

**Wireless Network Security
802.11, Bluetooth™, and
Handheld Devices
March 7, 2003
ISART**



Presentation Outline

- **Mobile Workforce**
- **Wireless Security Issues**
- **802.11 WLAN**
- **Bluetooth**
- **Handheld Device**
- **Risks, Threats, and Vulnerabilities**
- **Wireless Security Countermeasures**
- **Summary/Recommendations**
- **Conclusion**
- **Contact**



Mobile Commerce

Mobile Commerce



m-commerce Security



Mobile Workforce

- **Explosive Growth of Wireless Technologies**
- **Small Home Offices**
- **University Campuses**
- **Military and Intelligence**
- **Manufacturing Shop Floor**
- **Access to Enterprise Resources**
- **Wireless Internet Service Providers**
- **First Responder Teams**

m-commerce Security





Mobile Device Market

- **Analysts predict 50 million handheld devices and 330 million smart phones in the work force by 2003. [Forrester Research]**
- **Wireless devices, such as PDA's, accessing the Internet will increase by 700% - from 7.4M in 1999 to 61.5M by 2003 in the U.S. alone. [IDC]**
- **98% of the 540 million cell phones sold in 2003 will be able to receive and display data by 2003. [IDC]**

m-commerce Security



mobile Applications

- **email**
- **Location-based Services**
- **Access Corporate Data**
- **Financial Transactions**
- **Sales Force Automation**
- **Supply Chain Management**
- **Entertainment**

m-commerce Security





m-commerce Projections

- **Global mobile commerce revenues will reach \$55.4B by 2003 according to Andersen Consulting.**
- **Renaissance Worldwide Inc., suggests that m-commerce will amount to as much as 45 percent of the total e-commerce market in 2004.**

m-commerce Security



Trends

- **Wi-Fi Hotspots - Boingo, Wayport, Cometa Networks**
- **Long-range Wi-Fi - Vivato**
- **Mesh Networks - SkyPilot, MeshNetworks, Moteran**
- **Smart Spaces, Sensors**
- **Ubiquitous Computing**
- **Last Mile - Apertonet**

m-commerce Security





Wireless Security Challenges

- **Wireless, by definition, means RF and absence of physical security safeguards**
- **Wireless cryptography, a critical element for wireless, is sometimes lacking, bad or inadequate**
- **Many technologies are new and new vulnerabilities should be expected**
- **Wireless topologies and complexities will increase**
- **Limited awareness of security risks**

m-commerce Security



In The News

- **Neutron Jack**
- **X10 Security Cameras**
- **“Lean Cuisine” Attack**
- **Pringles Cans**
- **War Driving**
- **Netstumbler, Aeropeek, Kismet**

m-commerce Security



802.11, Bluetooth, and Handheld Devices

802.11, Bluetooth, and Handheld Devices

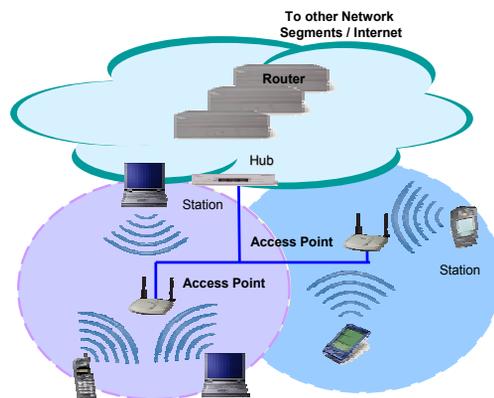


m-commerce Security



802.11 WLAN

- 802.11
- Avoids Wiring Costs
- Deployed Quickly
- Default Configurations easy to set up
- Good performance
- Inexpensive Access Points



m-commerce Security





Bluetooth™

- **Personal Area Networks**
- **Eliminates Desktop Clutter**
- **Networking Capabilities**
- **Consumer Electronics**
- **Smart Spaces**
- **Shipped with many consumer products**



m-commerce Security 



Handheld Devices

- **Handheld Devices are Ubiquitous**
- **Multiple Access Points – Serial, PCMCIA, IRDA, User Interface**
- **Personal and Business Use**
- **No longer just a calendar and address book**
- **PDA's, Smart Phones, Multimedia Devices**
- **Access to Enterprise Data**
- **Limited memory and computational power**

m-commerce Security 



802.11 Security

802.11 Security



m-commerce Security



802.11 Standards

- **802.11b**
 - Most widespread
 - 11Mb maximum, 2.4 GHZ band
- **802.11a**
 - Next generation
 - 54MB maximum, 5GHZ band
- **802.11g**
 - 54MB maximum, 2.4 GHZ band
 - Compatible with 802.11b
- **802.11X**
 - Uses Extensible Authentication Protocol (EAP)
 - Supports RADIUS
- **802.11i**
 - TKIP
 - Draft

