ISSN:0975-9646

Bluetooth Security Issues

Purvish Patel[1], Akash Merchant[2], Nisarg Tailor[3], Chintan Trivedi[4]
Uka Tarsadia University, Bardoli Mahuva Road,
Tarsadia, Dist: Surat - 394350, Gujarat (INDIA)

Abstract-Bluetooth Technology refers to short range radio frequency communication, which allows transfer of data within a particular range-on and around 10m. And is undergoing many crucial threats that either leads to data thefts or third party data access such as Bluejacking, Bluesnarfing, Bluebugging, etc., which may lead to dis-honour in Bluetooth security threats like Authentication, Confidentiality and Authorization. Several advantages and security threats have been discussed to ensure the working, structure and the architecture of the Bluetooth Technology.

Keywords: Bluetooth 4.0, Information Technology Security, Low-Power, High Speed, vulnerability.

1. INTRODUCTION

Bluetooth is a short range data transmission technology. Bluetooth technology is used primarily to build wireless personal area networks . Bluetooth technology has been linked up with many types of devices, including cell phones, laptops, automobiles, and many hand-held devices supporting this technology.

There are different types of version of Bluetooth which have their advantages and disadvantages. They have their own basic rates and data rates and different speeds. Bluetooth is generally used for transmission of data from one device to another device or one to more devices. Bluetooth devices can support multiple data rates.

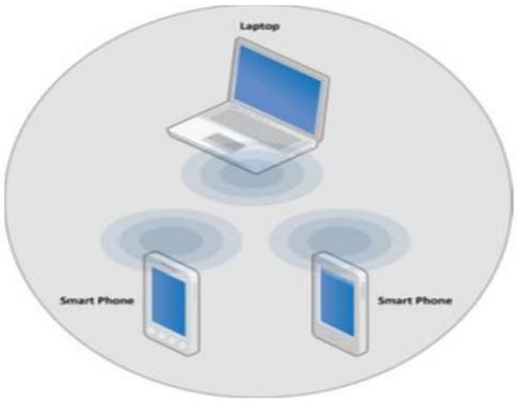
This paper summarizes the general security issues on the bluetooth technology. Especially, it describes the security features of the bluetooth 4.0 protocol and analysis combination and authentication security technology in the LP bluetooth 4.0. The security threats and security recommendations concerning to the pairing and authentication process of the bluetooth devices are shown

2. STRUCTURE OF BLUETOOTH

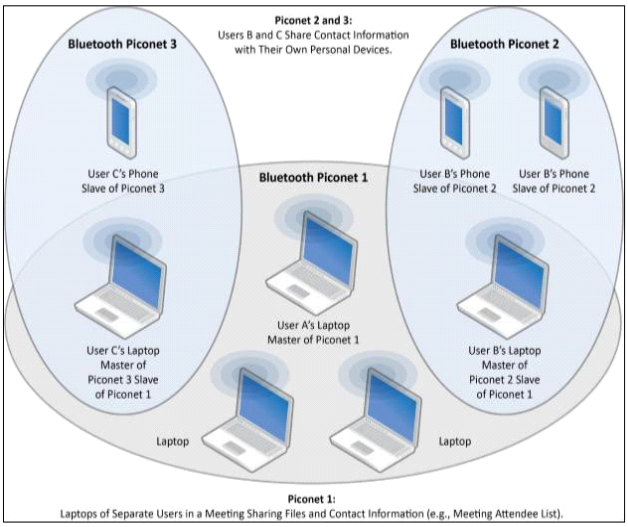
Bluetooth allows your devices to establish ad hoc (temporary) networks. Ad hoc networks allow easy connection between devices in the same physical area (e.g., in the range) without need of any infrastructure devices.

The master gadget manage and builds the network, including defining the network's frequency hopping scheme. Although one piconet can have only one master, time division multiplexing (TDM) allows a slave in one piconet to be master for another piconet simultaneously, hence creating a chain of networks, called a scatternet.

Even the topology gets changes once the device moves away or towards the master device, along with the relationships of the devices in the immediate network.



F-1 This shows the ad hoc topology of bluetooth. [Recommendations of the National Institute of Standards and Technology, June 2012]



F-2 This shows the multiple scatternets Bluetooth networks. [Recommendations of the National Institute of Standards and Technology, June 2012]

2.1 New Security Features Of Bluetooth

Due to limited computing and storage ability of Low-Power Bluetooth devices, its security technology is different with traditional BR/EDR/HS Bluetooth. One difference is that the Low-Power Bluetooth pairing results in Long-term Key (LTK), instead of the link key, which fundamentally performs the same secret key function as a link key. LTK is established in different ways. It is generated by using a key transport protocol, rather than using the BR/EDR negotiation. In other words, the Bluetooth device determines LTK.

