

## How I Hacked Your Wireless LAN (And how to stop me...)

### Disclaimer

- I *might* be smart enough to hack your wireless LAN, but I don't have time. I work for Aruba and have an 2 year old child to chase around. Don't blame me.



## Is This How You Think About Wireless?



The truth:  
Wireless is **MORE**  
secure than wired

(if you do it right)

**ARUBA**  
networks



## Wired Network Security Questions

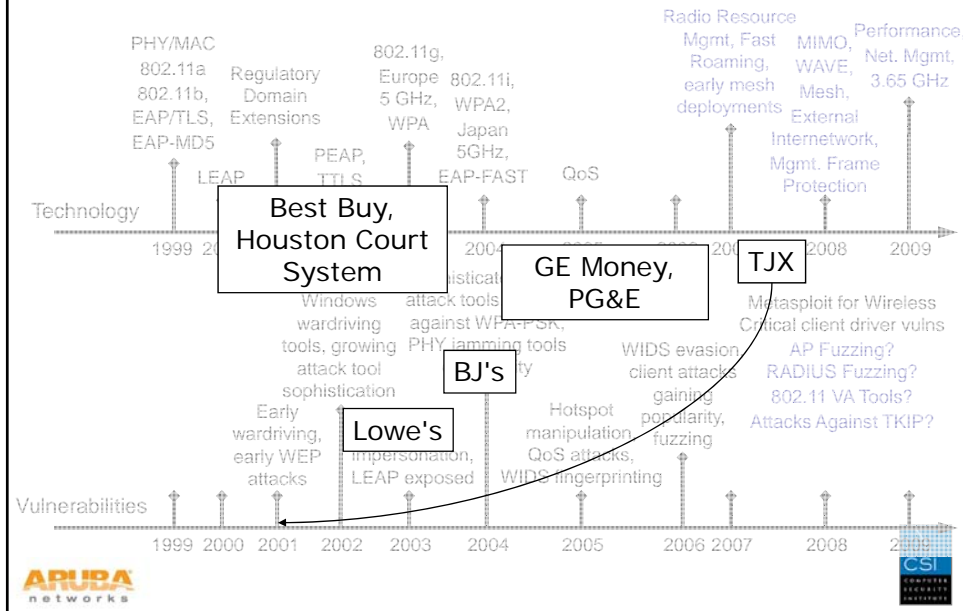
On your wired network...

- Do you **authenticate** all users and devices?
- Do you **encrypt** all traffic?
- Do you **control access** to network resources based on user identity?
  
- Wireless lets you do all of this – by design

**ARUBA**  
networks



## 802.11 Technology and Vulnerabilities



How NOT to Deploy Wireless!

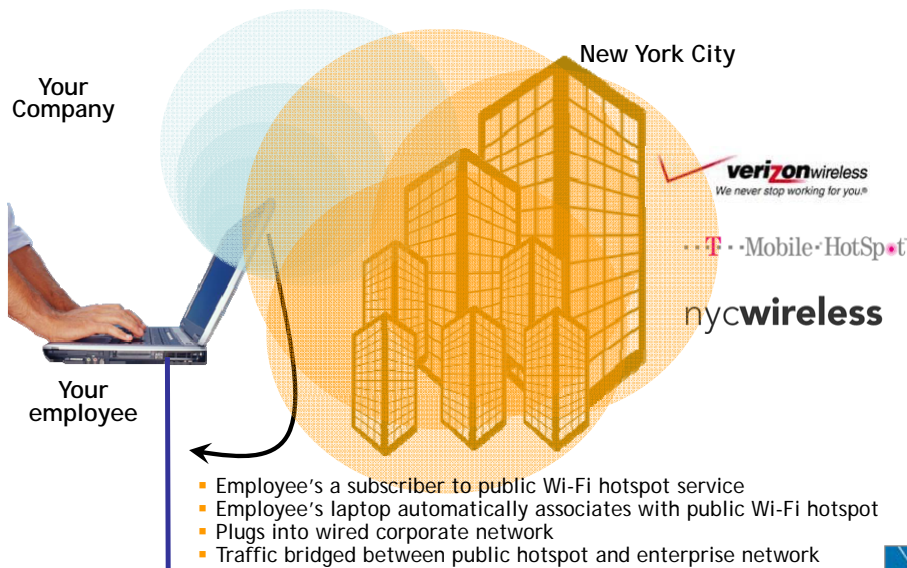


## Doing Nothing

- Wireless LAN equipment is cheap and easily available
  - If the IT department doesn't deploy wireless, someone else will
- Where is the "security perimeter" today?
- How do you enforce "No Wireless" policies?

