Session #G4
Mobile Device Insecurity

MIS TRAINING INSTITUTE

Mobile Device Insecurity

Session #G4

Joe Grand

Grand Idea Studio, Inc.

Thursday, 10:30am - 12:00pm

Goals

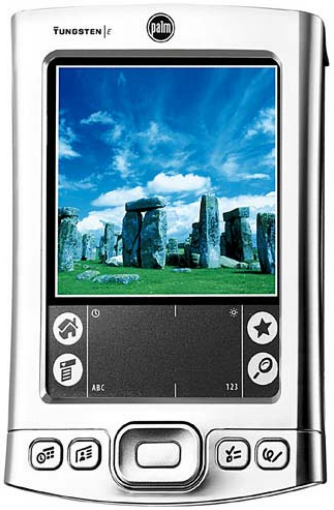
- Understand classes of problems
- Learn security risks and protection methods
- Education by demonstration

By The Numbers...

- Palm OS: Over 30 million units sold to date, 4.5 million units sold in 2005
- Windows Mobile (Pocket PC/Windows CE): 48.1% of Q3 2004's 2.8 million PDA sales
- Over 15 million Symbian-based devices sold to date, 6.67 million sold in 2003 alone
- Over 1 million RIM BlackBerry devices sold to date
- About 200 million North Americans use mobile phones

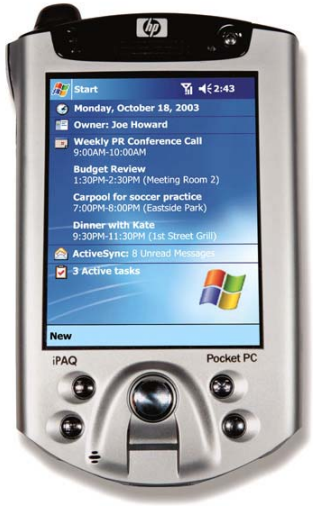
The Major Players: Palm OS

- Ex.: Palm, Sony, IBM, Kyocera, Samsung, Qualcomm, Symbol



The Major Players: Windows CE / Pocket PC

- Ex.: Microsoft, HP, Compaq, Sony, Cingular, Gateway, JVC, Dell, Fujitsu, Toshiba, Panasonic, Symbol



The Major Players: Symbian OS

- Ex.: Nokia, Psion, Sony Ericsson, Motorola, Siemens, FOMA, Panasonic

The Major Players: Others

- Ex.: T-Mobile SideKick II, RIM BlackBerry 7250

Common Uses

- Personal
  - **Phone numbers, memos, to do lists, diaries**
- Security/Network Admin
  - **IP addresses, network maps, usernames & passwords, authentication tokens, one-time-password generation**
- Medical
  - **Patient information, medications, treatments**

Common Uses 2

- Government/Military
  - **Schedules, sensitive/secret information**
- Wireless
  - **WWW, E-mail, Instant Messaging, e-commerce**
- Gaming/Social Networking

Current Risks

- Mixing business with pleasure
- Admin, users not aware of the existing security problems
  - **Existing security mechanisms weak and/or flawed**
- Most devices have no security framework
  - **No access control or data/memory protection**
  - **Data is stored as plaintext in accessible memory**
  - **Hardware can be directly accessed by the user through software**
  - **No physical secure hardware design methods**

Current Risks 2

- Being employed in security-related apps
  - **One-time-passwords & authentication tokens**
  - **Storage of private/confidential information**
  - **E-commerce, wireless payment**
- Cannot have secure apps on top of an insecure platform
  - **Third-party apps are simply a road-block for an attacker, not 100% protection**

Current Risks 3

- "Always on" technologies
  - **Open to the outside world...all the time**
  - **Ex.: WiFi, Bluetooth, IR**
  - **Ex.: Laptops on airplane trying to connect w/ no user interaction**
- External memory cards
  - **Supported on most all new mobile devices**
  - **Easy to steal**
  - **Some devices load apps upon insertion**

The Good News

- New devices are taking security more seriously
- Some vendors used to get defensive…now they are actually incorporating changes
- Security features designed into Palm OS Cobalt 6.1
- Windows Mobile 2003, Windows Mobile 5.0, Linux, Java devices provide abstraction of user v. OS v. hardware
- But...device should still be fully tested and analyzed before deployment

