WLAN SECURITY FUNDAMENTALS
Centralized Architecture = More Secure

Better visibility, better control, seamless mobility

“Fat” Access Points
- Management
- Policy
- Mobility
- Forwarding
- Encryption
- Authentication
- 802.11a/b/g
- Antennas

“Thin” Access Points

Centralized Mobility Controller
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
**Client Tarpit Containment**

- Does not waste air-time during threat mitigation
- Works against any brand and type of wireless device
Controlling Uncontrolled Wireless

Public Network

Bridge

Internal Network

Windows XP Laptop
Wireless Intrusion Prevention - RFProtect

• **Uncontrolled wireless devices**
  - Rogue APs
  - Laptops acting as bridges
  - Misconfigured laptops
  - Ad-Hoc networks

• **Attacks against the WLAN**
  - Denial of Service/flooding
  - Forged de-authenticate/disassociate
  - Man-in-the-Middle
  - WEP cracking
  - WPA-PSK cracking
TotalWatch Full Spectrum Monitoring

- Complete Coverage
  - 2.4-GHz and 5-GHz scanning
  - 4.9-GHz public safety band
- 5-MHz channel increment scanning
  - Rogue detection in-between channels

2.4 GHz

4.9 GHz

5.0 GHz
Authentication

- 802.1X is best for Wi-Fi. Works with all modern client operating systems
- Makes use of EAP (Extensible Authentication Protocol)
- 802.1X authentication happens at L2 – users will be authenticated before an IP address is assigned
Authentication with 802.1X: PEAP

EAPOL (EAP over LAN)  RADIUS

Encrypted Tunnel
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
    - Flaw is getting worse with more research
    - *Not currently recommended*
  - **CCMP/AES**
    - Encryption using AES
    - Considered state-of-the-art
    - Government approved (FIPS, CESG, etc.)
    - Works on all modern 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 keys
  - WPA-Personal == pre-shared authentication key – careful!
WPA-Personal? Be careful..

• WPA Personal does not use 802.1X
  • Pre-shared key
  • Easier
  • But less secure

• Problem 1: Scalability
  • Need to re-key any time an employee/user leaves the organization

• Problem 2: Using weak keys
  • WPA-PSK keys that are weak can be cracked (dictionary attack)
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
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
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

We meet again, 007!
PEF to Control Wireless Performance

Lack of Policy Impacts Network Reliability & Performance

- What are Multicast and Broadcast currently being used for?
- What problems am I creating by using large VLANs to solve mobility issues?
- What non-critical applications are consuming bandwidth?
- Should users be connecting to 3rd party WLANs?
- Should users be setting up their own WLANs?
- Should users be connected to wireless while wired?
- How are “Power” Users affecting others?
- How are unauthorized users affecting network availability?
Network Access Control (NAC)

- **Identity-Based Policy Control**
  - Assess user role, device, location, time, application.
  - Policies follow users throughout network
  - (Aruba PEF)

- **Health-Based Assessment**
  - Client health validation
  - Remediation
  - Ongoing compliance
  - (ClearPass OnGuard)

- **Network-Based Protection**
  - Stateful firewalls to enforce policies and quarantine
  - User/device blacklisting based on Policy Validation
  - (Integration with ESI)
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
  - Authentication using 802.1X and EAP-TLS
  - 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