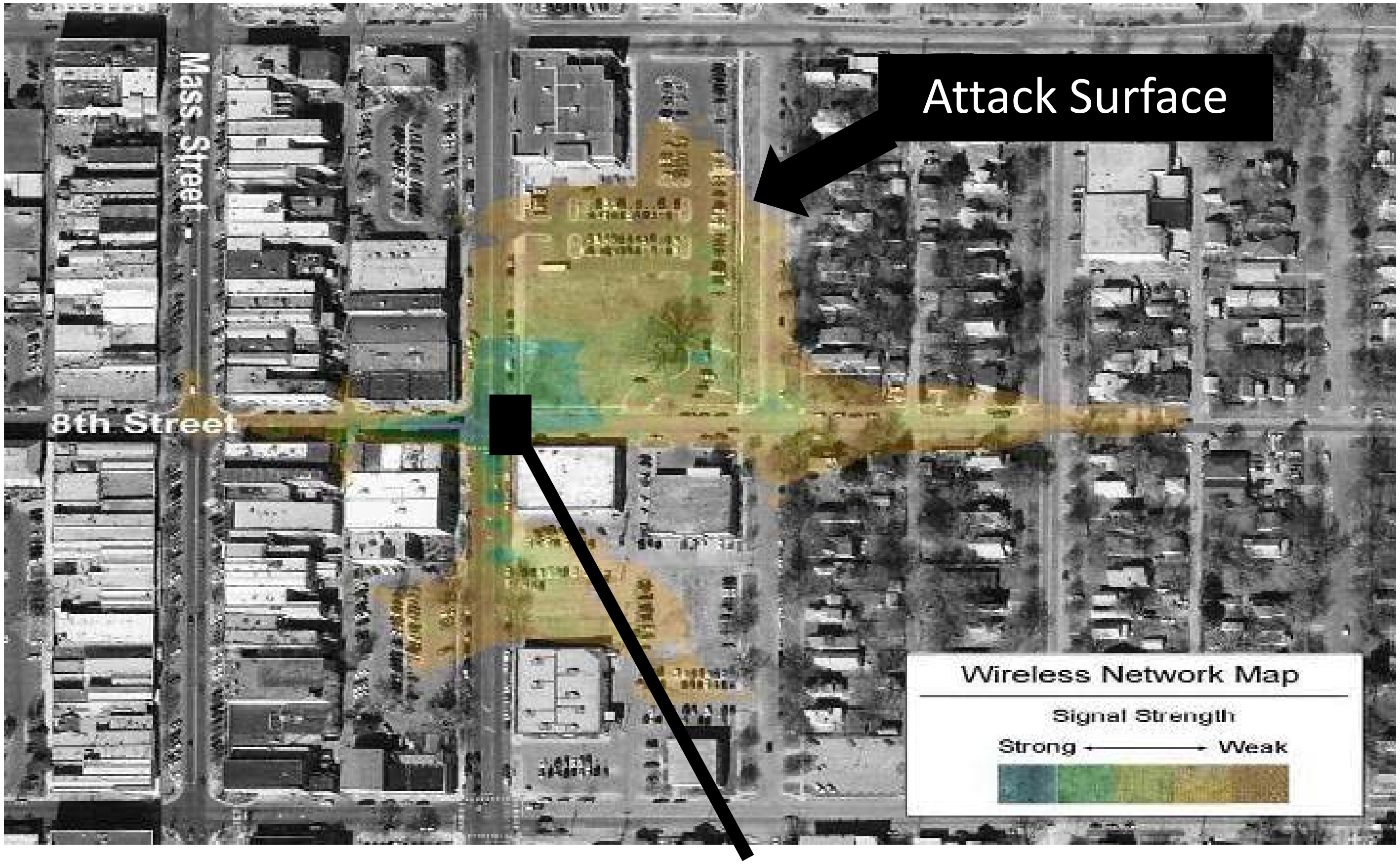


Wireless Changes Everything

Network Edge Blurred, New Attack Vectors ‘Behind’ the Firewall


INTERNET
Hacker in Parking Lot
Server
Rogue AP
Users
Trouble Connecting to WLANs
Users Connecting to Neighboring Networks

Wireless Propagation is Hard to Control



Attack Surface

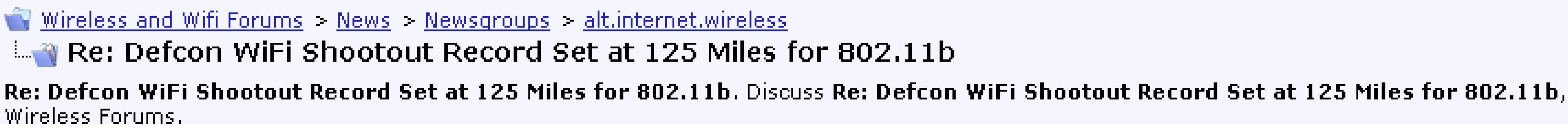
Wireless Increases the attack surface dramatically

High Gain Antennas Increase Range

Pringles Can

Yagi Antenna

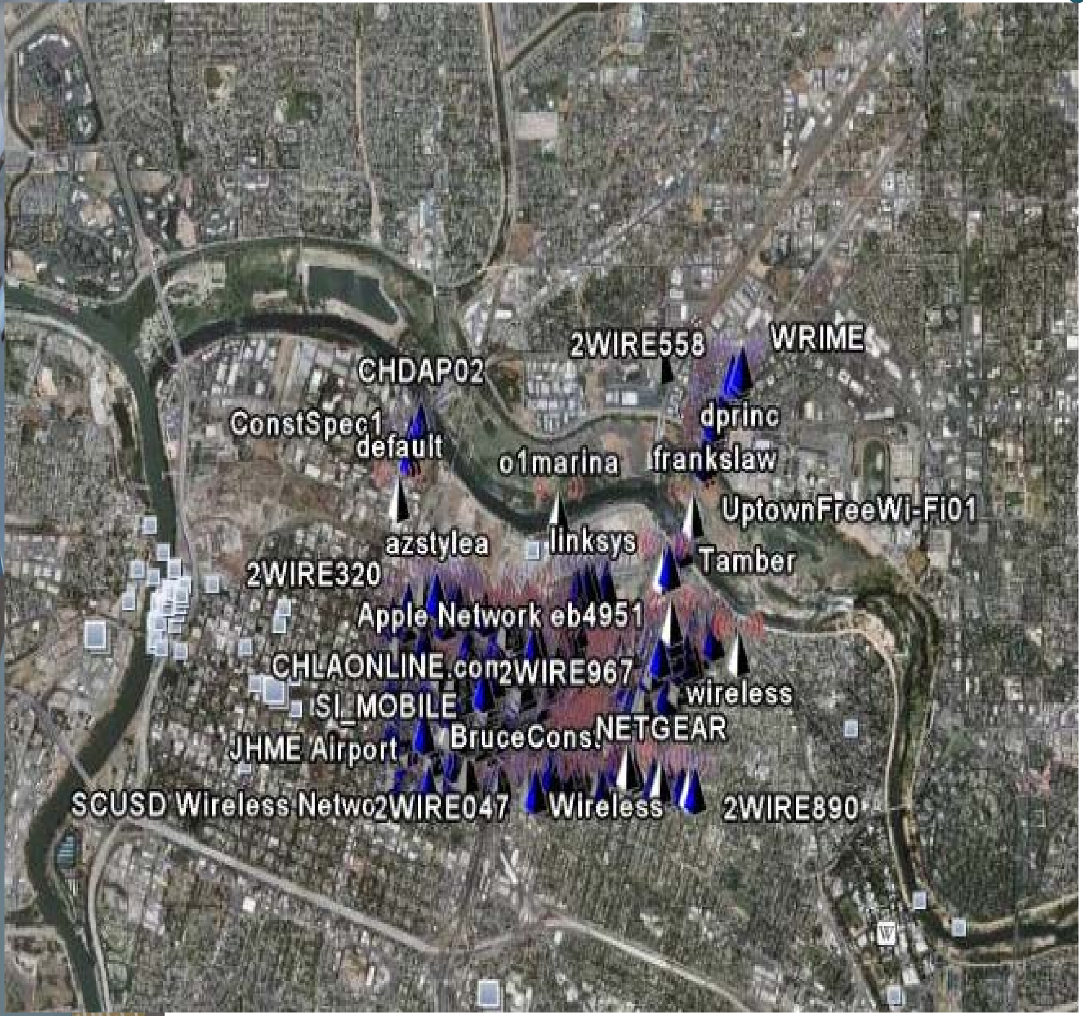
Yagi Sniper Antenna (we're not kidding)


Wireless and Wifi Forums > News > Newsgroups > alt.internet.wireless

Re: Defcon WiFi Shootout Record Set at 125 Miles for 802.11b

Re: Defcon WiFi Shootout Record Set at 125 Miles for 802.11b. Discuss **Re: Defcon WiFi Shootout Record Set at 125 Miles for 802.11b**, Wireless Forums.

What Hackers Already Know About You



Documented Wireless Networks
In the Sacramento Area

- Online hacker reference database with maps
  - Documents SSID, encryption, MAC address, location on a map
  - 14M+ wireless networks documented
  - Searchable by any variable
  - Enter your own address at www.wigle.net

Why Hack Wireless Networks?

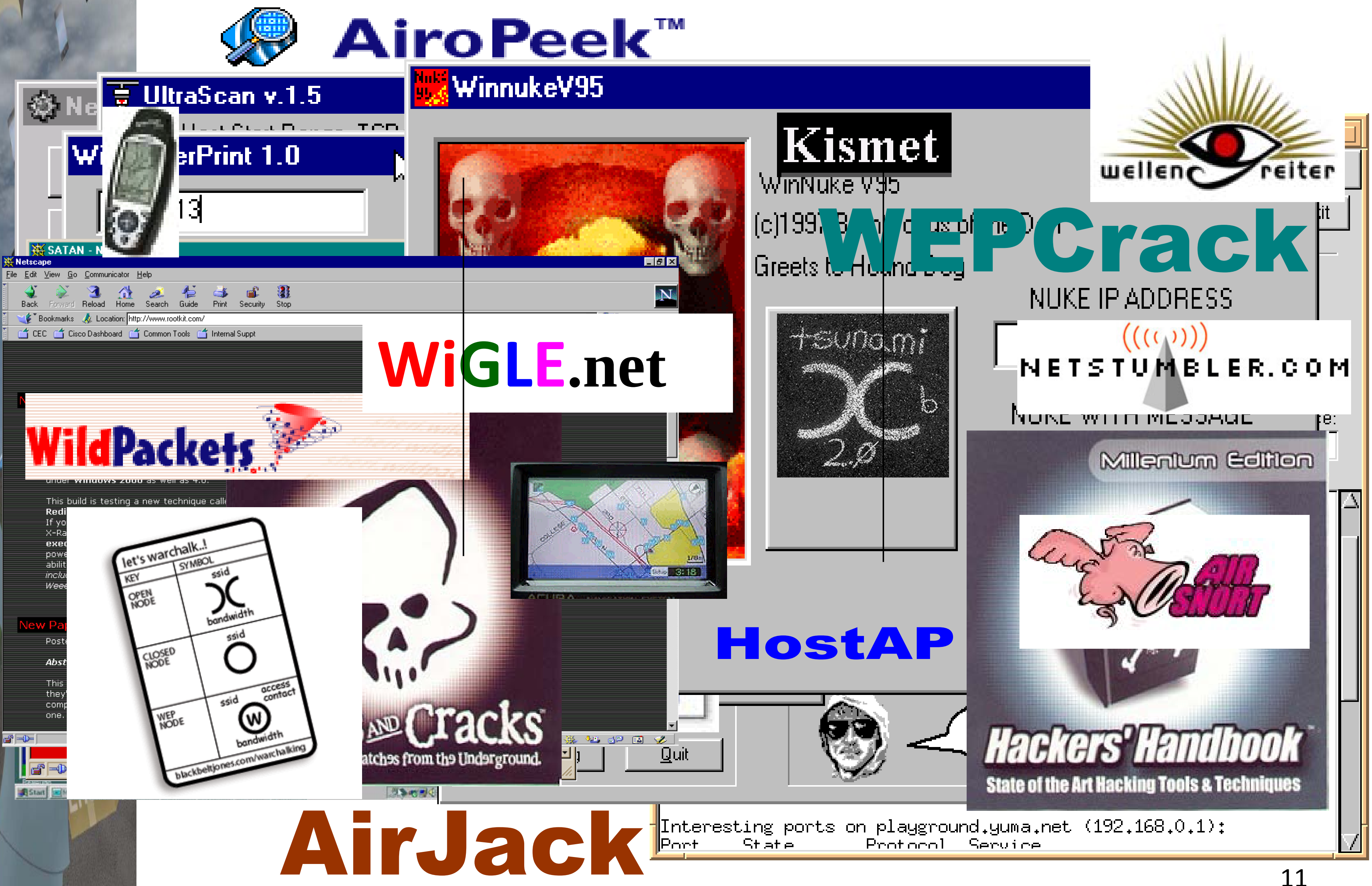
- Attacks bypass traditional security controls
- Complete anonymity
  - No risk of being traced
  - Wireless not being watched
- Tools abundant, cheap & easy to use
- Mobility adds capability & cover
- Huge attack surface

Firewall Myths

Firewalls:

- Cannot stop rogue wireless devices
- Do not eliminate the need for wireless scanning for rogues
- Do not protect against wireless attacks
- Once a hacker is on the network they can punch through open ports
- Access Control Lists are weaker than Firewalls
- Best bet is to keep hackers off the network

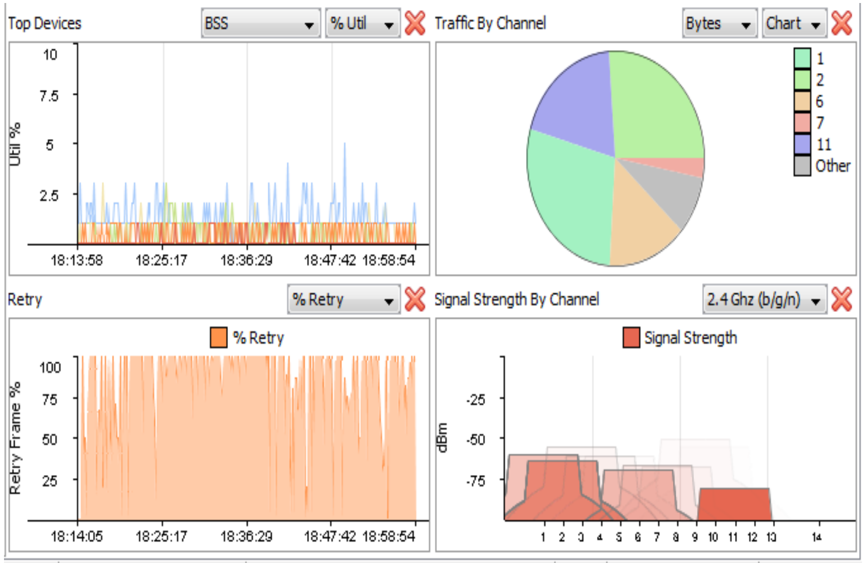
Tools are Abundant



```
Interesting ports on playground.yuma.net (192.168.0.1):
Port       State       Protocol   Service
```

