Wireless Security

What Works and What Doesn't

Andy Logan, CWSP
alogan@arubanetworks.com

ARUBA networks

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

The Myths...

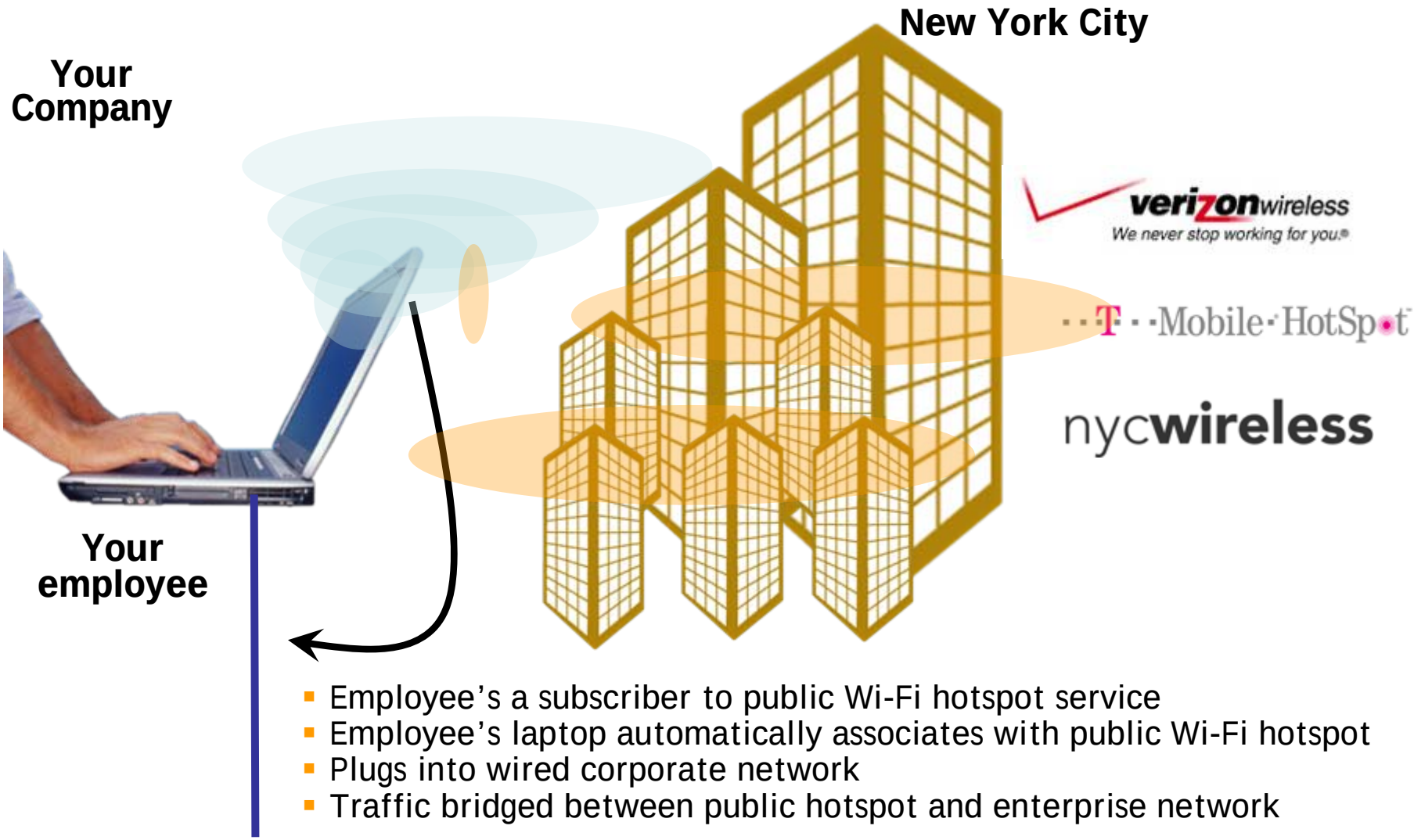
ARUBA networks

No Wireless Policies or Doing Nothing

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

ARUBA networks

The Existence of Wireless LANs is a Security Threat

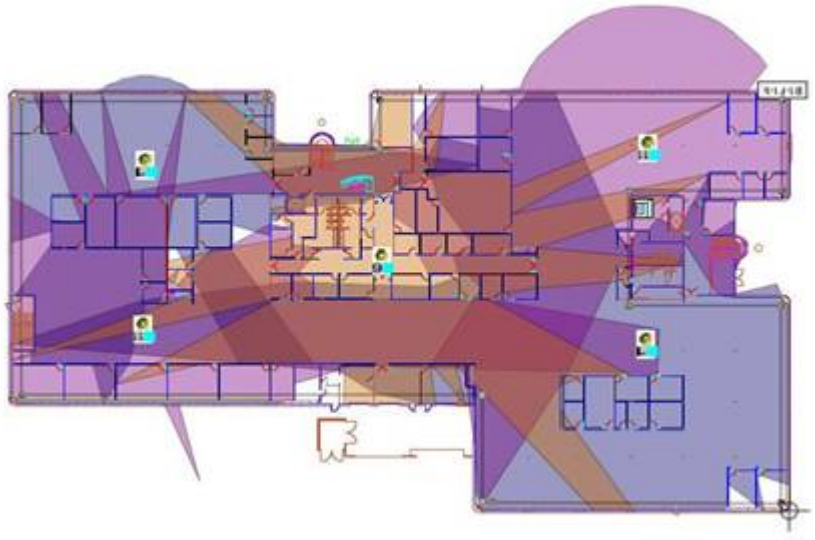


- Employee's a subscriber to public Wi-Fi hotspot service
- Employee's laptop automatically associates with public Wi-Fi hotspot
- Plugs into wired corporate network
- Traffic bridged between public hotspot and enterprise network