m-commerce Security



802.11 Security

- Authentication – open system & shared key
- Confidentiality - WEP
- Integrity – Cyclic Redundancy Check (CRC)

m-commerce Security

802.11 Security

- Authentication

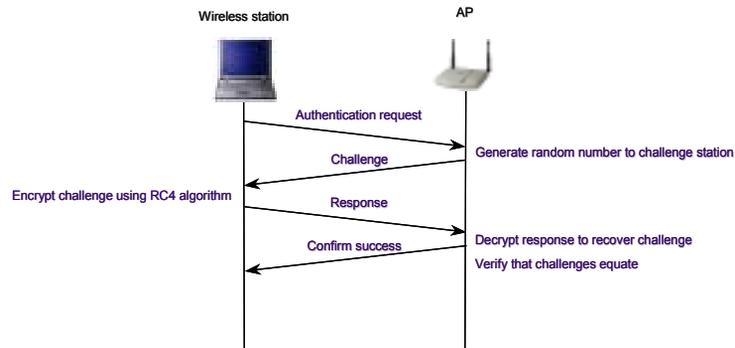
802.11 Authentication

<p>Open System Authentication</p> <p><i>1-stage Challenge-Response</i></p> <p>Non-cryptographic Does not use RC4</p> <p>A station is allowed to join a network without any identity verification. (Required)</p>	<p>Shared-key Authentication</p> <p><i>2-stage Challenge-Response</i></p> <p>Cryptographic Uses RC4</p> <p>A station is allowed to join network if it proves WEP key is shared. (Fundamental security based on knowledge of secret key) (Not required)</p>
--	--

m-commerce Security

802.11 Security

- **Shared Key Authentication**



802.11 Security Issues

- Security features in vendor products are frequently not enabled.
- IVs are short (or static).
- Cryptographic keys are short.
- Cryptographic keys are shared.
- Cryptographic keys cannot be updated automatically and frequently.





802.11 Security Issues

- RC4 has a weak key schedule and is inappropriately used in WEP.
- Packet integrity is poor.
- No user authentication occurs.
- Authentication is not enabled; only simple SSID identification occurs.
- Device authentication is simple shared-key challenge-response.
- The client does not authenticate the AP

m-commerce Security



Threats and Vulnerabilities

- All the vulnerabilities that exist in a conventional wired network apply to wireless technologies.
- Malicious entities may gain unauthorized access to an organization's computer network through wireless connections, bypassing any firewall protections.
- Sensitive information that is not encrypted (or is encrypted with poor cryptographic techniques) and that is transmitted between two wireless devices may be intercepted and disclosed.
- Denial of service (DoS) attacks may be directed at wireless connections or devices.
- Malicious entities may steal the identity of legitimate users and masquerade on internal or external corporate networks.

m-commerce Security





Threats and Vulnerabilities

- Sensitive data may be corrupted during improper synchronization.
- Malicious entities may be able to violate the privacy of legitimate users and be able to track their actual movements.
- Handheld devices are easily stolen and can reveal sensitive information.
- Data may be extracted without detection from improperly configured devices.
- Viruses or other malicious code may corrupt data on a wireless device and be introduced to a wired network connection.
- Malicious entities may, through wireless connections, connect to other organizations for the purposes of launching attacks and concealing their activity.
- Interlopers, from insider or out, may be able to gain connectivity to network management controls and thereby disable or disrupt operations.

m-commerce Security



Management Countermeasures

- Identify who may use WLAN technology in an organization
- Identify whether Internet access is required
- Describe who can install access points and other wireless equipment
- Provide limitations on the location of and physical security for APs
- Describe the type of information that may be sent over wireless links
- Describe conditions under which wireless devices are allowed
- Define standard security settings for access points
- Describe limitations on how the wireless device may be used
- Describe the hardware and software configuration of any access device
- Provide guidelines on reporting lost devices and security incidents
- Provide guidelines on the use of encryption and other security software
- Define the frequency and scope of security assessments

m-commerce Security





Operational Countermeasures

- Maintaining a full understanding of the topology of the wireless network.
- Labeling and keeping inventories of the fielded wireless and handheld devices.
- Creating frequent backups of data.
- Performing periodic security testing and assessment of the wireless network.
- Performing ongoing, randomly timed security audits to monitor and track wireless and handheld devices.
- Applying patches and security enhancements.
- Monitoring the wireless industry for changes to standards to enhance to security features and for the release of new products.
- Vigilantly monitoring wireless technology for new threats and vulnerabilities.