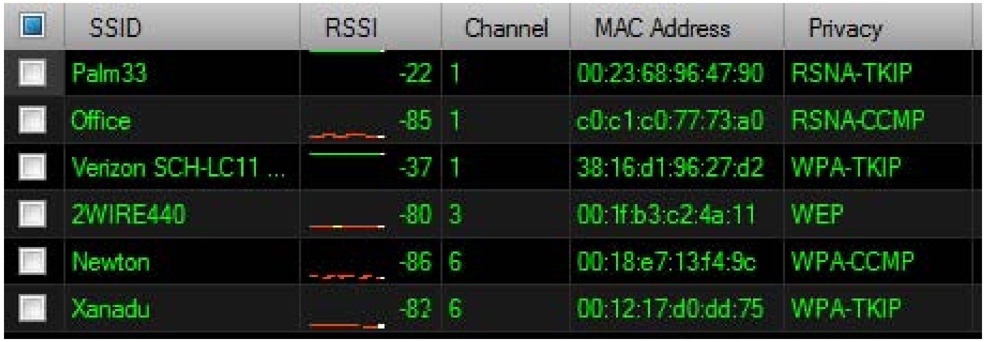
Step1 - Recon

Airodump-ng



AirDefense Mobile

Open Source WiFi Finder



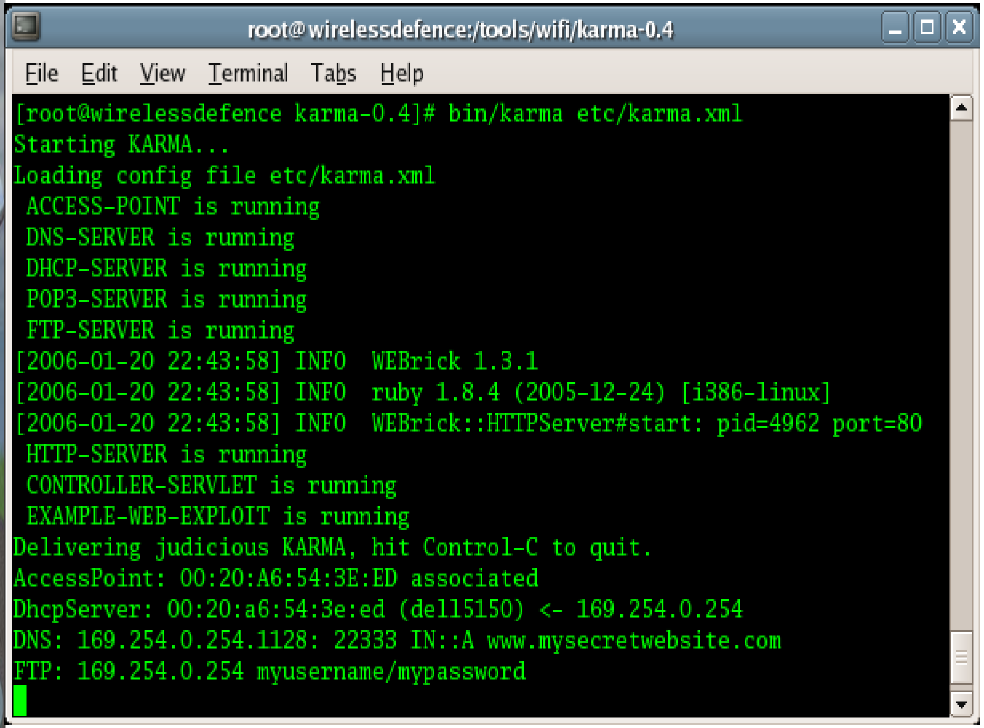
☐	SSID	RSSI	Channel	MAC Address	Privacy
☐	Palm33	-22	1	00:23:68:96:47:90	RSNA-TKIP
☐	Office	-85	1	c0:c1:c0:77:73:a0	RSNA-CCMP
☐	Verizon SCH-LC11 ...	-37	1	38:16:d1:96:27:d2	WPA-TKIP
☐	2WIRE440	-80	3	00:1f:b3:c2:4a:11	WEP
☐	Newton	-86	6	00:18:e7:13:f4:9c	WPA-CCMP
☐	Xanadu	-82	6	00:12:17:d0:dd:75	WPA-TKIP

Wi-Spy

Step 2 – Pick your hack

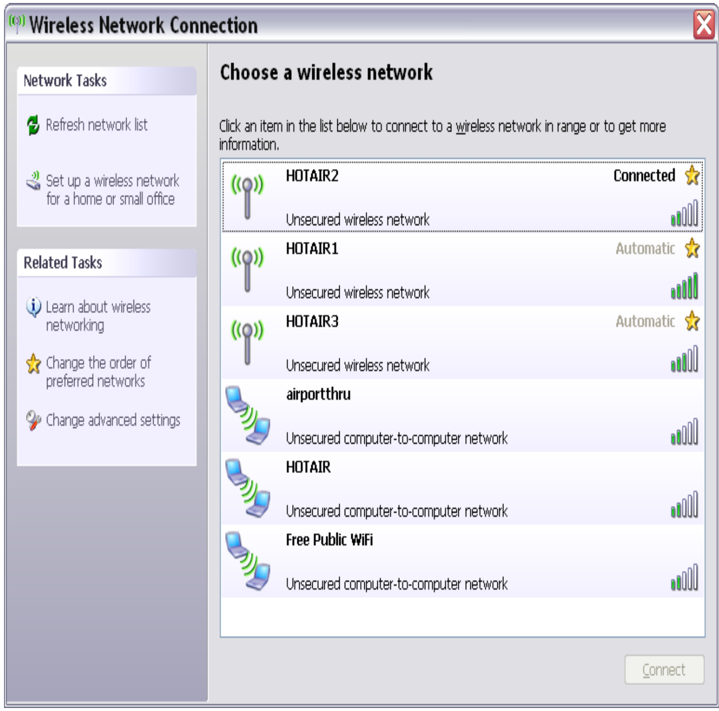
- Catch and Release (SSL Strip)
- PEAP Man-In-The –Middle / Fake RADIUS
- Captive Portal Metasploit
  - Java App exploit
- Captive Portal
  - Snatch and Grab User Name / Password
  - Catch and Release (Fire sheep)
- Recon / Eavesdropping Tools

Windows Zero Config Exploit



root@wirelessdefence:/tools/wifi/karma-0.4

```
[root@wirelessdefence karma-0.4]# bin/karma etc/karma.xml
Starting KARMA...
Loading config file etc/karma.xml
 ACCESS-POINT is running
 DNS-SERVER is running
 DHCP-SERVER is running
 POP3-SERVER is running
 FTP-SERVER is running
[2006-01-20 22:43:58] INFO  WEBrick 1.3.1
[2006-01-20 22:43:58] INFO  ruby 1.8.4 (2005-12-24) [i386-linux]
[2006-01-20 22:43:58] INFO  WEBrick::HTTPServer#start: pid=4962 port=80
 HTTP-SERVER is running
 CONTROLLER-SERVLET is running
 EXAMPLE-WEB-EXPLOIT is running
Delivering judicious KARMA, hit Control-C to quit.
AccessPoint: 00:20:A6:54:3E:ED associated
DhcpServer: 00:20:a6:54:3e:ed (dell5150) <- 169.254.0.254
DNS: 169.254.0.254.1128: 22333 IN::A www.mysecretwebsite.com
FTP: 169.254.0.254 myusername/mypassword
```



Wireless Network Connection

Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Connect

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

HOTAIR2 — Connected ☆ — Unsecured wireless network

HOTAIR1 — Automatic ☆ — Unsecured wireless network

HOTAIR3 — Automatic ☆ — Unsecured wireless network

airportthru — Unsecured computer-to-computer network

HOTAIR — Unsecured computer-to-computer network

Free Public WiFi — Unsecured computer-to-computer network

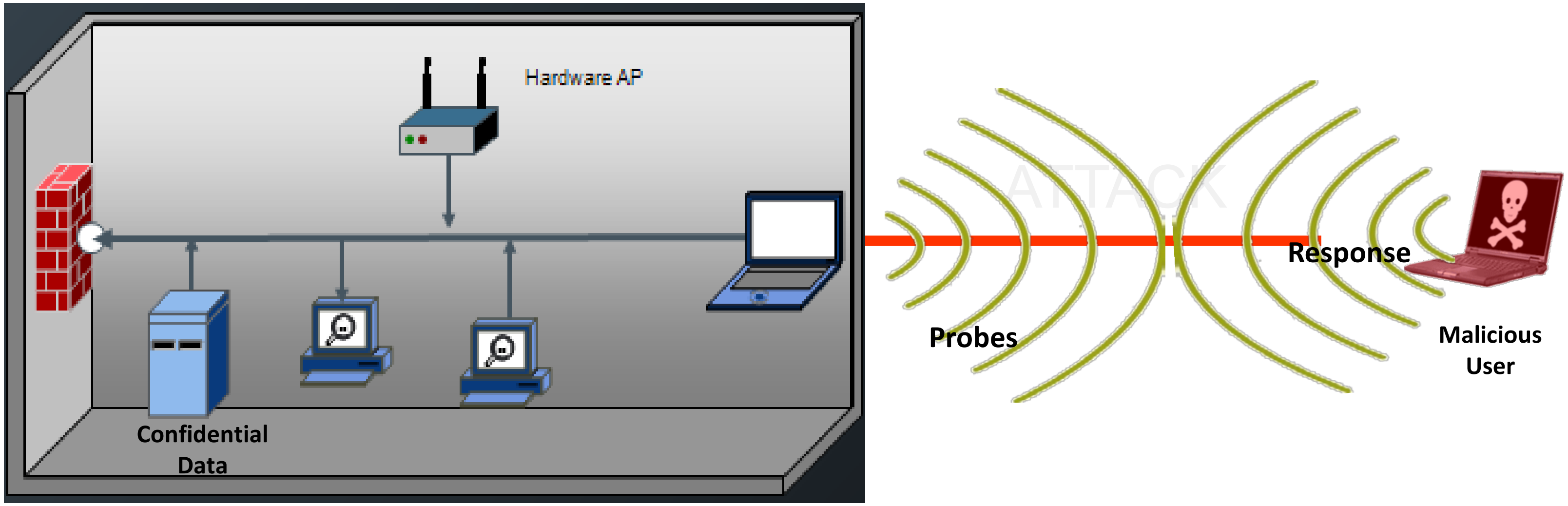
Tools such as Karma can Respond to ANY Client Probe Request

Variety of Services (POP, FTP and HTTP) to Lure Unsuspecting Users

No Authentication of “Pervasive Wireless Cloud”

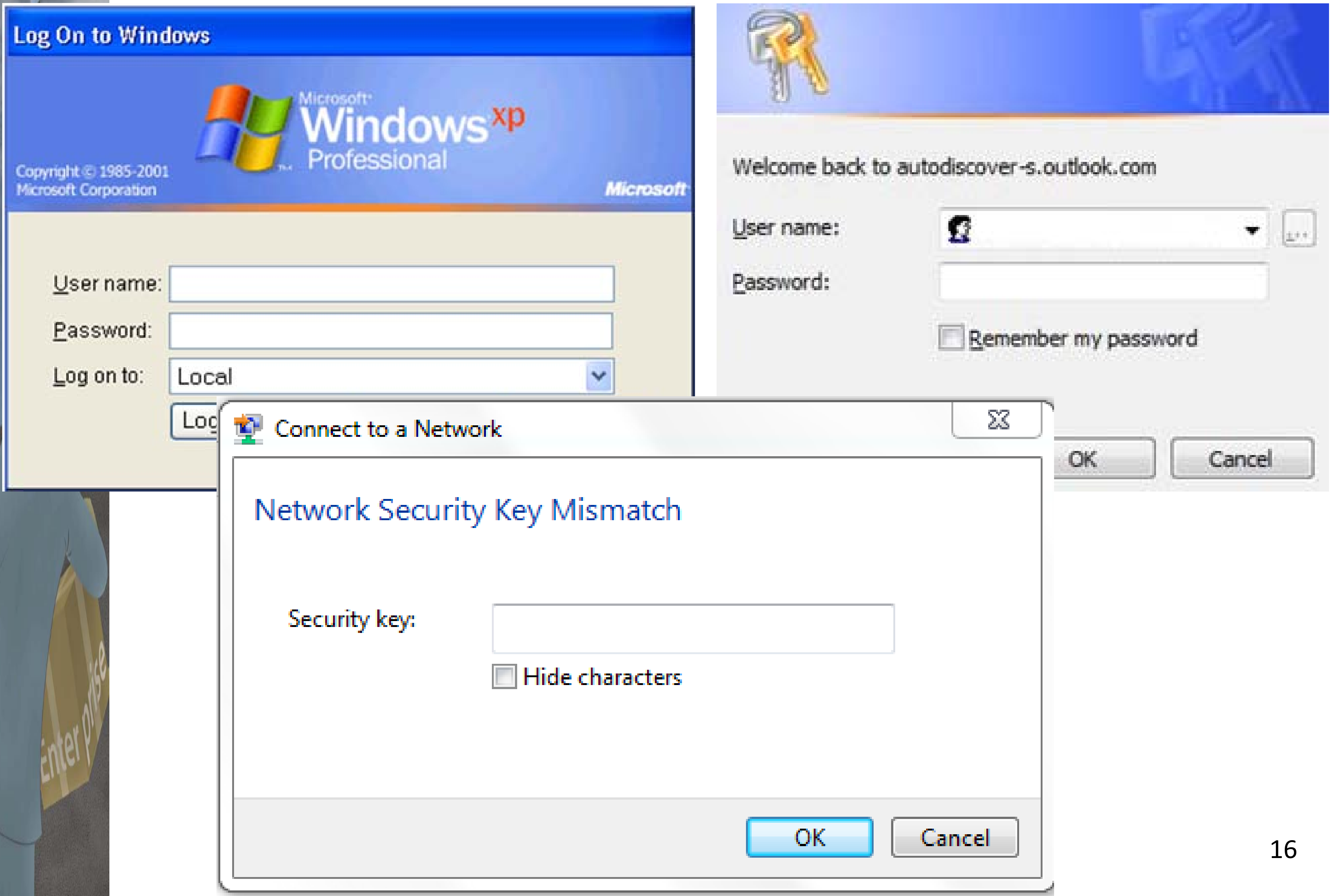
Automatic Network Selection in Windows (Zero Configuration Client)

How do Hackers Exploit Laptops?