ARUBA networks

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



ARUBA networks

Defeating RF Engineering

http://www.oreillynet.com/lpt/wlg/448

SSID Cloaking

- Best practice?
  - “Configure APs to not broadcast the SSID”
- At best, this can *discourage* a bad guy
- At worst, this is downright dangerous
- The SSID is not the same as a password

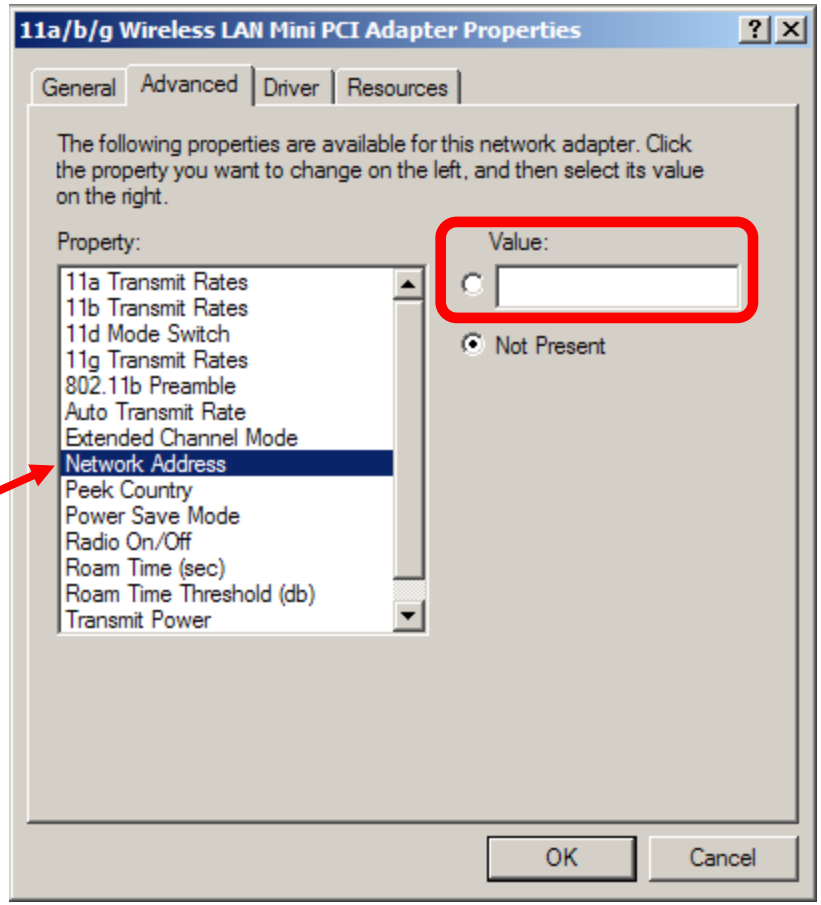
ARUBA networks

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 <bssid> [ -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 essid 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”
- Based on RC4
- Part of original 802.11 specification
- Horribly broken

Static or Dynamic WEP?

- Two different ways to use WEP:

- Static WEP: everyone uses the same key, all the time
- Dynamic WEP: everyone uses a different key, assigned at each authentication

Is WEP really that bad?

- Short answer: Yes.
- Static WEP is evil. Avoid it.
- Dynamic WEP is slightly better than static WEP, but it is still WEP

Feds Hack Wireless Network in 3 Minutes

Posted by CmdrTaco on Tue Apr 05, '05 12:26 PM
from the still-can't-balance-budget dept.

xs3 writes *At a recent ISSA (Information Systems Security Association) meeting in Los Angeles, a team of FBI agents demonstrated current WEP-cracking techniques and broke a 128 bit WEP key in about three minutes. Special Agent Geoff Bickers ran the Powerpoint presentation and explained the attack, while the other agents (who did not want to be named or photographed) did the dirty work of sniffing wireless traffic and breaking the WEP keys. This article will be a general overview of the procedures used by the FBI team.."*

ARUBA networks

Other things to Avoid...

- Cisco LEAP (vulnerable to dictionary attacks)
- EAP-FAST (doesn't securely provide mutual authentication)
- Use caution with WPA-Personal/WPA-PSK (more later...)
- "WEP Cloaking" (doesn't work)
- Proprietary "shielding" or "scrambling" (easy to defeat)
- Don't assume your "no wireless" policy means that you don't have wireless

ARUBA networks

Scan Your Network

- Turn on your Wi-Fi adapter and let your OS scan the environment where you work
  - You may be surprised at the number of networks your system will detect
- Download tools to help you audit your systems
  - http://www.netstumbler.com/downloads/
  - http://www.remote-exploit.org/backtrack.html

The Reality...

