



Mobile User Security

Dave Piscitello
**MediaLive International &
Core Competence, Inc.**

What We'll Cover ...

- **Mobile user landscape and forecast**
- **Threats to Mobile users and devices**
- **Policy considerations for mobile users**
- **Security measures for mobile users**



What We'll Cover ...

- **Mobile user landscape and forecast**
- **Threats to Mobile users and devices**
- **Policy considerations for mobile users**
- **Security measures for mobile users**



Mobile User Landscape and Forecast

- **Workforces are becoming more mobile**
 - **60% of workers owned multiple mobile devices at the end 2003**
 - **65% of Global 2000 companies to support mobile data by 2004**
(Source: Gartner)
- **Handheld adoption continues to grow**
 - **Global sales to grow from 15M units (2001) to 61M (2008)**
(Source: In-Stat/MDR)
- **Laptops**
 - **25% percent of global system shipments in 2003**
 - **Expected to climb to 36.6 percent of the total by 2008**
(Source: IDC)

Handhelds and tablets: the Future?

- **Improved application platforms**
 - Mobile phones becoming more like handhelds, handhelds more like laptops, and laptops are more versatile than ever
 - Faster CPU, more RAM, improved Operating Systems
 - Form factors to satisfy diverse user needs
 - Internet applications replace PIM as reason to use handhelds
 - ◆ Email, IM, SMS, Web, and enterprise web services
- **Better bandwidth and connectivity**
 - By 2007, 75% of PDAs will offer integrated Internet access
 - Nearly all new laptops come with 802.11, IrDA
 - Higher-bandwidth options increasing
 - Dual Mode will soon mean “3G telephony and 802.11”

Mobile Devices Extend Network Perimeters

- Travelers, field staff, and teleworkers need connections to their organization's resources
 - Usually it's some form(s) of wireless
- Connection speed, distance vary
 - Wireless Personal Area Networks (WPANs)
 - ◆ IEEE 802.15 Bluetooth, IrDA
 - Wireless Local Area Networks (WLANs)
 - ◆ IEEE 802.11 (a,b,g) Wi-Fi
 - Wireless Wide Area Networks (WWANs)
 - ◆ 2nd and 3rd generation cellular telephony

The Remote Endpoint Conundrum

- **Once connected, mobile devices**
 - **Are clients on the company network, like stationary PCs**
 - **Provide access to business-critical applications, as well as potentially sensitive and regulated information**
- **Remote endpoints increase business productivity, convenience, and flexibility but they also pose challenges**
 - **Assigning and tracking mobile device assets**
 - **Provisioning software and services**
 - **Controlling mobile device access to corporate resources**
 - **Monitoring health, usage**
 - **Defending against loss, compromise, attack**

What We'll Cover ...

- Mobile user landscape and forecast
- Threats to Mobile users and devices
- Policy considerations for mobile users
- Security measures for mobile users



Threat: Lost or Stolen Mobile Devices

- **Handhelds are small, portable – and forgettable!**
 - **Easily mis-placed or mis-appropriated**
 - **Usually lost in a public venue (airport, hotel, customer site)**
 - **Ultra-lite laptops and tablets have same properties**
- **Possible consequences**
 - **Loss of proprietary data stored on device**
 - **Abuse of stolen user credentials (logins, passwords)**
 - **Unauthorized wireless Internet use**
 - **Wireless attack on company's network portal**

Threat: Compromised Mobile Devices

- **Handhelds are relatively easy to attack**
 - Defaults promote ease of use, not security
 - Insecure boot process, little/no memory protection
 - Fewer/different security tools available for handhelds
 - Browsers vulnerable to ActiveX object and Javascript attacks
 - Users don't realize that data remains when you throw it away
- **Possible consequences**
 - Downloaded malware can erase information and applications, infect other devices and enterprise servers
 - Devices can be crashed by simple network-borne attacks
 - Trojan on a handheld can be used to attack other systems

Mobile phones are vulnerable, too!