1. Corporate laptop sends probe SSIDs in profile (tmobile, home, linksys, etc..)
   Malicious User observes the probes and SSIDs
2. Malicious user sets up AP with appropriate SSID
3. Station automatically connects to the malicious AP at Layer 2.
   Hacker issues DHCP Address and Captive DNS portal
4. Malicious user scans laptop for vulnerabilities
   Potentially gains control and bridges into network

Effective Phishing attacks…



Log On to Windows

Copyright © 1985-2001 Microsoft Corporation

User name:

Password:

Log on to: Local

Welcome back to autodiscover-s.outlook.com

User name:

Password:

□ Remember my password

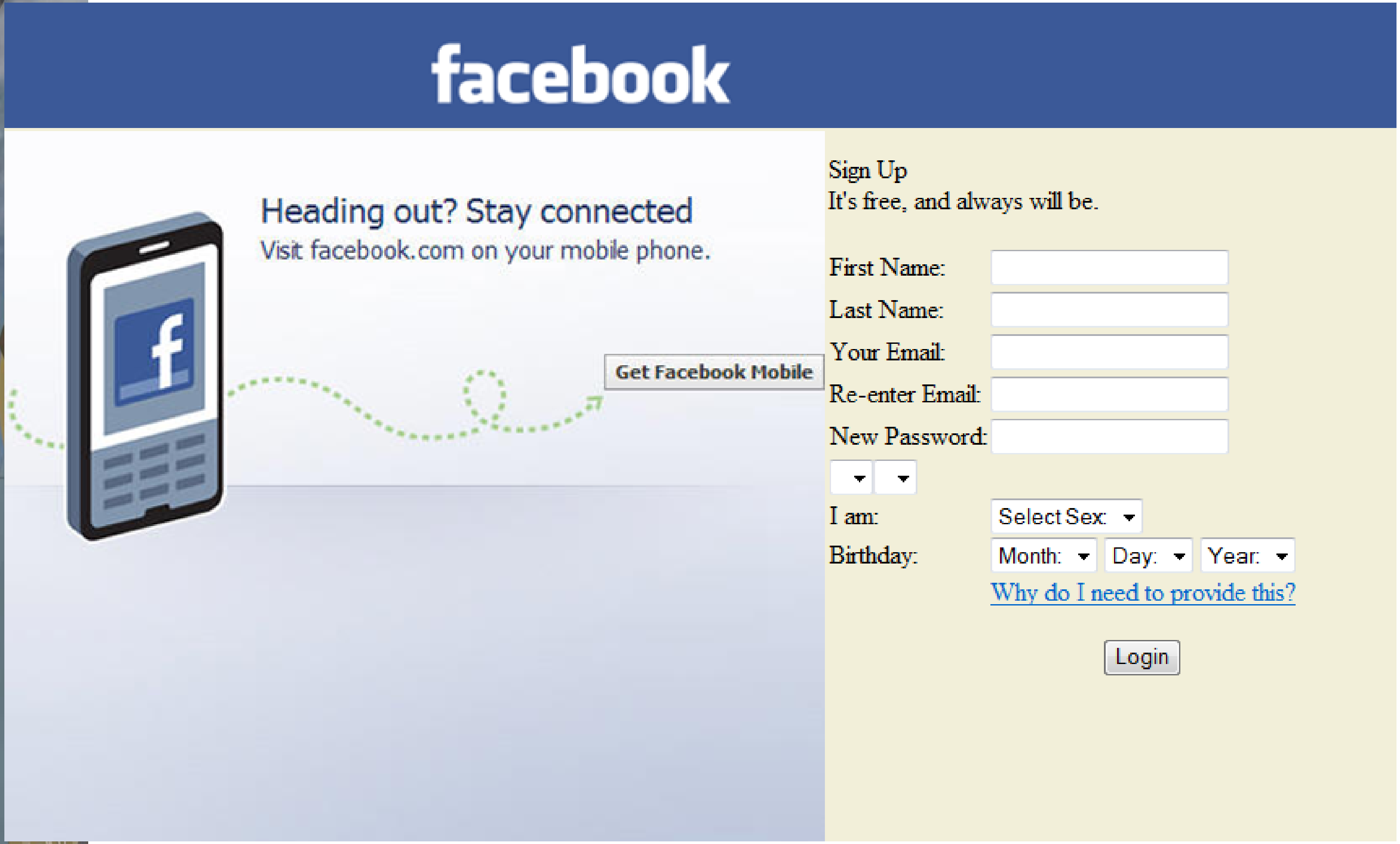
Connect to a Network

Network Security Key Mismatch

Security key:

□ Hide characters

Effective Phishing attacks…



facebook

Heading out? Stay connected

Visit facebook.com on your mobile phone.

Sign Up

It's free, and always will be.

First Name:

Last Name:

Your Email:

Re-enter Email:

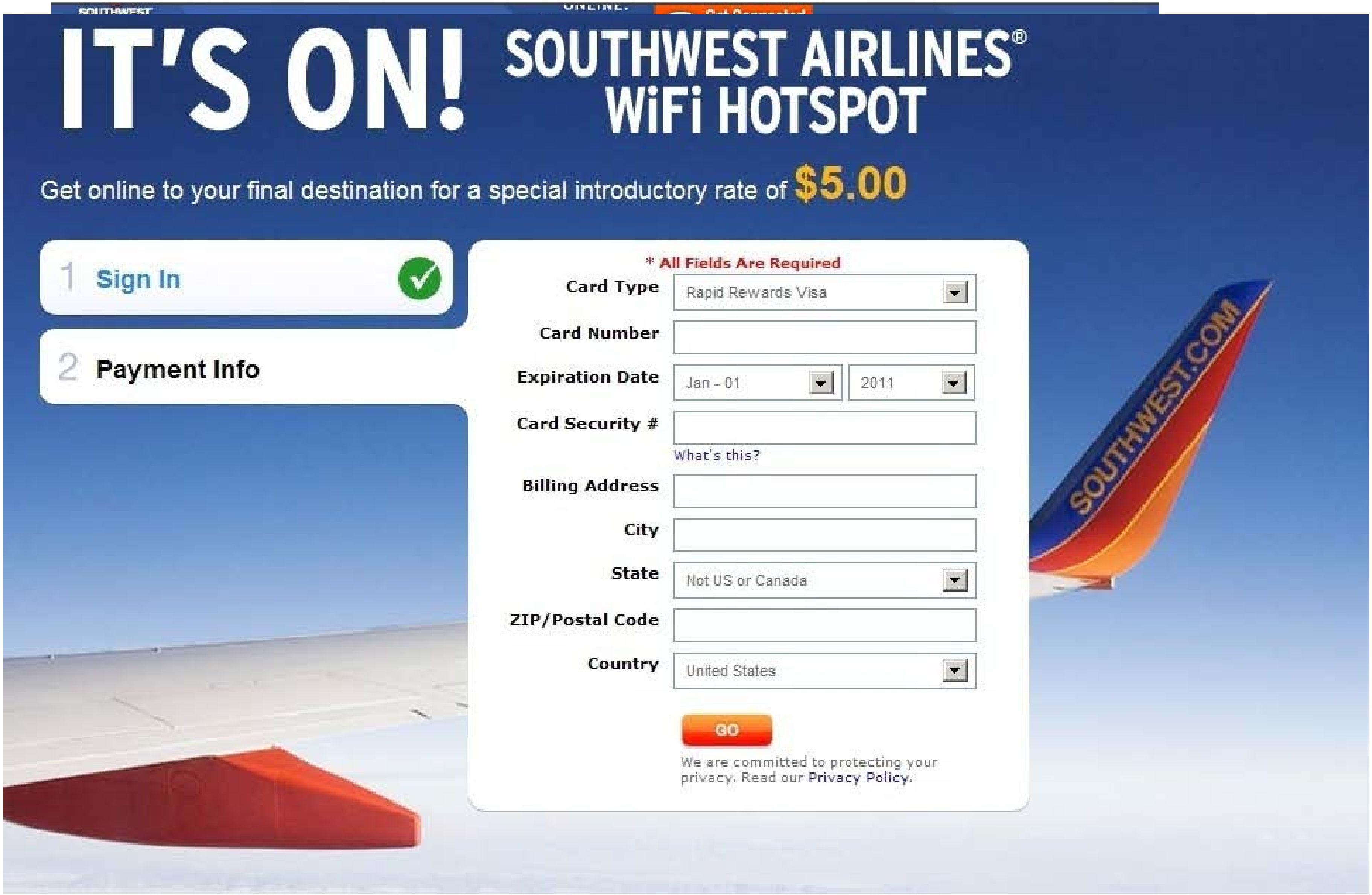
New Password:

I am: Select Sex:

Birthday: Month: Day: Year:

Why do I need to provide this?

Fake AP..



IT'S ON! SOUTHWEST AIRLINES® WiFi HOTSPOT

Get online to your final destination for a special introductory rate of $5.00

1 Sign In ✓

2 Payment Info

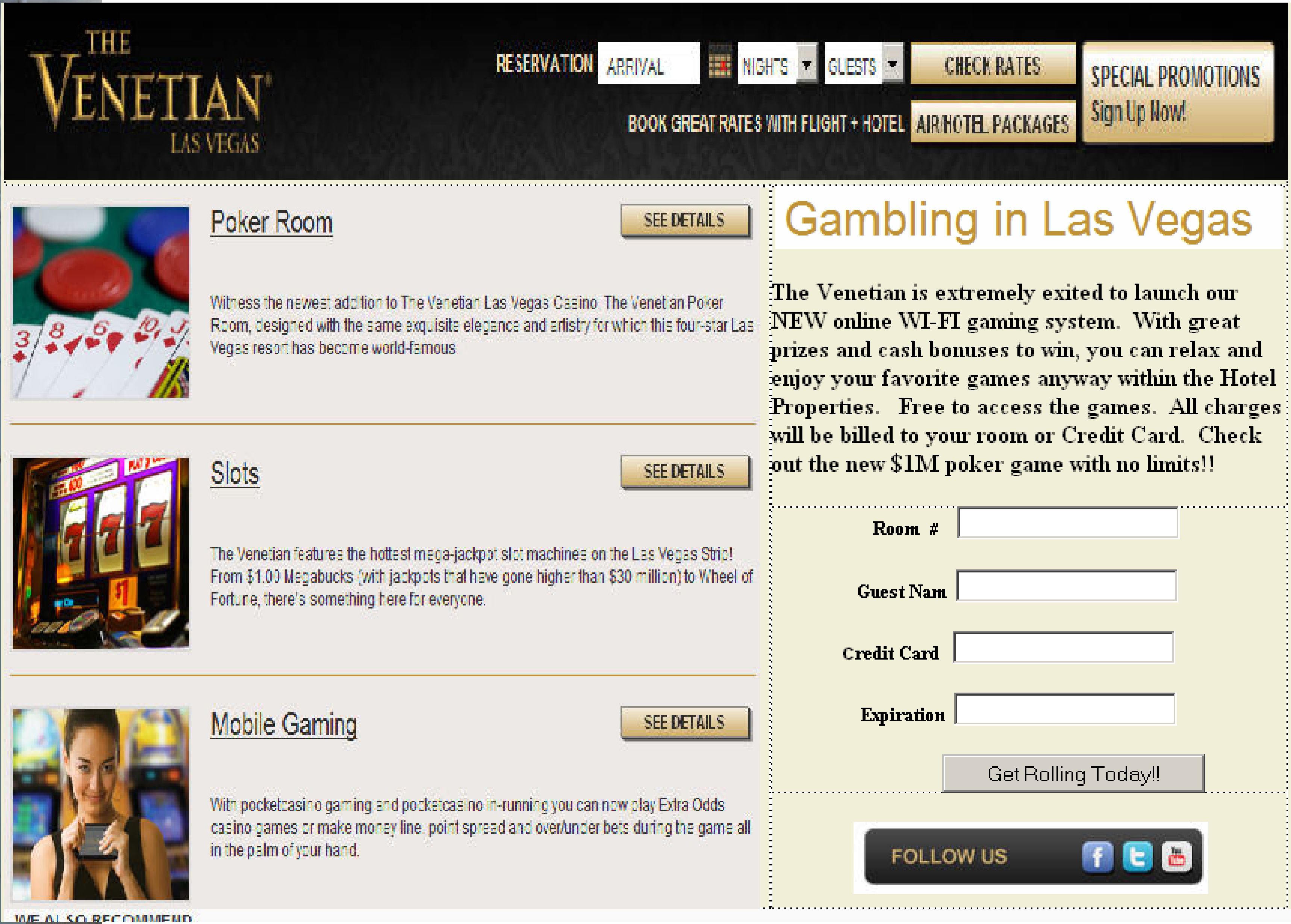
* All Fields Are Required

Card Type	Rapid Rewards Visa
Card Number	
Expiration Date	Jan - 01 / 2011
Card Security #	 What's this?
Billing Address	
City	
State	Not US or Canada
ZIP/Postal Code	
Country	United States

GO

We are committed to protecting your privacy. Read our Privacy Policy.

Online Gambling -Easy Target



Poker Room

Witness the newest addition to The Venetian Las Vegas Casino. The Venetian Poker Room, designed with the same exquisite elegance and artistry for which this four-star Las Vegas resort has become world-famous.

Slots

The Venetian features the hottest mega-jackpot slot machines on the Las Vegas Strip! From $1.00 Megabucks (with jackpots that have gone higher than $30 million) to Wheel of Fortune, there's something here for everyone.

Mobile Gaming

With pocketcasino gaming and pocketcasino in-running you can now play Extra Odds casino games or make money line, point spread and over/under bets during the game all in the palm of your hand.

WE ALSO RECOMMEND

Gambling in Las Vegas

The Venetian is extremely exited to launch our NEW online WI-FI gaming system. With great prizes and cash bonuses to win, you can relax and enjoy your favorite games anyway within the Hotel Properties. Free to access the games. All charges will be billed to your room or Credit Card. Check out the new $1M poker game with no limits!!

