



NIH Perspective on Handheld and Wireless Technology: Security

By:
Jean-Paul Boucher



Agenda

- Introduction: What can wireless handheld technology do?
- What is Wireless?
- How do Handhelds Connect?
- Handheld Security Concerns
- Current and Potential Applications
- The Future
- Summary



What can Wireless Handhelds Do?

- **Changes the way work is done**
 - No longer constrained by physical interconnection mechanisms
 - No longer tied to specific computing platforms
 - No longer bounded by traditional working hours
- **Benefits – Improving effectiveness**
 - Increased responsiveness
 - Increased productivity
 - Increased efficiency

.....
Allows the right information to be made accessible to the right person where ever and whenever needed



What is Wireless?

- Personal Area
 - Bluetooth
 - IrDA
- Local Area
 - 802.11b
- Wide Area
 - CDPD
 - SMS
 - GSM/GPRS



Personal Area Network (PAN)

- **Infrared (IR)**

- Line of sight and short distance
- Generally well supported on laptops



- **BlueTooth**

- Multi-device cable replacement technology - IEEE open standard
- First generation interoperability issues
- Immediate Security concerns with auto-negotiation and auto-discovery



Local Area Wireless Networking (LAWN)

- 802.11b, 802.11a, 802.11g, ...
- Wi-Fi for interoperability “certification”
- Security Concerns
 - Poor configuration control
 - Protect wireless network like a Internet connection
 - Encrypt at link layer and data layer (do NOT rely on WEP alone)
 - Protect the perimeter with firewalls
- Wireless “hotspots” lead to personal firewalls



Wireless Wide Area Networking (WWAN)

- 2-way Pager Networks
 - Mobitex
 - DataTac
- Cellular Networks – speeds in Kbps
 - CDMA – 14.4K
 - TDMA – 14.4K
 - GSM (and GPRS) – 200-300 K (but expect 20-30)
 - 3G – now 144K



How do Handhelds Connect?

- Synchronize
 - Data on device is static once removed from cradle
- Pull
 - User makes a wireless connection manually (basically a wireless synchronization)
- Push
 - Device automatically connects to data and gets any new changes without interfering with workflow

.....
Appropriate connection types will be determined by the application and user need



Handheld Security Concerns

- On Device Security
 - Password Locking / Remote Locking/Wiping
 - On Device Data Encryption
 - External Connection Locking
- Wireless Network Security
 - WEP
 - Encryption
- Data Security
 - Digital Signatures (PKI)
 - VPN



On Device Security

- Locking the Device
 - Screen Lock
 - Should only give a certain number of tries before locking the device completely
 - Should be activated after a certain amount of time (non-use)
 - Remote Lock / Wipe
 - Should have system for locking and wiping lost or stolen devices
 - Lock should control all access to device, including external ports (serial, SD, etc.)
- Data Encryption on Device
 - Screen locks do not encrypt the databases on the device



Wireless Network Security

- WEP (Wired Equivalent Privacy)
 - Supposed to provide same security as wired networks
 - Security is very low and should never be relied on solely to encrypt data communications
- Authentication
 - To gain access to wireless network, the user must have rights
- Encryption
 - How data is actually sent on wireless network

.....
NIH Wireless TLC Group currently drafting wireless network policy to address situation