- **Denial of service attacks: IM, SMS and email flooding**
 - Messages can be sent anonymously
 - Many phones cannot reject or disable incoming messages
 - Once DOS'd, phones cannot message or place/receive calls
 - ◆ Examples: PPC2002/2003, Treo 300/600, Nokia 3595
- **Buffer overflow attacks**
 - Use ringtone payload or attack application client on smartphone
 - “Own the phone”, embed program in payload to
 - ◆ Send SPIT
 - ◆ Upload sensitive data (e.g., contacts) to attacker's system
 - ◆ Propagate worm via SMS

Threat: Compromised Airlink

- **Wireless links increase mobile device vulnerability**
 - **Eavesdropping on cleartext wireless traffic**
 - **Message forgery and replay over wireless**
 - **Weak authentication and access controls are common**
- **Possible attack vectors for anyone within radio range**
 - **Attackers may use device's address to gain network access**
 - **Captured login traffic can be analyzed to crack passwords**
 - **Rogue access point can intercept, modify wireless traffic**
 - **Airlink itself can be used to launch denial-of-service attacks**

Won't happen to you?

- **1.6M computers stolen 2001-2003, majority were laptops**
(Source: SafeWare Insurance)
- **Fewer than 30% of the 250,000 phones and PDAs lost, left or stolen at airports in 2001 were recovered**
(Source: Gartner)
- **Virus infection & corruption/damage are top 2 mobile device hazards (more frequent than loss/theft)**
(Source: Tech Republic)
- **51% of companies surveyed had experienced WLAN security incidents during past year**
(Source: JupiterMedia)

What We'll Cover ...

- Mobile user landscape and forecast
- Threats to Mobile users and devices
- Policy considerations for mobile users
- Security measures for mobile users



Begin by Developing a Mobile User Policy

- **Ignoring mobile devices is not a viable option**
 - **Employees buy their own, and use them anyway**
 - **Mobile devices will invariably hold your sensitive information**
 - ◆ **Customer contacts, calendars**
 - ◆ **Marketing data, contracts, proposals**
 - ◆ **Email and messaging archives**
 - ◆ **User accounts and credentials**
- **No policy usually results in little or no security**
 - **How many users lock personal mobile devices?**
 - **How many users realize their PDA or laptop may accept Infrared connections by default?**

Manage Risk

- **Just because it CAN happen doesn't mean it WILL**
- **Put threats into perspective**
- **Create a policy that eliminates or reduces identified risks, by defining:**
 - **Business considerations**
 - **Scope**
 - **Security objectives**
 - **Formal risk assessment**
 - **Methods for usage monitoring, auditing, enforcement**
- **Obtain approval of policy**

Define business considerations

- **Why are we allowing mobile access?**
- **What objectives will we satisfy?**
- **Define policy relationships**
 - **Are you extending an existing policy?**
 - ◆ **Remote access**
 - ◆ **AUP**
 - ◆ **General security policy**
 - **Is this a new and unique policy “experience” for your organization?**

Define Scope

- **Who's allowed mobile access?**
 - **Employees? Business partners? Customers? Guests?**
- **What devices are approved for access?**
 - **Laptops, handhelds, phones**
- **What communications media?**
 - **Internal WLANs? Public WLANs? WWANs (cellular)**
- **What identity management policy will apply?**
 - **Authentication, auditing, group/individual accounts**
- **What information assets may be accessed?**
 - **Authorization, access controls**

Define Security Objectives

- **What do you expect from your security measures and practices?**
 - **Ensure mobile access availability**
 - **Prevent attacks on (wireless) infrastructure**
 - **Prevent attacks on sensitive data from mobile access**
 - **Avoid legal liability resulting from mobile access abuse**
 - **Enable visitor-supplied security measures on guest WLANs**