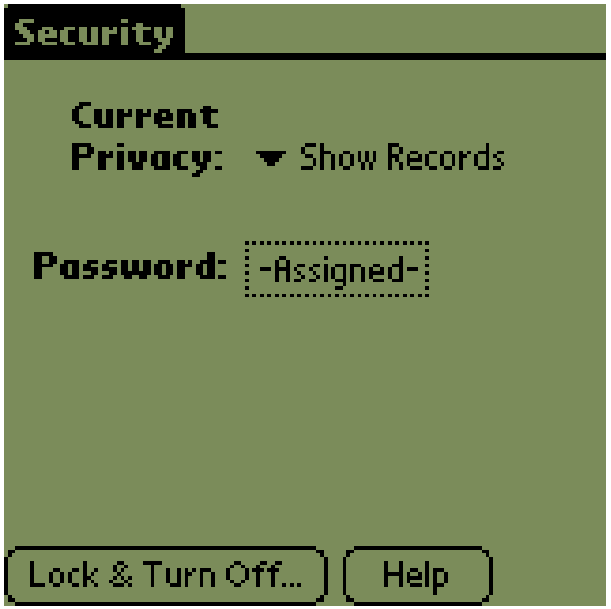
Access to Data

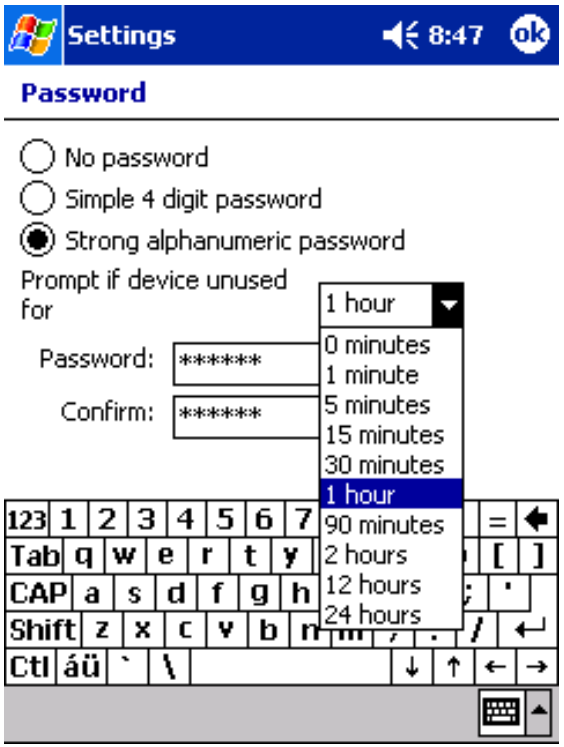
- Double-edged sword
  - **Could be used for good or evil**
- Many tools exist
  - **Ex.: pdd, PDA Seizure, Cell Seizure, pilot-link, plp-tools, PDAZap**
- System Password Retrieval
- Debug Modes and Sync Interfaces
- Physical Access

System Password Retrieval

- Power-on and data protection using a password
- Often weak obfuscation, not encryption
- Password re-use
  - **Human nature: Easier to remember a single password**
  - **Can lead to attacks on other computers, ATM, voicemail**

System Password Retrieval 2



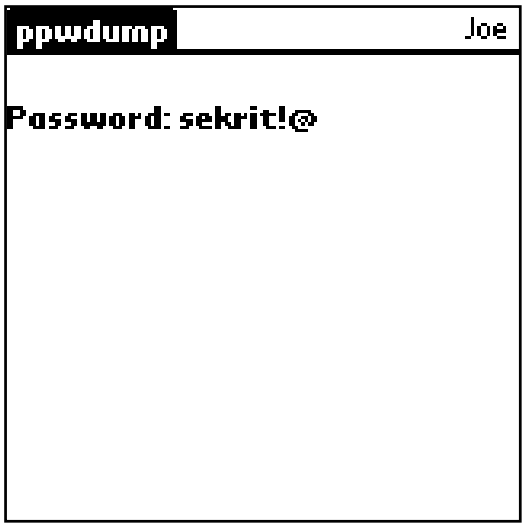


System Password Retrieval: Palm OS < 4.0

- Max. 32 characters ASCII
- Reversible obfuscation method (XOR against constant)
- Can retrieve password/hash [1]:
  - **During HotSync operation (IR, Serial, Network)**
  - **“Unsaved Preferences” database**
  - **On host PC: `\Palm\users.dat`**
  - **On host Mac: `Palm:Users:Palm Users`**
  - **On Palm: ppwdump, NotSync**

