Bluetooth Security

Composed by : Bo Yang
Qi Liu

Email: Bo.Yang.9686@student.uu.se
Qi.Liu.9792@student.uu.se

Abstract

This article is about an introduction of Bluetooth Technology Security. We introduced what Bluetooth Technology is at first, and then discussed the problems the technology meets. Finally we described 3 security modes which were used to implement the Bluetooth Security.

I. Introduction of Bluetooth

At the beginning of our introduction of Bluetooth Technology Security, we would like to introduce some properties of Bluetooth Technology by comparing it with other two wireless communication technology, Infrared and Wireless LAN .

	Distance	Data type	Speed
Infrared	1m	Data only	4Mbps
Wireless LAN	More than 100m	Data, voice and others	11Mbps
Bluetooth	10m	Data and voice	1 Mbps

From the table above, we see that Bluetooth Technology has its advantage when the distances range from 1 to 10 meters. Also as we all know that the Bluetooth components like headsets and adapters are cheaper than that of Wireless LAN Technology. Therefore, people usually prefer using Bluetooth to send/receive/forward information between devices, like mobile phones, laptops, personal computers, etc. to Infrared or Wireless LAN Technology whose devices connect the networks by any multiple tangled physical medium like the cables and cords which may cost them too much.

II. Problems of Bluetooth Security

As we mentioned above, the Bluetooth Technology has many advantages, so many people believe that there must be no security problems and they don't worry about it because of the short distance range. However, there are many security problems when we use Bluetooth Technology to contact others, especially in public.

First of all, we should explain an important term called "pairing" before we go on with the article. Pairing happens in this situation: If one Bluetooth wants to communicate with another Bluetooth and this one agrees to do it, a pairing will occur. At that time, the two devices which connect to each other called a trusted pair. When one device recognizes another device in an established trusted pair, each device automatically accepts communication by passing the discovery and authentication process that

normally happen during Bluetooth interactions.

Suppose that you are using the Bluetooth function of your mobile phone. If you want to make a call, involving in a “Dial-Up” service, to your friend whose mobile phone also provides the Bluetooth function, you need to input the same authentication to the both devices, usually an identical PIN code which is an ASCII string up to 16 characters in length, to show that you have the right to do this operation. Once you have entered this same PIN code to the both devices, they will generate a link key and this key can be stored either in the devices themselves (like the devices’ memories) or in a persistent storage. And this link key will be used when another “pairing” happens between these two devices in the future.

Actually, by default, Bluetooth communication is not authenticated, and thus almost any device can freely connect to another. This vulnerability allows malicious hacker to steal phone books, photos and calendar information, or to make a phone call, send an SMS using one's mobile because of lack of authentication of pairing which happens between two devices. Try to imagine what would happen if an attacker do something bad using your mobile phone just like what we mentioned before: he will call your friend or send a message which carries a threat to your friend. The record of his/her mobile phone will point directly to you, the real owner of the phone, and identify you as the bad guy because the Bluetooth doesn’t keep any logs or copies of your message. What’s more, you may even not notice you “have sent” this message unless the status notification of message on your mobile phone is turned on.

Therefore, we know that the Bluetooth vulnerability is quite harmful and if we want to solve this problem we must be aware of the vulnerabilities which may occur in Bluetooth security first. Then we list some typical threats below:

1. Bluejacking – sends a Vcard (electronic business card) which contains some messages or photos to another Bluetooth user anonymously.
2. War-snipping – takes lots of small bits of data, while finding unsecured or unpatched Bluetooth connections.
3. Bluesnarfing – the theft of information from a wireless device through a Bluetooth connection.
4. Bluebugging – allows the attacker to initiate the phone calls, send and receive text messages, read and write phonebook contacts, eavesdrop on phone conversations, and connect to the Internet.

As we discussed above, the attacks may occur in different ways, like sending the insecure messages to a crucial receiver, e.g. to the government, from your mobile devices directly, cutting off the connection between two mobile devices who are using the Bluetooth function or attacking the server who provides the wireless service to you. If we want to solve this security problem, we should focus on the security models involved in it in advance.