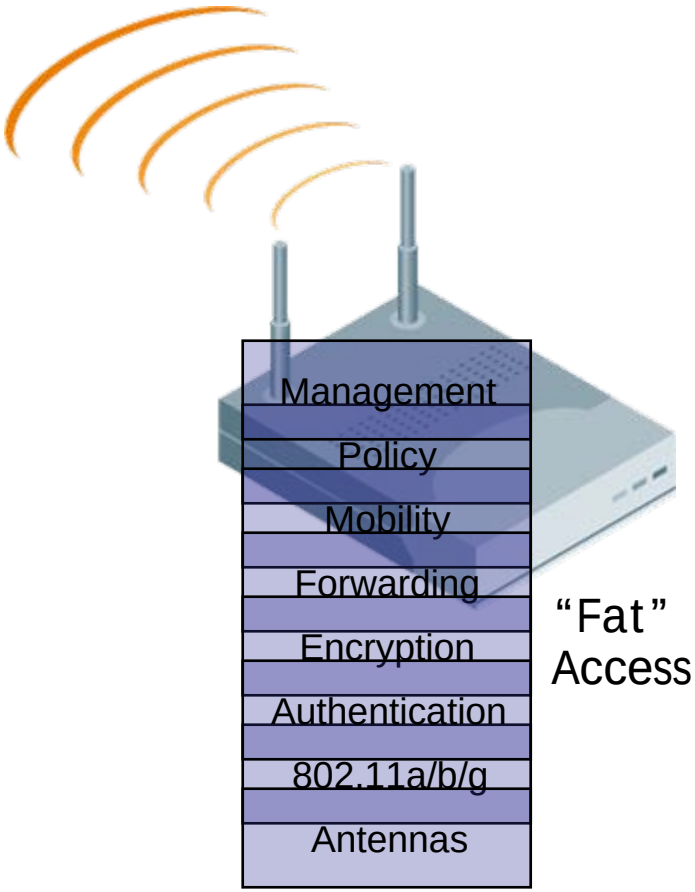
ARUBA networks

Key Security Principles

- Principle of Least Privilege
  - Authentication, identity-based security, firewalls
- Defense in Depth
  - Authentication, encryption, intrusion protection, client integrity
- Prevention is ideal, detection is a must
  - Intrusion detection systems, log files, audit trails, alarms and alerts
- Know Thy System
  - Integrated management, centralization