System Password Retrieval 2: Palm OS < 4.0

- Demo: Retrieve and decode password using ppwdump
- Recommendations:
  - **Upgrade to device running newer version of Palm OS**



System Password Retrieval: Palm OS >= 4.0

- Max. 32 characters ASCII
- Encoded block is 128-bit MD5 hash
- One-way hash (not reversible)
- Dictionary attack using common words
  - **Take advantage of short passwords**
  - **Can use pre-computed hashes for quick comparison (`www.rainbowtables.net`)**

System Password Retrieval: Windows Mobile

- ActiveSync used for all communication between PC and device
  - **Available through serial, USB, IR, TCP/IP, Bluetooth**
  - **No confidentially of transferred data**
- For ActiveSync <= 3.0, reversible obfuscation method (XOR against constant)
  - **Can retrieve password/hash in host PC registry [2]:** `HKEY_CURRENT_USER\Software\ Microsoft\Windows Ce Services\Partners`

System Password Retrieval: Windows Mobile 2

- On some devices, 4-digit PIN used for authentication can be brute-forced manually or programmatically [3]
- Pocket PC registry accessible by any user on the device
  - **Ex.: PHM Registry Editor, `www.phm.lu/Products/PocketPC/RegEdit` and PPTools**
  - **Ex.: PPP network passwords stored in plaintext**

System Password Retrieval: Windows Mobile 3

- Can change Control Panel Applet (cpl) entry in registry to load another app on power-up
  - **Microsoft "Let Me In: Pocket PC User Interface Password Redirect Sample" example, Q314989, `http://support.microsoft.com/default.aspx?scid=kb;en-us;314989`**

System Password Retrieval: Mobile Phones

- Password/PIN is usually limited to 4 digits
  - **Ex.: Last 4 digits of phone number, pattern (0000, 1111, 1234, etc.)**
  - **Users often use same PIN on phone as they do for voicemail and ATMs**
- Most, if not all, have diagnostic/administration menu
  - **Some accessible through keypad, others with hardware cable**
  - **Ex.: Nokia DCT-3 and DCT-4 series phones**

Palm Backdoor Debug Mode

- Exists for debugging during app development
- Can use to bypass “System Lockout” functionality [4]
- Can install/delete/run apps, view raw memory, hard reset, export databases
- Third-party security apps at risk
  - **Ex.: Obtain plaintext components from memory, install “keystroke monitor” to retrieve passwords**

Palm Backdoor Debug Mode 2

- Demo: Display databases and memory
- Demo: pdd to retrieve exact device RAM image
- Recommendations:
  - **Physically prevent access to HotSync port**
    - Hardware lock (Ex.: Kensington, Targus, Belkin)
    - Plastic glued into place, permanently disabling port
    - Cutting specific traces on circuit board
  - **Employ a third-party security solution**
    - Ex.: Credant Mobile Guardian, Utimaco SafeGuard PDA

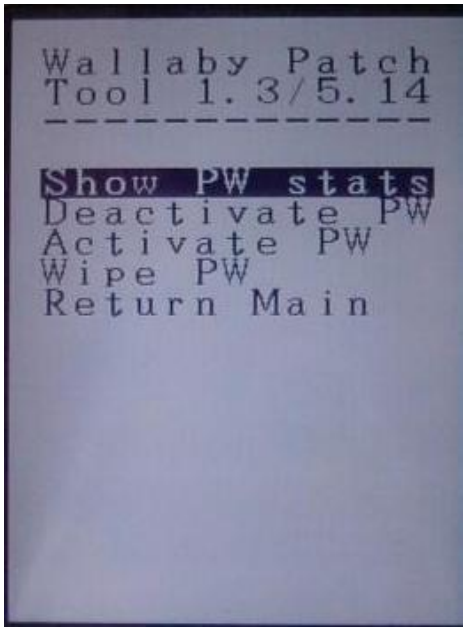
Visual Studio .Net Debugger

- Exists for debugging during app development
  - **Provides remote debugging and device access to Windows Mobile**
  - **Developer's documentation publicly accessible**
  - **Uses ActiveSync protocol**
- Can access Pocket PC registry, install/delete/run apps, export databases

XDA

- OEM/private label PDA manufactured by HTC in Taiwan
- Resold as the O2 XDA, Otek, MDA, SX-56, etc.
- Commonly used in Europe
- Special mode to recognize diagnostic external memory cards and can execute code directly from them
- Provides a detailed debugging and diagnostics interface through sync port
- Bootloader allows access to a device without passing any access controls