III. Solutions of Bluetooth Security

The link layer security is usually used in wireless network. However, this kind of security can not satisfy the user's demand in upper layer. To meet with different requirements of data security in Bluetooth technology, Bluetooth technology provides three security modes to enforce the flexibility of its secure mechanism and the device manufacture determine which mode should be used.

The three modes are:
Mode1: non-secure
Mode2: Service-level security
Mode3: link-level security

Since Mode 1 means no secure protection. Devices in Mode 1 will never initiate any security procedure.[1]

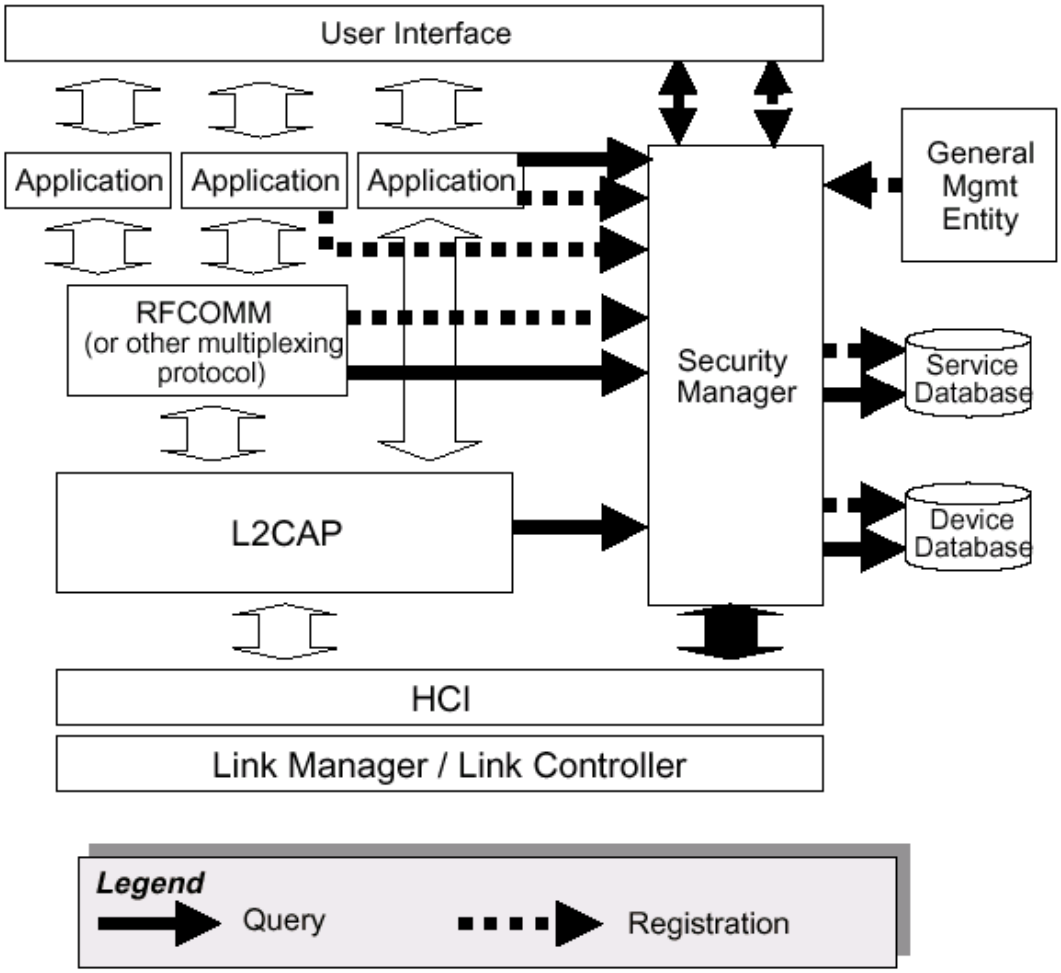
We would like to introduce Mode 3 before Mode 2 since Mode 3 is built on lower layer with simpler principle. The link-level security functions in Mode 3 are implemented by link keys which are 128-bit random numbers and stored by each pair of communication devices. When the first time two devices initialize a communication, a procedure called *pairing* asks the user to enter a *Bluetooth security code* into the paired devices and uses this code to generate a common random number initialization key. Through authentication, the Bluetooth security code is checked to make sure both of the paired devices use the same code. Then, a common 128-bit random-number link key is generated and stored temporarily in the paired devices. Although the Bluetooth security code is often referred to as a PIN (Personal Identification Number), however, user does not need to remember it since it is only used once by the pairing procedure. Finally, after authentication and getting the current link key, a new encryption key is generated from link key each time a communication session is established.