Determine Exposure, Then Develop a Risk Profile

- **What is your acceptable risk?**
 - **What is the value of business assets put at risk?**
 - **Assess the probability of attack**
 - **What measures (if any) are to be taken to eliminate or reduce the threat**
 - **What are the costs and consequences of a successful attack?**
 - **User accountability and Policy enforcement?**
- **How is approval of risk profile obtained?**

Assess Risk, Then Enumerate Threats

- **Assign value to each asset exposed, for each access scenario, and identify threats that apply...**
- **Example: Threats common to WLAN access**
 - **Unauthorized use of WLAN Bandwidth**
 - **Unauthorized access to the Internet, intranet services**
 - **Wireless peer and AP compromise**
 - **Replay and frame forgery attacks**
 - **Disclosure of private data**
 - **Traffic analysis**
 - **MAC and IP address spoofing**
 - **Rogue APs and “Man in the Middle” attacks**
 - **Radio Jamming, interference, & 802.11 denial-of-service**

Policy Implementation Follows Policy Approval

- **What security measures are required?**
- **How is current topology affected?**
- **How are current ops practices affected?**
- **What new practices complement existing practices and new measures?**
 - **Compliance criteria**
 - **Testing methodologies**
 - **Education and training**

Taking Steps to Secure Mobile Devices

- **Implement security measures that mitigate highest-priority business risks**
- **Different measures address different threats**
 - **Platform security**
 - **Airlink security**
 - **Network-layer security**
 - **Transport-layer security**
 - **Application security**

What We'll Cover ...

- Mobile user landscape and forecast
- Threats to Mobile users and devices
- Policy considerations for mobile users
- Security measures for mobile users



Platform Security

- **Control device access**
 - **Enable any built-in locks (handhelds) or logons (laptops, tablets)**
 - **Consider 3rd party software to strengthen access controls**
 - ◆ **Enforce password length/complexity/update rules**
 - ◆ **Wipe data after N unsuccessful login attempts**
 - ◆ **Use graphic, handwriting, or token authentication**
- **Protect Data stored on devices and removable media**
 - **Back up (synchronize) regularly to reduce risk of loss**
 - **Use encryption (Windows EFS or 3rd party)**
 - ◆ **File system**
 - ◆ **Passwords**
 - ◆ **Databases, spreadsheets, contacts**

Platform Security

- **Deploy Anti-Virus measures**
 - Resident AV scanners on device itself
 - Desktop AV scanners that scan during synchronization
 - Configure to scan mail, messaging, active content
- **Deploy anti-spyware measures**
 - Consider scanners that detect, block and protect against unsolicited installation and active content
- **Use host IDS to protect critical files from unauthorized changes**
 - OS files
 - Configuration files
 - Application executables

Secure Wireless Adapters and Access

- **Prevent unauthorized wireless activity**
 - **Disable interfaces when not in use (IR port, WLAN card)**
 - **Add 3rd party firewall software (or use SP2 WF)**
- **Avoid saving (unencrypted) email passwords, network logins, and other company resource access credentials**
 - **Use multiple passwords, interactive/token authentication**
- **Track and deny access to lost/stolen devices and cards**
 - **Lo-jack solutions for laptops and tablets**
 - ◆ **Many! Google “laptop theft protection”**
 - **Anti-theft inscription and tagging**
 - **Removable media protection software (Reflex Data)**
 - **BIOS and Host Protected Area (HPA) signatures**

Airlink Security: Wireless PANs

- **IrDA does not provide any link-level security**
 - **Turn your IrRA port off when not in use**
 - **Do not use IrDA to beam sensitive information**
- **Bluetooth provides basic airlink security**
 - **Avoid Non-Secure Mode: No authentication, encryption**
 - **Challenge-Response authentication based on static PIN**
 - **Encryption key derived following successful authentication**
 - **Use Link-Level Security to protect all data frames**
 - **Use Service-Level Security to protect data frames between specific device pairs**
- **Bluetooth best practices**
 - **Use at least 30' away from public area, at low power**
 - **Use long, random PINs and avoid saving PINs**
 - **Use mutual authentication**
 - **Negotiate longest possible encryption keys**