XDA 2



Source: "The Phone in the PDA," Job de Haas, Black Hat Amsterdam 2003

Psion Link Protocol (PLP)

- Proprietary protocol between device and PC
- Partially reverse-engineered and documented
- Full access to data on all drives (internal and external)
- Can be accessed even if system lock-out is enabled
- Ex.: plp-tools, PDA Seizure (hopefully soon)

Physical Access to Data

- Physical attack often more difficult than software attack, but still possible with the right tools and without detection
- Secure hardware design principals not employed
  - **Possible to open device and read memory**
  - **No detection of tampering**
  - **No erasure or protection of critical data**
  - **Access data using manufacturing test interfaces (e.g., JTAG)**

Physical Access to Data 2

- Recommendations:
  - **Be aware of physical location at all times**
  - **Store critical data on external memory card and remove when not in use**
  - **Look for physical anomalies on housing (e.g., stripped screw heads, pry marks on case)**

Attack Vectors & Malicious Code

- Three stages:
  - **Infection**
  - **Storage**
  - **Actions**
- Threat not as pervasive as on PC, yet...
  - **McAfee: 50 mobile malware threats in the wild**
  - **McAfee: By 2005, malicious mobile phone attack will have potential to infect 33% of users within 3 days**

Infection

- Application installation procedure
- Desktop conduits
- External memory cards
- Network connectivity
- Wireless communications
- Telephony

Infection: Application Installation

- Installation procedure for Palm, Pocket PC, and BlackBerry all very simple and similar
  - **Palm: Apps to be loaded are copied into `/Palm/<user>/Install`**
  - **Pocket PC: Apps to be loaded are copied into directory listed in `HKLM\Software\Microsoft\Windows CE Services\InstalledDir`**
- No confirmation or authentication exists
- Recommendations:
  - **Manually check installation directory before sync**

Infection: Desktop Conduits

- Used to enable transfer of data between device and specific desktop application
- Standard conduits exist
  - **Palm: HotSync**
  - **Pocket PC: ActiveSync**
  - **Psion/EPOC16/EPOC32: PsiWin, plp-tools**
- Route data to Personal Information Manager (PIM) or third-party application
  - **Microsoft Outlook/Exchange/Office, iCal, Lotus Notes, etc.**

Infection: Desktop Conduits 2

- Possible for cross-architecture transfer
  - **Mixing business with pleasure**
  - **Ex.: Windows PC to/from Pocket PC**
- Could exploit a known security problem in the destination desktop app
- Recommendations:
  - **Only synchronize your device with trusted desktop**
  - **Use anti-virus software on both platforms to scan incoming data before passing it to destination app**

Infection: External Memory Cards

- Most all devices have support for external memory cards
  - **Ex.: SD, MemoryStick, SmartMedia, CompactFlash**
- Some devices will auto-run applications directly from memory card upon insertion
  - **Pocket PC: AutoRun**
    - Will bypass system password protection
    - Copious amounts of documentation on MSDN
  - **Palm (Sony): MemoryStick Autorun**
  - **XDA**

Infection: Network Connectivity

- Devices with TCP/IP or other network functionality provide additional attack vectors
  - **Ex.: Remote attacks against device**
  - **Ex.: Attacks against network from compromised device**
- Pocket PC: ActiveSync listens on Port 5679 for remote connection
  - **Can launch Denial of Service by continuously establishing and closing connection**

Infection: Network Connectivity 2

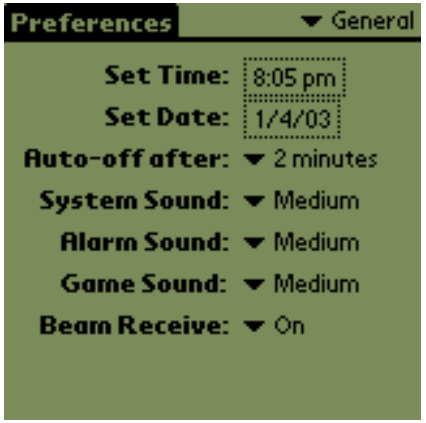
- Palm: System password hash can be retrieved by sniffing network traffic
- Recommendations:
  - **Don't use Palm HotSync or Windows ActiveSync on an unencrypted/ untrusted network**
  - **Disable all unneeded network connections, if possible**
    - Ex.: ftpd, telnetd