Centralization is the First Step

Centralization solves security *and* TCO for WLANs

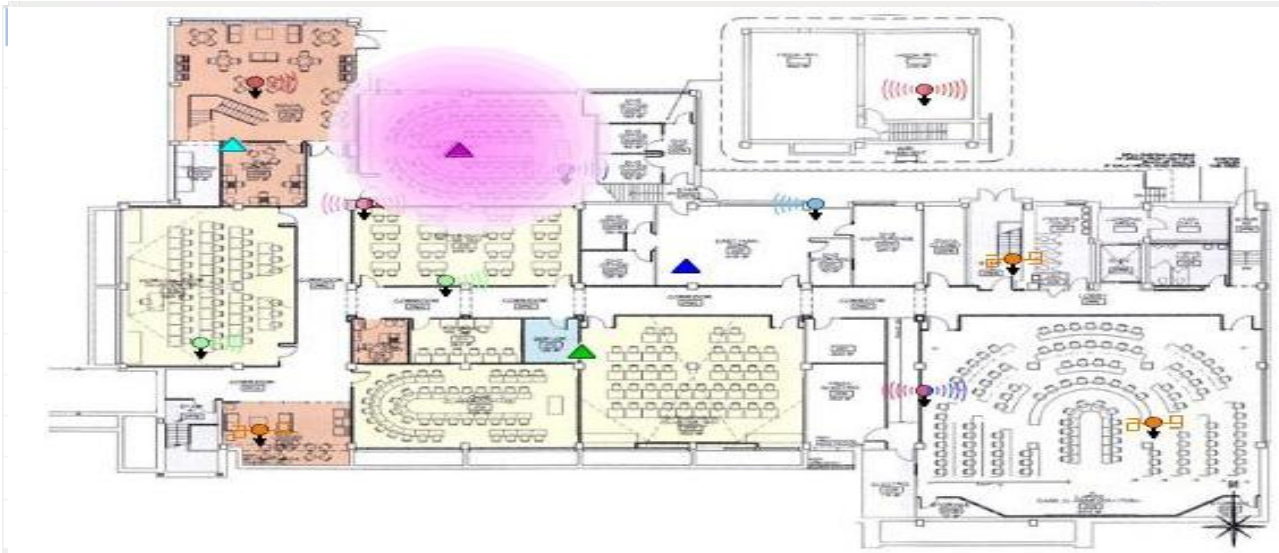


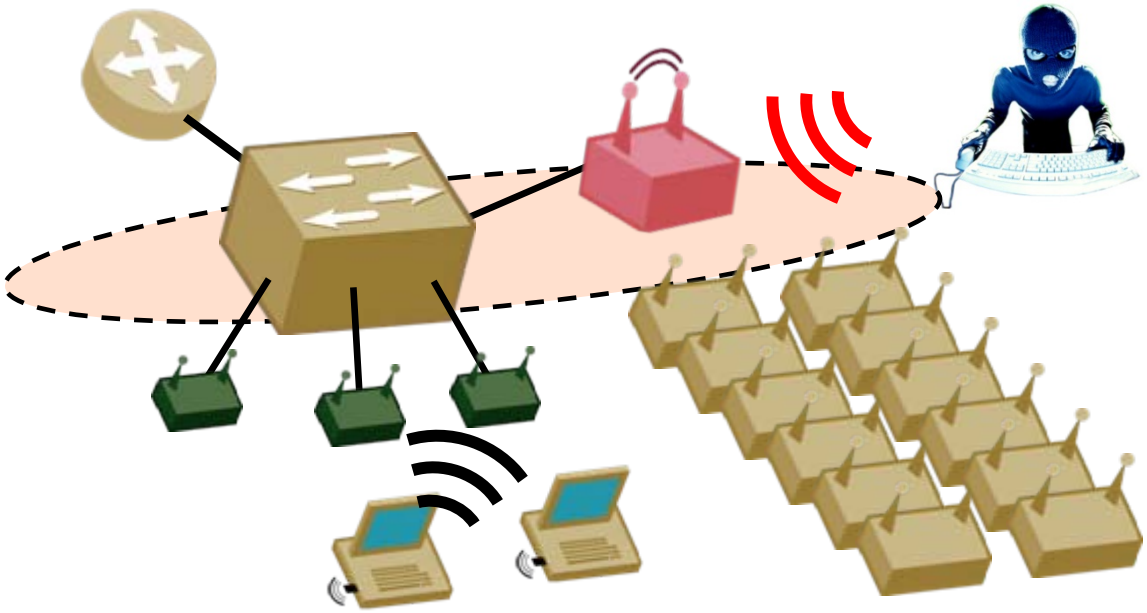
"Fat"
Access Points

Centralized
Mobility Controller

"Thin"
Access Points

Controlling Rogue APs





1. AP detection
- See all APs

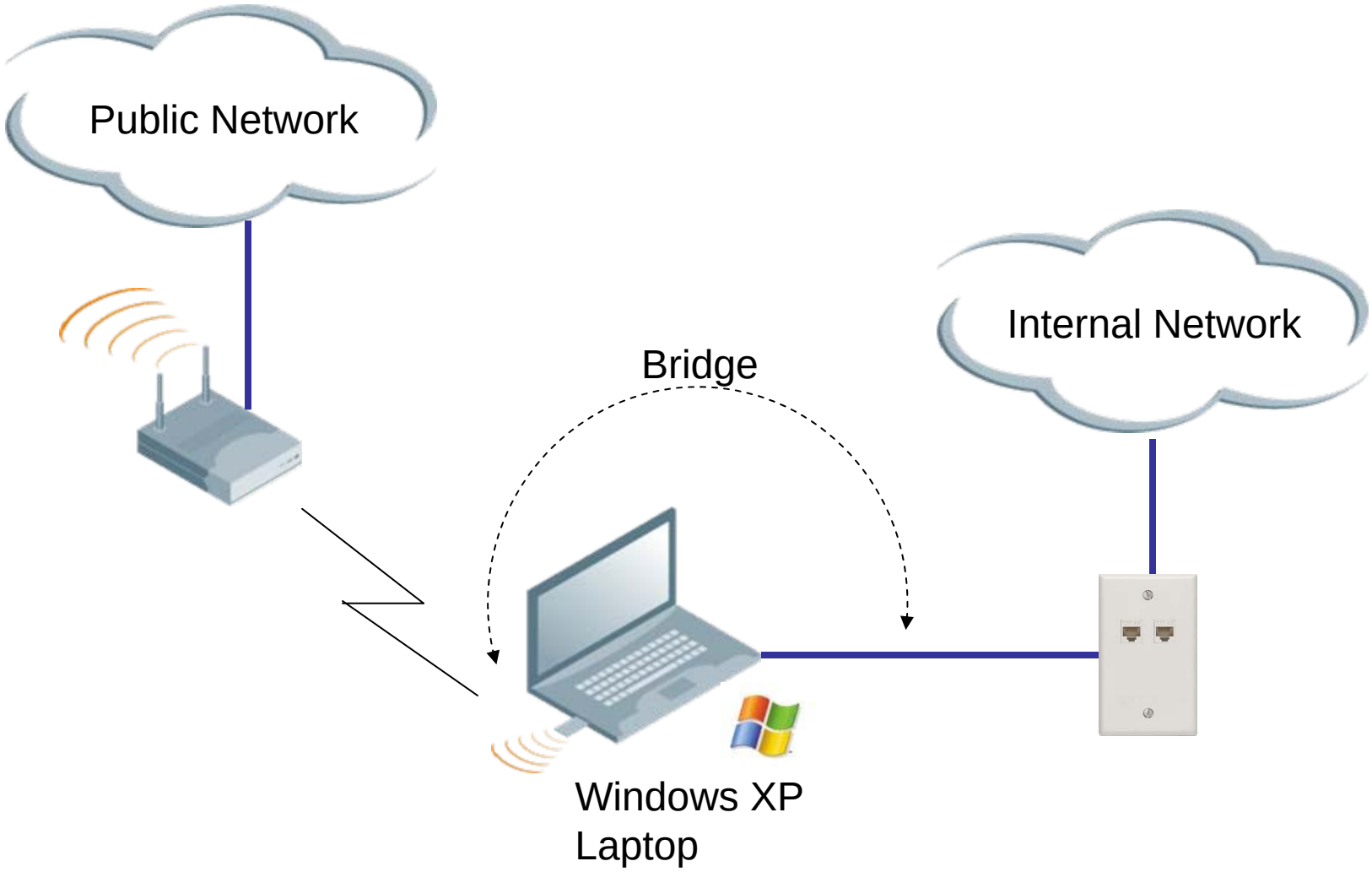
2. AP classification
- Are they neighbors?
- Or are they a threat?

