Bluetooth™ Security

Nelli Gordon and Sean Vakili

May 10th 2011

What is Bluetooth?

- Bluetooth is an open standard for short-range radio frequency (RF) communication. Bluetooth technology is used primarily to establish wireless personal area networks (WPAN), commonly referred to as ad hoc or peer-to-peer (P2P) networks.
- Bluetooth is a low-cost, low-power technology that provides a mechanism for creating small wireless networks on an ad hoc basis, known as *piconets*.

Bluetooth devices

Origin of the name 

Bluetooth was named after a late 900s king, Harald Blåtand (Harald Bluetooth) King of Denmark and Norway. He is known for his unification of previously warring tribes from Denmark (including Scania, present-day Sweden, where the Bluetooth technology was invented), and Norway. Bluetooth likewise was intended to unify different technologies, such as computers and mobile phones.

History

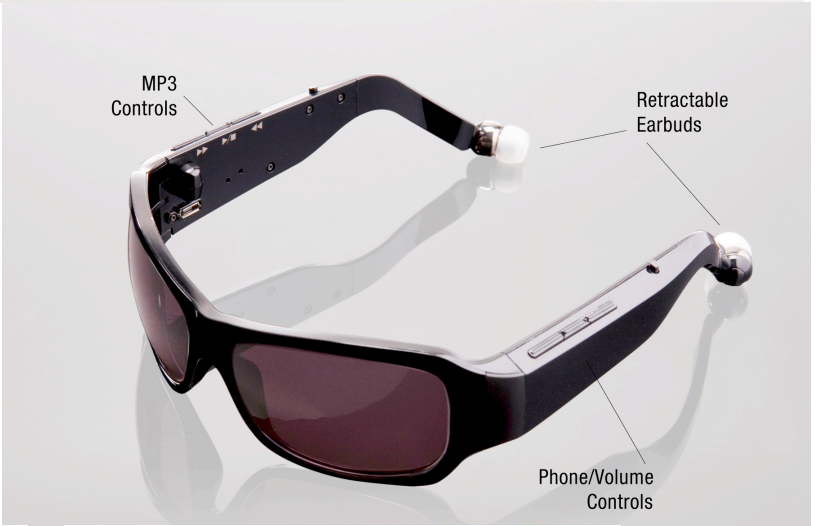
- The Bluetooth specification was developed in 1994 by Jaap Haartsen and Sven Mattisson, who were working for Ericsson in Lund, Sweden. The specification is based on frequency-hopping spread spectrum technology.
- The specifications were formalized by the Bluetooth Special Interest Group (SIG). The SIG was formally announced on May 20, 1998. Today it has a membership of over 14,000 companies worldwide. It was established by Ericsson, IBM, Intel, Toshiba and Nokia, and later joined by many other companies.

Where we can find it? Bluetooth technology has been integrated into many types of business and consumer devices, including:

- Cellular phones
- Personal digital assistants (PDA)
- Laptops
- Automobiles
- Printers
- Headsets

This allows users to form ad hoc networks between a wide variety of devices to transfer voice and data. This presentation provides an overview of Bluetooth technology and discusses related security concerns.

More Bluetooth devices



Why do we need Bluetooth (key benefits of Bluetooth technology are):

- **Cable replacement.** Bluetooth technology replaces a variety of cables, such as those traditionally used for peripheral devices (e.g., mouse and keyboard connections), printers, and wireless headsets and ear buds that interface with personal computers (PC) or mobile telephones.

- **Ease of file sharing.** A Bluetooth-enabled device can form a piconet to support file sharing capabilities with other Bluetooth devices, such as laptops.

- **Wireless synchronization.** Bluetooth provides automatic synchronization between Bluetooth- enabled devices. For example, Bluetooth allows synchronization of contact information contained in electronic address books and calendars.

- **Internet connectivity.** A Bluetooth device with Internet connectivity can share that access with other Bluetooth devices. For example, a laptop can use a Bluetooth connection to have a mobile phone establish a dial-up connection, so that the laptop can access the Internet through the phone.

Bluetooth vs. Wi-Fi

Bluetooth and Wi-Fi have many applications: setting up networks, printing, or transferring files.

- Wi-Fi is intended for resident equipment and its applications. The category of applications is outlined as WLAN, the wireless local area networks. Wi-Fi is intended as a replacement for cabling for general local area network access in work areas.

- Wi-Fi uses the same radio frequencies as Bluetooth, but with higher power, resulting in a faster connection and better range from the base station.

- Bluetooth was intended for non-resident equipment and its applications. The category of applications is outlined as the wireless personal area network (WPAN). Bluetooth is a replacement for cabling in a variety of personally carried applications in any setting.