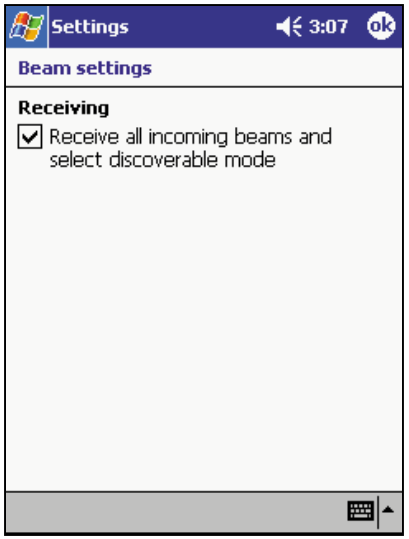
Infection: Wireless, IR/IrDA

- Point-to-point, close quarters
- No native authentication
- Viable conduit for propagation with collusion on the receiving end
- Ex.: Trick the recipient into accepting a malicious program

Infection: Wireless, IR/IrDA 2

- Recommendations:
  - **Disable IR port until needed**
  - **Common sense: Do you trust the other party?**
  - **Extreme: Do not accept any beamed connections**
  - **Extreme: Put electrical tape over the IR port to prevent connections**





Infection: Wireless, RF

- Suitable for longer-distance communications
- Many different protocols, each with their own security problems
  - **WiFi/802.11b, Bluetooth, GPRS, Mobitex**
- Ex.: Sending malicious e-mail or attachment to the device
  - **Buffer overflow or SMS message to intentionally crash device**

Infection: Wireless, RF 2

- Recommendations:
  - **Disable wireless functionality until needed**
  - **Disable all server applications (e.g., web, FTP)**
  - **Add passwords to Bluetooth services if possible**

Infection: Telephony (SMS/GPRS)

- SMS Attacks
  - **Broken UDH caused crash in some Nokia phones**
  - **Spoofed SMS messages: Originating Address field can be arbitrarily set to anything**
  - **Ex.: Virus propagated via SMS by resending itself to all phone numbers in the device's address book**
- Pocket PC: GPRS connections do not require user confirmation
  - **Ex.: Connection can be established by Trojan horse**

Infection: Telephony (MMS)

- Multimedia Message Service (MMS)
  - **Advanced version of SMS to send pictures, sound, video, etc.**
  - **March 7, 2005: First confirmed virus "CommWarrior" for Symbian OS 6.1 Series 60 (`www.infosyncworld.com/news/n/5835.html`)**
    - Scans the infected phone's address book and sends MMS messages and a copy of itself to randomly selected contacts
    - Also attempts to infect nearby devices w/ Bluetooth

Storage and Payload Hiding

- User data areas
- Flash memory

Storage: User Data Areas

- User data and applications typically stored in RAM
- Malicious code would save program or payload into a standard area
  - **Palm: Database**
  - **Pocket PC: Application Shared Space**
- Possible on many portable devices due to lack of protection/access control of data
  - **Palm OS >= 5.0 and Windows Mobile > 2003 has code signing support to verify integrity of data on device**

Storage: Flash Memory

- Flash ROM increasingly being used for OS storage
  - **Current devices vulnerable due to no protection or secure hardware mechanisms**
- Unused space likely for malicious app storage
  - **Anti-virus software does not currently detect access**
  - **Palm: 128-2424kB free**
  - **Pocket PC: Many MB free**

Storage: Flash Memory 2

- Legitimate third-party applications exist to backup data into free areas of Flash
- Ex.: HandEra JackFlash, Datalight FlashFX
  - **Malicious code could use same functionality**

Actions

- Flash memory modification
- Register manipulation
- Further attacks or virus propagation

Actions: Memory Modification

- Any data not stored in protected Flash ROM areas is subject to erasure or modification
- Ex.: Rewriting OS with Trojan, modifying or destroying critical system data
- Devices provide "boot loader" for OS and Flash upgrades
  - **Ex.: XDA, Pocket PC Phone, Zaurus**
- Recommendations:
  - **Use an older device that stores OS in read-only memory (ROM) which is non-rewritable**

Actions: Register Manipulation

- Lack of layer control allows user apps to directly access hardware via memory mapping
- How to detect with anti-virus software?
  - **Hard to distinguish between legitimate and malicious access**