m-commerce Security



Technical Countermeasures

- Updating default passwords.
- Establishing proper encryption settings.
- Controlling the reset function.
- Using MAC ACL functionality.
- Changing the SSID.
- Changing default cryptographic keys.
- Changing default SNMP Parameter.
- Disable remote SNMP. Use SNMPv3.
- Changing default channel
- Deploy personal firewalls and antivirus software on the wireless clients

m-commerce Security





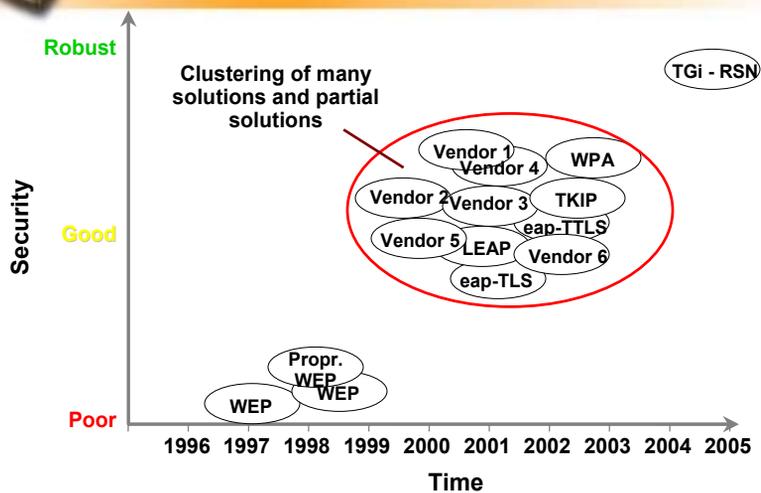
Technical Countermeasures

- Suppress AP broadcast beacon
- Test AP boundaries
- Intrusion Detection Systems
- Personal Firewalls
- Virtual Private Networks
- Consider other forms of authentication – RADIUS, Kerberos
- Complete Checklists for 802.11, Bluetooth, and Handheld devices are available in the guidance document.
- <http://csrc.nist.gov>

m-commerce Security



WiFi Security Evolution



m-commerce Security





Robust Secure Networks (RSN)

- Long-term security solution for 802.11 wireless LANs
- Developed by IEEE 802.11 Task Group i (TGi)
- Will apply to 802.11a, 802.11b and 802.11g
- Will fix the known, existing problems with WEP
- Builds on lessons-learned from IPsec
- Key features include:
 - TKIP (Temporal Key Integrity Protocol)
 - 802.1X port-based access control
 - Extensible Authentication Protocol techniques
 - Advanced Encryption Standard (AES) – in hardware

m-commerce Security



Bluetooth Security

Bluetooth Security



m-commerce Security





Overview

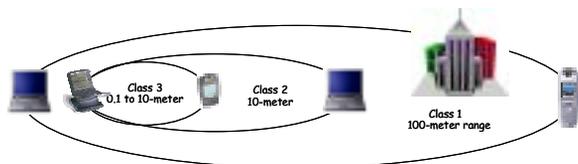
- Ad Hoc Networks
- Short Range RF at 2.45GHZ called ISM
- 720 Kbps – 4 Mbps
- Transceiver has unique 48-bit address
- Piconet
- Up to 8 devices per Piconet
- Scatternet
- Each Piconet is identified by a different Frequency Hopping Sequence

m-commerce Security 



Operating Range

- Class 1 100 meter range – 100mW
- Class 2 10 meter range – 2.5mW
- Class 3 0.1 to 10-meter range – 1mW



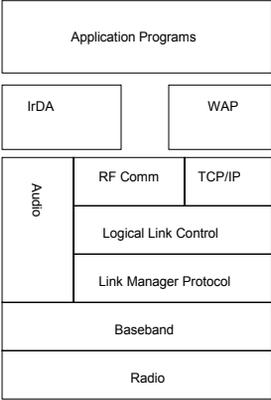
The diagram illustrates the operating ranges of three Bluetooth classes. It shows three overlapping ellipses representing the range of each class. The innermost ellipse is labeled 'Class 3 0.1 to 10-meter' and contains icons for a laptop and a mobile phone. The middle ellipse is labeled 'Class 2 10-meter' and contains a laptop icon. The outermost ellipse is labeled 'Class 1 100-meter range' and contains a building icon. The ellipses overlap, showing that Class 3 is contained within Class 2, and Class 2 is contained within Class 1.