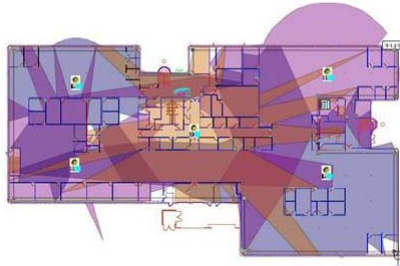


## What if we ignore wireless?



## RF Engineering

- Using directional antennas to direct and limit RF coverage does not work
  - RF is invisible
  - Physical environments change
- Lowering transmit power or placing access points (APs) away from outside walls to limit RF “leakage” does not work
- Set RF coverage to optimize user experience – not to control leakage



## SSID Cloaking

- Some APs offer a feature to hide the SSID (Service Set Identifier or “wireless network name”) in advertisements
- Hiding the SSID can *discourage* but cannot *secure*
- A person intent on network intrusion can run a simple tool to instantly reveal the SSID
  - The SSID should *never* be treated as though it were a password



## Discovering Cloaked SSIDs

```
linux:~# ./essid_jack -h
```

Essid Jack: Proof of concept so people will stop calling an ssid a password.

```
Usage: ./essid_jack -b <ssid> [-d <destination mac> ] [-c <channel number> ] [-i  
ccc.gif <interface name> ]
```

-b: bssid, the mac address of the access point (e.g. 00:de:ad:be:ef:00)

-d: destination mac address, defaults to broadcast address.

-c: channel number (1-14) that the access point is on, defaults to current.

-i: the name of the AirJack interface to use (defaults to aj0).

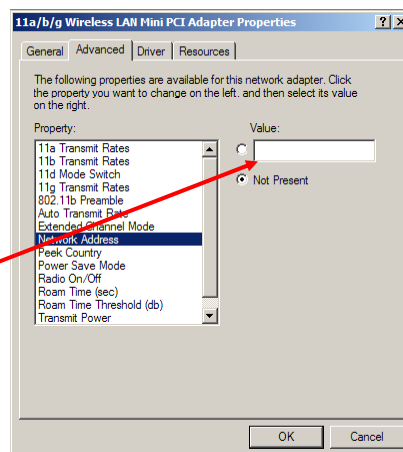
```
linux:~# essid_jack -b 00:03:2d:de:ad: -c 11
```

Got it, the ssid is (escape characters are c style):

```
"s3kr1t_wl4n"
```

## MAC Address Filtering

- Some APs offer "MAC address filtering"
- Does not scale to large networks
- Trivial to defeat



## WEP

- WEP stands for “Wired Equivalent Privacy”
- Badly broken
- Static versus Dynamic WEP
  - Static WEP: everyone uses the same key, all the time
  - Dynamic WEP: everyone uses a different key, assigned at each authentication
- Static WEP is **evil**. Avoid it.
- Dynamic WEP is slightly better, but it is still WEP



## Attacking WEP - Aircrack

- Goal: Capture frames with weak IVs (Initialization Vectors)
- Need 50K-200K frames for 64-bit key, 200K-700K for 128-bit key

```
E:\Software\aircrack-ng-0.6.2-win\bin\aircrack-ng.exe 0205ch11.cap
Opening 0205ch11.cap
Read 794434 packets.

# BSSID          ESSID          Encryption
1 00:09:58:31:84:34 zodiac         WEP (238036 IVs)
2 00:14:8E:F4:A7:82 mountainhouse WEP (31 IVs)
3 00:0F:B5:6C:5C:E6 PADAM          WEP (31 IVs)
4 00:0F:83:1E:1E:82 FRA_wi13t45_  No data - WEP or WPA
5 00:19:E4:12:5A:B1 2w1R4402     No data - WEP or WPA

Index number of target network ? 1
```

```
Aircrack-ng 0.6.2
[00:00:07] Tested 4688 keys (got 238036 IVs)

KB  depth  byte(vote)
0  0/ 1  3f( 42) 16( 13) 10( 12) c2( 12) f1( 7) 0a( 3) 3c( 3)
1  0/ 1  89( 103) 35( 16) e1( 15) 8a( 13) a6( 12) 44( 5) 68( 4)
2  0/ 6  35( 20) 77( 15) 16( 15) 86( 12) 78( 12) d8( 10) 10( 5)
3  0/ 1  70( 31) e0( 15) 38( 12) 0a( 5) 01( 5) 89( 5) 71( 5)
4  0/ 1  60( 58) 40( 13) f4( 12) 30( 5) d1( 5) ba( 5) 41( 5)
5  2/ 4  2a( 22) 15( 18) 0c( 8) 18( 6) 91( 6) f6( 6) 3f( 5)
6  0/ 1  dc( 69) 89( 26) 91( 17) ee( 10) 8c( 6) 6a( 5) 3d( 5)
7  0/ 1  f2( 258) 72( 73) a1( 41) 04( 32) 0b( 23) 79( 20) 02( 19)
8  0/ 1  84( 188) fc( 28) c3( 20) e1( 20) ab( 19) da( 18) 53( 18)
9  0/ 5  85( 28) 16( 19) 11( 18) 75( 15) 18( 15) 2f( 13) 68( 13)
10 0/ 1  60( 196) 72( 15) 24( 13) fd( 13) 0f( 12) 84( 10) 66( 7)
11 0/ 3  27( 39) 04( 23) cf( 23) f5( 17) dc( 11) 63( 10) 44( 10)

KEY FOUND! [ 57:b9:33:70:60:2a:dc:f2:88:b5:60:27:4e ]

E:\Software\aircrack-ng-0.6.2-win\bin>
```



