

Cell Phone Security

CMPT 495 / 585
Computer and Data Security
Fall 2005
Montclair State University
Jay Trent

Introduction

- Cell phones communicate through the air by radio waves with a base station.
- Cell phones depend on areas, or cells, each with its own base station which can use the same frequencies as the other cells.
- The base station connects to the operator's backbone network and the wider public telephone network as well as the networks of other mobile phone operators.

Cell Phone Tower



Functions

- Cell phones have all the basic functions of land line phones.
- Cell phones also support other services such as: Short Message Service (SMS) for text messaging, packet switching for access to the Internet and Multimedia Messaging (MMS) for sending and receiving photos.
- There are PDA (personal digital assistant)/phone hybrids known as smartphones that have Microsoft Office applications and can access data from the corporate office.

Why Security?

Personal Use:

- Prevent fraudulent billing: It is possible to intercept the signal and clone the phone's ID numbers, charging for calls from another phone.
- Prevent a denial of service attack: An attack text messaging a large number of cell phones numbers would leave no bandwidth for calls.
- Prevent others from listening to your private conversations.
- Prevent having your address book posted on web page as happened to **Paris Hilton**. Details to follow.

M-Commerce

- M-Commerce stands for **Mobile Commerce**, or transactions conducted from a cell phone, or mobile device.
- The SIM (Subscriber Identification Module or Subscriber Identity Module) card - a.k.a. "smart card" - holds all of a subscriber's personal information and phone settings.
- The practice of swiping an ATM card or a credit card at the supermarket is already established. Putting that same technology into a cell phone's SIM card is the next logical step.

M-Commerce

- As far as security issues are concerned, mobile devices are capable of using the same technologies (WTLS) as traditional PCs.
- M-Commerce is more common in Europe and Japan, but is growing rapidly in the United States.
- Following this trend, as M-Commerce grows, so will the interest of cyber criminals.

Why Security?

Business Use:

- Protect technology resulting from large R&D expenditures.
- Protect market research results.
- Protect a customer or vendor list.
- Protect sensitive financial information which could affect stock prices.
- Protect emails/conversations revealing corporate strategy.

Vulnerabilities

- Eavesdropping is a problem for analog phone users. The FM radio signals are easily monitored using readily available radio receivers, called scanners.
- Digital cell phones are less vulnerable to eavesdropping. The overwhelming majority of cell phones today are digital.
- Most threats today involve **Bluetooth**.



Bluetooth

- **Bluetooth** is a radio standard designed for low power consumption which lets **Bluetooth**-enabled devices talk to each other when they come within ranges of up to 100 meters.
- Common uses are connecting computer peripherals, and also PDAs, cameras and cell phones to computers.
- The problem is that cell phones can also talk to other cell phones.



Bluetooth Vulnerabilities

- When it's set to "discoverable" mode, a **Bluetooth** enabled cell phone sends a signal indicating that it's available to "pair" with another **Bluetooth** device, ie transmit data back and forth.
- An attacker who detects this signal could also attempt to pair with the device and hack in to steal the PIN.



Bluetooth Threats

With the PIN, attackers can:

- Steal information stored on the device including contact lists, e-mail, and text messages.
- Send unsolicited text messages to other **Bluetooth**-enabled devices.
- Use the mobile phone commands, which allows the attacker to perform just about any function.
- Install a virus which could slow or disable the phone, or destroy or copy information.



Bluetooth Security

To improve security:

- Keep setting to “non-discoverable” (transmission disabled)

Also applies to cell phones in general:

- Use a strong PIN code which will be harder to crack.
- Avoid storing sensitive data such as social security number or credit card numbers
- Stay informed on security issues and keep the device up to date with software updates.