m-commerce Security 



Bluetooth Communication

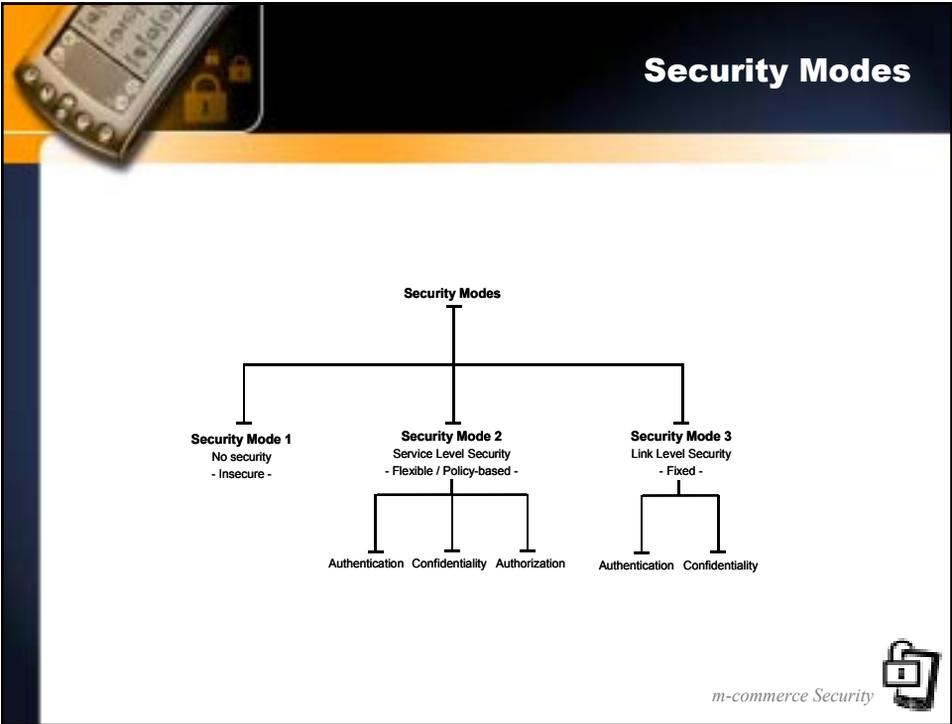
- Radio Frequency Communications
 - Controls frequency hopping
- Logical Link Control (LLC)
 - Link Management
 - Security Management
 - QoS Management
 - Transmission Scheduling
- Link Manager Protocol (LMP)
 - Configure, authenticate and handle connections
 - Power Management



Bluetooth Security

- **Security Mode 1—Non secure mode**
 - authentication and encryption bypassed
- **Security Mode 2—Service-level enforced security mode**
 - data link layer
 - Security manager controls access to services
- **Security Mode 3—Link-level enforced security mode**
 - mutual authentication & encryption
 - secret link key shared by device pair





- 
- ## Bluetooth Security Issues
- Strength of the challenge-response pseudo-random generator is not known.
 - Short PINs are allowed.
 - An elegant way to generate and distribute PINs does not exist.
 - Encryption key length is negotiable (8-128 bits).
 - Unit key is reusable and becomes public once used.
 - The master key is shared.
 - No user authentication exists.
- m-commerce Security* 



Bluetooth Security Issues

- Attempts for authentication are repeated.
- E_0 stream cipher algorithm is weak.
- Key length is negotiable.
- Unit key sharing can lead to eavesdropping.
- Privacy may be compromised if the Bluetooth device address (BD_ADDR) is captured and associated with a particular user.
- Device authentication is simple shared-key challenge-response.
- End-to-end security is not performed.
- Security services are limited

m-commerce Security



Technical Countermeasures

- Change the default settings of the Bluetooth device to reflect the agency's security policy.
- Set Bluetooth devices to the lowest necessary and sufficient power level so that transmissions remain within the secure perimeter of the agency.
- Ensure that the Bluetooth "bonding" environment is secure from eavesdroppers (i.e., the environment has been visually inspected for possible adversaries before the initialization procedures during which key exchanges occur).

m-commerce Security





Technical Countermeasures

- Choose PIN codes that are sufficiently long (maximal length if possible).
- Ensure that no Bluetooth device is defaulting to the zero PIN.
- Configure Bluetooth devices to delete PINs after initialization to ensure that PIN entry is required every time and that the PINs are not stored in memory after power removal.
- Use an alternative protocol for the exchange of PIN codes, e.g., the Diffie-Hellman Key Exchange or Certificate-based key exchange methods at the application layer. Use of such processes simplifies the generation and distribution of longer PIN codes.

m-commerce Security



Operational Countermeasures

- Ensure that combination keys are used instead of unit keys.
- Invoke link encryption for all Bluetooth connections regardless of how needless encryption may seem (i.e., no Security Mode 1).
- Ensure that encryption is enabled on every link in the communication chain.
- Make use of Security Mode 2 in controlled and well-understood environments.
- Ensure device mutual authentication for all accesses.
- Enable encryption for all broadcast transmissions (Encryption Mode 3).
- Configure encryption key sizes to the maximum allowable.

m-commerce Security





Operational Countermeasures

- Establish a “minimum key size” for any key negotiation process.
- Ensure that portable devices with Bluetooth interfaces are configured with a password to prevent unauthorized access if lost or stolen.
- Use application-level (on top of the Bluetooth stack) encryption and authentication for highly sensitive data communication. For example, an IPsec-based Virtual Private Network (VPN) technology can be used for highly sensitive transactions.
- Use smart card technology in the Bluetooth network to provide key management.
- Install antivirus software on intelligent, Bluetooth-enabled hosts.
- Fully test and deploy software Bluetooth patches and upgrades regularly.