Room #

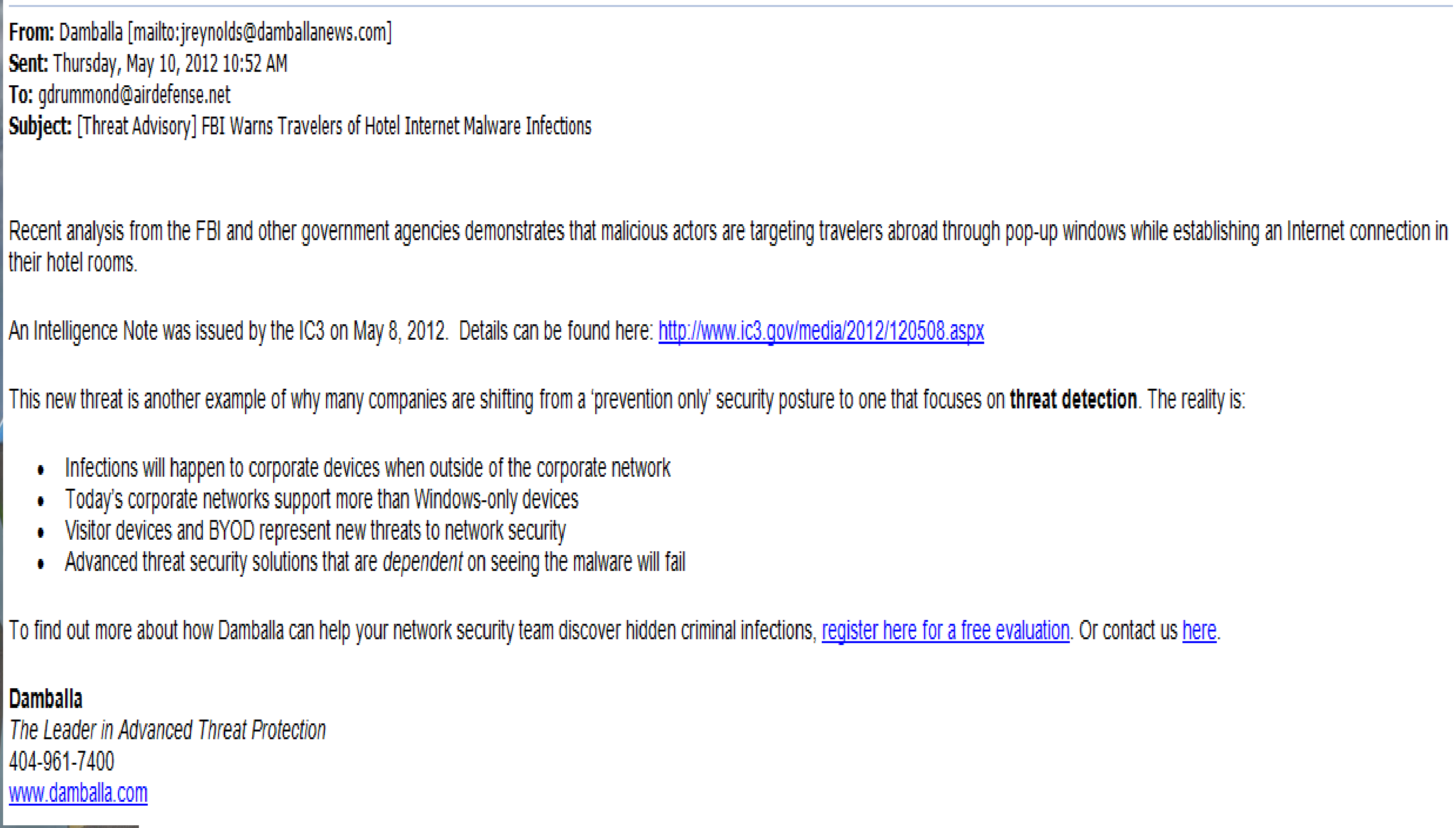
Guest Nam

Credit Card

Expiration

Get Rolling Today!!

FBI on Phising



From: Damballa [mailto:jreynolds@damballanews.com]
Sent: Thursday, May 10, 2012 10:52 AM
To: gdrummond@airdefense.net
Subject: [Threat Advisory] FBI Warns Travelers of Hotel Internet Malware Infections

Recent analysis from the FBI and other government agencies demonstrates that malicious actors are targeting travelers abroad through pop-up windows while establishing an Internet connection in their hotel rooms.

An Intelligence Note was issued by the IC3 on May 8, 2012. Details can be found here: http://www.ic3.gov/media/2012/120508.aspx

This new threat is another example of why many companies are shifting from a 'prevention only' security posture to one that focuses on **threat detection**. The reality is:

- Infections will happen to corporate devices when outside of the corporate network
- Today's corporate networks support more than Windows-only devices
- Visitor devices and BYOD represent new threats to network security
- Advanced threat security solutions that are *dependent* on seeing the malware will fail

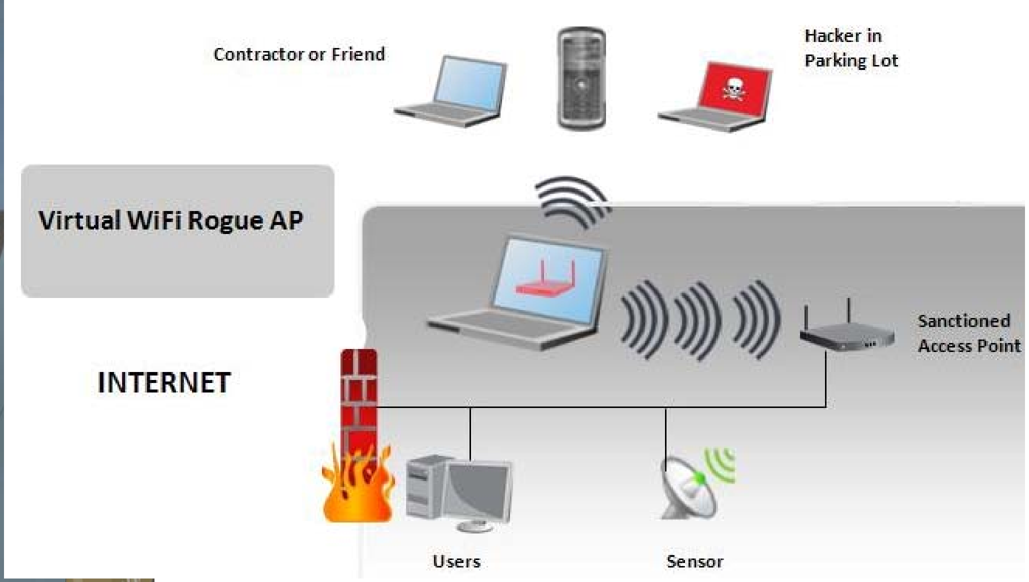
To find out more about how Damballa can help your network security team discover hidden criminal infections, register here for a free evaluation. Or contact us here.

Damballa
The Leader in Advanced Threat Protection
404-961-7400
www.damballa.com

New Window 7 Threats

Protection from Virtual WiFi Enabled Threats

- Detection of devices operating in Virtual Wifi Mode (New feature in Windows 7 and other OS)
- Automatic Protection from Rogue or Extrusion Threats Resulting form Windows 7 Virtual Wifi

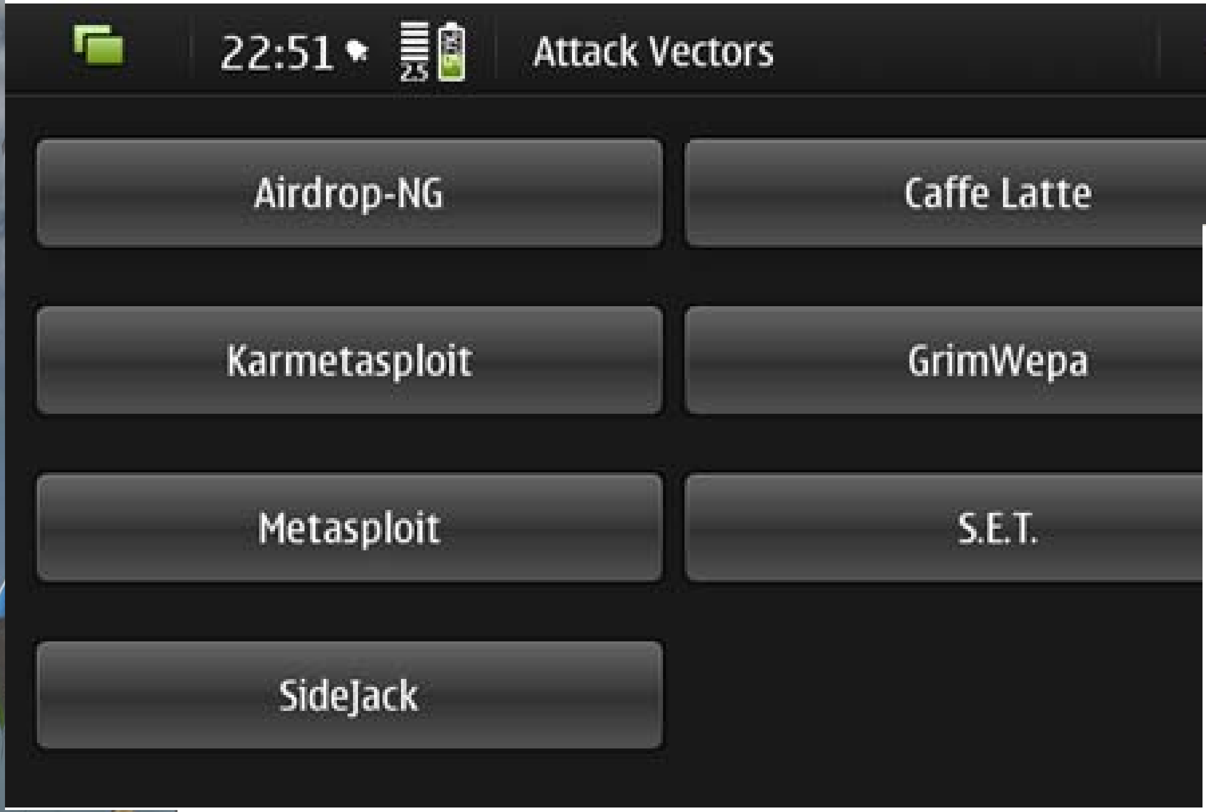


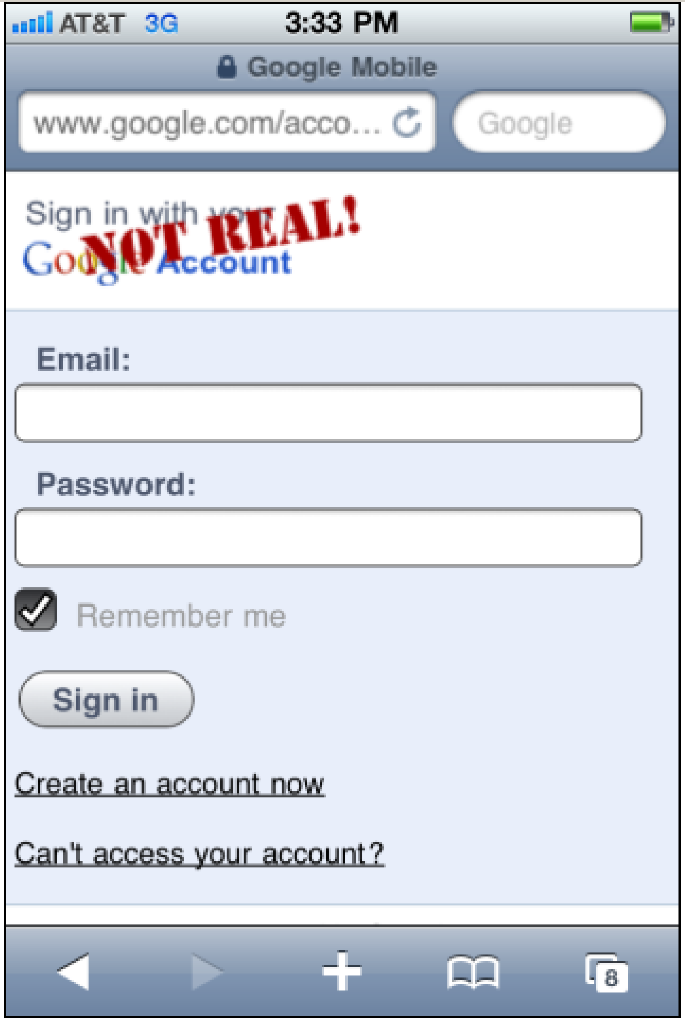
Windows 7 New Threats

- Virtual WiFi Detected
- Rogue Client on network via Virtual WiFi
- Sanctioned Client Associated to Unsanctioned Virtual Wifi
- Sanctioned Client with Rogue Virtual WiFi
- Unsanctioned Client Associated to Sanctioned Client Wifi

Protection from Continued Evaluation of Threats

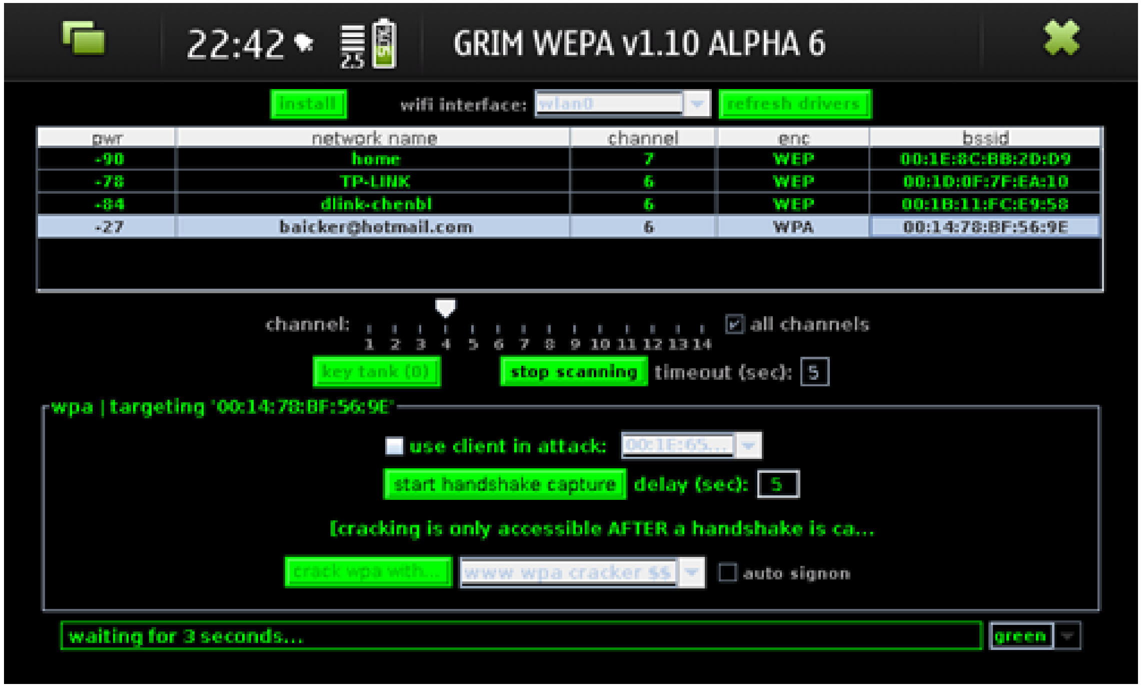
Mobile / Phone Hacks





Captive Portals now being pushed out via smart phones

Mobile Hacks on the Increase



GRIM WEPA v1.10 ALPHA 6

wifi interface: wlan0

pwr	network name	channel	enc	bssid
-90	home	7	WEP	00:1E:8C:BB:2D:D9
-78	TP-LINK	6	WEP	00:1D:0F:7F:EA:10
-84	dlink-chenbl	6	WEP	00:1B:11:FC:E9:58
-27	baicker@hotmail.com	6	WPA	00:14:78:BF:56:9E

channel: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 ☑ all channels

timeout (sec): 5

wpa | targeting '00:14:78:BF:56:9E'

