



Integrated WLAN/LAN Security

**Phil Kwan,
Foundry Networks**

The Case for Wireless

The Benefits of Wireless

- Improved Productivity
- Anywhere, Anytime Access
- Rapid Deployment
- Cable Plant Reduction

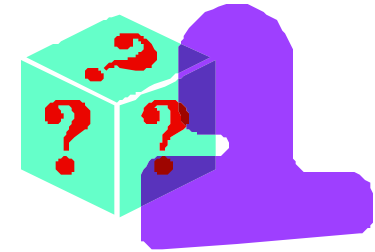
The Drawbacks of Wireless

- Unauthorized Access
- Difficult to contain RF
- Rogue Access Points
- Easier to Attack and DoS
- Viruses, Worms, No Security (hot spots)

Wireless Security Design Considerations

- **Understand Your WLAN Security Requirements**

- Who will access?
- How should they authenticate?
- How many users will need access, both now and in the future?
- Where will users need this access
- What applications will be running over the WLAN?
- How much bandwidth will each application require?
- How many users will be using each application?
- What data should be protected?
- What security devices are currently available?



- **Review and understand your Corporate Wireless Security Policy**
- **If necessary, meet with management to define new WiFi Security Requirements**

Don't Guess – Test each security component and perform the necessary Site Surveys to determine coverage, AP location, “dark spots”, and RF Leakage.

WLAN Security Is NOT Wired Security

- Wireless Security is not the same as wired security – it involves many more components
- Things that complicate wireless security:
 - Not all wireless devices can use the same authentication and data encryption schemes
 - Bar code scanners, PDA's, ID tags, 802.11 phones, laptops
 - Consistent security across mobility domains
 - authentication, user policies, and performance are affected by layer 3 roaming
 - Verifying the user and their location is more difficult
 - RF is not contained within corporate borders like wired networks
 - Applications that require strong data encryption or high bandwidth are affected
 - performance and usability trade-offs with strong security
 - Wireless is a shared medium with limited bandwidth that is affected by many factors

5 Components of Wireless Security

1. Authentication

- MAC Filtering, Shared Key, WEB-Based, 802.1X with EAP

2. Data Encryption

- Static WEP, Dynamic WEP, WPA TKIP/MIC, AES-CCMP at Layer 2, IPSEC at Layer 3

3. User Access Control

- Dynamic VLANs, User Policies, Location-based

4. Monitoring

- RF Scans, Rogue APs/Ad-Hoc Users, Malicious Traffic, Usage Reports, Authentication Intrusion Detection, Notification with Traps, Syslog

5. Client Security

- Personal Firewalls, VPN (no split tunnelling), Centrally Managed Profile

Performance vs. Security Considerations

- Strong Authentication using 802.1X and EAP will affect the speed of authentication, association and roaming – affecting latency sensitive applications such as Voice over WLAN
- Many users requiring 802.1X Authentication will require tiered RADIUS servers to provide redundancy and scalability
- Strong Data Encryption using TKIP/MIC and AES will affect the WLAN throughput performance – more time and CPU required to encrypt and decrypt
- WLAN Appliances centralizes authentication, encryption, key rotation, etc. may yield lower throughput as user demand and throughput rises
- APs that perform authentication, data encryption, or key rotation can offset performance bottlenecks and allow better AP density and scalability

**Understand your security requirements
before you deploy!**



802.11 Security – User Access Control

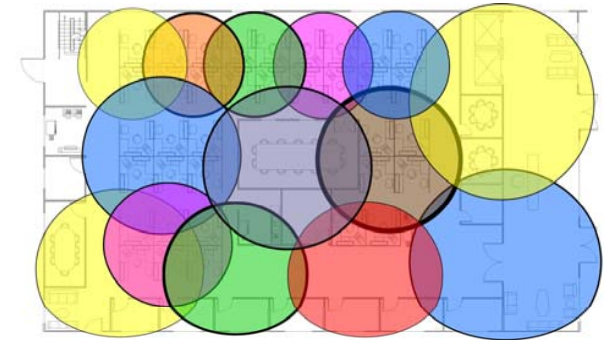
- Controlling user access after authentication is an additional layer of security (Defense-in-Depth)
- Popular methods of controlling user access include:
 - Port Based VLANs with Dedicated APs
 - VLAN Tagging per SSID
 - Dynamic VLAN with 802.1X
 - Dynamic User Policies (per user ACLs)

Challenges of User Access Control:

- Reauthentication: Will users have to re-authenticate?
- Mobility Issues: Can policies roam?
- VoIP Issues: Must have 50-100 ms roam and policy handoff
- Software or Hardware solutions can affect performance greatly

802.11 Security – RF Monitoring

- One of the major threats to WLAN Security is rogue APs - one rogue AP can defeat the strongest secured WLAN design
- Not all Rogue Detection is the same
 - Integrated Rogue solutions are limited
 - Polling intervals
 - Channel scanning (2.4 and 5 Ghz)
 - Limited information
 - RF Sensors are dedicated to RF Monitoring
 - Scans all 2.4 and 5 Ghz frequencies
 - Continuous scanning for more accurate RF anomaly detection
 - Rich information: rogue APs, Ad-hoc users, client associations, IDS



RF Monitoring is very important for securing wireless LANs against improper use and malicious intent!

Secondary Defenses – Do They Work?

- Layering security by doing the following will only help secure the Wireless LAN from casual users and amateurs:
 - Hiding the SSID Broadcasts
 - Good WLAN sniffers will find them – ESSID Jack
 - Maximize connect speed, minimize transmit power to contain coverage within your facility
 - You can never contain 100% of RF signals
 - Using directional antennas to contain RF within buildings
 - There will always be leakage - Never 100% effective

The Case For Airwave Monitoring

- Strong defences MUST include 24x7 monitoring of airwaves
 - Visibility and control of the RF and what is using it
 - Autonomic scans for rogue APs, Ad-Hoc users, hackers, etc.

Layer Your Security – Both Wired and Wireless

- Use strong authentication, consider two factor token cards in addition to 802.1X
- Implement the strongest data encryption that makes sense for your company and applications – Dynamic WEP should be a minimum
- Consider WPA TKIP/AES for all new purchases to start migration to 802.11i
- Control access after users login to limit access and potential breaches
- RF Monitoring and user session reporting is much more critical with WiFi access - Invest in a good RF monitor and IDS/IPS system
- Protect the WiFi devices as well and not just the infrastructure – consider centrally managed policy based firewalls
- Make sure your WLAN hardware is software upgradeable to 802.11i to support your future security needs