3. Rogue containment
- Stop users from accessing rogue APs over the wire & over wireless
- Leave neighbors alone

4. Locate Rogue
- Find where it is and disconnect

ARUBA networks

Controlling Uncontrolled Wireless



Wireless Intrusion Detection/Protection

IDS: Node Rate Anomaly
Node=00:04:23:5c:e0:4a PktCount=51 RSSI=63
IDS: Node Rate Anomaly
An anomaly has been detected for a frame rate for a node. This could indicate a flood attack at/from the node.

IDS: Signature Match
SignatureName="Deauth-Broadcast"
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
IDS: Signature Match
A match with one of the configured signatures has been detected.

IDS: Signature Match
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
IDS: Signature Match
A match with one of the configured signatures has been detected.

IDS: Signature Match
SignatureName="Null-Probe-Response"
Src=00:0b:86:80:34:40 Dst=00:04:23:5c:e0:4a
Bssid=00:0b:86:80:34:40 Channel=11 RSSI=57
IDS: Signature Match
A match with one of the configured signatures has been detected.

IDS: Sequence Number Anomaly
MAC=00:0b:86:80:34:40 RSSI=83 Seq1=107 Seq2=0
MismatchCnt=10
IDS: Sequence Number Anomaly
A sequence number anomaly has been detected for a node. This indicates MAC address spoofing, i.e., another machine is masquerading as this node.

IDS: Disconnect Station Attack
SrcMAC=00:0b:86:80:34:40 RSSI=56 DeauthSeq=163
NormalSeq=3593 MC=7 SC=10
IDS: Disconnect Station Attack
An attack to disconnect a station by spoofing either the Deauth, Auth, Disassoc or Reassoc frames, has been detected.

IDS: Channel Rate Anomaly
PacketCount = 14
IDS: Channel Rate Anomaly
A frame rate anomaly is detected for a channel. This could indicate a flood attack on a channel.

IDS: Wireless Bridge Detected
Channel=6 Transmitter=00:00:00:00:00:01
Receiver=00:00:00:00:00:01
Destination=00:00:00:00:00:01 RSSI=57
IDS: Wireless Bridge Detected
AP-AP Communication has been detected.

IDS: Fake AP Flood Detected
Spurious APs = 60
IDS: Fake AP Flood Detected
A number of spurious APs have been detected in the vicinity.

AP Impersonation
AP Impersonation
A man in the middle attack tool like Air Jack is impersonating an access point.

IDS: Signature Match
SignatureName="NetStumbler Version 3.3.0x"
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
IDS: Signature Match
A match with one of the configured signatures has been detected.

IDS: Signature Match
SignatureName="NetStumbler Generic"
Src=00:00:00:00:00:01 Dst=00:00:00:00:aa:01
Bssid=00:00:00:00:aa:01 Channel=6 RSSI=53
IDS: Signature Match
A match with one of the configured signatures has been detected.

IDS: Signature Match
SignatureName="Linksys-defaultssid"
Src=00:00:00:00:00:aa:01 Dst=ff:ff:ff:ff:ff:ff
Bssid=00:00:00:00:aa:01 Channel=6 RSSI=54
IDS: Signature Match
A match with one of the configured signatures has been detected.

IDS: Signature Match
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
IDS: Signature Match
A match with one of the configured signatures has been detected.

IDS: EAP Handshake Rate Anomaly
Channel = 6 PktCount = 10
IDS: EAP Handeshake Rate Anomaly
A anomalous number of EAP handshakes have been seen on a channel. This could indicate that a station is under a DOS attack.

IDS: Ad-hoc Network Detected
Channel = 11 Src = 00:04:23:5c:e0:4a Dst = ff:ff:ff:ff:ff:ff
RSSI = 6
IDS: Ad-hoc Network Detected
A station that is part of an Ad-hoc network has been detected. The SSID of the network and the BSS used is available.