The security Mode 2 concentrates on defining the security levels for devices and services. Devices have two levels of "trust", which determines which devices should be trust and which ones should not be trust. Services have three levels of security, which defines what kind of devices can access certain services. Each service in Bluetooth equipment should set its security level independently.

The Bluetooth security architecture is design to implement the Mode 2 Bluetooth security on Bluetooth devices. It is built on the top of the link-level security features, used to find when to involve a user and what the lower Bluetooth protocol layers should do to support the desired security check.[2] The key component of this architecture is the security manager. The security manager is responsible for variety of tasks like storing security-related information, responding to access request, initiating pairing and query PIN entry and so on. The policy for access control is stored in the

security manager, therefore every time a connection request goes through L2CAP (Logic Link Control and Adaptation Protocol, which resides in data link layer and provides services to upper layer protocol with protocol multiplexing capability, segmentation and reassembly operation, and group abstractions), the L2CAP queries the security manager with the information it received. The security manager performs a lookup in its service/device database, enforces authentication and encryption if it is necessary, and replies the protocol entity whether access is granted or refused ultimately.

This figure below is the security architecture:



Reference

[1] Karen Scarfone，Derrick Dicoi，Wireless Network Security for IEEE 802.11a/b/g and Bluetooth(DRAFT)，retrieved from http://csrc.nist.gov/publications/drafts/800-48-rev1/Draft-SP800-48r1.pdf

[2] Nathan J. Muller. Bluetooth Demystified. McGraw-Hill, 2001.

[3]Jennifer Bray, Charles F Sturman ,Bluetooth [1.1] : connect without cables, Upper Saddle River, N.J. ; London : Prentice Hall PTR, cop. 2002

[4]Robert Morrow ,Bluetooth operation and use [Elektronisk resurs], New York : McGraw-Hill, c2002

Before we explain current Bluetooth security, we should go back in time a bit. Bluetooth was invented in 1989, but really came into use during the 2000s. There is no one Bluetooth protocol; it is a collection of different protocols grouped together under a single specification. Bluetooth is managed by the Bluetooth Special Interest Group, also referred to as Bluetooth SIG. In an effort to explain a concept like LE Privacy, we must explain a chunk of the Bluetooth history of security implementations. BluetoothÂ® Security Response Program. The Bluetooth SIG is committed to promptly addressing vulnerabilities in the Bluetooth specifications that may impact our member companies and the broader Bluetooth ecosystem. The BluetoothÂ® Security Response Program addresses reported vulnerabilities within the Bluetooth specifications. The program collaborates with the security research Bluetooth security is increasingly important with hackers using Bluejacking & Bluebugging and other techniques, but Bluetooth security is now improving. Bluetooth Tutorial / Summary Includes: Bluetooth technology basics Radio interface File transfer Bluetooth profiles Pairing & networking Security. Bluetooth security like that for any other wireless system is very important. With hackers gaining access to an ever increasing number of systems, Bluetooth security is increasingly important. Bluetooth connections to your mobile devices can be used to connect to wireless headsets, transfer files, and enable hands-free calling while you drive, among other things. Most of the time, a user must allow a Bluetooth connection to occur before data is shared - a process called "pairing" - which provides a measure of data security. But just like Wi-Fi connections, Bluetooth can put your personal data at risk if you are not careful. Here are some steps you may wish to take when using Bluetooth