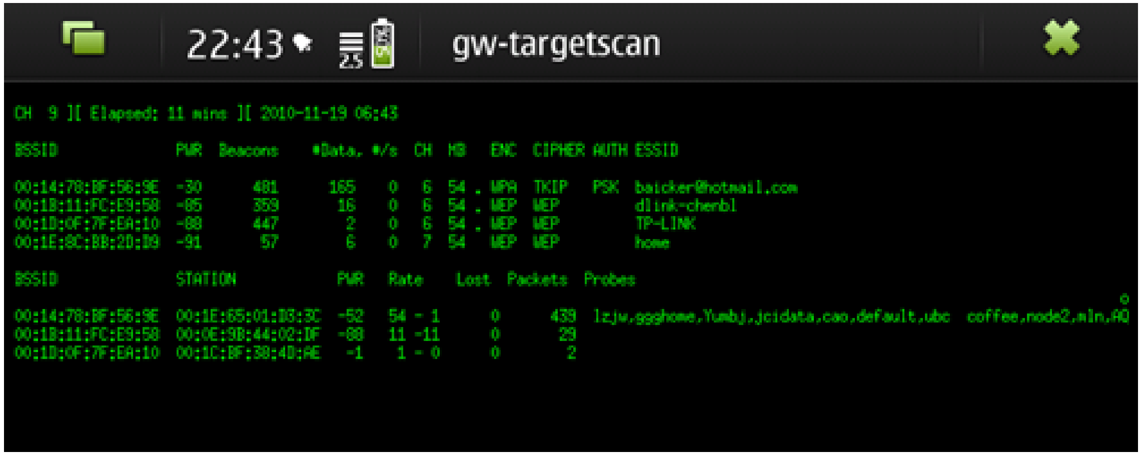
□ use client in attack: 00:1E:65...

delay (sec): 5

[cracking is only accessible AFTER a handshake is ca...

www wpa cracker $$ □ auto signon

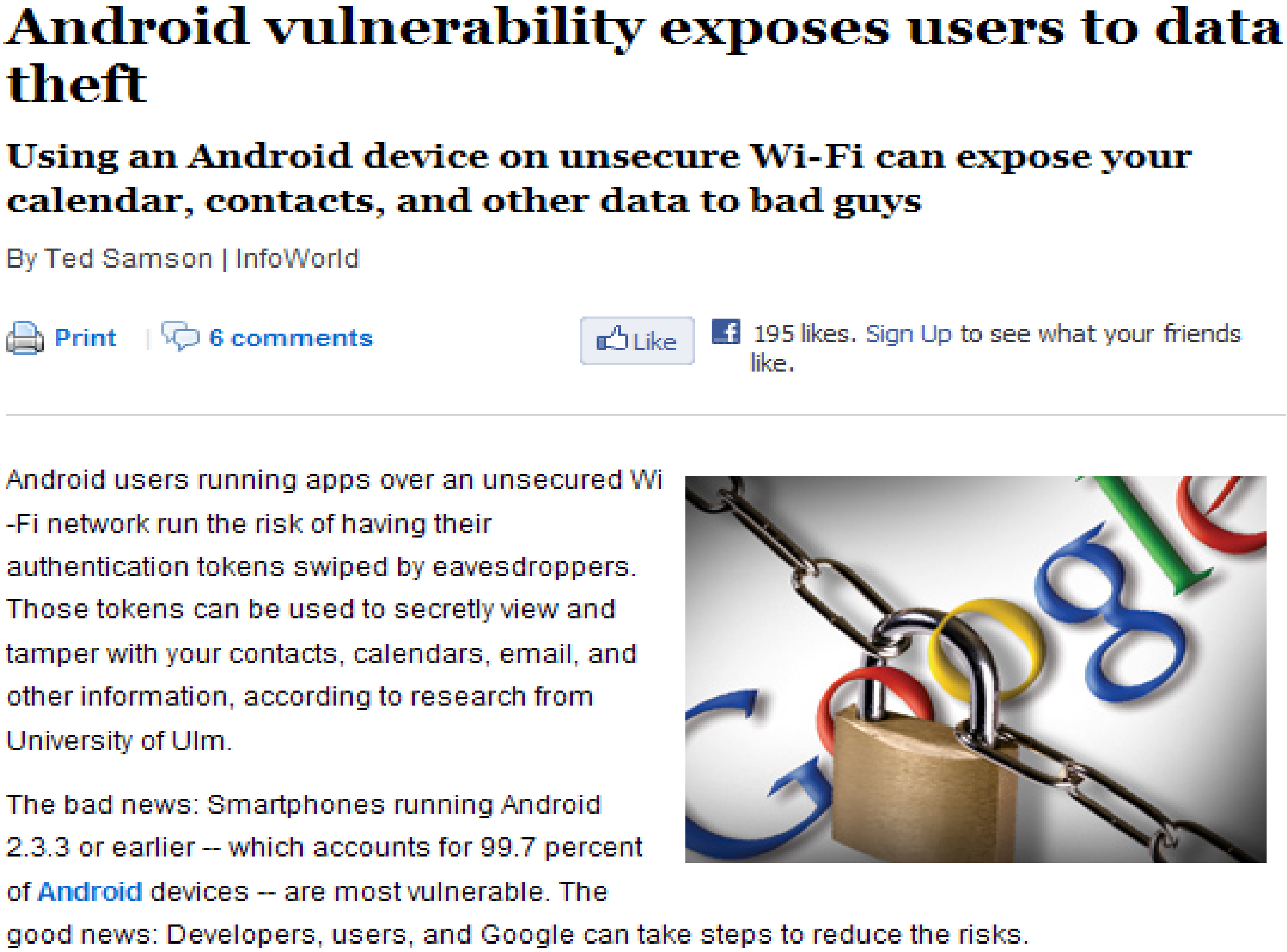
waiting for 3 seconds...



gw-targetscan

```
CH  9 ][ Elapsed: 11 mins ][ 2010-11-19 06:43

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:14:78:BF:56:9E  -30      481      165    0   6  54 . WPA  TKIP   PSK  baicker@hotmail.com
00:1B:11:FC:E9:58  -85      359       16    0   6  54 . WEP  WEP         dlink-chenbl
00:1D:0F:7F:EA:10  -88      447        2    0   6  54 . WEP  WEP         TP-LINK
00:1E:8C:BB:2D:D9  -91       57        6    0   7  54   WEP  WEP         home

BSSID              STATION            PWR   Rate    Lost  Packets  Probes
                                                                                                      ©
00:14:78:BF:56:9E  00:1E:65:01:D3:3C  -52   54 - 1     0      439  lzjw,ggghome,Yumbj,jcidata,cao,default,ubc  coffee,node2,mln,AQ
00:1B:11:FC:E9:58  00:0E:9B:44:02:DF  -88   11 -11     0       29
00:1D:0F:7F:EA:10  00:1C:BF:38:4D:AE   -1    1 - 0     0        2
```

In the News lately….



Android vulnerability exposes users to data theft

Using an Android device on unsecure Wi-Fi can expose your calendar, contacts, and other data to bad guys

By Ted Samson | InfoWorld

Print | 6 comments

Like 195 likes. Sign Up to see what your friends like.

Android users running apps over an unsecured Wi-Fi network run the risk of having their authentication tokens swiped by eavesdroppers. Those tokens can be used to secretly view and tamper with your contacts, calendars, email, and other information, according to research from University of Ulm.

The bad news: Smartphones running Android 2.3.3 or earlier -- which accounts for 99.7 percent of Android devices -- are most vulnerable. The good news: Developers, users, and Google can take steps to reduce the risks.

Man-in-the-Middle Exploit

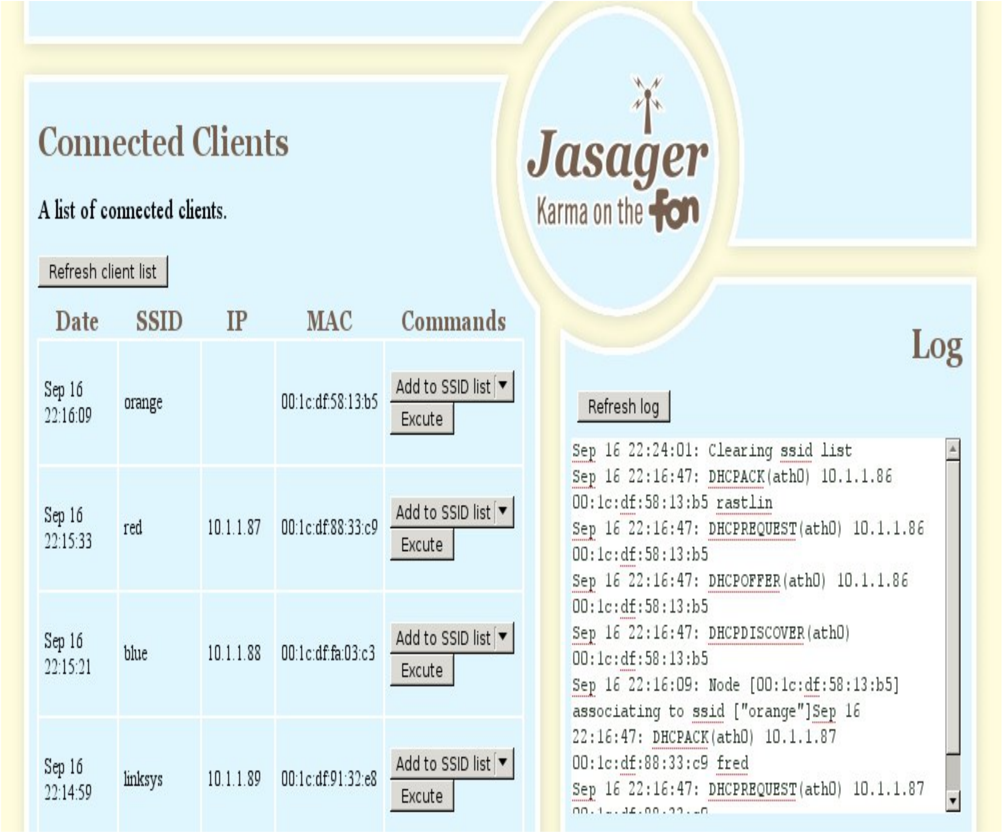
Example of Attacks and Tools

- Evil Twin – In this attack an attacker simply provides their own access point running with the name of your network's SSID. In the case of Karma, the software simply monitors for a client requesting a network name such as T-mobile, Facebook, Google etc …and pretends to be that network.

  In these attacks the amount of damage that can be done is limited by the attackers skill and imagination.

Weaponizing Karma

Jasager – German for “Yesman”, takes the Karma framework and puts it onto an open source wireless router. The favorite of these is the FON router.



Connected Clients

A list of connected clients.

Date	SSID	IP	MAC	Commands
Sep 16 22:16:09	orange		00:1c:df:58:13:b5	Add to SSID list ▼ Excute
Sep 16 22:15:33	red	10.1.1.87	00:1c:df:88:33:c9	Add to SSID list ▼ Excute
Sep 16 22:15:21	blue	10.1.1.88	00:1c:df:fa:03:c3	Add to SSID list ▼ Excute
Sep 16 22:14:59	linksys	10.1.1.89	00:1c:df:91:32:e8	Add to SSID list ▼ Excute

Log

```
Sep 16 22:24:01: Clearing ssid list
Sep 16 22:16:47: DHCPACK(ath0) 10.1.1.86
00:1c:df:58:13:b5 rastlin
Sep 16 22:16:47: DHCPREQUEST(ath0) 10.1.1.86
00:1c:df:58:13:b5
Sep 16 22:16:47: DHCPOFFER(ath0) 10.1.1.86
00:1c:df:58:13:b5
Sep 16 22:16:47: DHCPDISCOVER(ath0)
00:1c:df:58:13:b5
Sep 16 22:16:09: Node [00:1c:df:58:13:b5]
associating to ssid ["orange"]Sep 16
22:16:47: DHCPACK(ath0) 10.1.1.87
00:1c:df:88:33:c9 fred
Sep 16 22:16:47: DHCPREQUEST(ath0) 10.1.1.87
```

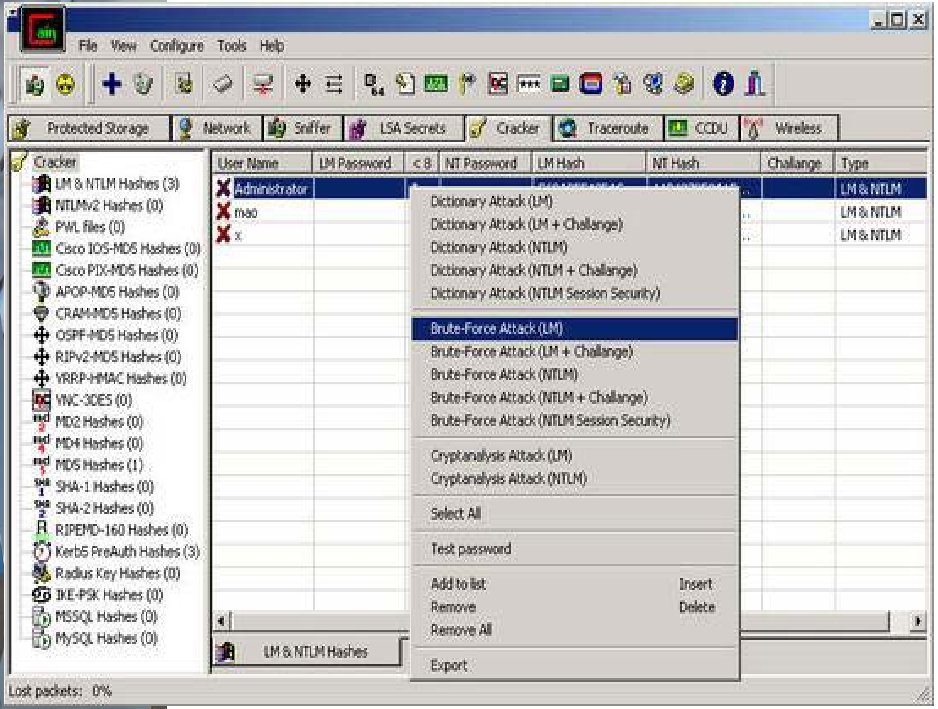
Weaponizing Karma

- Karmetasploit – added to Metasploit (an open source exploit framework), Karma became the latest wireless component to be added.