ARUBA networks

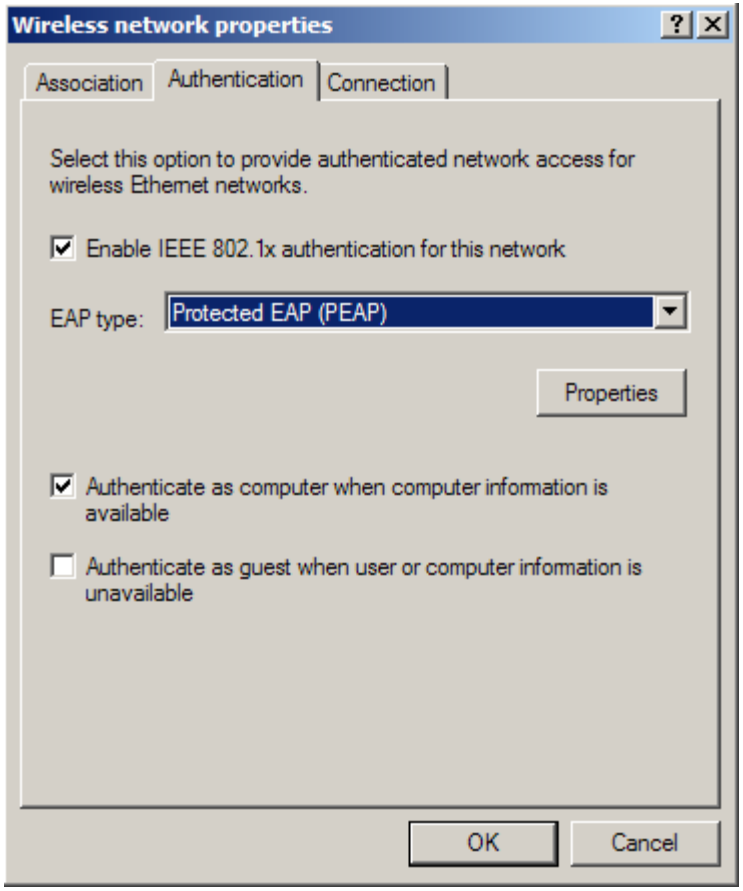
Why Worry About Authorization?

Where is the "network perimeter" today?

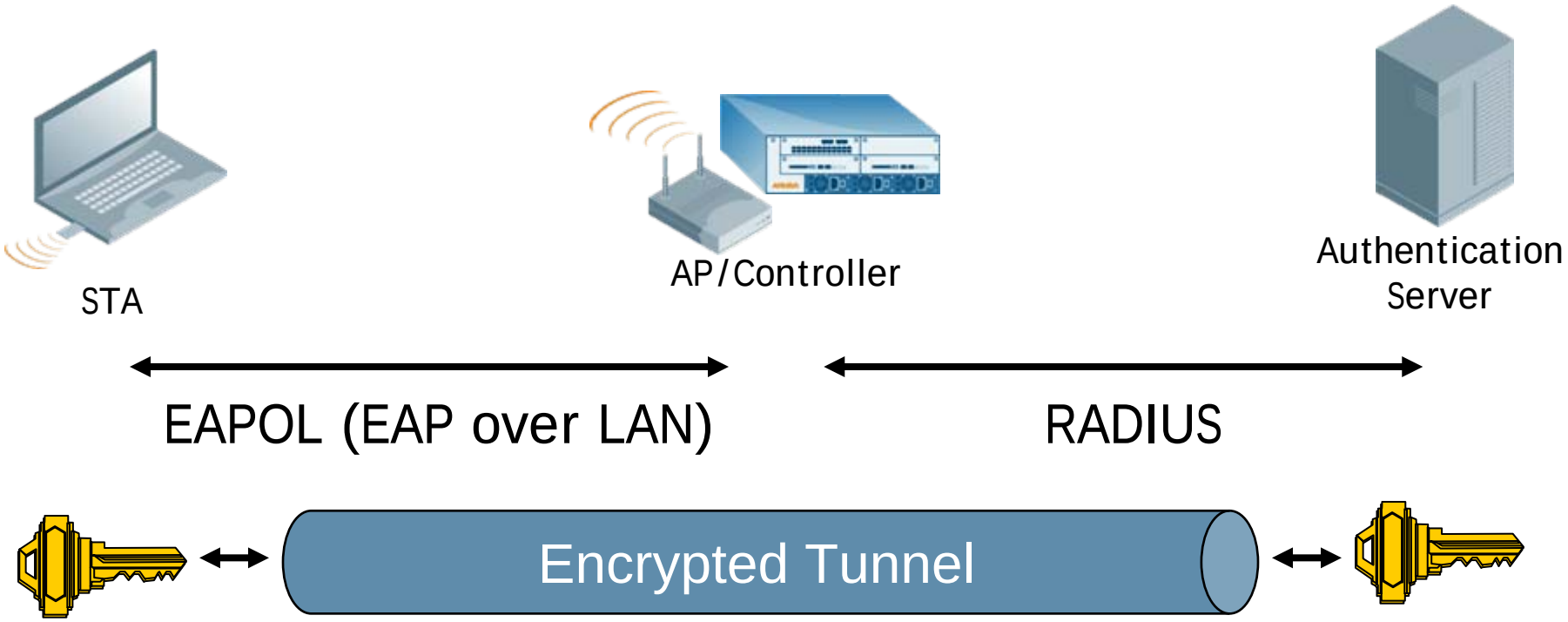
- Mobility brings us:
  - Disappearance of physical security
  - New mobile users, devices appearing everyday
  - Increased exposure to malware
- Assuming that "the bad guys are outside the firewall, the good guys are inside" is a recipe for disaster