Motorola DragonBall Register(s)	Potential Effects
Phase-Locked Loop (PLL) and Power Control	System can be halted
Chip-Select and Addressing	Corrupt memory maps making code and data fetches impossible
LCD Control Module	Affect LCD functionality

Actions: Further Attacks & Virus Propagation

- Platform could be used as a launch pad for additional attacks or malicious code propagation
- Ex.: Attacker to use device to mask steps
- Ex.: Virus propagated via SMS by resending itself to all phone numbers in the device's address book

General Recommendations

- Make regular backups of mobile device data
- Keep up to patch level on all desktop and handheld apps (e.g. Palm Desktop, MS ActiveSync, etc.)
- Use power-on password and encryption to protect data
  - **Adds an additional layer of “security”**
- Anti-virus tools exist
  - **Do not protect from many of weaknesses (yet)**
  - **Install anyway to add another "layer" of security**

General Recommendations 2

- Be aware of:
  - **Physical location**
  - **What critical information you are storing**
  - **What apps are being installed onto the device**
- Store critical data on removable memory and keep with you at all times
- Monitor synchronization logs
- Use VPNs on mobile device if possible

Conclusions

- Understand the risks and implement recommendations
- Hard, if not impossible, to detect tampering and data theft
- Most products not designed for security
  - **Vendors are starting to take steps**
- Simplistic and common classes of problems
  - **No access control**
  - **Weak user authentication**
  - **Many avenues for malicious code**

Conclusions 2

- Malicious code propagation is a real threat, though not yet fully realized
  - **As mobile device use becomes more widespread, risks become amplified**

References

1. J. Grand (Kingpin), “Palm OS Password Retrieval and Decoding,” September 2000, **`www.grandideastudio.com/files/security/mobile/palm_password_decoding_advisory.txt`**
2. Hernan Ochoa, “ActiveSync 3.0 Vulnerability: Obtaining the Partnership's Password.”
3. Pascal Meunier, et al, "ActiveSync, TCP/IP and 802.11b Wireless Vulnerabilities of WinCE-based PDAs," CERIAS Technical Report 2002-17.
4. J. Grand (Kingpin), “Palm OS Password Lockout Bypass,” March 2001, **`www.grandideastudio.com/files/security/mobile/palm_backdoor_debug_advisory.txt`**

Additional Resources: Palm OS

- PalmSource, Palm Software and Palm OS Web Page, **`www.palmsource.com`**
- Grand Idea Studio, Mobile Device Security Web Page (pdd, Ointment, NotSync, PalmCrypt, TBA, BeamCrack), **`www.grandideastudio.com/portfolio/index.php?id=1&prod=17`**
- HandEra, JackFlash, **`www.handera.com/Products/JackFlash.aspx`**

Additional Resources: Pocket PC

- Microsoft, Windows Mobile Web Page, **`www.microsoft.com/windowsmobile/default.mspx`**
- Pocket PC Developer Network, **`www.pocketpcdn.com`**
- ITSX Pocket PC Resources, **`www.itsx.com/pocketpc`**
- XDA Developers, **`www.xda-developers.com`**
- Datalight, FlashFX, **`www.datalight.com`**

Additional Resources: Forensics

- J. Grand, “pdd: Memory Imaging and Forensic Analysis of Palm OS Devices,” Proceedings of the 14th Annual Computer Security Incident Handling Conference, Waikoloa, Hawaii, June 2002, **`www.grandideastudio.com/files/security/mobile/pdd_palm_forensics.pdf`**
- Paraben Forensics, PDA Seizure and Cell Seizure, **`www.paraben-forensics.com`**
- M. Burnette, “Forensic Examination of a BlackBerry Wireless Device,” **`www.rh-law.com/ediscovery/Blackberry.pdf`**

Additional Resources: Wireless

- William Arbaugh, Wireless Research Web Page, **`www.cs.umd.edu/~waa/wireless.html`**
- Ollie Whitehouse, "War Nibbling: Bluetooth Insecurity," October 2003, **`www.atstake.com/research/reports/acrobat/atstake_war_nibbling.pdf`**
- Job de Haas, “SMS Security,” 2001, **`www.itsx.com/hal2001/hal2001-itsx.ppt`**

Additional Resources: Anti-Virus

- F-Secure, Handheld Solutions Web Page, **`www.f-secure.com/wireless`**

Thanks!

Joe Grand
Grand Idea Studio, Inc.

joe@grandideastudio.com