m-commerce Security



Operational Countermeasures

- Deploy user authentication such as biometrics, smart cards, two-factor authentication, or PKI.
- Deploy intrusion detection agents on the wireless part of the network to detect suspicious behavior or unauthorized access and activity.
- Fully understand the impacts of deploying any security feature or product prior to deployment.
- Designate an individual to track the progress of Bluetooth security products and standards (perhaps via the Bluetooth SIG) and the threats and vulnerabilities with the technology.
- Wait until future releases of Bluetooth technology incorporate fixes to the security features or offer enhanced security features.

m-commerce Security





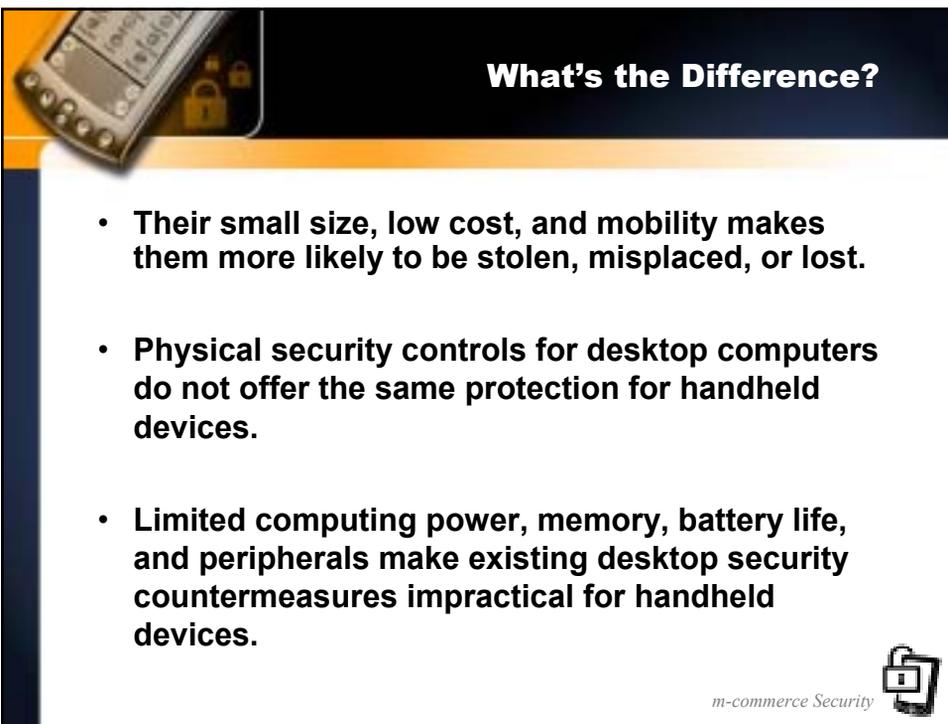
Handheld Device Security

Handheld Devices Security



m-commerce Security 

This slide features a dark blue header with the title 'Handheld Device Security' in white. Below the header is a white content area with the same title in black. A central icon shows a handheld device with a lock symbol overlaid on its screen. The bottom right corner contains the text 'm-commerce Security' and a small icon of a handheld device with a lock.



What's the Difference?

- Their small size, low cost, and mobility makes them more likely to be stolen, misplaced, or lost.
- Physical security controls for desktop computers do not offer the same protection for handheld devices.
- Limited computing power, memory, battery life, and peripherals make existing desktop security countermeasures impractical for handheld devices.

m-commerce Security 

This slide features a dark blue header with the title 'What's the Difference?' in white. Below the header is a white content area with the same title in black. The main content consists of three bullet points. The bottom right corner contains the text 'm-commerce Security' and a small icon of a handheld device with a lock.



What's the Difference?

- **Multiple access points such as the user interface, USB, expansion modules, wireless modems, Bluetooth, IR ports, and 802.11 connectivity.**
- **Handheld devices have a number of communication ports, but limited capabilities in authenticating the devices with which they exchange data.**

m-commerce Security 



What's the Difference?

- **Users are not familiar with the potential security risks introduced by these devices.**
- **Many handheld devices not originally designed with security or networking in mind.**
- **Few publications offering guidance, and the publications become quickly outdated.**

m-commerce Security 



What's the Difference?

- **New models, new capabilities, and new applications are being rapidly introduced to the market.**
- **Several new operating systems that have not been thoroughly tested by the market to expose potential vulnerabilities.**
- **There are few, if any, auditing capabilities or security tools available.**

m-commerce Security 



What's the Difference?