Airlink Security: Wireless WANs

- **Security features vary, but all attempt to**
 - **Authenticate subscriber's device to carrier's network**
 - ◆ **For GSM: challenge/response authentication based on mobile station's key, implemented in SIM**
 - **Prevent eavesdropping on airlink only**
 - ◆ **For GSM: 64-bit key-based privacy algorithm may be used between mobile station and carrier's base station**
- **3G standards support mobile VPNs**
 - **GPRS, CDMA 2000, UMTS**
 - **Will allow carriers to offer tunneling**

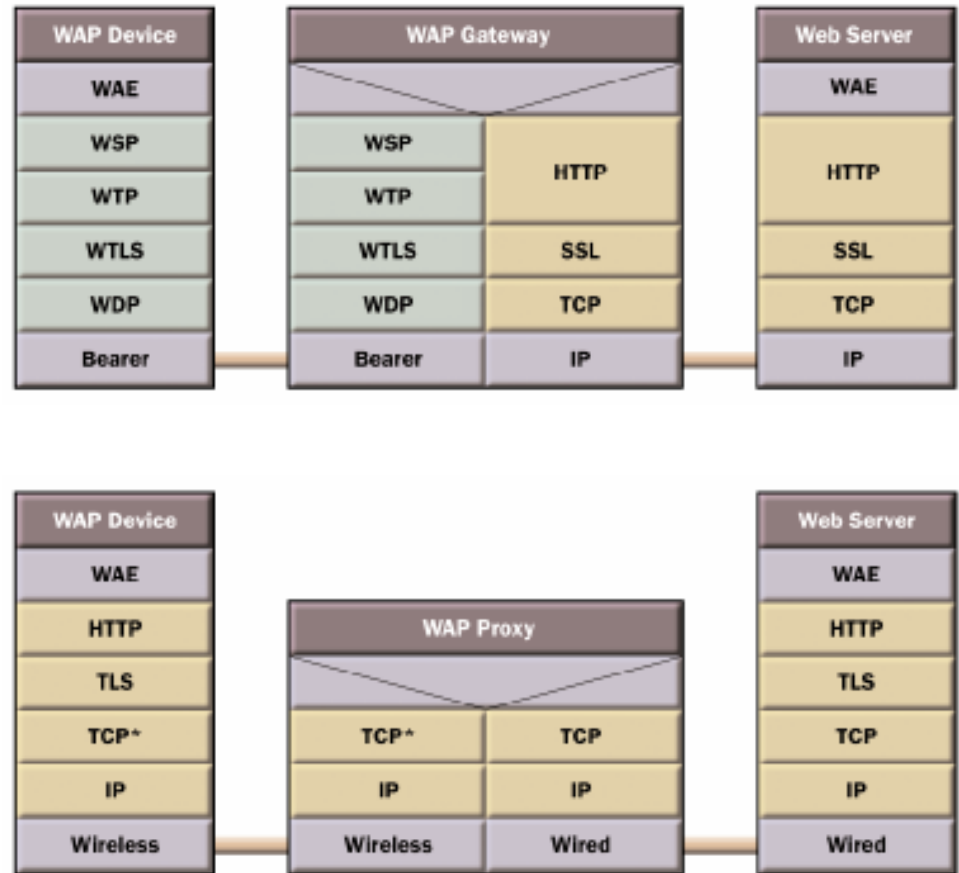
WAP Versions

WAP 1.1 used a gateway to map between WTLS & SSL

Left a “WAP gap” that prevented end-to-end security

WAP 2.0 uses a proxy to transparently forward TLS

Permits end-to-end TLS authentication, privacy, integrity and non-repudiation



Source: WAP Forum White Paper

Airlink Security: Wireless LANs

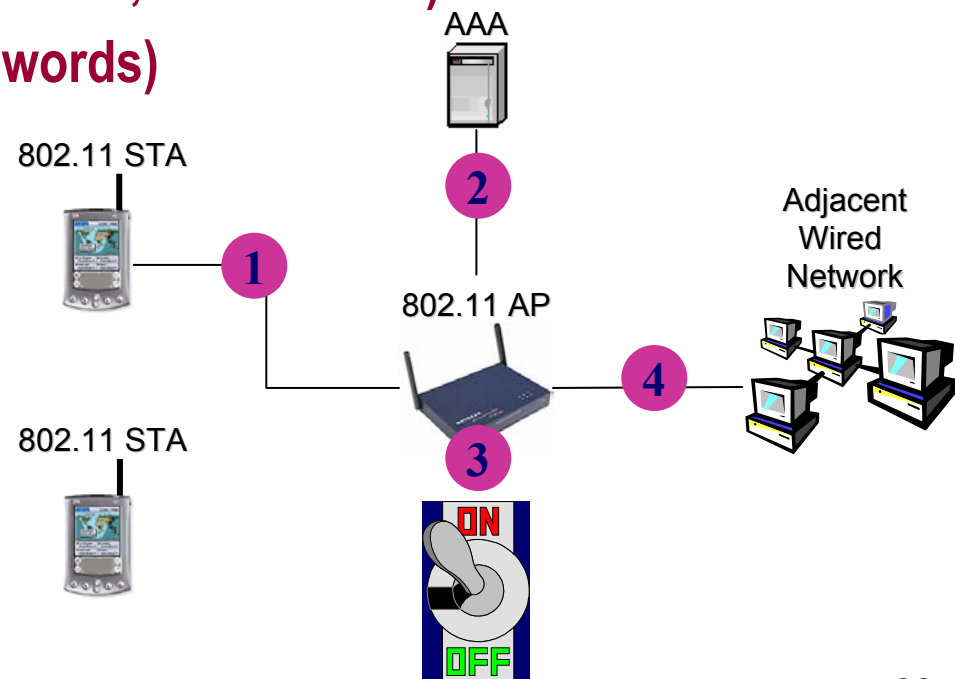
- **802.11 provides (optional) airlink security**
 - **Wired Equivalent Privacy (WEP)**
 - ◆ **Uses RC4 to encrypt traffic over airlink only**
 - **Shared key authentication**
 - ◆ **Any station with the shared key can join WLAN**
- **WEP weaknesses**
 - **Can detect corruption, but cannot prevent modification**
 - **WEP keys are static, reused, easily cracked**
 - **Shared keys used directly for encryption**
- **Authentication weaknesses**
 - **Stations are not individually authenticated**
 - **Lost or stolen device compromises shared key for all**
 - **Relatively weak defense against unauthorized access**

Airlink Security: Wi-Fi Protected Access (WPA)

- **Near-term “WEP fix” for existing 802.11 products**
 - **Wi-Fi Alliance snapshot of 802.11i Enhanced Security**
 - **Wi-Fi Protected Access Components**
 - ◆ **Temporal Key Integrity Protocol (TKIP)**
 - ◆ **802.1X and Extensible Authentication Protocol (EAP)**
- **Whenever possible, use TKIP instead of WEP**
 - **Based on stronger, derived encryption keys**
 - **Ensures very long time between key reuse**
 - **Protects against forgery, replay**
 - **Defines distribution method to avoid static base keys**
 - ◆ **SOHO WLANs can derive keys from preshared secret**
 - ◆ **Enterprise WLANs should use 802.1X to deliver keys**