  Features include:
- Capture POP3 and IMAP4 passwords (clear-text and SSL)
- Accept outbound email sent over SMTP
- Parse out FTP and HTTP login information
- Steal cookies from large lists of popular web sites
- Steal saved form fields from the same web sites
- Use SMB relay attacks to load the Meterpreter payload
- Automatically exploit a wide range of browser flaws
- Karmetasploit is on the Backtrack3 CD and abaove

Check out http://www.metasploit.com/dev/trac/wiki/Karmetasploit for more info

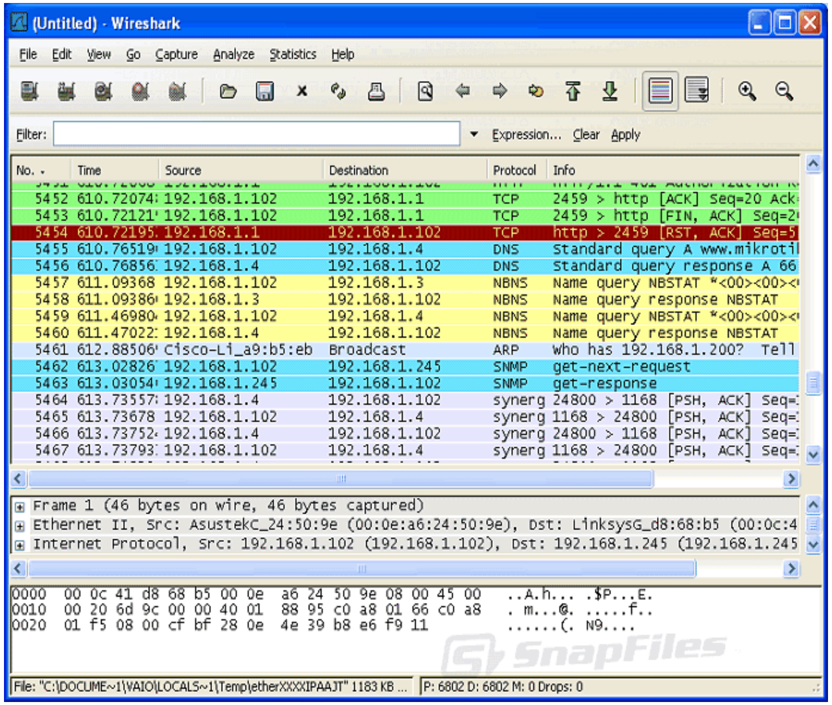
Sniffing Enterprise Secrets



User Name	LM Password	< 8	NT Password	LM Hash	NT Hash	Challange	Type
Administrator							LM & NTLM
mao							LM & NTLM
x							LM & NTLM

Lost packets: 0%

Cain /Able


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

```
No.   Time        Source              Destination     Protocol  Info
5452  610.72074:  192.168.1.102       192.168.1.1     TCP       2459 > http [ACK] Seq=20 Ack
5453  610.72121'  192.168.1.102       192.168.1.1     TCP       2459 > http [FIN, ACK] Seq=2
5454  610.72195:  192.168.1.1         192.168.1.102   TCP       http > 2459 [RST, ACK] Seq=5
5455  610.76519   192.168.1.102       192.168.1.4     DNS       Standard query A www.mikrotil
5456  610.76856:  192.168.1.4         192.168.1.102   DNS       Standard query response A 66
5457  611.09368   192.168.1.102       192.168.1.3     NBNS      Name query NBSTAT *<00><00><
5458  611.09386   192.168.1.3         192.168.1.102   NBNS      Name query response NBSTAT
5459  611.46980   192.168.1.102       192.168.1.4     NBNS      Name query NBSTAT *<00><00><
5460  611.47022:  192.168.1.4         192.168.1.102   NBNS      Name query response NBSTAT
5461  612.88506   Cisco-Li_a9:b5:eb   Broadcast       ARP       Who has 192.168.1.200?  Tell
5462  613.02826   192.168.1.102       192.168.1.245   SNMP      get-next-request
5463  613.03054   192.168.1.245       192.168.1.102   SNMP      get-response
5464  613.73557:  192.168.1.4         192.168.1.102   synerg    24800 > 1168 [PSH, ACK] Seq=
5465  613.73678   192.168.1.102       192.168.1.4     synerg    1168 > 24800 [PSH, ACK] Seq=
5466  613.73752   192.168.1.4         192.168.1.102   synerg    24800 > 1168 [PSH, ACK] Seq=
5467  613.73793:  192.168.1.102       192.168.1.4     synerg    1168 > 24800 [PSH, ACK] Seq=
```

```
⊞ Frame 1 (46 bytes on wire, 46 bytes captured)
⊞ Ethernet II, Src: AsustekC_24:50:9e (00:0e:a6:24:50:9e), Dst: LinksysG_d8:68:b5 (00:0c:4
⊞ Internet Protocol, Src: 192.168.1.102 (192.168.1.102), Dst: 192.168.1.245 (192.168.1.245
```

```
0000  00 0c 41 d8 68 b5 00 0e  a6 24 50 9e 08 00 45 00   ..A.h... .$P...E.
0010  00 20 6d 9c 00 00 40 01  88 95 c0 a8 01 66 c0 a8   . m...@. .....f..
0020  01 f5 08 00 cf bf 28 0e  4e 39 b8 e6 f9 11         ......(. N9....
```

File: "C:\DOCUME~1\VAIO\LOCALS~1\Temp\etherXXXXIPAAJT" 1183 KB ... P: 6802 D: 6802 M: 0 Drops: 0

Wireshark

Hackers can Sniff Passwords and Credentials Over the Air – Nmap, Nessus, John the Ripper, WinZapper

Cleat-text Passwords Sniffed - FTP, HTTP, POP3, IMAP …

Certificates and Keys Stolen, Hashes can be Cracked – NTLM, MDx, SHA-x, OSPF, CDP

Listen to VoIP Conversations – hack tool called Viper , exploits SIP / Skinny protocol

WPA/WPA2 Exploit

Eavesdropping and Injection Attacks

- **Wireless networks are akin to using network hubs. That is that once you've joined its really simple to monitor or "sniff" someone's traffic.**

- **Security Flaw – By its very nature, networking is assumed to be a shared medium so little to no protections were put into place to provide privacy. It wasn't until switches and Vlans came into place that network segregation started catching on.**

Breaking WEP

History of Cracking WEP

2001	Uncrackable
2003	Years
2004	Days
2005	Hours
2006	Minutes
2007	Seconds

Dozens of Attacks

Key Cracking

No Replay Protection

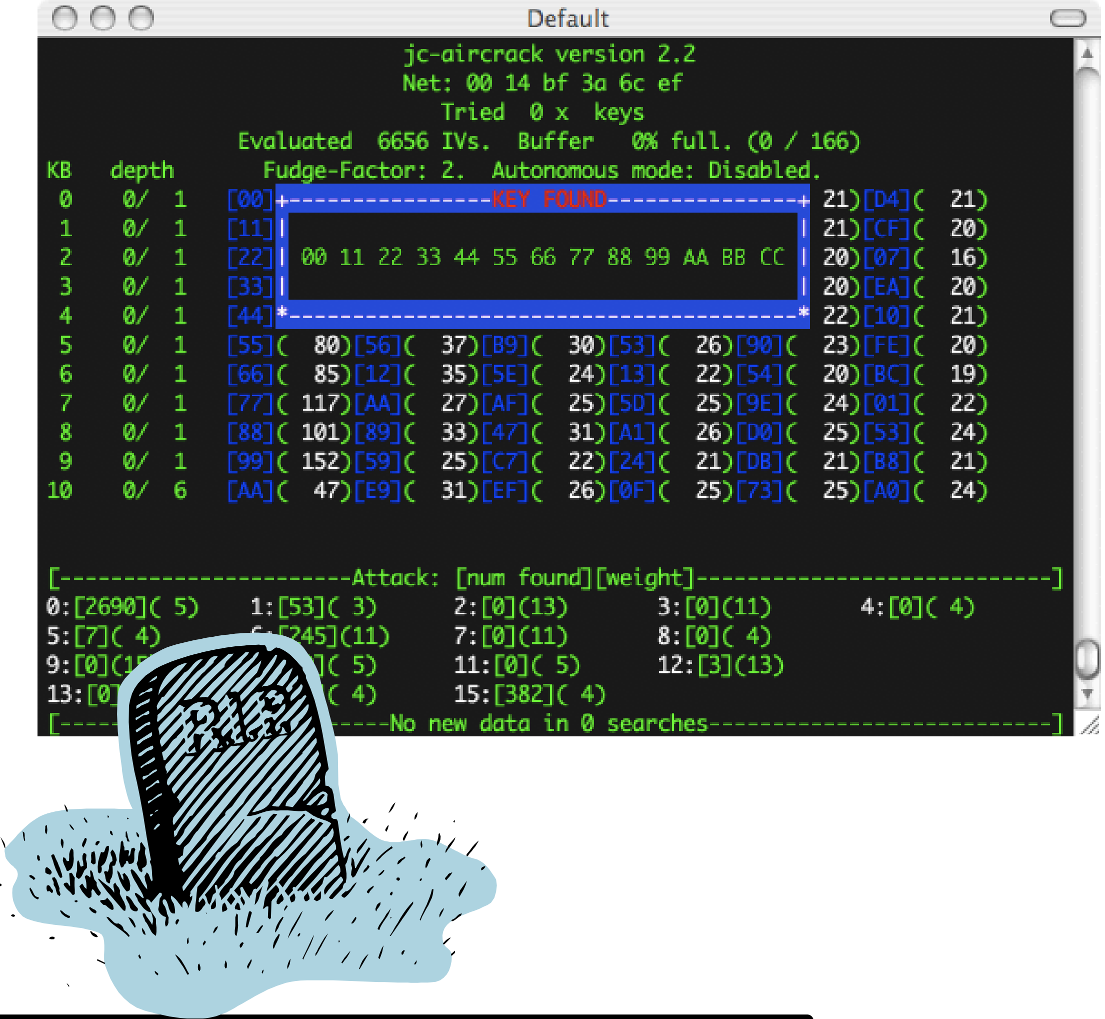
Lack of Message Integrity

Shared Keys

Poor RC4 Implementation

64 –bit WEP uses 40 bit key / 24-bit IV to form the RC4 traffic key

128-bit WEP protocol using a 104-bit key size (WEP-104).



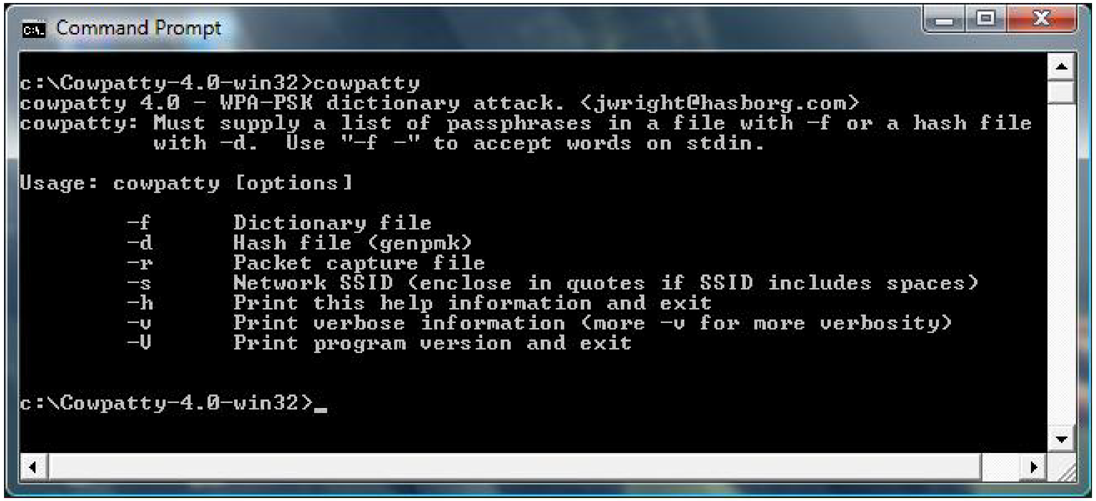
```
                        jc-aircrack version 2.2
                        Net: 00 14 bf 3a 6c ef
                           Tried  0 x  keys
              Evaluated  6656 IVs.  Buffer   0% full. (0 / 166)
KB   depth      Fudge-Factor: 2.  Autonomous mode: Disabled.
 0    0/  1   [00]+----------------KEY FOUND---------------+ 21)[D4](  21)
 1    0/  1   [11]|                                        | 21)[CF](  20)
 2    0/  1   [22]| 00 11 22 33 44 55 66 77 88 99 AA BB CC | 20)[07](  16)
 3    0/  1   [33]|                                        | 20)[EA](  20)
 4    0/  1   [44]*----------------------------------------* 22)[10](  21)
 5    0/  1   [55](  80)[56](  37)[B9](  30)[53](  26)[90](  23)[FE](  20)
 6    0/  1   [66](  85)[12](  35)[5E](  24)[13](  22)[54](  20)[BC](  19)
 7    0/  1   [77]( 117)[AA](  27)[AF](  25)[5D](  25)[9E](  24)[01](  22)
 8    0/  1   [88]( 101)[89](  33)[47](  31)[A1](  26)[D0](  25)[53](  24)
 9    0/  1   [99]( 152)[59](  25)[C7](  22)[24](  21)[DB](  21)[B8](  21)
10    0/  6   [AA](  47)[E9](  31)[EF](  26)[0F](  25)[73](  25)[A0](  24)


[-----------------------Attack: [num found][weight]----------------------------]
0:[2690]( 5)    1:[53]( 3)      2:[0](13)       3:[0](11)       4:[0]( 4)
5:[7]( 4)         [245](11)     7:[0](11)       8:[0]( 4)
9:[0](1           ]( 5)         11:[0]( 5)      12:[3](13)
13:[0             ]( 4)         15:[382]( 4)
[----               -----No new data in 0 searches---------------------------]
```

Upgrade from WEP to WPA2 as Soon as Possible

Breaking WPA

History of Cracking WPA

2006	80 Keys/Second
2007	130 Keys/Second
2007	30,000 Keys/Second
2008	100,000 Keys/Second



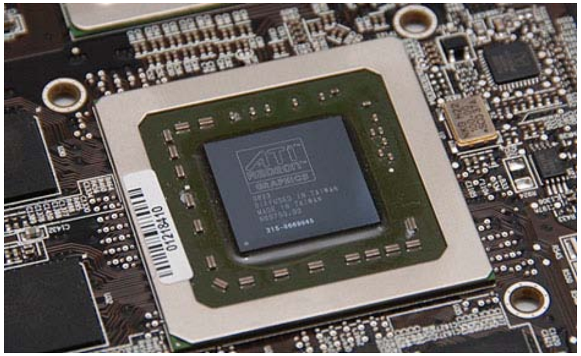
```
c:\Cowpatty-4.0-win32>cowpatty
cowpatty 4.0 - WPA-PSK dictionary attack. <jwright@hasborg.com>
cowpatty: Must supply a list of passphrases in a file with -f or a hash file
          with -d.  Use "-f -" to accept words on stdin.

Usage: cowpatty [options]

        -f      Dictionary file
        -d      Hash file (genpmk)
        -r      Packet capture file
        -s      Network SSID (enclose in quotes if SSID includes spaces)
        -h      Print this help information and exit
        -v      Print verbose information (more -v for more verbosity)
        -V      Print program version and exit


c:\Cowpatty-4.0-win32>_
```

New Attacks Emerging

WPA Pre-Shared Key is Not Very Secure

Use of Parallel Processing (Graphics Cards & FPGA Accelerators) to Speedup Brute Force PSK Cracking

WPA TKIP Compromised - Subject to Small Frame Decodes and Slow Injection of Arbitrary Frames

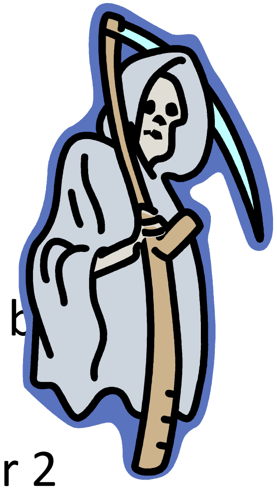


Use WPA2 with AES Encryption and Enterprise Mode 802.1X Authentication

WPA/WPA2 TKIP Hacking

- Who is Impacted
  - WPA/WPA2 using TKIP Encryption (introduced 2003)
  - Regardless of PSK or 802.1x/EAP authentication
  - TKIP networks using QOS Enabled
- Impact
  - Attacker can decrypt Plaintext packet between AP/Stations
  - Attacker can inject up to 15 arbitrary packets
  - If QOS is enabled the attack can lead to an injection attack
- How is it done
  - 802.11e Replay Injection
  - TKIP Chop Chop ICV attack
- Detection/Mitigation
  - WIPS solutions can detect Replay Injection attacks
  - Infrastructure : Frequent TKIP rotation
  - Transition to AES Encryption

Leaked Wired-side Traffic



#1 Corporate Vulnerability

- Even if the data is encrypted, the services that are run b the MAC address can be detected
- Remember wireless is LAYER 2; it will send out all Layer 2 traffic
  - VRRP, HSRP, Spanning Tree, OSPF, VTP/VLAN, CDP
  - VLAN don’t help unless filtered
  - MOST USE HASHES or PASSWORDS
    - **Clear-Text**
- Broadcast/Multicast key rotation is **OFF** by **Default**
- Client devices using static WEP cannot use the AP w n you enable broadcast key rotation

It’s a two-way street, what goes out can also come in!

