



EDS
1962 40 years 2002

Best Practices For Securing Wireless Systems

October 15, 2002

Topics to be Covered



- Wireless Security – A Brief Overview
- Wireless LAN Security
- Wireless Handheld Security
- Wireless Messaging and Email Security

❖❖ Wireless Security – A Brief Overview

“As a bank or government employee...what do I need to know about wireless security?”

First, let’s talk about the differences between securing wired and wireless networks



❖❖ Wireless Security – A Brief Overview

Similarities:

- Same security principles
 - Authentication
 - Confidentiality
 - Data integrity
 - Non-Repudiation
- Same layered “Defense In Depth” approach used for the security infrastructure
 - Network security components
 - Firewalls, Authentication Servers, VPN’s
 - Device security components
 - Antivirus, Personal Firewall, File Encryption
 - Application security components
 - Access Control, Data Encryption



❖❖❖ Wireless Security – A Brief Overview

Differences:

- Data transmissions are easily intercepted
- Handheld devices easily lost or stolen
- Different set of data/security protocols
- Easy to flood the airwaves with connection requests in a Denial of Service (DOS) attack
- Wireless spectrum can be jammed

❖❖❖ Wireless Security – A Brief Overview

Wireless security service is dependent on several factors

- Security features built into the mobile device by the device manufacturer
- Security features provided by the transmission protocol used by the wireless operator
- Security features implemented by the wireless operator
- Security features available from the mobile device operating system
- Configuration of the mobile gateway – open vs closed
- Availability of third party security products for specific mobile devices

❖❖ Wireless Security – A Brief Overview



“Are there any wireless security standards I need to know about?”

- *FIPS 140-2 (Federal Information Processing Standard)*
 - *OMB Circular A-130 requires federal government agencies to use FIPS to protect government data*
 - *FIPS 140-2 defines standard for the design of the cryptographic module used in products that encrypt government data*
 - *Many financial institutions also specifying FIPS compliance*
- *WEP (Wired Equivalent Privacy) Protocol*
 - *Security protocol that is with IEEE 802.11a/b/g wireless LAN systems*
 - *Has several documented security vulnerabilities (more details later)*
 - *Does not meet FIPS requirements*

❖❖ Wireless Security – A Brief Overview

More Wireless Security Standards....

- *IEEE 802.11i*
 - *New wireless LAN security protocol*
 - *Will include AES encryption*
 - *Expected to be released in 2003*
- *IEEE 802.1x & EAP*
 - *802.1x defines authentication standards for wired and wireless LANs*
 - *EAP (Extensible Authentication Protocol) is the authentication standard under 802.1x*
 - *Includes provisions for dynamic change of WEP encryption key*
 - *Has several documented security vulnerabilities for certain implementations*

❖❖ Wireless Security – A Brief Overview



More Wireless Security Standards...

- *WAP (Wireless Application Protocol)*
 - *Defines a standard for transmitting data to wireless phones and other wireless devices and displaying the data on the device (wireless browser)*
- *WTLS (Wireless Transport Layer Security)*
 - *Security component of WAP*

❖❖ Wireless Security – A Brief Overview

“What about wireless security guides”?

- *NIST Special Publication 800-48 Wireless Network Security (Draft)*
 - *Released for public comment in July*
 - *Covers 802.11, Bluetooth and handheld devices*
 - *Document can be found at <http://csrc.nist.gov/publications/drafts.html>*

Wireless LAN Security

- Wireless LANs can improve office productivity and reduce IT infrastructure costs
 - Allow employees to stay connected to the corporate network as they roam around the building or country (while in airports and hotel rooms)

BUT.....

- Security is a significant concern

Fortunately, reliable and secure wireless LAN systems are available



War driving
team finds local security weakness
Most WLANs aren't using encryption

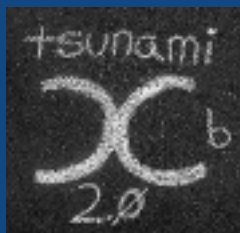
❖❖ Wireless LAN Security

Ananova: 'War chalking': New hacking threat to firms? 4 Aug 2002

Business leaders are warning a new craze called "war chalking" can leave firms open to hackers.

It involves drawing symbols in chalk on walls and pavements to mark points where signals from nearby office networks can be tapped into.

❖❖ Wireless LAN Security



❖❖ Wireless LAN Security

“What are the security issues in the press all about?”

- Most wireless LANs have no security turned on!!!
- The majority of all wireless LAN products are based on the IEEE 802.11b standard
 - IEEE 802.11b security is based on the WEP protocol
 - WEP provides only weak security
 - Provides only device authentication, not user authentication
 - Encryption process is weak – the encryption key based on two components – one rarely changes and one may change on a preset pattern that can be guessed
 - All users on a wireless LAN network use the same encryption key to connect to the access point
 - No key management included in protocol

❖❖ Wireless LAN Security

- *IEEE 802.11 WLANs do not meet security requirements for data encryption for financial institutions and government agencies*

“OK..... So how do I implement a secure wireless LAN?”

- Use a VPN to meet strong encryption requirements

❖❖ Wireless Security – A Brief Overview



“Tell me about VPNs working with Wireless LANs...”