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

ARUBA networks

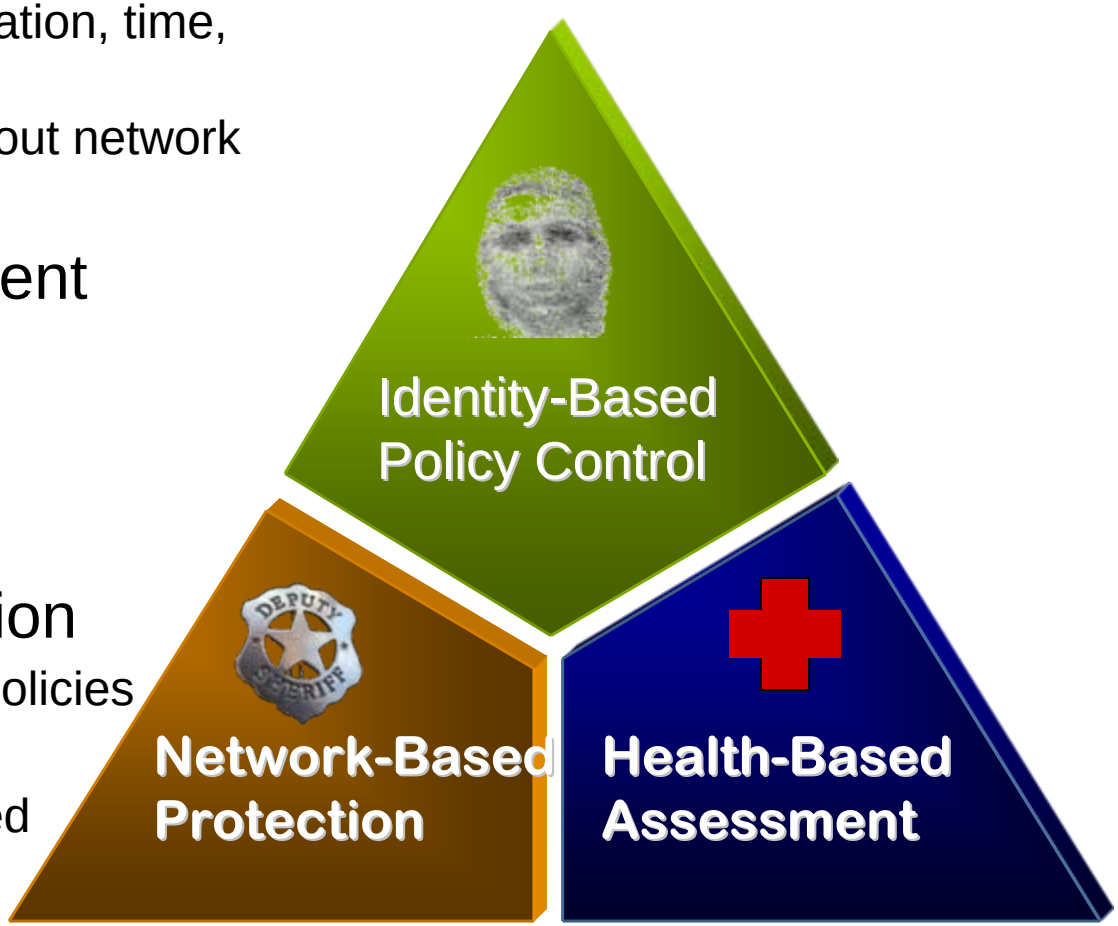
Captive Portals

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

ARUBA networks

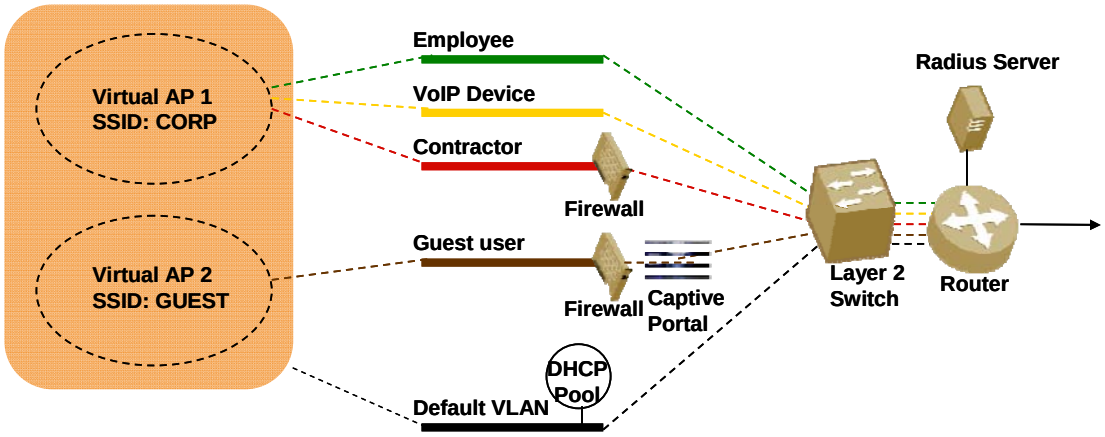
Remember “NAC”?

