Security Issues with IEEE 802.11

Bob Beach
Symbol Technologies
Temptations of WLANs

- Everything is available for the taking
- Nonphysical access to corporate networks
  - Bypasses corporate firewall
- MU and AP technology readily available
- New Technology
  - Users still learning to install/use it
  - Protocol is moderately defenseless
Attacks and Attackers are Varied

• Breaking into Enterprise
  – Steal data, corrupt operation
  – Collect IP addresses for other attacks

• Simple disruptions are as bad as break-ins
  – Fed Ex, UPS use wireless LANs for package sorting

• Attackers are worldwide and organized
  – Mischief/fun, ideological, commercial
802.11 Security Problems

- Assumes a relatively benign environment
  - Lightweight Authorization/encryption
- Some Problem Areas
  - Integrity of RF protocol
  - MAC Address Forgery
  - Detection of Unauthorized APs
  - Interaction of 802.11 authorization mechanism and other mechanisms
Integrity of RF Protocol

• Generation of phony management frames
• No means to verify identity of sender
• May completely (or partially) disrupt network
Some RF Protocol Attacks

- Phony associate requests consume AP resources
- Phony power management mode changes
- Phony RTS/CTS Packets waste bandwidth
- Phony Disassociate requests disconnect MUs
- Phony beacons to consume MU battery power
- Phony probe responses confuse MU roaming
- Phony poll requests steal MU’s data
RF Protocol Integrity Reqmts

• Means to verify identity of sender
• Means to prevent replay attacks
  – capture and retransmission of “good packets”
MAC Address Forgery

• MAC Addresses are subject to Forgery
  – Many Vendors NIC cards can be reprogrammed
  – Buy development kits from vendors
• Many vendors rely on Access Control Lists for security
• Need means to verify MAC address/MU map
Unauthorized Access Points

• “AP in the parking lot”
  – Same MAC address as real AP
  – Attracts Mobile Units

• Goal may be simple mischief or worse
  – i.e. Disrupt operation of network
  – Everything looks okay, but nothing works

• Attack Mobile Unit weaknesses
  – Connected to MU, break into it
Casual User Access Points

• User buys AP and attaches it to office LAN
  – To Experiment/Play
  – To assist others in breaking into corporate net
• Once attached, the corporate net is wide open
• System Admins are unaware of new AP
  – and that corporate security has now been completely compromised
Detection of Access Points

- Need means to detect presence of AP
- System Administrators can detect all APs
- Cannot be disabled
802.11 Authentication Issues

- There are enterprise authentication solutions on the horizon
  - Windows 2000 uses Kerberos
  - IPsec
- Such mechanisms may support WLAN authentication and key distribution
- 802.11 authentication may interfere with such mechanisms
802.11 Authentication Issues

• No levels of access
  – All or nothing

• The authenticate, then associate model prevents limited access framework
  – MU may communicate with authentication servers but nothing else.
  – For example, Kerberos may use Network Time Protocol to obtain timestamps
Authentication Improvements

• Different levels of access
  – No access
  – Access to authentication servers only
  – Full Access

• Separate out authentication and encryption functions
  – Enterprise authentication, but WEP for privacy
Conclusions

• IEEE 802.11 was designed for a generally benign environment

• WLANs are very tempting to hackers
  – Increasing attached to corporate networks
  – Many types of attacks

• Lots of issues that need addressing
  – More than just WEP key length