Summary of 802.11 Vulnerabilities

Type	Attacks	Tools
Reconnaissance	▪ Rogue APs ▪ Open/Misconfigured APs ▪ Ad Hoc stations	Netstumbler, Kismet, Wellenrighter
Sniffing	▪ WEP, WPA, LEAP cracking ▪ Dictionary attacks ▪ Leaky APs	AirSnort, Wepcrack, Cowpatty, WinSniffer, Cain, Ettercap
Masquerade	▪ MAC spoofing ▪ AirSnarf/HotSpot attacks ▪ Evil Twin/Wi-Phishing attacks	AirSnarf, Hotspotter, HostAP, SMAC
Insertion	▪ Multicast/Broadcast injection ▪ Routing cache poisoning ▪ Man in the Middle attack	Airpwn, WepWedgie, ChopChop, Vippr, irpass, CDPsniffer
Denial-of-Service	▪ Disassociation ▪ Duration field spoofing ▪ RF jamming	AirJack, void11, Bugtraq, IKE-crack

Implementing a Best Practice Approach to Wireless Security

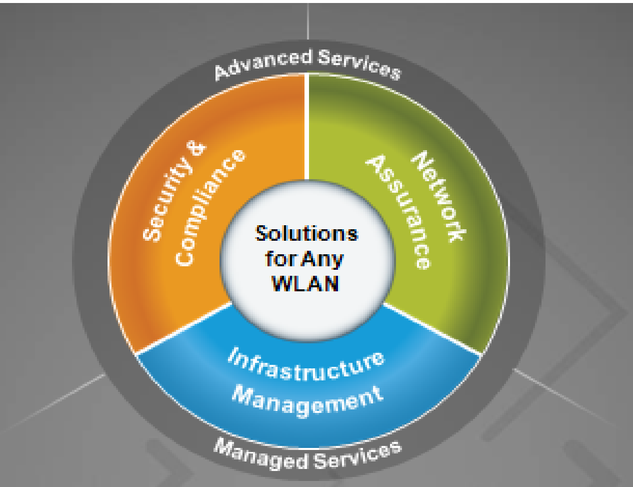
Why the need for Wireless Protection?

- Wireless is a dynamic environment
  - Need for Rogue Detection and Mitigation
  - Prevent Wireless Phishing of Corporate Laptops
- Compliance and Reporting
  - Ability to meet/exceed auditor requirements
  - PCI / SOX / HIPAA

Best Practice Approach for Wireless Security

1. Implement: 1st Line of Defense
   - Breach of Policy (Full-time vs Part-time monitoring)
2. Implement: 2nd Line of Defense
   - Indentify and Fix the Vulnerabilities –prior to any loss or incident occurring
3. Implement: 3rd line of Defense
   - Target Aware Intrusion Detection and Prevention

AirDefense Management Service Platform



Security & Compliance

- Rogue Elimination
- Intrusion Prevention
- Automated Defenses
- Forensic Analysis
- Wireless Vulnerability Assessment
- Mobile Protection
- 24x7 Policy Monitoring
- Custom Reporting: PCI, HIPAA, GLBA, US DoD, SOX Reports

Infrastructure Management

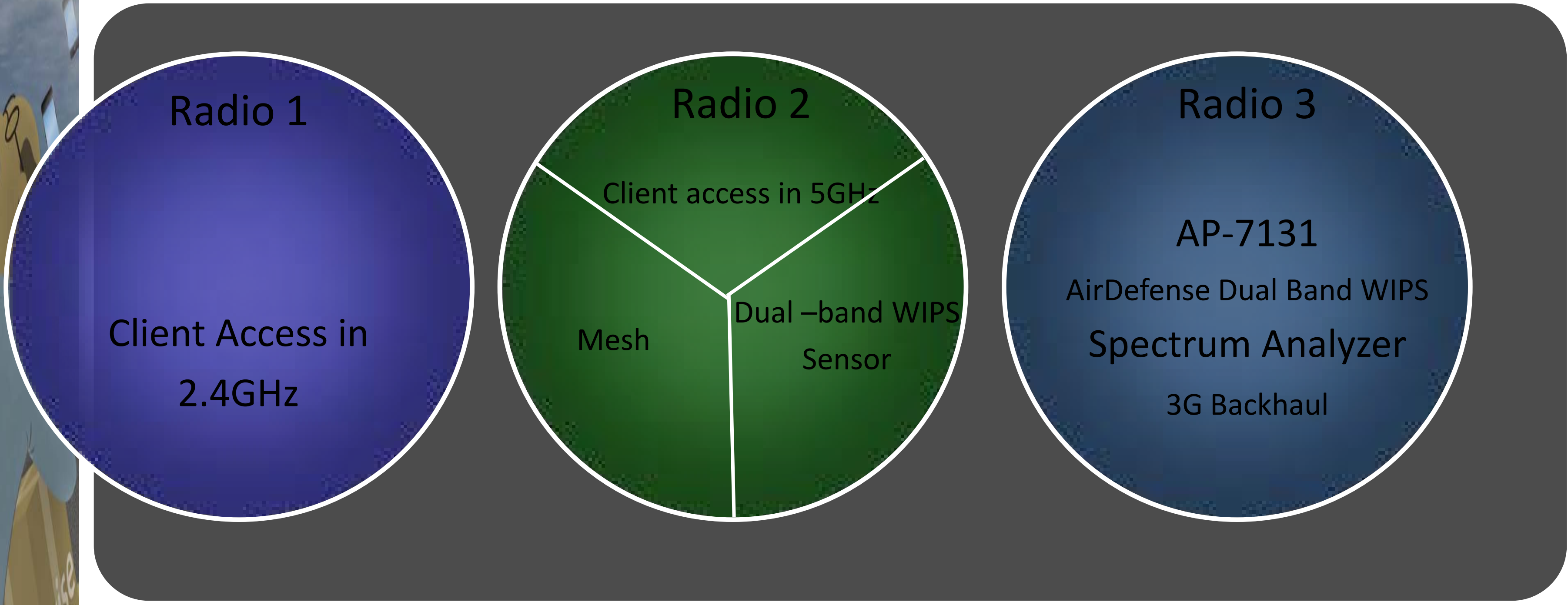
- Multi-vendor Management
- Centralized Configuration
- Policy-based Fault Mgmt
- Automated Discovery
- Network Visualizations
- Firmware Management

Network Assurance

- Solve Issues Remotely
- Level 1 Helpdesk
- Proactive Monitoring
- Spectrum Analysis
- Interference Detection
- Coverage Visualizations
- Remote Packet Capture
- Historical Analysis
- Mobile Laptop Analyzer

Band-unlocked APs that just do more

- More: Access, MESH, 3G Backhaul, WIPS Spectrum Analysis all on one AP!



Radio 1

Client Access in 2.4GHz

Radio 2

Client access in 5GHz

Mesh

Dual –band WIPS Sensor

Radio 3

AP-7131

AirDefense Dual Band WIPS

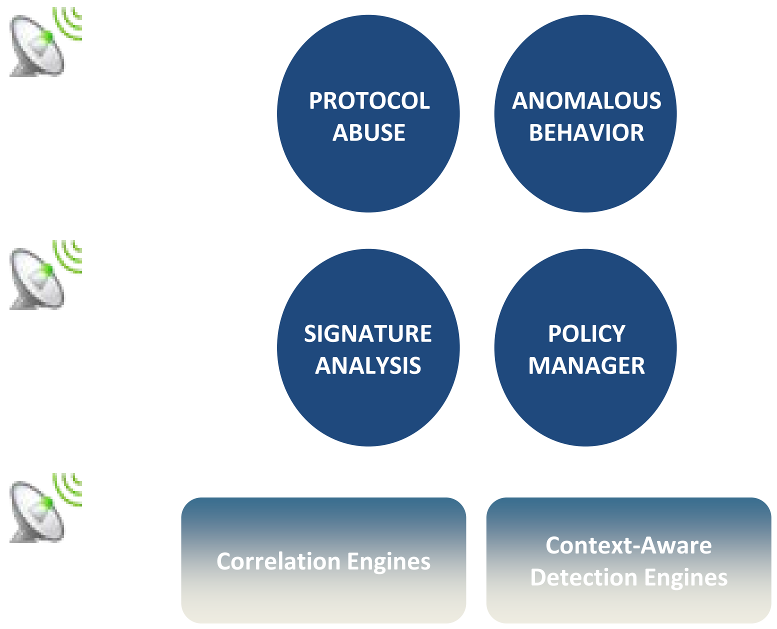
Spectrum Analyzer

3G Backhaul

Tremendous flexibility, Great ROI : Full AP functionality with concurrent 24x7 sensor

Comprehensive Intrusion Detection

DETECT—ANALYZE—ELIMINATE



275+ Threats Detected

Reconnaissance & Probing

Denial of Service Attacks

Identity Thefts, Malicious Associations

Dictionary Attacks; Security Policy Violations

Minimal False Positives

Correlation Across Multiple Detection Engines Reduces False Positives

Most Accurate Attack Detection

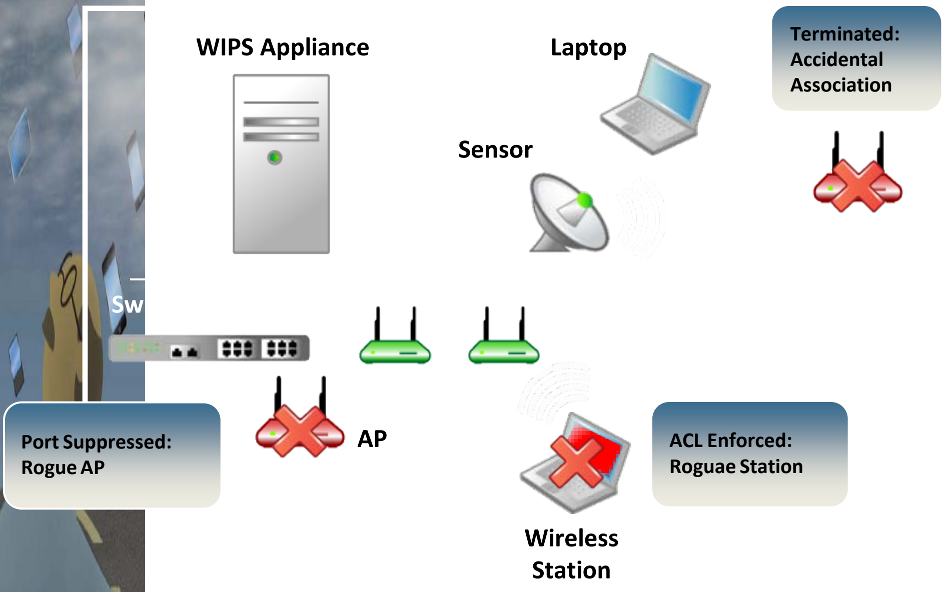
Differentiate Between Neighbors and Rogue Devices Automatically

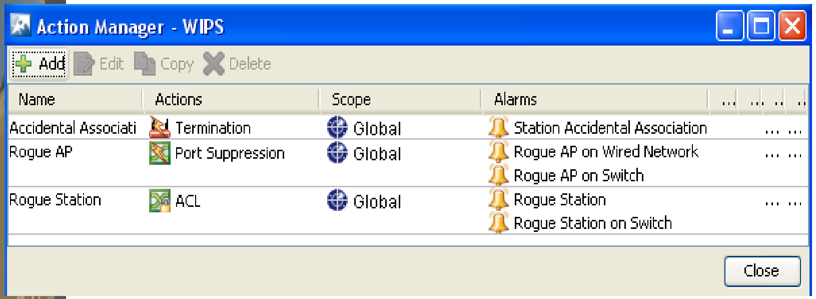
Identify Every Type of Rogue Device Connected to the Network

Historical Record of Associations & Traffic

Automatic Elimination

Automated Intrusion Prevention


WIPS Appliance
Laptop
Terminated: Accidental Association
Sensor
Sw
AP
Port Suppressed: Rogue AP
ACL Enforced: Roguae Station
Wireless Station



Name	Actions	Scope	Alarms	...	...
Accidental Associati	Termination	Global	Station Accidental Association	...	...
Rogue AP	Port Suppression	Global	Rogue AP on Wired Network Rogue AP on Switch	...	...
Rogue Station	ACL	Global	Rogue Station Rogue Station on Switch	...	...

