


Security in a Wireless World


Byron Brantley & Kelley Ealy



Wireless Networks Today

- Corporations – laptops, PDA's, smart phones
- Hospitals – computer carts, PDA's
- Hospitality – airports, coffee shops, parks
- Retail – handhelds for stocking, security tags

© CINCINNATI BELL COMPANY

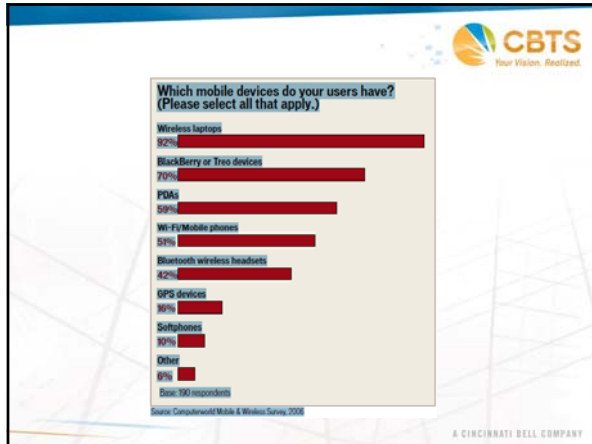


Why Wireless?

Wireless usage is on the rise:

- Costs are decreasing
- Availability is increasing
 - Mobile devices
 - Notebooks surpassing desktops
- Ease of deployment
- Wireless comes standard on many devices today

© CINCINNATI BELL COMPANY



- ### Biggest Risks In a Wireless World
- Data leakage or compromise (CIA Risks)
 - #1 Concern
 - Data stored in plain-text in accessible memory
 - Wireless is always on
 - Devices authenticated, not always users
 - Rogue access points
 - Wireless Malware
 - Some existing security mechanisms flawed and/or weak
 - Not everyone implementing best security practices

“Through 2010, 90% of WLAN security incidents will be the result of misconfigured systems.”
 – Gartner

Wireless Network Threats



- Evil Twin (wi-fi phishing) Attack
- Promiscuous client
- Sniffing or traffic analysis
- Ad-hoc networks
- Unauthorized computer access
- Wireless network viruses
- Shoulder surfing
- Man-in-the-middle
- DoS
- MAC Spoofing



A CINCINNATI BELL COMPANY

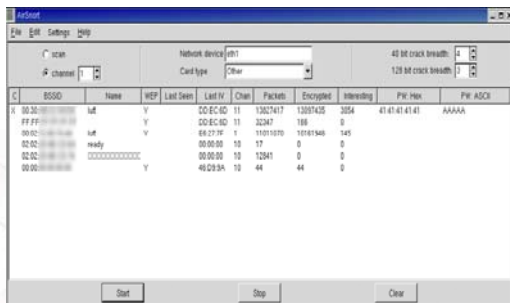
WLAN Hacker Tools



- NetStumbler
- Aircrack
- Kismet
- WEPCrack
- THCLEapCracker
- CoWPAtty
- ASLeap
- Silica
- KARMA
- AirJack

A CINCINNATI BELL COMPANY

Aircrack



A CINCINNATI BELL COMPANY

802.1x Authentication Protocols

- LEAP
- PEAP
- EAP-FAST
- EAP-TLS
- EAP-TTLS
- EAP-MS-CHAP-v2

A CINCINNATI BELL COMPANY

Best Authentication Methods

1	WPA2 enterprise mode with EAP-TLS or PEAP and AES for airlink encryption
2	WPA2 enterprise mode with EAP-TLS or PEAP and TKIP for airlink encryption
3	WPA enterprise mode with EAP-TLS or PEAP and TKIP for airlink encryption
4	EAP-FAST on Cisco hardware
5	LEAP on Cisco hardware
6	Open access

A CINCINNATI BELL COMPANY

Protecting the “CIA”

- Confidentiality
 - Eavesdropping
- Integrity
 - Compromised network
- Availability
 - DoS
 - Performance Issues

A CINCINNATI BELL COMPANY

Wireless Protection

CBTS
Your Vision. Realized.

