

Providing Wireless Security In Dispersed Environments

by

Barry Gavrich

Scholarship for Service Program

13 April 2005



**New Mexico Tech**

Presentation Outline

- ❖ Mobile Devices
- ❖ Network Environments
- ❖ Wireless Security Issues and Challenges
- ❖ Wireless Security Mechanisms
- ❖ Security Policy and Enforcement
- ❖ Questions

Mobile Devices..

- ❖ Mobile Computers and Peripherals
 - Laptops
 - Tablet PCs
 - Wireless Keyboards
- ❖ Portable Electronic Devices (PEDs)
 - Personal Digital Assistants (PDAs)
- ❖ Messaging Devices
 - Blackberry Devices

Mobile Devices

❖ Mobile Phones

- Analog Cellular

- Native format uses frequency modulation (FM), provides no security

- Digital Cellular

- Provides limited security through the use of code or time division multiplexing (CDMA / TDMA) schemes

- Smart Phones

- Cellular phone with integral PDA
- Blackberry with integrated cellular phone

Network Environments..

❖ Mobile Workforces

- Military and Intelligence
 - Department of Defense (DoD) – Global Information Grid (GIG) serves as the information backbone for all agencies involved
 - Army – Future Combat Systems (FCS), large wireless component will rely on Information Systems technology as “armor” for field operations
- Intelligence Community
 - Greater reliance on sharing of data and inter-agency field communications

Network Environments

❖ Homeland Security

- Numerous dispersed agencies with overlapping requirements for data analysis and use

❖ Other Federal Agencies

- Adopting a more “mobility oriented” model including the use of a wireless infrastructure for efficiency and flexibility
- Although technically not under the DoD umbrella, many still deal with “sensitive but unclassified” level of information that is subject to Federal Information Processing Standards (FIPS) requirements

Wireless Security Issues...

❖ Open Network Perimeters

- A “wireless edge” presents additional security issues not encountered with traditional LANs
 - Harder to defend as the surrounding environment is both qualitatively and quantitatively unknown

❖ Mobility of Devices

- Greater chance of being lost or stolen
- Remote environments can not be adequately surveyed or monitored for potential threats
 - Ad-Hoc systems deployed in hostile environments

Wireless Security Issues..

❖ Mobile Devices

- Provide a greater opportunity to serve as a conduit for viruses via Access Points (APs)
- Difficult to monitor devices beyond the wireless edge of the network
 - Remote disable / data erasure needed by command and control centers to maintain operation security and reliability

Wireless Security Issues

- Statistically greater chance of data being intercepted during transmission
 - Sensitive but unclassified or classified information (if decrypted) can compromise ongoing intelligence operations
- ❖ Capture of Data / Voice Traffic
 - Passive eavesdropping harder to detect in a wireless environment
 - Not always feasible to place sensors or “sniffers” into the environment

Wireless Security Challenges..

❖ Adapting Emerging Technologies

- Bluetooth devices provide limited range functionality for small temporary deployments
 - Wireless Personal Area Networks (WPANs) are fast to deploy, but security is very limited in scope

❖ Limited Device Availability

- S/MIME Enhanced Blackberry is currently the only National Security Agency (NSA) approved device for sensitive but unclassified information
 - Text messaging only of sensitive but unclassified information

Wireless Security Challenges

❖ Secure Wireless Local Area Networks (SWLANs)

- Harris SecNet 11 is currently the only (NSA) approved solution for SWLAN connectivity to the DoD Secret Internet Protocol Router Network (SIPRNet)
 - Provides complete voice / data access
 - Certified for Type 1 encryption for transmission of classified information in an RF environment
 - Uses 802.11b based protocol, 11Mbps data rate
 - Supports both Windows and Linux OS platforms

Security Mechanisms.....

- ❖ IEEE 802.11i Standard Amendment (WPA2)
 - 802.11i subset using Wi-Fi Protected Access (WPA) incorporating:
 - Advanced Encryption Standard (AES)
 - Counter-mode Cipher Block Chaining (CBC)
 - Key lengths of 192 or 256 for Top Secret level
 - Robust Secure Network (RSN)
 - Defined and implemented at the wireless edge of a wired network as opposed to WLAN components
 - Time intensive processing routines

Security Mechanisms...

- ❖ Use of Multi-Layered Defense-In-Depth Strategy
- ❖ Identification and Authentication
 - Use of Public Key Infrastructure (PKI) or two-factor authentication
 - Security token (character sequence) generated by authentication server and password entry
 - Use of strong passwords
 - Smart cards
 - Proven technology, card control issues



Security Mechanisms..

- Biometrics
 - Conceptually good alternate two-factor authentication method
 - Voice recognition – promising technology, relatively high rejection rate, requires stable voice patterns
 - Fingerprint scanners – reliable and portable, but somewhat limited for field applications
 - Retinal scanners – more secure than fingerprint or other physical geometries, not as portable

Security Mechanisms

- ❖ Antivirus Software
- ❖ Software Firewalls
- ❖ Intrusion Detection Systems (IDS)
 - Host-based – loaded into the OS of each supportable mobile device
 - Network-based – data packets are examined and compared against known attack patterns
 - Anomaly-based – uses pattern recognition, compared against “established” traffic patterns, has scalability and flexibility issues

Policy And Enforcement..

- ❖ Multiple Agency Authority and Development
- ❖ Department of Defense (DoD)
 - National Security Agency (NSA)
 - Defense Information Systems Agency (DISA)
- ❖ National Institute of Standards and Technology (NIST)
 - National Information Assurance Project (NIAP)
 - In partnership with the NSA

Policy And Enforcement

- ❖ Policy Enforcement is Rigorous
- ❖ Difficult in Remote Environments
 - Monitoring of mobile devices is not always possible under the best of circumstances
 - Command and control centers may not be in constant communication for monitoring
 - Users can defeat / bypass certain security features of mobile devices

Providing Wireless Security In Dispersed Environments

Questions ?