## Attacking WEP – Speeding things up

- Use “void11” to deauthenticate clients from the WLAN, then let them reassociate – this generates valid data traffic
  - But this interferes with normal WLAN operation – people will notice
- Use “Aireplay”
  - Capture a valid ARP packet
  - Replay it to the WLAN over and over
  - Generate lots of frames
- Result:
  - 64-bit keys cracked in ~5 minutes
  - 128-bit keys cracked in ~10 minutes.



## Cisco LEAP

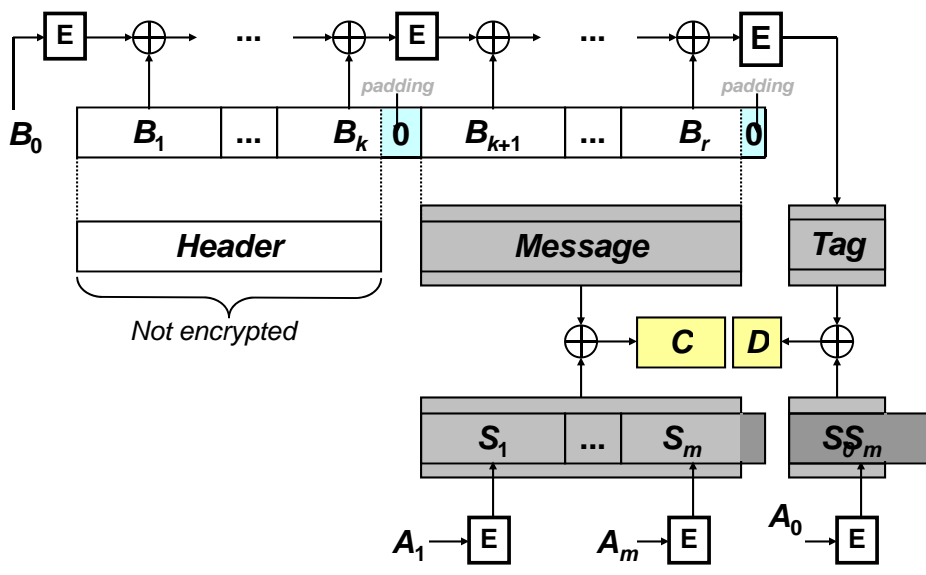
- Cisco invented LEAP to solve key distribution problems
- Vulnerable to dictionary attacks
- LEAP cracking tool is called ASLEAP
- Currently considered broken and unsuitable for use



# How to Stop Me

Let's start here...