- Two types – traditional wired network VPN and new wireless LAN VPN
- Traditional VPN
 - Meets FIPS compliance requirements
 - Can be quickly set up
 - BUT....
 - Management of VPN can be cumbersome
 - Can be hard to scale to wireless LAN network

❖❖ Wireless LAN Security

- New Wireless LAN VPNs
 - Easy to integrate into wired network
 - Can be quickly set up
 - Most products have easy to use interface
 - Has features optimized for wireless LAN network
 - Support for session persistence
 - Security policy management – down to access point and wireless device
 - 8+ vendors selling wireless LAN VPN products
 - BUT....
 - Only one product currently FIPS certified - several others expected to be certified before the end of 2002

❖❖ Wireless LAN Security

“What should I look for when I buy a Wireless LAN system for my bank or agency?”

- Wireless LANs should have these features:
 - 128-bit encryption
 - Ability to change encryption key on a frequent basis
 - Supports IEEE 802.1x authentication with mutual authentication between the authentication server and the user
 - Is a component of a wireless LAN system that includes a FIPS compliant traditional or wireless LAN VPN

❖❖ Wireless LAN Security

“Ok....what are the industry best practices for installing and configuring my wireless LAN?”

- Change wireless LAN default settings
 - Change the SSID to a non-descriptive word. Example: A3!2bcf3
 - Turn off SSID broadcast mode
 - Set WEP to 128-bit encryption
- Implement MAC address filtering
 - May not be practical for large wireless systems
 - Check to see if your wireless LAN or wireless VPN manager can push MAC address ACL list to APs

❖❖ Wireless LAN Security



More Best Practices.....

- Segregate wireless network from wired network
 - Place wireless AP in a VLAN, or
 - Place wireless APs in a firewall DMZ
- When using an IEEE 802.1x capable wireless LAN
 - Configure for mutual authentication between the user and authentication server
- Protect the wireless LAN network with a FIPS compliant VPN
- Disable AP management protocols when not being used

❖❖ Wireless LAN Security



More Best Practices.....

- AP location considerations
 - Place AP towards center of building
 - Limit AP transmit power to lowest setting possible that provides an acceptable signal strength at the edge of the building
- Configure the AP to forward its logs to a log server
- Add wireless war dialing and penetration testing to agency security inspection procedures

❖❖❖ Wireless Handheld Security

- Employees with cell phones and wireless PDAs connect to agency network via the internet to use network resources (e.g. to file an expense report)
- Primary security issues include:
 - Confidentiality and integrity of data in-transit
 - Security of data stored in mobile device if it is lost or stolen (data is usually more valuable than the device)
 - Authentication and access control of user connecting to corporate network
 - Transfer of viruses from mobile device to corporate network

❖❖❖ Wireless Handheld Security

“Ok....so how do I use wireless PDAs and other handheld devices in a secure manner”?

- For data confidentiality and integrity, numerous encryption products available
 - Security solution highly dependent on mobile device or wireless service used
 - VPN solutions are becoming popular

BUT

- No FIPS compliant products currently available to secure data while it is being transmitted or data on the PDA.

Banks and government agencies should clearly understand all security risks before approving the use of handheld devices for storing, processing, or transmitting government information.



❖❖❖ Wireless Handheld Security

“What security features are available with my mobile phone or wireless PDA?”

Within a wireless device and network, security services may be found at three points:

- Radio Transmission – many radio protocols (GSM, CDMA, CDPD, etc.) provide device authentication and data encryption
 - Security is provided between the wireless device radio and the wireless service provider base station

❖❖❖ Wireless Handheld Security



- Network Connection – many wireless operators provide secure data tunnels (VPN) between the device and the network enterprise – data encryption and device authentication
 - Security is provided between the wireless device and the wireless service operator or the corporate network
- Application – user authentication and application data encryption including biometric solutions
 - End-to-end security is provided between the application client on the wireless device and the application server located on the corporate network

❖❖ Wireless Handheld Security

“My bank has decided to use handheld devices.....what are the best practices for security”?

- Use a power-on password
 - Follow Bank/Agency password management policy
- Install only Bank/Agency approved applications
- Install antivirus software on handheld
 - Use handheld version of Bank/Agency enterprise antivirus software
- Turn off IR ports when not in use
- Install personal firewall on handheld
- Insure devices have timeout mechanisms that will require a password after a period of inactivity

❖❖ Wireless Handheld Security

More best practices

- Regularly synchronize handheld with PC
 - Handhelds used for work should not be synchronized with personal/home PCs
 - Synchronization management software should only be active during synchronization process
 - Synchronization management application should not be launched as part of the PC boot-up process
 - Disable wireless transmitter during synchronization
- Use a FIPS compliant VPN for wireless connections to the internet to access government networks
 - Limit remote user access to specific resources



❖❖❖ Wireless Messaging and Email Security

- The security issues associated with wireless handheld devices apply

PLUS.....

- Some wireless email services do not provide end-to-end data confidentiality
 - Email is not secure from bank email server to the wireless email device
- Wireless messaging services (e.g. SMS, pin-to-pin) provide only minimal data protection for messages

❖❖❖ Wireless Handheld Security

“We need wireless email at my Bank/Agency.....what are the best practices for security”?

- Follow the best practices for handheld devices
- Use only messaging services with FIPS compliant data encryption
 - Blackberry Pin-to-Pin messages do not meet this requirement. Blackberry Pin-to-Pin should be disabled
 - Consider enabling Pin-to-Pin service ONLY during emergencies (Agency COOP Plan)
- Use only email services with FIPS compliant data encryption
- Use only enterprise server email redirectors



 eds.com

Point of Contact

Alex Froede
EDS Security & Privacy Professional
Services
Office: 703-733-3196
e-mail: alex.froede@eds.com