- POLICY
- Wireless Security = Layered Security
- Educate Users

A CINCINNATI BELL COMPANY

CBTS
Your Vision. Realized.

To prevent shoulder surfing...

1. Launch Quicktime Player
2. Start "New Movie Recording"
3. Leave MacBook's cam running
4. Scare off people watching your screen from behind
5. You are omniscient!

A CINCINNATI BELL COMPANY

Myths for Securing the WLAN World

CBTS
Your Vision. Realized.

- WEP is better than nothing...
- No one will find my network...or...who would want to use my network?
- VPN's will protect my network...
- MAC Filtering will secure my wireless network...
- I authenticate my users with LEAP...
- All my antenna's are in the middle of the building...
- I turned off DHCP...

A CINCINNATI BELL COMPANY


Attack Demo



http://www.lucidlink.com/over_shoulder.swf

A CINCINNATI BELL COMPANY


WLAN Best Practices



- Change the default Admin password on the AP
- Update AP and wireless card firmware
- Implement the highest level of encryption possible
- Authenticate users with secure protocols
- Standardize wireless equipment
- Configure wireless equipment properly
- Ban rogue access points
- Protect the client (personal firewall, IPS, secure the client before connecting)

A CINCINNATI BELL COMPANY

WLAN Best Practices



- Strong encryption for applications used over wireless
 - HTTPS
 - TLS
 - SSH
- Encrypt wireless traffic with a VPN
- Segment the wireless network from the wired network and restrict access
- Proxy with access control for outgoing requests
- Test wireless network regularly for vulnerabilities
- Enable logging on wireless devices
 - Review logs on regular basis
- Implement WIPS
- Audit Wireless Network

A CINCINNATI BELL COMPANY

Protecting the Corporate Office



- Move all wireless equipment to the latest standards
- Use the strongest user/device authentication & airlink encryption
- Implement centrally managed security appliances
- Implement a Wireless IPS
- Consider NAC on the LAN
- Segment the WLAN from rest of network
- Educate users for home wireless security best practices

A CINCINNATI BELL COMPANY

Protecting the Guest Network



- Guest access policy should:
 - No access to Intranet
 - No frills Internet access
- Varied guest roles should:
 - Require role-based provisioning
 - Bandwidth control
 - Connectivity limitations
- Monitor guest access logs

A CINCINNATI BELL COMPANY

Protecting the Wireless Client




- Install personal firewalls
- Keep wireless card drivers up-to-date
- Turn off ad-hoc networking
- Do not allow more than one connection manager to be active
- Do not allow wireless and wired NICs to be on at the same time
- Do not allow split tunneling or ensure modify personal firewall rules to protect client ports
- Turn off wireless access when not in use

A CINCINNATI BELL COMPANY

Protecting the Traveling Client 


- Use Non-Wi-Fi wireless services
- Install personal firewalls with connection-specific policies
- Keep devices up-to-date with patches
- Use remote connection agents whenever possible
- Pay for hot site usage with cash instead of a credit card if possible
- Access to company resources from non-company machines should use SSL/VPN
- Authenticate with two-factor authentication
- Do not allow split tunneling

A CINCINNATI BELL COMPANY

Emerging Technologies 

- Exchange 2007
 - Exchange ActiveSync
 - Communication protocol enables mobile access to messages, schedules, contacts, etc. from the Exchange mailbox
 - HTTPS connection for Direct Push of e-mail
 - Windows Mobile-based devices, Exchange ActiveSync-enabled devices
 - Device Security & Management
 - Enforce policies on devices
 - PINS
 - Device Wipe for Data & Applications
 - Per User policies
 - Track device usage
 - Centrally manage devices within Exchange environment

A CINCINNATI BELL COMPANY

Emerging Technologies 

- Wireless Intrusion Prevention Systems
 - Adopted early for vulnerability assessment
 - More popular now for IPS capabilities
 - Wireless more mainstream
 - Wireless attacks increasing
 - WLAN modulations increasing (WiMAX, 802.11n)
- WPA3 by 2010
 - Software upgrade
- 802.11n
 - High-speed Wi-Fi / Increased bandwidth

A CINCINNATI BELL COMPANY

Compliance & Regulations



- Many regulations & laws should take wireless security into consideration
 - PCI
 - SOX
 - HIPAA
 - GLBA
 - Data Privacy Laws

A CINCINNATI BELL COMPANY

Mobile Computing Devices



A CINCINNATI BELL COMPANY

Smartphones



- “Smartphones aren’t just about email anymore – they are mobile computing devices – more like laptops than mobile phones”
- Fortunately, we haven’t seen any major breaches in this area, but are we really paying attention as needed ?