## AES-CCMP Block Diagram



## A Layered Approach to Wireless Security

### PROTECTING THE USER

Stateful Per User Firewalls

### PROTECTING THE CONNECTION

Per-Packet Authentication, Centralized Encryption

### PROTECTING THE NETWORK

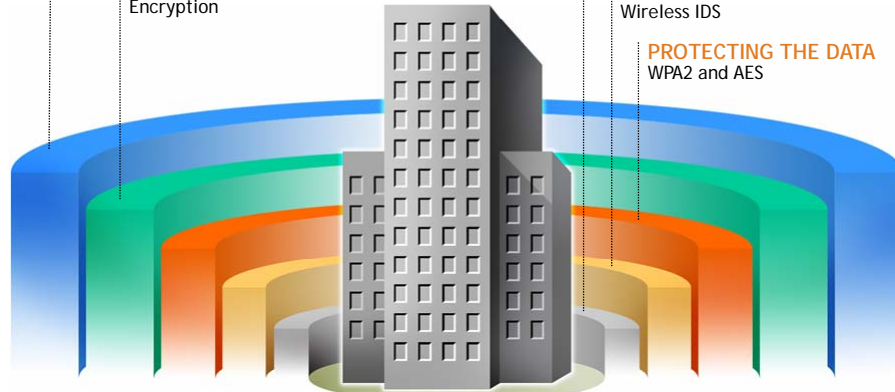
Strong Authentication

### PROTECTING THE AIR

RF Spectrum Security  
Wireless IDS

### PROTECTING THE DATA

WPA2 and AES



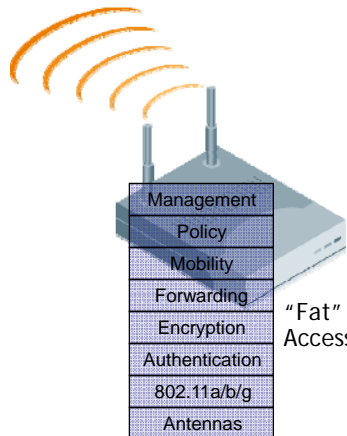
Enterprise Assets

ARUBA  
networks

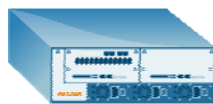
CSI  
CORPORATE  
SECURITY  
INSTITUTE

## Centralization is the First Step

Centralization solves security *and* TCO for WLANs



"Fat"  
Access Points



Centralized  
Mobility Controller



"Thin"  
Access Points

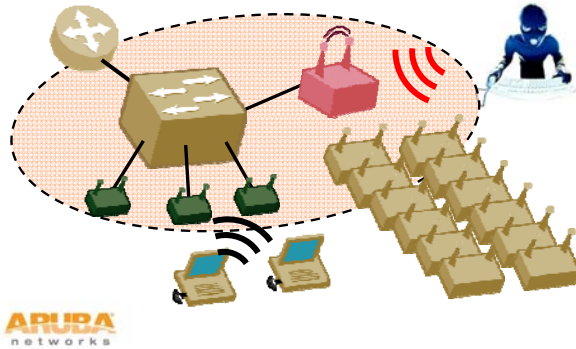
ARUBA  
networks

CSI  
CORPORATE  
SECURITY  
INSTITUTE

# Controlling "Uncontrolled Wireless"

AP Type	Manufacturer	Radio	Channel	SSID	BSSID	Clients	Last Seen	Status
WVLD	Aruba Networks	802.11a	34	aruba-ap	00:0b:3c:91:66:00	0	15:12:51 6/10/2004	up
WVLD	Aruba Networks	802.11a	34	aruba-ap	00:0b:3c:91:77:80	0	15:12:50 6/10/2004	up
WVLD	Melco Inc.	802.11g	11	000740GAD7L	00:07:40:54:60:00	0	19:25:26 6/17/2004	up
WVLD	Aruba Networks	802.11a	34	JACK	00:0b:3c:90:26:88	0	18:28:34 6/17/2004	up
WVLD	Aruba Networks	802.11a	34	JACK	00:0b:3c:90:21:48	0	12:10:48 6/15/2004	up
ROGUE	Cisco Systems	802.11b	6	cisco-test	00:0b:0e:15:7:5d	0	15:38:04 6/14/2004	up
WVLD	Melco Inc.	802.11a	6	vomato	00:07:40:5a:0b:0e	0	11:03:54 6/14/2004	up
WVLD	Aruba Networks	802.11b	1	demo-open	00:0b:3c:91:66:00	0	15:49:27 6/11/2004	up
WVLD	Aruba Networks	802.11b	1	demo-wep	00:0b:3c:91:66:d1	0	15:49:27 6/11/2004	up
WVLD	Aruba Networks	802.11g	1	laurel	00:0b:3c:80:80:e0	0	15:49:27 6/11/2004	up

- AP detection
- See all APs
- AP classification
- Are they neighbors?
- Or are they a threat?