- **Synchronization allows PCs to mirror data stored on a handheld device, and allows the handheld device to mirror data stored on the desktop.**
- **Handheld device users can download a number of productivity, connectivity, games, and utilities freeware and shareware programs from untrusted sources.**

m-commerce Security 



What's the Difference?

- Users often subscribe to third party WISPs and access the Internet through wireless modems.
- Often purchased and used without consulting with or notifying the organization's network administrator.
- Used for both personal and business affairs.



Risks, Threats, and Vulnerabilities

Risks, Threats, and Vulnerabilities





Risks, Threats, and Vulnerabilities

- **Theft, Loss**
- **Human User Interface**
- **Insecure Default Settings**
- **Network Synchronization with Desktop PCs**

m-commerce Security 



Risks, Threats, and Vulnerabilities

- **Viruses, Trojan Horses, Worms**
- **Data Mirrored on PC and Handheld**
- **Limited PKI Support**
- **Flaws in Protocols**

m-commerce Security 



Risks, Threats, and Vulnerabilities

- **Send/Receive Information through IR Port, Bluetooth, and 802.11**
- **Network administrators have little control over these access points**
- **Limited Support for Strong Authentication**
- **Limited Auditing Capabilities**

m-commerce Security 



Risks, Threats, and Vulnerabilities

- **Personal and Business Use**
- **Wide availability of Freeware and Shareware**
- **Expansion Modules**
- **Rogue Modules**
- **Sensitive Data Stored on Removable Modules**

m-commerce Security 



Risks, Threats, and Vulnerabilities

- Ad Hoc Networks
- Untrusted networks
- Network sniffers on wireless PDAs
- WISP



Risks, Threats, and Vulnerabilities

- DoS, Spamming, SMS
- Soon to have “always-on” connectivity
- New virus strains affecting both PDA and PC
- Location Privacy
- Smart Phones





Handheld Security Checklist

Handheld Security Checklist



m-commerce Security 



Handheld Security Checklist

- **Has the security team performed a risk assessment before purchasing the devices?**
- **Are users trained or provided educational material about the device?**
- **Has a handheld device security policy been created?**
- **Does the security policy allow users to store sensitive information on the devices?**

m-commerce Security 



Handheld Security Checklist

- Are device users trained and periodically reminded of the device security policies?
- Are the devices labeled with the owner and organization's information?
- Do the users know where to report a lost or stolen device?
- Are random security audits being performed at regular intervals to monitor and track devices?

m-commerce Security

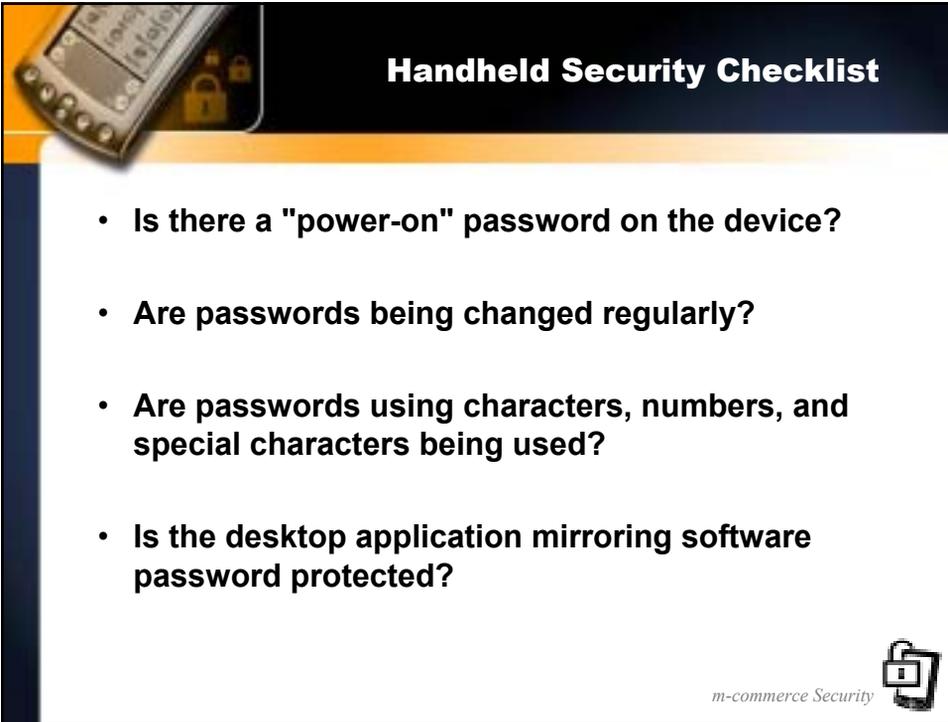


Handheld Security Checklist

- Are the devices securely stored when left unattended?
- Are add-on modules adequately protected when not in use?
- Is the risk of loss or theft minimized through the use of physical controls such as locks and cables?
- Are physical access controls in place such as photo identification or card badge readers?