A CINCINNATI BELL COMPANY

Smartphone Risks



- Physical loss of the device
- Loss of general company information & files
- Key sales contacts – competitor or lost
- Employee time to recover from loss
- Network & Admin time to replace device
- Introduction of viruses & malware to pc base
- Phone fraud
- Using device to steal company information

A CINCINNATI BELL COMPANY

Considerations



- Business or personal property?
- Can enterprise “control” devices?
- Legal liability issues
- Contingency plans for compromises
- Device selection
- Dual-mode converged handsets
- “Virtual” devices – business & personal
- Outsourcing management of mobile devices

A CINCINNATI BELL COMPANY

Considerations




- Regulations – HIPPA
- Password / PIN on mobile devices
- Key authentication
- Biometric safeguards
- Authentication
- Encryption
- Controlling software loads
- Device configuration

A CINCINNATI BELL COMPANY

The Good News 


- BlackBerry Enterprise Server (BES)
 - “CIA” standards
- Middleware platforms for device management
 - iPass, Afaria, Securewave, Synchronica
- MS Exchange 2007
 - Manage individual profiles versus global
- Software for the device
 - Kaspersky, F-Secure, Symantec, Trend

© CINCINNATI BELL COMPANY

What should we do ? 

- Employ “protection systems” for lost devices
 - Notification, disable, & swipe
 - Encrypt data storage on device
- Employ power-up password protection on devices
- Track mobile devices like other assets (laptops)
- “Section-up” databases into authorized segments by user to limit exposure to company information
- Limit synchronization to OTA only– no pc or Bluetooth

© CINCINNATI BELL COMPANY

What else should we do ? 


- Evaluate upgrade to MS Exchange 2007
- Evaluate middleware for device management
 - Synchronica, Securewave, Afaria
- Evaluate malware software on device
 - Kaspersky, F-Secure, Airscanner
- Limit access to network to company-owned devices
- Activity monitors
- Limit internet site access for devices

© CINCINNATI BELL COMPANY



THANK YOU!


A CINCINNATI BELL COMPANY



Resources

- www.MobileComputing.com
- "Mobile devices: Corporate security strategies," Lisa Phifer, February 14, 2007.
- "Smartphones opening up enterprise risks," Marcia Savage, *Information Security* magazine, July 24, 2008
- "Using Exchange Server for mobile device security," Brien M. Posey, May 3, 2007
- "Mobile device security: Guarding the gate.," Lisa Phifer, march 20, 2008
- "Mobile-specific management solutions: Mobile management," Daniel Taylor, July 31, 2007
- "Mobile device security: Improving mobile authentication," Lisa Phifer, December 5, 2007
- "VPN clients for handheld devices," Barry Sosinsky, Jan 5, 2005
- "Mobile devices: Business or personal property?," Craig Mathias, March 14, 2007
- "Mobile device management – Controlling risks and costs for better security," Simon Forge, June 20, 2007
- "Top 4 Mobile Anti-Virus Products for Your Smart Phone," Ashwin Satyanarayana, September 5, 2008.

A CINCINNATI BELL COMPANY



Resources

- www.lucidlink.com
- "MarketScope for Wireless LAN Intrusion Prevention Systems" – John Pescatore & John Girard, Gartner.com
- "Hype Cycle for Wireless Networking Infrastructure, 2008" – Sylvain Fabre, Gartner.com
- "FAQ: 802.11n Wireless Networking" – David Haskin, ComputerWorld, Inc.
- "Five Wireless Threats You May Not Know" – Joshua Wright, SANS.org
- "Wireless Security", Wikipedia.org
- <http://farm4.static.flickr.com>

A CINCINNATI BELL COMPANY