- Rogue containment
- Stop users from accessing rogue APs and leave neighbors alone



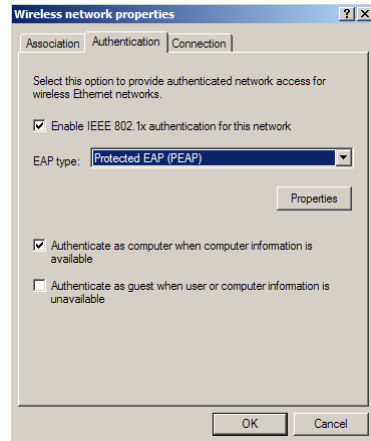
# Wireless Intrusion Detection/Protection

<p><b>IDS: Node Rate Anomaly</b></p> <p>Node=00:04:12:35:e6:14 PktCount=51 RSSI=63</p> <p>IDS: Node Rate Anomaly</p> <p>An anomaly has been detected for a frame rate for a node. This could indicate a flood attack at/from the node.</p>	<p><b>IDS: Disconnect Station Attack</b></p> <p>SrcMAC=00:0b:86:80:34:40 RSSI=56 DeauthSeq=163</p> <p>NormalSeq=3593 Pkt=7 Seq=10</p> <p>IDS: Disconnect Station Attack</p> <p>An attempt to disconnect a station by spoofing either the Deauth, Auth, Disassoc or Reassoc frames, has been detected.</p>	<p><b>IDS: Signature Match</b></p> <p>SignatureName="NetStumbler Generic"</p> <p>Src=00:00:00:00:aa:01 Dst=00:00:00:aa:01 Bssid=00:00:00:00:aa:01 Channel=6 RSSI=53</p> <p>IDS: Signature Match</p> <p>A match with one of the configured signatures has been detected.</p>
<p><b>IDS: Signature Match</b></p> <p>SignatureName="Deauth-Broadcast"</p> <p>Src=00:0b:86:80:34:40 Dst=ff:ff:ff:ff:ff:ff Bssid=00:0b:86:80:34:40 Channel=6 RSSI=71</p> <p>IDS: Signature Match</p> <p>A match with one of the configured signatures has been detected.</p>	<p><b>IDS: Channel Rate Anomaly</b></p> <p>PacketCount=14</p> <p>IDS: Channel Rate Anomaly</p> <p>A frame rate anomaly is detected for a channel. This could indicate a flood attack on a channel.</p>	<p><b>IDS: Signature Match</b></p> <p>SignatureName="Linksys-defaultssid"</p> <p>Src=00:00:00:00:aa:01 Dst=ff:ff:ff:ff:ff:ff Bssid=00:00:00:00:aa:01 Channel=6 RSSI=54</p> <p>IDS: Signature Match</p> <p>A match with one of the configured signatures has been detected.</p>
<p><b>IDS: Signature Match</b></p> <p>SignatureName="Wellenreiter" Src=00:00:00:00:aa:01 Dst=ff:ff:ff:ff:ff:ff Bssid=00:00:00:00:aa:01 Channel=6 RSSI=58</p> <p>IDS: Signature Match</p> <p>A match with one of the configured signatures has been detected.</p>	<p><b>IDS: Wireless Bridge Detected</b></p> <p>Channel=6 Transmitter=00:00:00:00:00:00:01 Receiver=00:00:00:00:00:00:01 Destination=00:00:00:00:aa:01 RSSI=57</p> <p>IDS: Wireless Bridge Detected</p> <p>AP-AP communication has been detected.</p>	<p><b>IDS: Signature Match</b></p> <p>SignatureName="AirJack" Src=00:0b:86:80:34:40 Dst=ff:ff:ff:ff:ff:ff Bssid=00:0b:86:80:34:40 Channel=6 RSSI=74</p> <p>IDS: Signature Match</p> <p>A match with one of the configured signatures has been detected.</p>
<p><b>IDS: Signature Match</b></p> <p>SignatureName="Null-Probe-Response"</p> <p>Src=00:0b:86:80:34:40 Dst=00:04:12:35:e0:4a Bssid=00:0b:86:80:34:40 Channel=11 RSSI=57</p> <p>IDS: Signature Match</p> <p>A match with one of the configured signatures has been detected.</p>	<p><b>IDS: Fake AP Flood Detected</b></p> <p>SpuriousAPCount=1</p> <p>IDS: Fake AP Flood Detected</p> <p>A number of spurious APs have been detected in the vicinity.</p>	<p><b>IDS: EAP Handshake Rate Anomaly</b></p> <p>Channel=6 PktCount=10</p> <p>IDS: EAP Handshake Rate Anomaly</p> <p>A anomalous number of EAP handshakes have been seen on a channel. This could indicate that a station is under a DOS attack.</p>
<p><b>IDS: Sequence Number Anomaly</b></p> <p>MAC=00:0b:86:80:34:40 RSSI=83 Seq1=107 Seq2=0</p> <p>NormalSeq=10</p> <p>IDS: Sequence Number Anomaly</p> <p>A sequence number anomaly has been detected for a node. This indicates MAC address spoofing, i.e., another machine is masquerading as this node.</p>	<p><b>AP Impersonation</b></p> <p>AP Impersonation</p> <p>A rogue in the middle attack tool like Air Jack is impersonating an access point.</p>	<p><b>IDS: Ad-hoc Network Detected</b></p> <p>Channel=11 Src=00:04:23:5c:e0:4a Dst=ff:ff:ff:ff:ff:ff RSSI=6</p> <p>IDS: Ad-hoc Network Detected</p> <p>A station has been seen in an ad-hoc network has been detected. The SSID of the network and the BSS used is available.</p>
<p><b>IDS: Signature Match</b></p> <p>SignatureName="NetStumbler Version 2.3.0x"</p> <p>Src=00:00:00:00:00:01 Dst=00:00:00:00:aa:01 Bssid=00:00:00:00:aa:01 Channel=6 RSSI=58</p> <p>IDS: Signature Match</p> <p>A match with one of the configured signatures has been detected.</p>		