Methods of Attack

Users of wireless e-mail must be aware of:

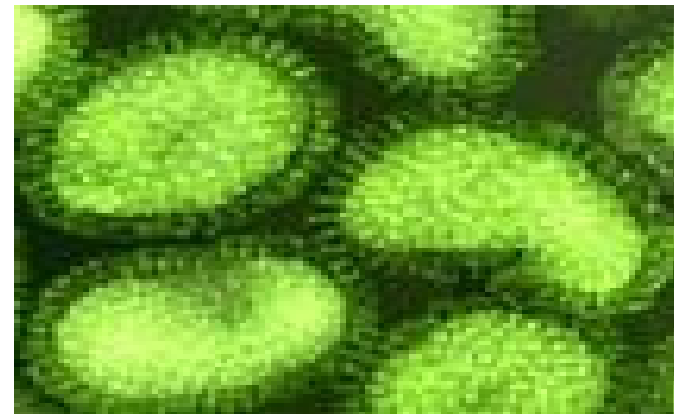
- Phishing is e-mail fraud where the perpetrator sends out legitimate appearing e-mails in an attempt to gather personal and financial information from the recipient.
- Spoofing is the forgery of an e-mail header so that the message appears to have originated from someone or somewhere other than the actual source. Senders insert commands in headers that will alter message information.

Methods of Attack

Users of all cell phones must be aware of:

- Zombie Network - A number of computers that have been covertly taken over usually to transmit messages for a denial of service (DOS) attack.
- Cloning - A cloned cell phone is one that has been reprogrammed to transmit the electronic serial number (ESN) and telephone number (MIN) belonging to another cell phone whose owner then gets billed for the calls.

Viruses



Viruses

- Current viruses target mostly the Nokia smartphones running the Symbian operating system . This is only about 4% of all cell phones.
- The Cabir worm, written in 2004 by a white hat hacker from Spain, was the first successful program targeting cellular phones. Several malicious variations have been created.
- Cabir spreads through **Bluetooth**.

How Viruses Spread

- A phone infected with the Cabir virus uses **Bluetooth** to attempt to send infected SIS files (a Symbian file format) to any **Bluetooth**-enabled device it can find.
- The worm arrives at the target device, which must be running the Symbian OS and have **Bluetooth** turned on in “discoverable” mode.
- The user must accept the message, before the virus will be installed.



Methods of Security

- **Passwords** - stronger if more permutations and changed frequently.
- **Physical** cards or keys
- **PINs** - Personal Identification Numbers
- **Biometrics** - fingerprint sensors in the wireless market are becoming more widely accepted.

Security Protocols

- **Secure Sockets Layer (SSL)** - a protocol for Internet transmissions using the asymmetric key scheme to encrypt data.
- **Wireless Transport Layer Security (WTLS)** - an SSL-like security protocol for Wireless Application Protocol (WAP) transaction-based Internet access applications such as banking and making purchases.

And Finally, Paris...



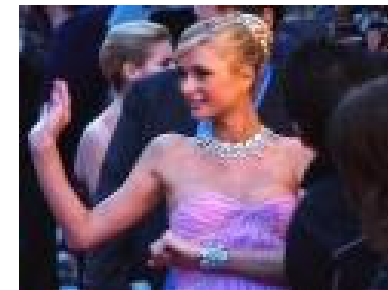
And Finally, Paris...

- **Paris Hilton** (born February 17, 1981) is an American model, singer and actress, known primarily for her partying ways and being the heiress to the Hilton Hotel fortune.
- Hackers succeeding in downloading her video, text and data files from her Sidekick cell phone.
- A Sidekick's data storage can be accessed from anywhere in T-Mobile's service area by someone with control of the account.

And Finally, Paris...

- It began with social engineering, when one of the hackers was able to get a user name and password for the Web site used by T-Mobile to manage customer accounts.
- The hackers then used the secure web site to look up Hilton's phone number and reset the password for her account, locking her out of it.
- Then the hackers downloaded all of her stored video, text and data files and posted her address book on the Internet.

And Finally, Paris...



The End