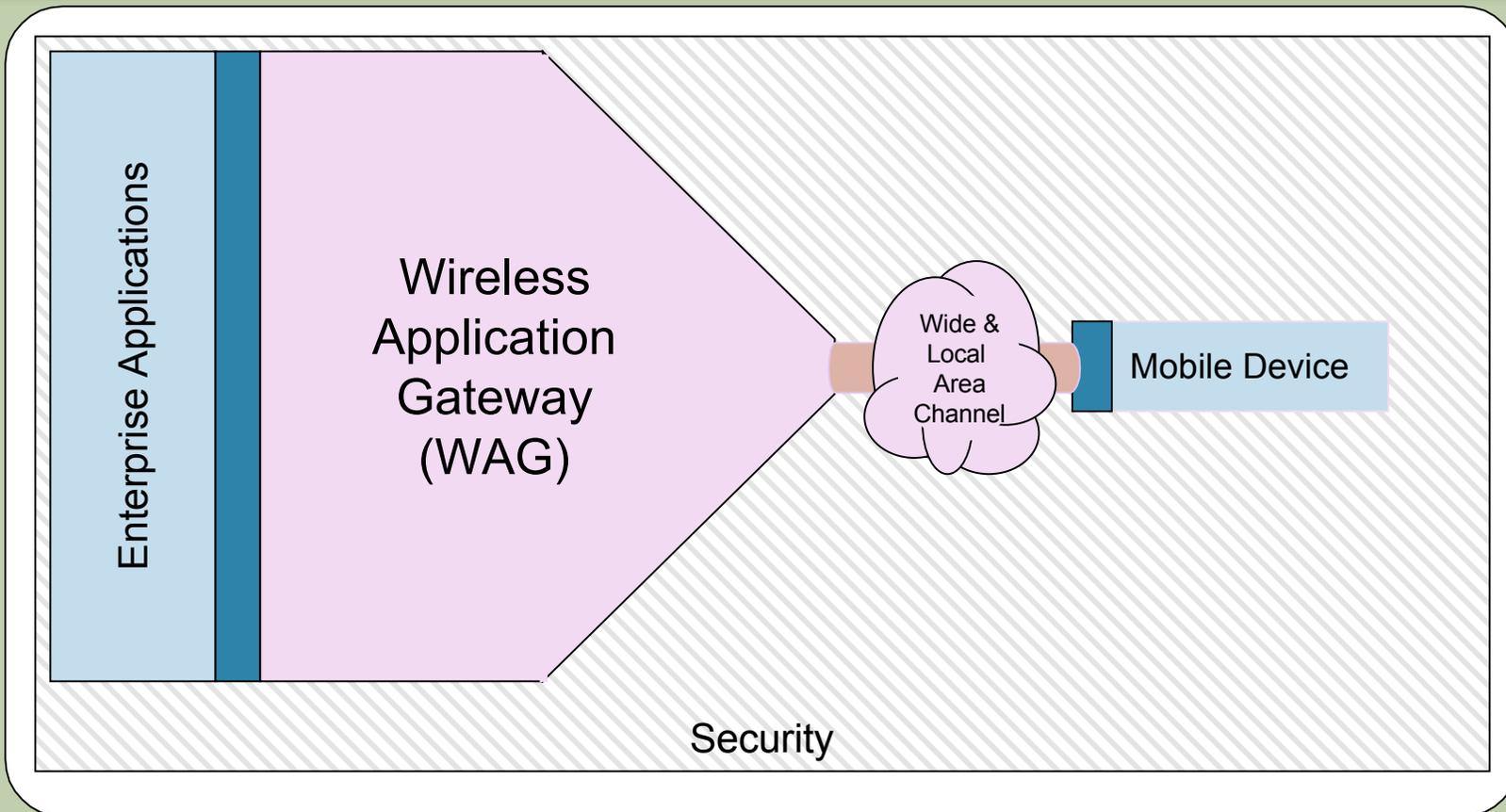


Data Security

- Digital Signatures (PKI- Public Key Infrastructure)
 - The capability of assuring that the information that was received is the same as the information that was sent
 - NIH and HHS already have PKI infrastructure
 - Secured mail for sending patient information is already being used in the Clinical Center and around NIH
- VPN (Virtual Private Network)
 - A way to “tunnel” into the internal network from the outside creating a secured connection
 - NIH has a pilot VPN solution undergoing testing