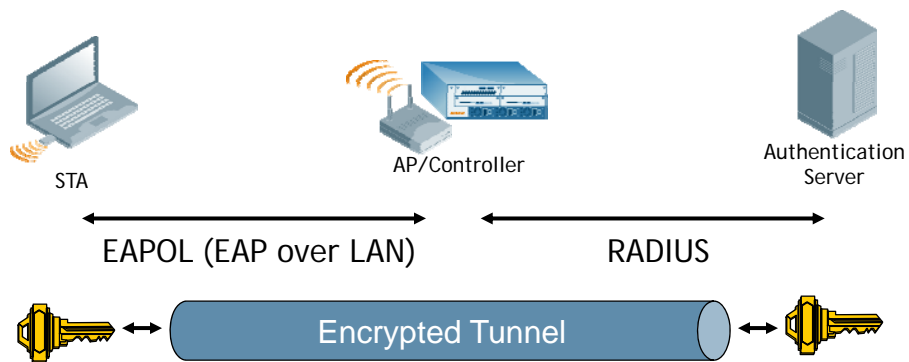


## Authentication with 802.1x

- Authenticates users before granting access to L2 media
- Makes use of EAP (Extensible Authentication Protocol) – evolved from PPP
  - PEAP, EAP-TLS, EAP-TTLS, etc.
- 802.1x authentication happens at L2 – users will be authenticated before an IP address is assigned



## Authentication with 802.1x



## 802.1x Acronym Soup

- PEAP (Protected EAP)
  - Uses a digital certificate on the network side
  - Password or certificate on the client side
- EAP-TLS (EAP with Transport Level Security)
  - Uses a certificate on network side
  - Uses a certificate on client side
- TTLS (Tunneled Transport Layer Security)
  - Uses a certificate on the network side
  - Password, token, or certificate on the client side
- EAP-FAST
  - Cisco proprietary
  - Do not use – known security weaknesses



## Encrypt the Data

- If intruders can't read the data, there's no need to worry where it goes
  - WEP
    - Encryption using RC4
    - Simple to do, easy to crack
    - No key management
    - **Don't do it**
  - TKIP (Temporal Key Integrity Protocol)
    - Encryption using RC4
    - Works on legacy hardware
    - No major weaknesses known
  - CCMP/AES
    - Encryption using AES
    - Considered state-of-the-art
    - FIPS 140-2 approved
    - May require new hardware



## Combining Authentication & Encryption: WPA

- WPA == Wi-Fi Protected Access
- WPA
  - Wi-Fi Alliance "standard" based on pre-802.11i
  - Includes TKIP for encryption
- WPA2
  - Wi-Fi Alliance "standard" based on ratified 802.11i
  - Includes TKIP and CCMP for encryption
- For both:
  - WPA-Enterprise == 802.1x for authentication, dynamic encryption
  - WPA-Personal == pre-shared authentication key