- Identity-Based Policy Control
  - Assess user role, device, location, time, application.
  - Policies follow users throughout network
- Health-Based Assessment
  - Client health validation
  - Remediation
  - Ongoing compliance
- Network-Based Protection
  - Stateful firewalls to enforce policies and quarantine
  - User/device blacklisting based on Policy Validation



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



Encrypt the Data

- If intruders can't read the data, there's no need to worry where it goes
  - WEP
    - Simple to do, easy to crack
    - No key management
    - Don't do it
  - TKIP (Temporal Key Integrity Protocol)
    - Works on legacy hardware (pre-2003)
    - First major flaw published in November 2008
    - Not currently recommended
  - CCMP/AES
    - Encryption using AES
    - Considered state-of-the-art
    - FIPS 140-2 approved
    - Works on all modern hardware

ARUBA networks

Combining Authentication & Encryption: WPA

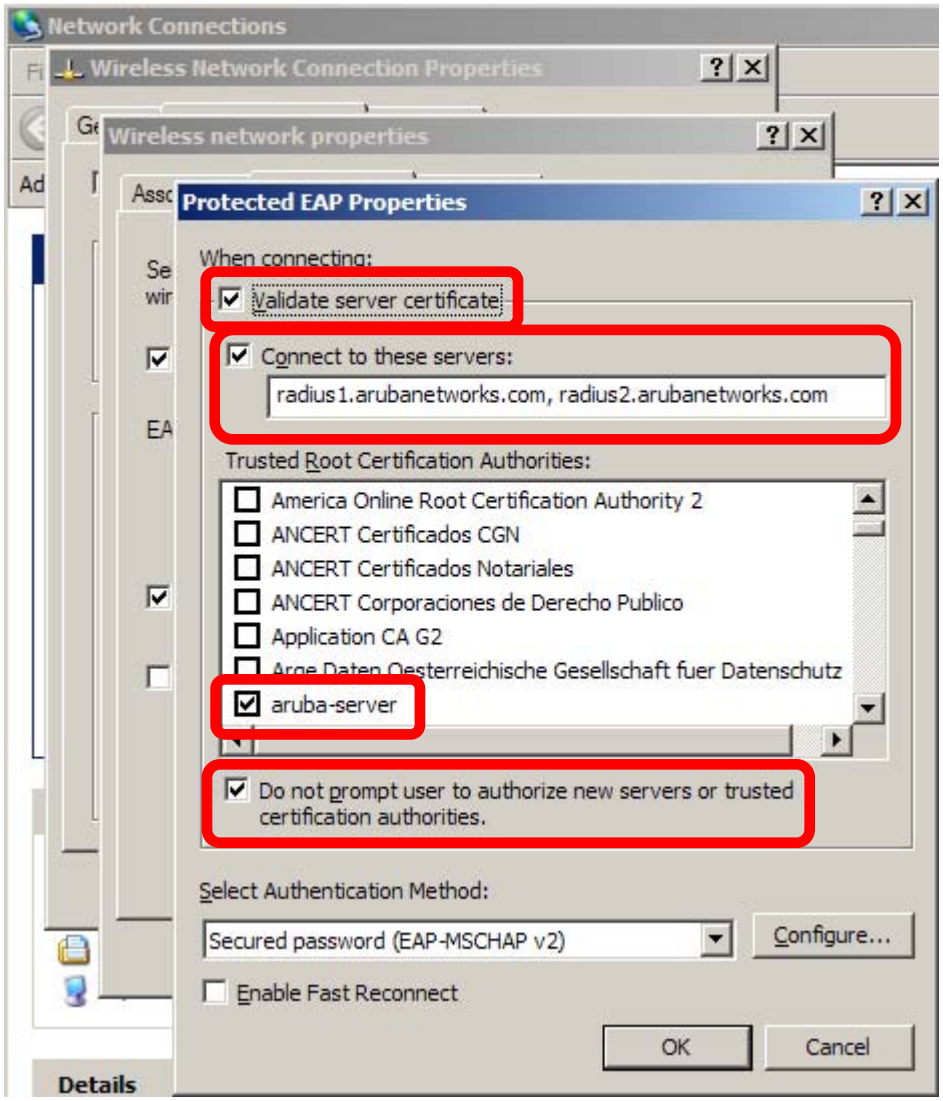
- WPA == Wi-Fi Protected Access
- WPA
  - Wi-Fi Alliance “standard” based on pre-802.11i
  - Includes TKIP for encryption
- WPA2
  - Wi-Fi Alliance “standard” based on ratified 802.11i
  - Includes TKIP and CCMP for encryption
- For both:
  - WPA-Enterprise == 802.1X for authentication, dynamic encryption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

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?

ARUBA networks

Configure EAP 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

ARUBA networks

Abusing Preferred Network Lists...

- 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 (dell5150) <- 169.254.0.254
DNS: 169.254.0.254.1128: 22333 IN::A www.mysecretwebsite.com
FTP: 169.254.0.254 myusername/mypassword
```


ARUBA networks

Pay Attention to NIC Driver Software

- 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 out there – lots of new driver software going into production
  - Are these well written? Well tested? Secure?

```
============================================================================
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.
```

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

> 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.

ARUBA networks

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
  - Enforce principle of least privilege
  - Provide separation of user/device classes

ARUBA networks

Q & A

alogan@arubanetworks.com

ARUBA networks