Purdue University proudly presents

October Cybersecurity Awareness Month

Phones and Tech Toys: Who can hear me now?

Aaron Jarvis, Network Engineer

www.purdue.edu/securepurdue
Any devices or software shown during this presentation are for demonstration purposes only. Purdue University does not endorse or support any devices or software being used in this presentation.
Agenda

- Cellular Security
- Bluetooth Security
- Flash Drive Security
- VoIP Security
Agenda

- Cellular Security
- Bluetooth Security
- Flash Drive Security
- VoIP Security
Cellular Security

- Global Statistics from Gartner
  - Estimated 2.6 Billion cell phones in circulation by 2009
  - Smart phones will represent $\frac{1}{5}$th of all phone sales in 2008
    - Voice, data, video
Cellular Security

- Cellular Networks
  - Analog
  - GSM
    - AT&T/Cingular, T-Mobile
  - CDMA
    - Verizon, Sprint
  - iDEN
    - Nextel
Cellular Security

- Cellular Networks
  - Analog
    - Analog Mobile Phone System (AMPS)
    - Deployed in 1980’s
      - Still in use today!
    - Transmit/Receive without encryption
      - Easily eavesdropped by using a scanner
Cellular Security

• Cellular Networks
  • GSM
    ▪ Global System for Mobile Communications
    ▪ Widespread use
  • SIM
    ▪ Stores private information allowing user to switch phones and take information with them
    ▪ Encrypted voice from mobile device to cellular network

www.purdue.edu/securepurdue
Cellular Security

- Cellular Networks
  - CDMA
    - Code Division Multiple Access
    - Originally developed by US Navy
    - Encrypted voice from mobile device to cellular network
    - No SIM card
    - Some carriers providing service that transfers private information between phones
Cellular Security

- Cellular Networks
  - iDEN
    - Integrated Digital Enhanced Network
    - Developed by Motorola
    - Push to talk
Cellular Security

- Risks with Cell Phones
  - Loss
  - Eavesdropping
  - Location
  - Financial
Risks with Cell Phones

- Loss
  - Physical
  - Address book, account numbers, passwords
- Treat your cell phone like it was a laptop
- Lock or password protect if possible
- Disable bluetooth when not in use
Risks with Cell Phones

- Eavesdropping
  - Voice
    - Can be intercepted with right equipment
    - Talking loud
  - Data
    - Bluetooth
      - More in next section
Cellular Security

- Risks with Cell Phones
  - Location
    - Many phones with integrated GPS receivers
    - Could be used for tracking
Risks with Cell Phones

- Financial
  - Report a lost or stolen phone immediately
    - May be liable for calls made if not reported in a timely fashion

- Roaming
  - International
    - Many countries > $1.00 min
  - Domestic
    - Automatic, can cost $$$
    - Less and less a problem due to greater coverage and agreements through providers
Cellular Security

- Upgrading or Replacing Cell Phones
  - Before discarding, recycling, etc
    - Perform a factory reset on the device
      - Erases all private information on the phone
Agenda

- Cellular Security
- Bluetooth Security
- Flash Drive Security
- VoIP Security
What is bluetooth?

- Wireless technology used to allow communication between electronic devices (phones, cars, keyboards, mice)
  - Typically around 30 feet range
- Creates a personal area network
How does Bluetooth work?
- Uses 2.4Ghz
  - Shared with Wifi, cordless phones, microwaves
- Low power transmitters
- Pairing between devices
  - Agree to communicate with each other
Bluetooth Security

- Versions of Bluetooth
  - 1.0/1.0B
    - Introduced in 1998
    - Not used much as device interoperability was not very good in this version
  - 1.1
    - First widely used version
    - Greater interoperability
Bluetooth Security

- Versions of Bluetooth
  - 1.2
    - Backwards compatible with version 1.1
    - Adaptable frequency hopping
    - 1Mbps data rate
    - Improved audio through retransmission
Bluetooth Security

- Versions of Bluetooth
  - 2.0 + EDR
    - Backwards compatible with previous versions
    - 3Mbps data rate
    - Lower power consumption
    - Improved multi-link connectivity
      - Pairing to more than one device at a time
According to the Bluetooth Special Interest Group (SIG)

- In order to break into a bluetooth device the following must take place
  - Force two paired bluetooth devices to break their connection
  - Steal/Capture the packets used to resend the PIN
  - Decrypt the PIN
Bluetooth Security

- Bluetooth Sniffing Equipment
  - Some commercially made equipment available but very expensive
  - Bluesniper rifle - Homemade
    - ~$300
    - Range ~ 1 mile
Bluetooth Security

- Bluetooth Security Threats
  - Bluejacking
    - Allows users to send business cards anonymously
    - Does not allow data access to your phone
    - Eliminate threat by
      - Making sure device is in non-discoverable mode
Bluetooth Security

- Bluetooth Security Threats
  - Bluesnarfing
    - Allows access to data on phone
    - Make phone calls
    - Send/Receive text messages
    - Requires advanced equipment and knowledge
    - Must be within 30ft range
    - Eliminate threat by
      - Making sure device is in non-discoverable mode
      - Still vulnerable, but much harder to exploit
      - Upgrade phone or obtain patched software
Bluetooth Security

- Bluetooth Security Threats
  - Bluebugging
    - Allows access to data on phone
    - Make phone calls
    - Send/Receive text messages
    - Requires advanced equipment and knowledge
    - Must be within 30ft range
  - Eliminate threat by
    - Making sure device is in non-discoverable mode
      - Still vulnerable, but much harder to exploit
    - Upgrade phone or obtain patched software
Bluetooth Security

- Bluetooth Best Practices
  - Disable when not in use
  - Use a PIN greater than 8 digits
  - Put device in non-discoverable mode
  - Update to newest software if using older phone to patch vulnerabilities
Agenda

- Cellular Security
- Bluetooth Security
- Flash Drive Security
- VoIP Security
Flash Drive Security

Examples of Portable Storage
Flash Drive Security

Examples of Portable Storage

Each of these can hold up to 256MB and beyond

www.purdue.edu/securepurdue
Flash Drive Security

- Risks with Flash Drives
  - Physical
    - Loss
      - If data is unencrypted then person has free access to content
  - Malware
    - Reported instances of digital picture frames with malware preloaded
    - Use a virus scanner on new devices to ensure its safe to use
Flash Drive Security

- Methods to Secure Data on Flash Drives
  - Encryption
    - Software
      - Truecrypt
      - FreeOTFE
    - Hardware
      - Ironkey
        - After 10 invalid attempt device issues a self destruct sequence and all data and encryption keys are erased
  - Biometrics
    - Fingerprint
Agenda

- Cellular Security
- Bluetooth Security
- Flash Drive Security
- VoIP Security
VoIP Security

- What is VoIP?
  - Voice-over IP
    - Make voice calls to PSTN or other users
    - Commonly uses Internet to reach service provider
    - Phone adapters allow for service similar to traditional analog phone service
    - Softphones allow for service to be used from a computer
VoIP Security

- Enterprise vs. Personal Solutions
  - Features
    - More than just dial tone
  - Security
    - Signaling and Media Encryption
  - Quality of Service
    - Ensure voice packets are treated as higher priority than data
VoIP Security

- Live Demo
  - Capturing a Phone Call made via Vonage USB Phone
Agenda

- Cellular Security
- Bluetooth Security
- Flash Drive Security
- VoIP Security
Questions

Questions or Comments?