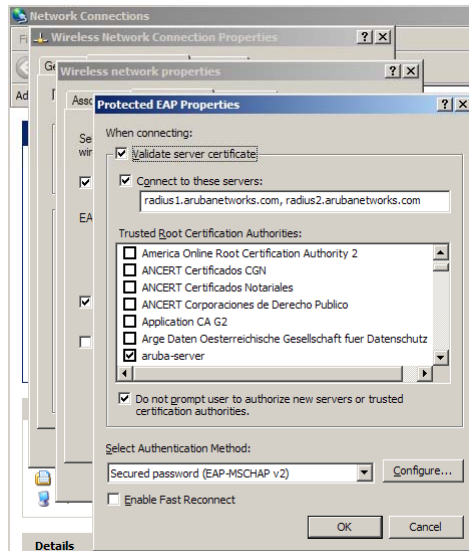


## Pre-Shared Key Authentication Cannot Scale

- WPA/WPA2 accommodates authentication using IEEE 802.1X or a pre-shared key
  - PSK authentication is "WPA-Personal", 802.1X is "WPA-Enterprise"
- WPA-Personal is deployed without the complexity of IEEE 802.1X, no EAP type configuration
  - Attractive to deploy, but insecure
- Like WEP, PSK authentication is weak and cannot scale
  - Subject to offline dictionary attacks
  - A stolen/lost device with PSK mandates rotation of all PSK's throughout the organization
  - How many people require knowledge of the key?
  - Is the key stored on laptops accessible to users?



## Configure WPA Properly



- Configure the Common Name of your RADIUS server (matches CN in server certificate)
- Configure trusted CAs (an in-house CA is better than a public CA)
- ALWAYS validate the server certificate
- Do not allow users to add new CAs or trust new servers
- Enforce with group policy



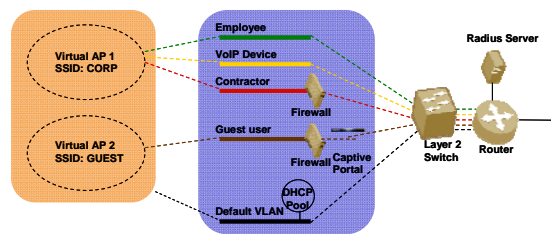
## Captive Portals

- Browser-based authentication
- SSL encrypted
- Permits registered user or guest access
- No inherent link-layer encryption
- Use with caution!



## Authorize the Data

- Most organizations do a decent job of authentication (who the user is), but a poor job of authorization (what the user is allowed to do)
- Mobile networks are typically multi-use
- Authentication provides you with user identity – *now use it!* Identity-aware firewall policies can restrict what a user can do, based on that user's needs

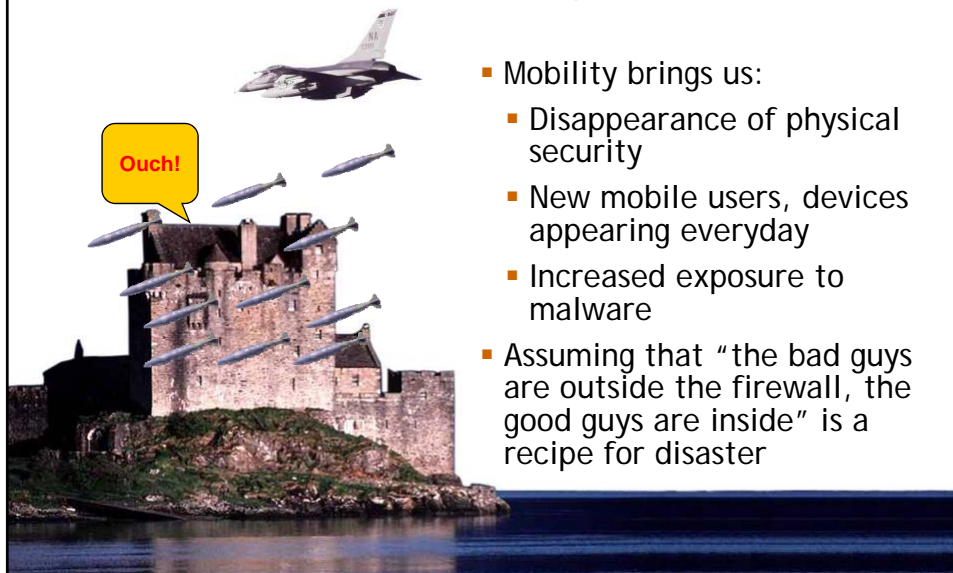


ARUBA  
networks

CSI  
COMPUTER  
SECURITY  
INSTITUTE

## Why Worry About Authorization?

Where is the "network perimeter" today?



- Mobility brings us:
  - Disappearance of physical security
  - New mobile users, devices appearing everyday
  - Increased exposure to malware
- Assuming that "the bad guys are outside the firewall, the good guys are inside" is a recipe for disaster

## Today's Wireless Gold Standard

- Centralized wireless
- Keep clients updated – drivers too!
- Wireless intrusion detection
  - Control uncontrolled wireless
  - Locate and protect against rogue APs
- WPA-2
  - Device authentication using 802.1x and PEAP
  - User authentication using 802.1x and PEAP
  - AES for link-layer encryption
- Strong passwords
  - SecureID or other token-card products
  - Strong password policies
- Authorization with identity-aware firewalls
  - Protect wireless users from other wireless users
  - Another layer of defense



What's Left?