m-commerce Security



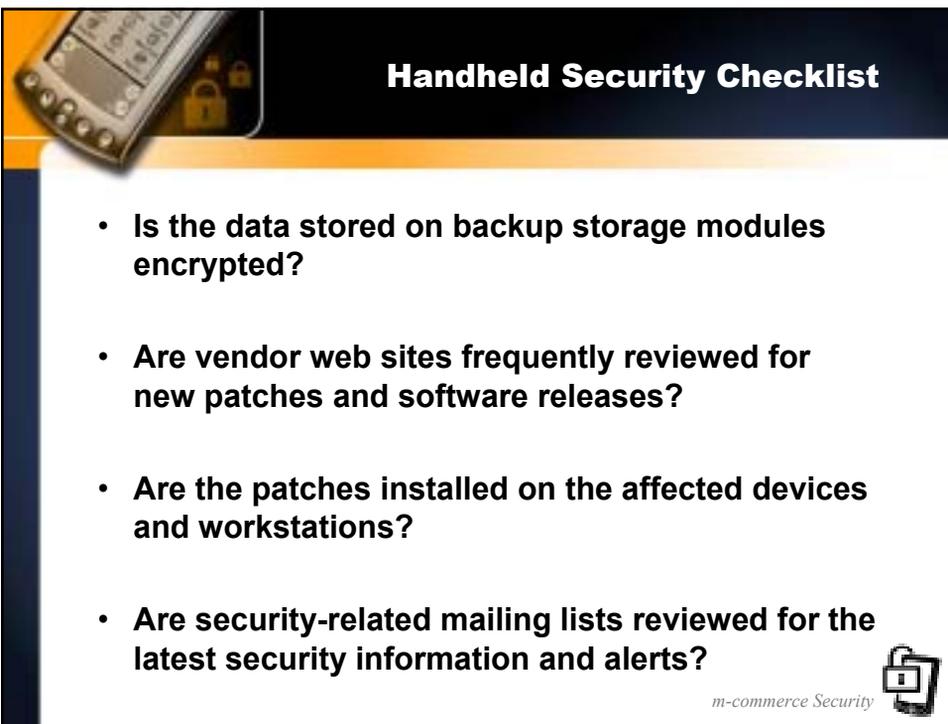


Handheld Security Checklist

- Is there a "power-on" password on the device?
- Are passwords being changed regularly?
- Are passwords using characters, numbers, and special characters being used?
- Is the desktop application mirroring software password protected?

m-commerce Security 

This slide features a dark blue header with the title "Handheld Security Checklist" in white. Below the header is a white content area with a blue vertical bar on the left. The content area contains a bulleted list of four security questions. In the bottom right corner, there is a logo for "m-commerce Security" consisting of the text and a small icon of a mobile device with a padlock.



Handheld Security Checklist

- Is the data stored on backup storage modules encrypted?
- Are vendor web sites frequently reviewed for new patches and software releases?
- Are the patches installed on the affected devices and workstations?
- Are security-related mailing lists reviewed for the latest security information and alerts?

m-commerce Security 

This slide features a dark blue header with the title "Handheld Security Checklist" in white. Below the header is a white content area with a blue vertical bar on the left. The content area contains a bulleted list of four security questions. In the bottom right corner, there is a logo for "m-commerce Security" consisting of the text and a small icon of a mobile device with a padlock.



Handheld Security Checklist

- Are default insecure settings for 802.11 and Bluetooth changed to reflect the security policy?
- Have 802.11 peer-to-peer settings been set to comply with security policy?
- Do all devices have password protection that has been changed from the default setting?
- Does the device automatically prompt the user for a password after a period of inactivity?

m-commerce Security



Handheld Security Checklist

- Are the devices being synchronized with the PC regularly?
- Is sensitive data deleted from the handheld device and archived on the PC when no longer needed on the handheld?
- Are the IR ports turned off during periods of inactivity?
- Can the handheld devices be uniquely identified for client-level authentication?

m-commerce Security





Handheld Security Checklist

- Are the devices using either a form of biometrics or smart cards?
- Has anti-virus software been installed on the handheld device and the desktop PC?
- Is the anti-virus software regularly updated?
- Does the handheld device support a firewall?

m-commerce Security 



Handheld Security Checklist

- Are internet-enabled devices using VPN technology?
- Do the devices support PKI?
- Are the PDA's provided with secure authorization software/firmware?
- Can a user be securely authenticated, both for local operations of the device and for access to remote systems?