Wireless Termination

Targeted Disruption of Wireless Connections

No Impact to Allowed Network Traffic

Compliant with Applicable Laws & FCC Regulations

Wired Port Suppression

Search Wired Network to Locate the Switch-port a Rogue Threat is Attached to

Safeguards Ensure Only Threat is Disconnected

Wireless ACL

Prevent Wireless Stations from Connecting to the WLAN

Comprehensive Threat Mitigation that is Powerful & Safe to Use

Forensic Analysis for Security

Extensive Forensic Data

325+ Statistics per Device per Minute

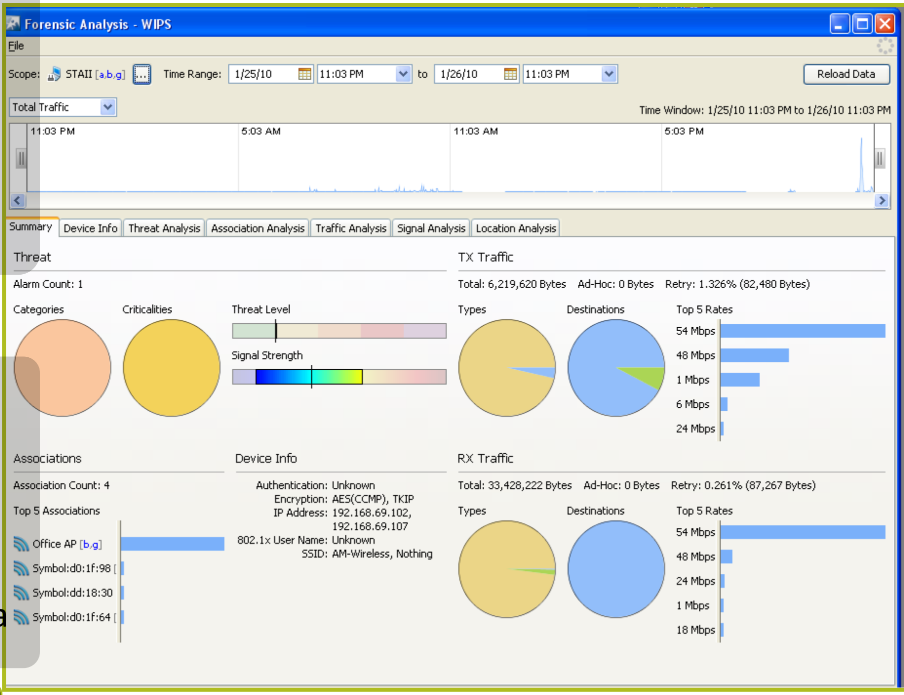
Record of Device Connectivity

Determine Exact Time & Impact of Security Incidents

Historical Data Storage

Benefits

- Understand Exposure From Transient Threats
- Reduces Need for 24/7 Staffing
- Simplifies Analysis of Large Volume of Data



Forensic Analysis - WIPS

Scope: STAII [a,b,g]   Time Range: 1/25/10 11:03 PM to 1/26/10 11:03 PM

Total Traffic

Time Window: 1/25/10 11:03 PM to 1/26/10 11:03 PM

Threat

Alarm Count: 1

TX Traffic

Total: 6,219,620 Bytes   Ad-Hoc: 0 Bytes   Retry: 1.326% (82,480 Bytes)

Associations

Association Count: 4

Device Info

Authentication: Unknown
Encryption: AES(CCMP), TKIP
IP Address: 192.168.69.102, 192.168.69.107
802.1x User Name: Unknown
SSID: AM-Wireless, Nothing

RX Traffic

Total: 33,428,222 Bytes   Ad-Hoc: 0 Bytes   Retry: 0.261% (87,267 Bytes)

Advanced Forensics Module Add-on:

- Adds Trend Analysis and Graphics
- Visual Representation of Incident Timeline
- Rewind & Review Detailed Wireless Activity

Forensic Summary

Comprehensive Visibility into Network Activity & Threats

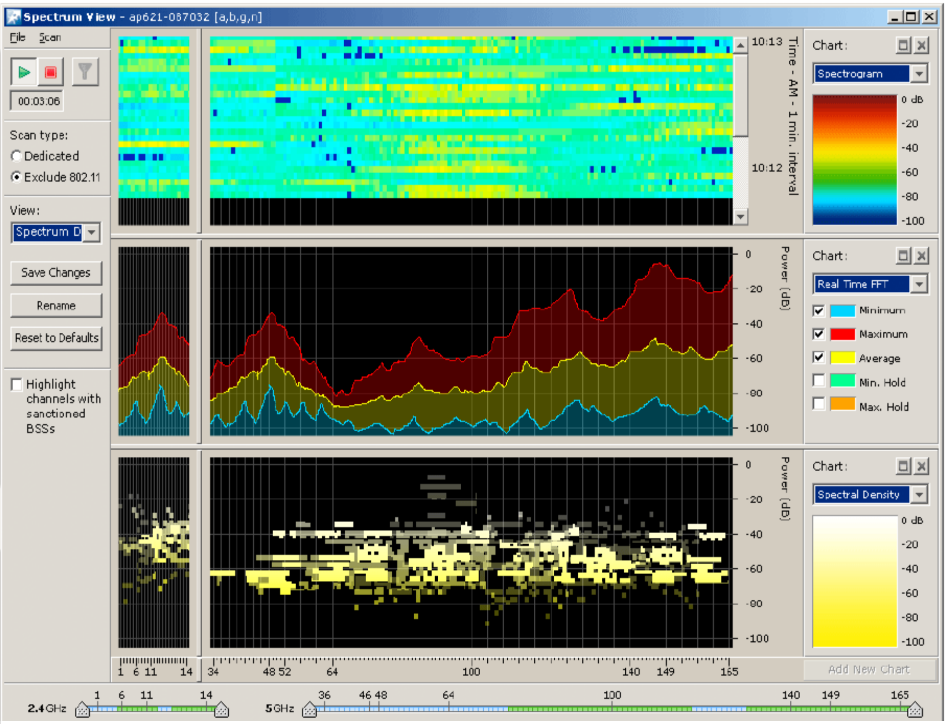
Physical Layer Troubleshooting

Spectrum Analysis Module

- Detect Non-802.11 Interference – Microwaves, Bluetooth, Frequency Hopping Devices, etc.
- 2.4 and 5 GHz Band Support
- Remote Real-time Spectrograms
- Use Existing Sensors – No Special Hardware Needed

Automated Interference Detection

- Proactive Detection of Application Impacting Interference
- Remote Real-Time Level1 Troubleshooting
- Improve Wireless Performance


Spectrum View - ap621-087032 [a,b,g,n]

Scan type:
○ Dedicated
● Exclude 802.11

View: Spectrum D

□ Highlight channels with sanctioned BSSs

Chart: Spectrogram

Chart: Real Time FFT
☑ Minimum
☑ Maximum
☑ Average
□ Min. Hold
□ Max. Hold

Chart: Spectral Density

Classify Interference Sources

Easily Identify the Source of Interference Problems

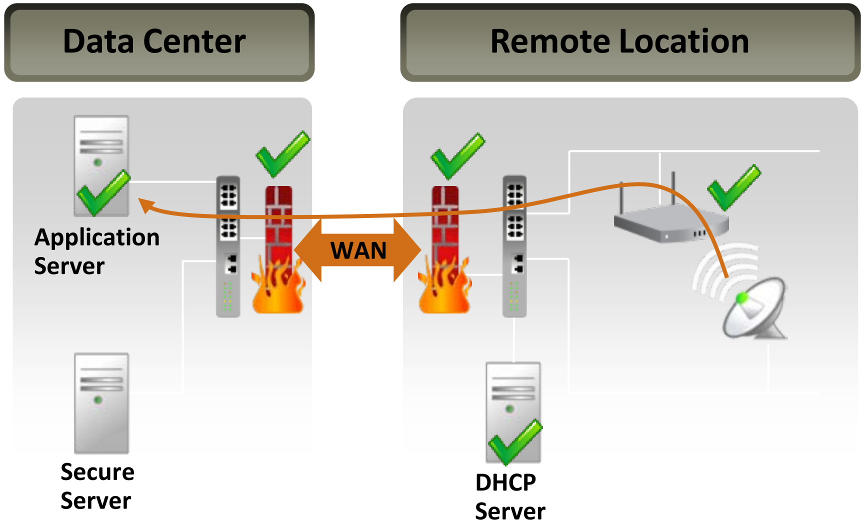
Proactive End to End Testing

AP Connectivity Test

- End-to-end Network Connectivity Testing from a Wireless Perspective
- Verify Access to Wireless Applications Servers
- Proactively Perform Network Tests

Benefits

- Find Problems Before End Users are Impacted
- Classify Network Issues – Know the Source of the Problem, Wired or Wireless
- Verify Remediation without Local Support
- Remote Testing Anywhere on the Network



Troubleshoot Wireless Connectivity without Onsite Resources

WLAN Analysis Tools

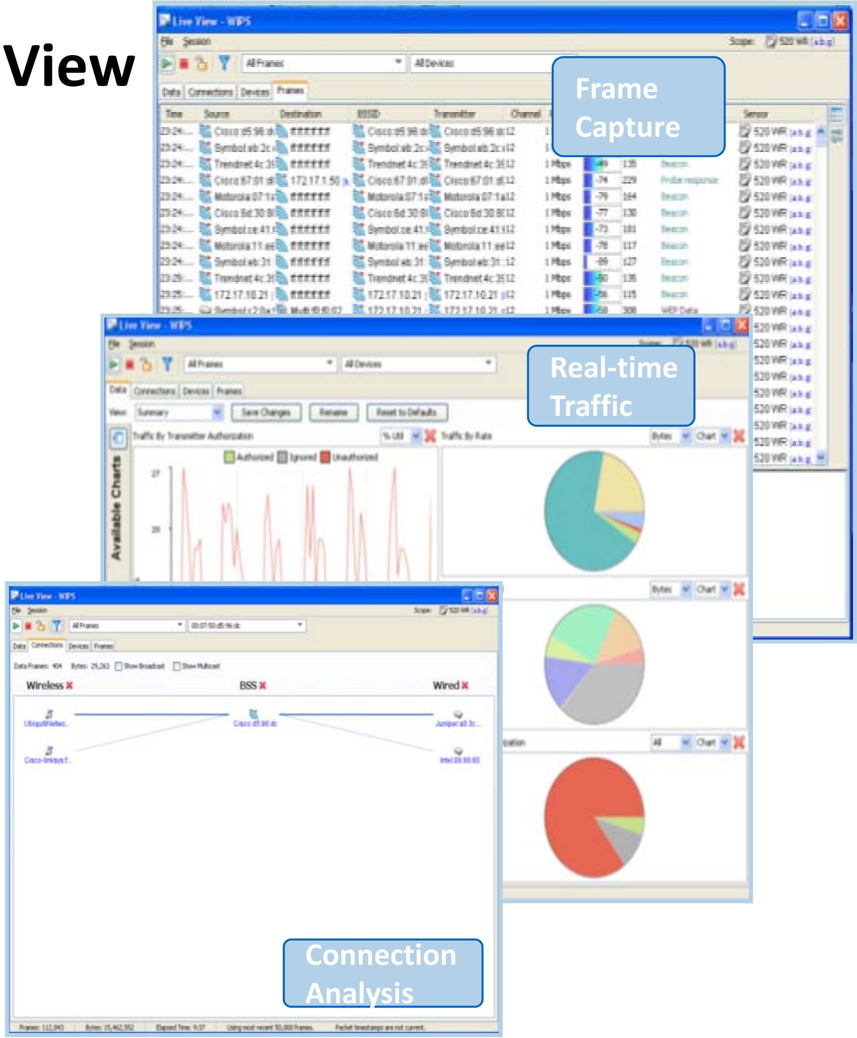
Remote Visibility with LiveView

Real-time View of WLAN

- Turn Any Sensor into a ‘Sniffer’
- Full Layer 2 Frame Capture
- Visualize Wireless Traffic Flow
- 28 Different Graphical Views

Low Network Support Costs

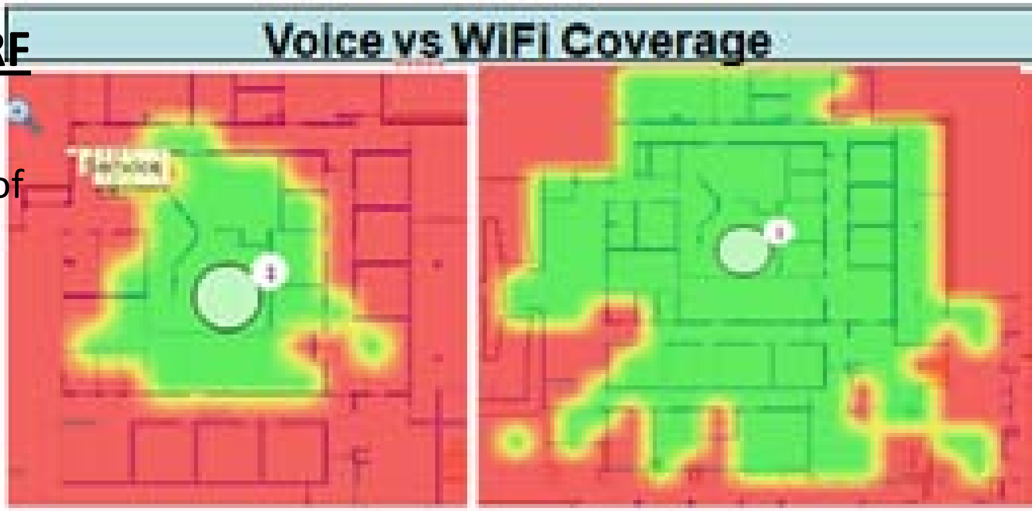
- Real-time View of Remote WLAN
- Advanced Centralized Troubleshooting
- Reduced On-site Support Cost
- Increased WLAN Uptime



WLAN ANALYSIS TOOLS

Visualize Coverage with LiveRF

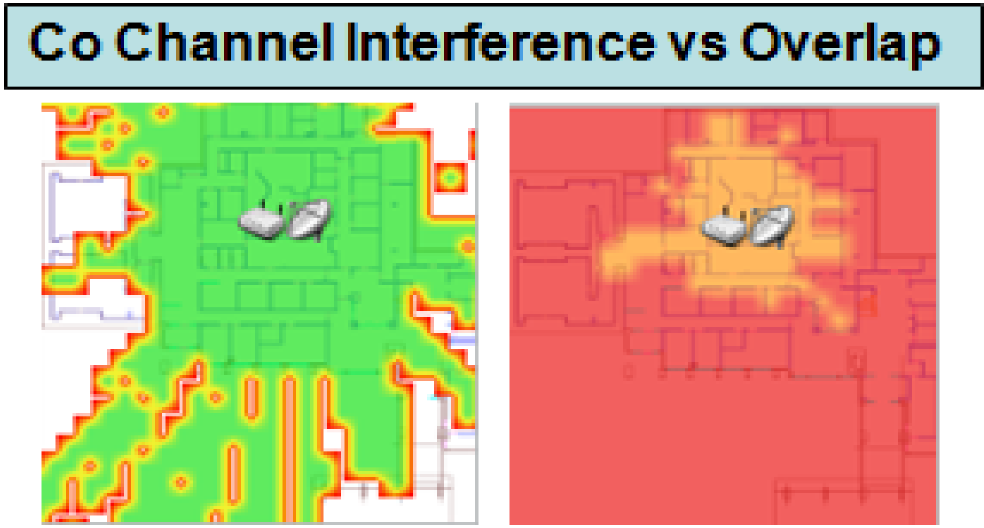
- Real-time RF Visualizations
- Proactive Monitoring and Alerting of Coverage Problems
- Application Specific Simulations – Voice, Video, Data, Custom
- Comparative Analysis of Current Environment to Known Healthy Environment



Voice vs WiFi Coverage

Enhance Network Reliability

- View Application Specific Coverage
- Detect and Remediate Problems Before End-user Effected
- See the Impact of Interference Sources
- Perform New Application Planning



Co Channel Interference vs Overlap

Questions