## Attacking Preferred Networks List (PNL)

- Multiple tools to abuse preferred network list on clients
  - Hotspotter
  - RawGlueAP
  - KARMA
- When and how stations roam still driver-implementation dependent
- Can be abused by attackers



## KARMA

- Listens for probes in monitor mode
- Becomes AP for all probed networks
- Includes extensive support for fake services to manipulate client connectivity (XML)
  - Fake SMB, FTP, HTTP
- Bring Your Own eXploit (BYOX) model

"... a number of client-side exploits have been written, tested and demonstrated within this framework. Some may be included in a future release. Automated agent deployment is also planned."

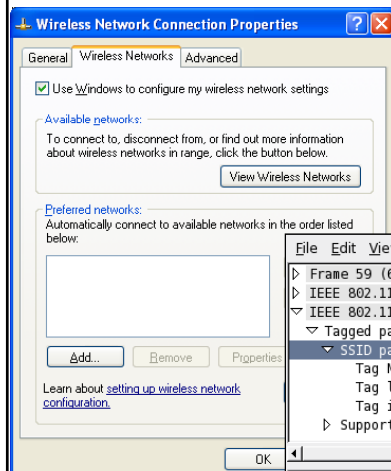


## KARMA Example

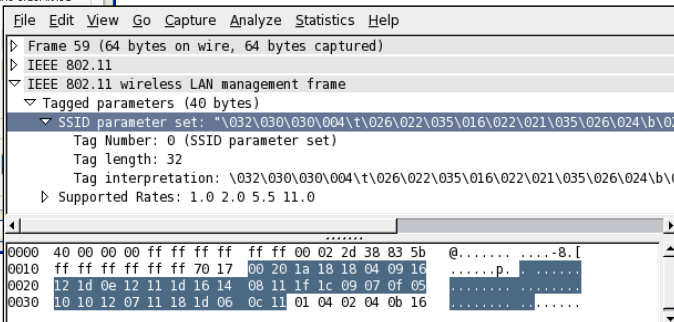
```
[root@wirelessdefence karma-0.4]# bin/karma etc/karma.xml
Starting KARMA...
Loading config file etc/karma.xml
ACCESS-POINT is running
DNS-SERVER is running
DHCP-SERVER is running
POP3-SERVER is running
FTP-SERVER is running
[2006-01-20 22:43:58] INFO WEBrick 1.3.1
[2006-01-20 22:43:58] INFO ruby 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 (dell15150) <- 169.254.0.254
DNS: 169.254.0.254.1128: 22333 IN::A www.mysecretwebsite.com
FTP: 169.254.0.254 myusername/mypassword
```



## Windows XP PNL Weakness



- Empty PNL, XP still probes with uninitialized memory contents as SSID
- Will associate to networks using this SSID, no popup notification



## Client Drivers

- Basic secure programming rule: Sanitize all user input
- “Fuzzing” attacks send random data to software inputs
  - Stuff that comes in over the air is user input
- 802.11n is around the corner – lots of new driver software going into production
  - Are these well written? Well tested? Secure?

### MOKB-11-11-2006: Broadcom Wireless Driver Probe Response SSID Overflow

AA-2006.0090                      AUSCERT Advisory

[OSX]  
Public Exploit Code Available for AirPort Wireless Driver Vulnerability  
6 November 2006

-----  
AUSCERT Advisory Summary  
-----

Operating System:    Mac OS X  
Impact:                Denial of Service  
Access:                Remote/Unauthenticated  
Member content until: Monday, December 04 2006

OVERVIEW:

Public exploit code is available for a recently announced vulnerability [1][2] in the driver for Orinoco based AirPort cards.

“The Broadcom BCMWL5.SYS wireless device driver is vulnerable to a stack-based buffer overflow that can lead to arbitrary kernel-mode code execution. This particular vulnerability is caused by improper handling of 802.11 probe responses containing a long SSID field. The BCMWL5.SYS driver is bundled with new PCs from HP, Dell, Gateway, eMachines, and other computer manufacturers.



## Summary

- At a minimum, you *must* put measures in place to control “uncontrolled wireless”
- Wireless networks are more secure than the average wired network
  - But only when properly secured
- Wireless security has evolved rapidly in the past 4 years – tools and information are not common knowledge
  - Use vendors to help you – they live this every day





# Q & A

[jgreen@arubanetworks.com](mailto:jgreen@arubanetworks.com)