m-commerce Security 

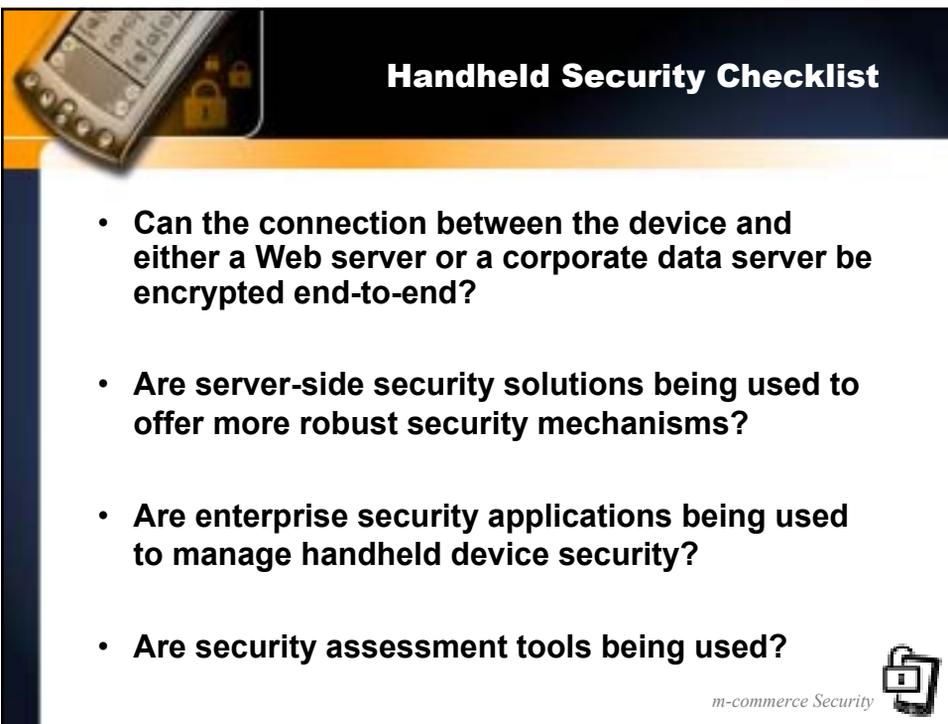


Handheld Security Checklist

- Are the devices using encryption and password protection for sensitive data files and applications?
- Is strong encryption available to protect confidential information stored on the device?
- Is strong encryption supported over both wired and wireless links?
- Are devices encrypting all data prior to transfer?

m-commerce Security 

This slide features a dark blue header with the title 'Handheld Security Checklist' in white. Below the header is a white content area with a blue vertical bar on the left. The content area contains a bulleted list of four security questions. In the top left corner, there is a graphic of a handheld device with a keypad and a lock icon. In the bottom right corner, there is a small icon of a smartphone and the text 'm-commerce Security'.



Handheld Security Checklist

- Can the connection between the device and either a Web server or a corporate data server be encrypted end-to-end?
- Are server-side security solutions being used to offer more robust security mechanisms?
- Are enterprise security applications being used to manage handheld device security?
- Are security assessment tools being used?

m-commerce Security 

This slide features a dark blue header with the title 'Handheld Security Checklist' in white. Below the header is a white content area with a blue vertical bar on the left. The content area contains a bulleted list of four security questions. In the top left corner, there is a graphic of a handheld device with a keypad and a lock icon. In the bottom right corner, there is a small icon of a smartphone and the text 'm-commerce Security'.



Security Guidance Documents

- **Computer Security Resource Center**
- **Wireless Network Security Guidance**
- **RFC April 2002**
- <http://csrc.nist.gov>
- **Other security publications**

m-commerce Security



Special Publication 800-48

The document examines the benefits and security risks of 802.11 WLAN, Bluetooth Ad Hoc Networks, and PDAs.

The document also provides practical guidelines and recommendations for mitigating the risks associated with these technologies

Over 100,000 downloads from over 50 countries

<http://csrc.nist.gov/publications/nistpubs/index.html>

m-commerce Security





Federal Information Processing Standard (140-20)

- **FIPS 140-2, Security Requirements for Cryptographic Modules, is mandatory and binding for federal agencies that have determined that certain information be protected via cryptographic means.**
- **As currently defined, the security of neither 802.11 nor Bluetooth meets the FIPS 140-2 standard.**
- **Must employ higher level cryptographic protocols and applications such as secure shell (SSH), Transport-Level Security (TLS) or Internet Protocol Security (IPsec) with FIPS 140-2 validated cryptographic modules and associated algorithms.**



Summary of Recommendations

- **Security is an ongoing process**
- **Understand Risks before wireless systems are deployed**
- **Understand technical and security implications**
- **Carefully plan deployment of these technologies**
- **Security management practices and controls are critical**
- **Physical controls are especially important**
- **Enable, use, and test security features**
- **(FIPS) 140-2 *Security Requirements for Cryptographic Modules***





Contact

- **T. Karygiannis**
NIST
Computer Security Division
karygiannis@nist.gov
- **Les Owens**
Booz Allen Hamilton
owens_les@bah.com