Airlink Security: 802.1X Port Access Control

- AP “ports” cannot be used until station is authenticated and access controls are in place
- AP relays RADIUS authentication between Station and AAA Server
- Base keys delivered to authenticated Stations
- Supports Extensible Authentication Protocol (EAP) methods
 - PEAP/EAP-TTLS (server certificate, client either)
 - Cisco Lightweight EAP (passwords)
 - EAP-TLS (digital certificates)

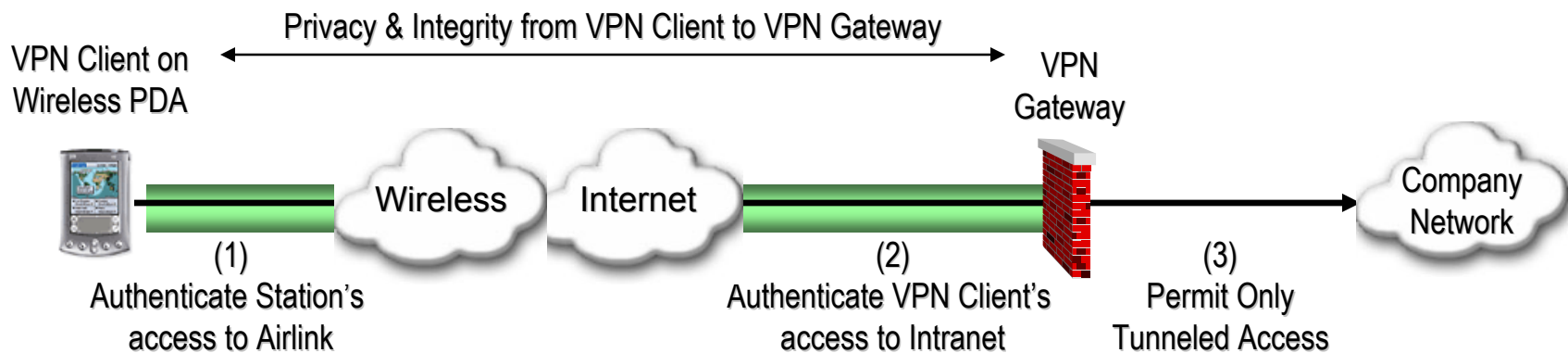


Higher-Layer Security

- **WWAN, WLAN, & WPAN link security is limited**
 - **Controls airlink access by authenticated stations**
 - **Inhibits eavesdropping and forgery on airlink only**
- **Airlink security is only a first layer of protection**
- **Add higher-layer security measures to**
 - **Control company network access by authorized users**
 - **Provide end-to-end privacy and integrity, from mobile station to gateway at the edge of the company network**
- **Multi-layered security prevents any single failure from penetrating your entire defense**

VPN Tunnels

- **Virtual Private Network (VPN) Tunneling provides**
 - **Confidentiality: Encrypt PPP, IP or TCP/UDP**
 - **Data Integrity: Detect modification in transit**
 - **Data Source Authentication: Prevent packet injection**
 - **System and/or User Authentication**
- **Protected subnet, port, protocol access controlled by VPN Gateway, based on VPN Client's ID**



VPN Tunneling Alternatives

- **Layer 2 VPN tunnels**
 - **Can secure PPP from wireless PDA to Intranet edge**
 - ◆ Layer Two Tunneling Protocol (L2TP)
 - ◆ Point to Point Tunneling Protocol (PPTP)
- **Layer 3 VPN tunnels**
 - **Can secure IP packets from wireless PDA to Intranet**
 - ◆ IPsec Encapsulating Security Payload (ESP)
 - ◆ Tunnels established by Internet Key Exchange (IKE)
- **Layer 4 VPN tunnels**
 - **Can secure TCP sessions to Intranet applications**
 - ◆ Secure shell
 - ◆ Secure Sockets Layer (SSL) [aka TLS]
 - ◆ Other “mobile VPN” tunneling protocols