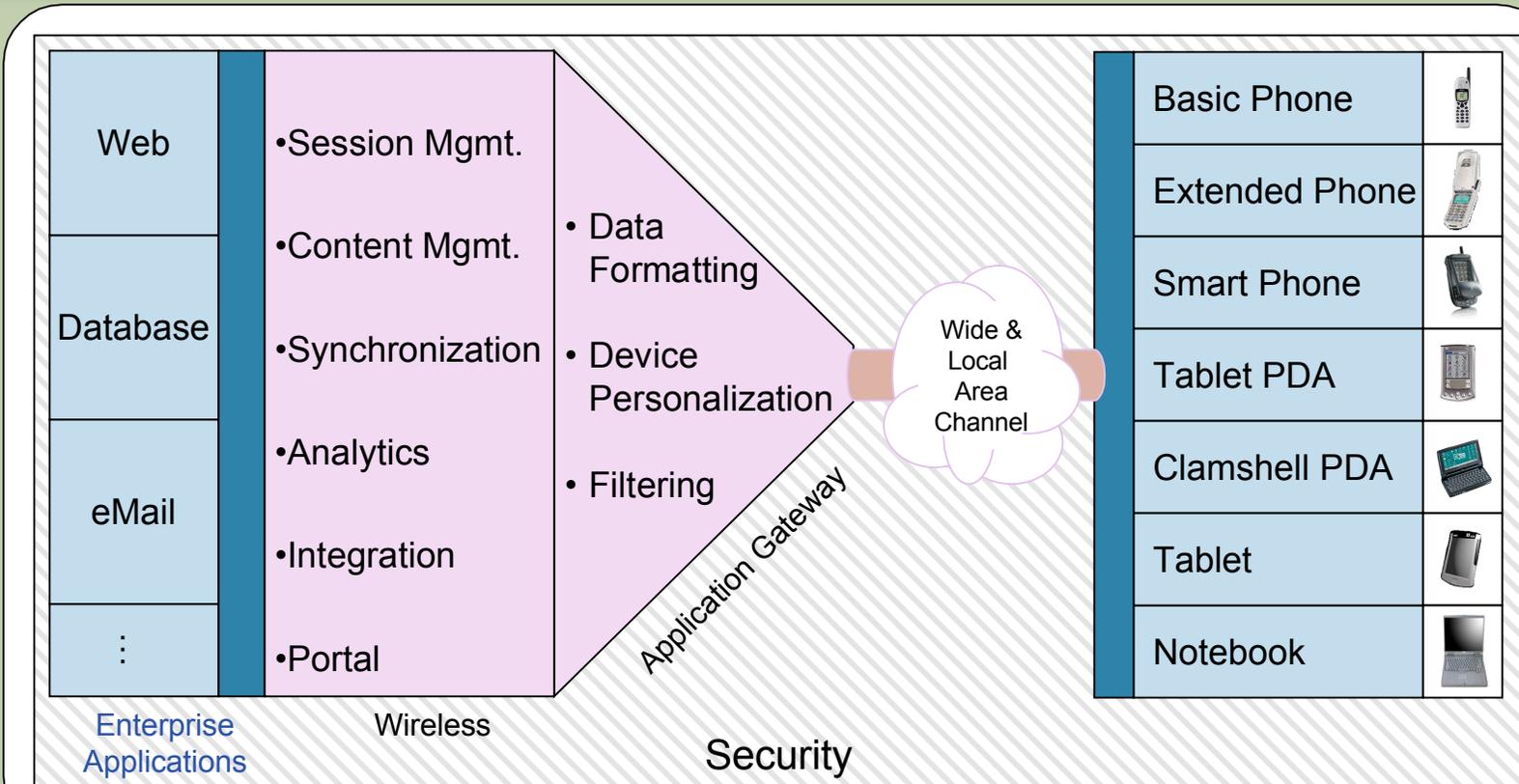
Wireless Application Components



View wireless gateway products like middleware products



Wireless Application Components



View wireless gateway products like middleware products



Current Wireless Applications

- NIH BlackBerry Service
 - Push data access to email, calendar, and databases
 - National and international service
- NIH AvantGo Service
 - Cross platform secured web service for handheld devices
 - Currently running wireless ITAS, PubMed, NCI Intranet, Portal, and several other applications
- Working with Johns Hopkins Antibiotic application



Current Wireless Continued

- Wireless Networking on Campus
 - Nearly every building and all IC's have implemented a test of wireless networking
 - Clinical Center has installed and is currently testing hospital wide system





Potential Application of Handhelds at the NIH

- Requirements Analysis
- Implementation Plan
- Enterprise Application Changes, if any
- Product Evaluation and Testing
- Application Development, if any
- Implementation and Rollout
- Post Deployment Support
- Technology Refresh and Upgrades

.....
Just like other types of implementation efforts



The Ideal Device?

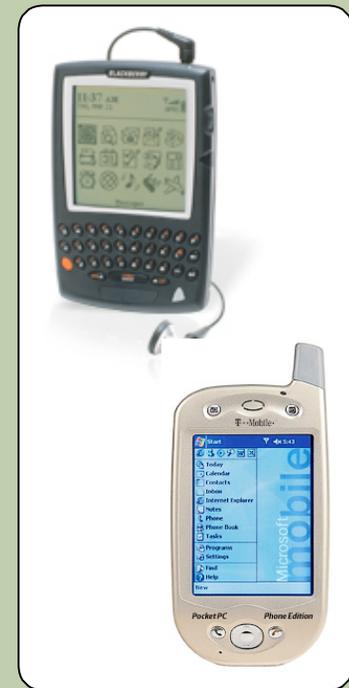


.....
Needs are different and so every user's ideal device will be different



The Future

- “Faster” wireless networks
 - LAWN - 802.11a/g “secure” 802.11i
 - WWAN - GPRS / 3G (CDMA2000)
- Hybrid Devices
 - Voice and data all in one and then back out
- Other radical changes
 - Input technologies - voice
 - Display technologies - virtual displays
 - Battery technologies - AM radio waves



Summary

- Wireless can change the way you work
- Security must be the first thought and must never be compromised just to include technology
- Real success comes with integration of essential toolsets, not just toys