Bluetooth Device Classes of Power Management

Type	Power	Power Level	Designed Operating Range	Sample Devices
Class 1	High	100 mW (20 dBm)	Up to 91 meters (300 feet)	AC-powered devices (USB dongles, access points)
Class 2	Medium	2.5 mW (4 dBm)	Up to 9 meters (30 feet)	Battery-powered devices (mobile devices, Bluetooth adapters, smart card readers)
Class 3	Low	1 mW (0 dBm)	Up to 1 meter (3 feet)	Battery-powered devices (Bluetooth adapters)

Bluetooth Spy Phone Spy Software

- http://www.youtube.com/watch?v=9qMdiguTluQ

Various versions of Bluetooth specifications define four security modes:

- Security Mode 1 is non-secure.
- In Security Mode 2, a security manager (as specified in the Bluetooth architecture) controls access to specific services and devices.
- In Security Mode 3, a Bluetooth device initiates security procedures before the physical link is fully established. Bluetooth devices operating in Security Mode 3 mandates authentication and encryption for all connections to and from the device. This mode supports authentication (unidirectional or mutual) and encryption.
- Similar to Security Mode 2, Security Mode 4 (introduced in Bluetooth v2.1 + EDR) is a service level enforced security mode in which security procedures are initiated after link setup. Security requirements for services protected by Security Mode 4 must be classified as one of the following: authenticated link key required, unauthenticated link key required, or no security required.

Confidentiality

In addition to the Security Modes, Bluetooth provides a separate confidentiality service to thwart eavesdropping attempts on the payloads of the packets exchanged between Bluetooth devices. Bluetooth has three Encryption Modes, but only two of them actually provide confidentiality. The modes are as follows:

- **Encryption Mode 1**—No encryption is performed on any traffic.

- **Encryption Mode 2**—Individually addressed traffic is encrypted using encryption keys based on individual link keys; broadcast traffic is not encrypted.

- **Encryption Mode 3**—All traffic is encrypted using an encryption key based on the master link key. Encryption Modes 2 and 3 use the same encryption mechanism.

Trust Levels, Service Levels, and Authorization

In addition to the four security modes, Bluetooth allows two levels of trust and three levels of service security. The two Bluetooth levels of trust are trusted and untrusted. A *trusted device* has a fixed relationship with another device and has full access to all services. An *untrusted device* does not have an established relationship with another Bluetooth device, which results in the untrusted device receiving restricted access to services.

- **Service Level 1**—Requires authorization and authentication. Automatic access is granted only to trusted devices; untrusted devices need manual authorization.

- **Service Level 2**—Requires authentication only; authorization is not necessary. Access to an application is allowed only after an authentication procedure.

- **Service Level 3**—Open to all devices, with no authentication required. Access is granted automatically.

Bluetooth Vulnerabilities

- After 1st use, unit key becomes public
  - Can lead to eavesdropping
- Pin management
- Encryption keystream repetition
- Secure storage of link keys
- Repeated authentication attempts (unlimited but time gap)

Threats

Bluetooth technology and associated devices are susceptible to general wireless networking threats, such as:

- Denial of service attacks
- Eavesdropping
- Man-in-the-middle attacks
- Message modification
- Resource misappropriation

They are also threatened by more specific Bluetooth-related attacks that target known vulnerabilities in Bluetooth implementations and specifications.

“Blue” Threats

- Bluesnarfing - Forces a connection to a Bluetooth device, allowing access to data stored on the device and even the device’s international mobile equipment identity (IMEI)
- Bluejacking - Initiated by an attacker sending unsolicited messages to a user of a Bluetooth-enabled device to entice the user to respond. Resembles spam and phishing attacks conducted against email users.
- Bluebugging - Security flaw in the firmware allows attacker to use the commands of the device without informing the user

Other Threats

- **Car Whisperer (European developed software tool)**
  - Allows an attacker to send to or receive audio from the car kit or receive from mic
- **Denial of Service**
  - Making a device's Bluetooth interface unusable and draining the mobile device's battery
- **Fuzzing Attacks**
  - Consist of sending malformed or otherwise non-standard data to a device's Bluetooth radio and observing how the device reacts

Risk Mitigation/Countermeasures

- Security measures
  - organizational security policy
  - aware of responsibilities
  - pre-cautionary measures
  - inventory list of devices and addresses

Risk Mitigation/Countermeasures (continued)

- Units set to lowest necessary power level to minimize range
- Complex pin codes
- Undiscoverable by default
- Maximum key size encryption
- Mutual authentication
- Service-level security mode 3 (most secure)
- Install software patches & upgrades

Future of Bluetooth

- Coming home
  - Home audio
  - Wireless mouse/keyboard
  - Home automation and energy efficiency (smart energy)
- **A2DP -** Bluetooth profile for streaming audio
  - Such as from a music phone to headphones
  - Supports stereo audio
  - One-way instead of two-way

Where you can find more information?

Guide to Bluetooth Security

Recommendations of the National Institute of Standards and Technology

by Karen Scarfone and John Padgette

Questions?