PPTP VPNs for Mobile Devices

- **Many SMBs still use PPTP VPNs because**
 - **PPTP Client is included with Pocket PC, Palm Tungsten C**
 - **Client is easy to configure (just point at VPN Gateway)**
 - **Supports simple login/password authentication**
 - **Passes through most wireless routers without trouble**
- **PPTP security weaknesses**
 - **TCP control channel is cleartext**
 - ◆ **Dictionary attack, DoS attack, buffer overflow**
 - **PPTPv2 fixes the worst flaws, but not all of them**
- **Useful in low business risk/low cost scenarios**

IPsec VPNs for Mobile Devices

- **Secure, mutually authenticated tunnels between host and network**
 - **Bulk encryption, integrity, mutual authentication**
 - **Remote access vendor extensions include user-level authentication, dynamic IP assignment, NAT pass-thru, automated policy configuration**
- **IPsec VPN clients available for laptops and PDAs**
 - **Windows 2000/XP/CE, PPC, Palm, Symbian Clients**
 - **May have security parameter/VPN gateway limitations**

Transport-Layer VPNs for Mobile Devices

- **Windows 2000/XP/CE laptops and tablets have SSL/TLS browsers**
- **New generation of SSL-based VPN Products for handhelds**
 - **Existing browser serves as “SSL VPN” client**
 - **Natural fit for web-enabled apps (e.g., webmail)**
 - **Java applets, thin clients may be required for other apps**
- **Popular for environments where**
 - **Configuration and software installation on mobile devices must be avoided**
 - **Dominant application(s) are browser-based**
- **SSL provides strong privacy and integrity, server authentication**
 - **SSL authenticates VPN gateway by its digital certificate,**
 - **Remote user authenticated using a sub-authentication method”**

Security and Network Roaming

- **“Mobility VPNs” provide end-to-end security, network roaming and session persistence**
 - **Pocket PC MVPN clients are now available, based on Mobile IP, Wireless TLS, and proprietary UDP protocols**
 - **Carrier MVPN services vs. roll-your-own MVPNs**
 - **Some enable secure roaming between different network types – for example, from Ethernet to 802.11 to GPRS**
 - **Some provide TCP session persistence to keep applications alive when client is briefly disconnected (e.g., out of range)**

Application Security for Mobile Devices

- **Do you really need a VPN for secure wireless access to one or two enterprise applications?**
- **Many, many application-specific security methods**
 - **Secure administration: Secure shell instead of Telnet**
 - **Secure File Transfer: SFTP, FTP over TLS**
 - **Secure Desktop Access: GoToMyPC, VNC over SSH**
 - **Secure Web Access: HTTP over SSL**
 - **Secure email: BlackBerry for Microsoft Exchange**
- **Use when business and security needs can be met by focusing on single application**

Resources @Core Competence

- <http://www.corecom.com/html/technology.html>
 - **Core Competence's Website** hosts dozens of articles, white papers on WLAN deployment and security
- <http://hhi.corecom.com/weblogindex.htm>
 - **Dave Piscitello's Weblog:** more articles, URLs to even more WLAN security and best practices papers
- <http://www.corecom.com/html/wlan.html>
 - **Lisa Phifer's WLAN corner:** hyperlinks to nearly 100 articles, white papers, product reviews, technology assessments
- <http://hhi.corecom.com/library.html>
 - **Core Competence's Security Resources Library,** hyperlinks to hundreds of security articles, white papers, ...

7 Key Points to Take Home

- Empowering mobile users without a security strategy is an incident waiting to happen
 - **An ounce of prevention is worth a pound of cure**
- If there were ever a reason to define a security policy...
- Policy is essential for mobile user security
- There are too many security technologies that can be implemented in conjunction with wireless and mobility
- Security properties, network environments, PDA platforms, and supported applications vary widely
- No one-size-fits-all solution
- Don't stand on Superman's cape,
Don't spit into the wind,
don't pull the mask off the ole Lone Ranger...

Your Turn!

Questions

**How to contact me:
dave@corecom.com**