Bluetooth security threats
Contents

1. What is bluetooth?
2. Statistics
3. Security threats
4. Possible vulnerabilities
5. How to use bluetooth safely
WHAT IS BLUETOOTH?
Things You have to know about Bluetooth [1]

- It's the simple choice for convenient, wire-free, short-range communication between devices
- The range for Bluetooth transmissions varies from about 1 meter up to 100 meters
- Its speed is limited to about 1 Mbps
Things You have to know about Bluetooth [2]

- Bluetooth can operate in one of three security models:
  - Mode 1 is non-secure
  - Mode 2 provides security at the service level, after the channel is established
  - Mode 3 provides security at the link level, before the channel is established
Things You have to know about Bluetooth [3]

- Bluetooth is an integral part of smartphones, PDAs and many notebooks.
The common uses of BT technology nowadays include [1]:

- Using a wireless mobile phone headset during a call while keeping a phone in the bag
- Transferring photos or ring tones between mobile phones
The common uses of BT technology nowadays include [2]:

- Connecting a printer, keyboard, or mouse to a PC without cables
- Synchronizing a calendar, phone book and other information between a PDA and a PC
STATISTICS
Bluetooth usage in devices

- Phone/Mobile: 1513; 67.1%
- Phone/Smart phone: 74; 3.3%
- Computer/Laptop: 521; 23.1%
- Phone/Cordless: 22; 1.0%
- Computer/Palm sized PC-PDA: 23; 1.0%
- Audio-Video/Hands free: 47; 2.1%
- Computer/Desktop: 32; 1.4%
- Miscellaneous: 11; 0.5%
- Audio-Video/Headset: 7; 0.3%
- Computer/Uncategorized: 1; 0.0%

http://www.viruslist.com
This graph shows that 92.02% of people, who have bluetooth enabled devices, use object transfer (transmitting/receiving files) in public place.
Proportion of vulnerable Bluetooth devices

- 89% Not vulnerable
- 11% Vulnerable
Total Number of Bluetooth End Points Shipped Per Year Estimate

Source: Merrill Lynch
SECURITY THREATS
Bluetooth dangers [1]

- Sensitive information that is not encrypted and that is transmitted between two wireless devices may be intercepted and disclosed.

- Sensitive data may be corrupted during improper synchronization.
Bluetooth dangers [2]

- Handheld devices are easily stolen and can reveal sensitive information
- Data may be extracted without detection from improperly configured devices
Bluetooth dangers [3]

- Malicious entities may gain unauthorized access to the computer network through wireless connections, bypassing any firewall protections.

- Malicious entities may, through wireless connections, connect to other organizations for the purposes of launching attacks.
Bluetooth dangers [4]

- The malicious hackers can benefit from mobile phone owners who keep their Bluetooth devices in discoverable mode
  - This happens most often because one mobile phone is required to be in discoverable mode before pairing with a new device
  - Often device owners forget to disable the discoverable mode afterwards
Secure Bluetooth interaction phases:

1. Pairing - in order to establish a "link" key, which will then be used for encryption and decryption for secure connections.

2. Initialization key is generated based on each device's address, and a PIN which is shared between the devices.

3. Once pairing has occurred, each device considers the other to be "trusted", and thus it grants its access to certain things on itself.
You should:

- Use a long passkey number and do not perform a pairing procedure in public
  - *If a hacker is able to discover the passkey, he can calculate possible initiation keys, and then from that, calculate the link key. Making the passkey long will make it much harder to accomplish the first step*
- Passkey changes should only be possible over an authenticated or encrypted connection
POSSIBLE VULNERABILITIES
Social engineering:

- Hackers can access information on a user's phone, either by using Bluetooth to establish a 'trusted device' connection, or by persuading the user to lower security/ disable authentication for Bluetooth connections.
Vulnerabilities in the protocol itself:

- Hackers can steal data from the telephone, make calls or send messages, conduct DoS attacks on the device, use a Bluetooth earpiece to listen to calls etc.
Malicious code:

- A telephone can be infected by a worm, which will then send itself to other devices, by Bluetooth or by MMS. Data on the victim telephone may be corrupted, stolen, or encrypted.
What is bluejacking?

- Bluejacking allows phone users to send business cards which typically contains a message in the name field to another bluetooth enabled device anonymously using Bluetooth wireless technology.
Bluejacking

- If a malicious individual names their phone something like "Click accept to win!!" then they can gain access to someone's Bluetooth device if the owner falls for the trick
What is bluesnarfing?

- Connects to Bluetooth phones without the phone owner's knowledge and download the phonebook, the calendar, and sometimes more.

- Advanced version of bluesnarfing can even alter those files in some bluesnarfed phones.
How bluesnarfing works [1]

- Bluesnarfing is realized by special software
- Bluesnarfing works through the mechanism for exchanging business cards
How bluesnarfing works [2]

1. The bluesnarfing software connects to a target Bluetooth device via Bluetooth's OBEX Push profile.

2. Then instead of pushing a business card, it pulls, using a "get" request for files with known names, such as the phonebook file (telecom/pb.vcf) or the calendar file (telecom/cal.vcs).
What is bluebugging?

- A bluebugger can wirelessly direct a phone to make calls without the owner's knowledge

- Set call forwarding and then receive calls intended for the bluebug victim
Bluebugging

- Bluebuggers also have bluesnarf capability, so they can read phonebooks and calendars and more
- They can even read a phone's call list to see who their victims called or who called them. They can even alter those lists.
HOW TO USE BLUETOOTH SECURE
Switch the phone into "invisible" mode when you do not need Bluetooth, so it will not be recognized by other Bluetooth devices.
Switch off the Bluetooth capability when you're not using it.
Never add funny sounding messages from unknown sources to your contacts/address book
Avoid storing sensitive data such as your social security number, credit card numbers, and passwords on any wireless device
Stay up-to-date on Bluetooth developments and security issues
Regularly check for news on software updates or any specific security vulnerabilities
Install security updates and antivirus software that is available
Compared to 40-bit encryption, 128-bit encryption offers 88 additional bits of key length. This translates to $2^{88}$ or a whopping $309,485,009,821,345,068,724,781,056$ additional combinations required for a brute-force crack.
Always use application-level security: Point-to-Point Tunneling Protocol, Secure Sockets Layer or VPN
Restrict access to trusted devices
Don't accept files transmitted via Bluetooth wireless technology or any other technology from unknown or suspicious entities.
Evaluate a product's user interface to decide how easily it lets users set up and manage security.
Require link-level security to be active in all Bluetooth devices