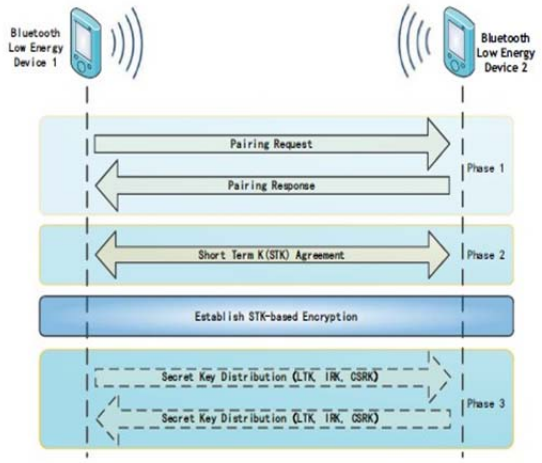
The pairing process will be sent to another Bluetooth device, rather than generating separate keys for the

same two devices. A Bluetooth specification, the Low-Power Bluetooth first describes how to use the Advanced Encryption Standard-Counter with CBC-MAC (AES-CCM). In addition to providing a strong, standard-based encryption, AES-CCM for local Low-Power Bluetooth devices FIPS-140 validation Paves roads of the future.

The Low-Power Bluetooth device also introduces a dedicated device address and signature functions. Called identity to solve key (IRK) and connect the new encryption key signatures solve key (CSRK) to support these functions. IRK is used to solve the public address mapping to the specialized equipment. This allows trusted devices to determine from the public (random) device into a dedicated device address. The new security features for a particular device provides secure privacy. Prior to this, the device will be assigned a static address in the search process. If the device remains can be found, its location can be opponents track. CSRK used data from a specific device authentication cryptographic signature frame. Bluetooth connectivity which allows the use of the data signature (integrity and authentication) to protect the connection instead of the connection data encryption, the AES-CCM provides confidentiality, integrity and authentication.

2.2 Security mode and level of the Low-Power Bluetooth

Low-Power Bluetooth security mode is similar to the level of security of the BR/EDR mode (Security Mode 2 and 4), which can have its own security requirements for each service. However, Low-Power Bluetooth also specifies each service request can have its own security requirements. Equipment to enforce the service following the appropriate security mode and level of security requirements. Low Power Security Mode 1 has a plurality of encryption related level. Level 1 does not specify the security, which means that no authentication and encryption. Level 2 requirements to unauthenticated paired encryption. Level 3 requirements with encrypted authentication.



F-3 This shows the pairing process of two LP bluetooth device.

[PairingandAuthenticationSecurityTechnologiesinLow-PowerBluetooth, June 2013]

The low power security mode 2 has a signature associated with the data at multiple levels. Data signature provides a powerful data integrity, but not confidentiality. Level 1 requirements unauthenticated data signature matching. Level 2 requires an authenticated signature matching and data.

If a service request and related services with different security model and (or) levels, and more powerful security requirements. For example, if any demand need security mode level 3, then Security Mode 1 Level 3 requirements be enforced.

2.3 BLUETOOTH SECURITY THREATS

- **Authentication**: prove the characteristics of communicate procedure base on their Bluetooth gadget address. Bluetooth does not give native client verification.
- **Confidentiality**: prevent information concession caused by eavesdrop by ensuring that only allowed devices can right to use and view transmit information.
- **Authorization**: allow managing resources by ensure that a gadget is official to use a service before permit it to do so.

2.3.1 BLUETOOTH CONFIDENTIALITY, AUTHENTICATION, INTEGRITY

- Modes weak protection : 'just works' linked mode during pairing provides MITM protection Which will result in unauthenticated link key. In order to obtain the highest level of security. Bluetooth devices in the SSP during MIMT protection, and neglected the 'just works' unauthenticated link key pair that are generated upon request.
- Weak password generated: SSP ECDH key may be static or weak generation. Weak ECDH key ssp eavesdropping protection minimized, which allow the attacker can determine the secret link key. all equipment shall have a unique, strong generates ECDH key pair.
- Password static: static SSP key to MITM attacker facilitated .key MITM protection during the ssp even wgen you do not need to re-key Bluetooth devices, while still using the last connection key. Bluetooth devices for each pair is connected using the random, unique key. Allowed to fall back to any other security mode ?mode switching vulnerabilities: security mode devices connection does not support security mode 4 Bluetooth devices. Then ,the worst case will fall device to return to the security mode, it provides no security authenticated connection
- Key compromise: connection authentication attempts repeatable. Bluetooth devices need to include a mechanism to prevent unrestricted identity verification request. Bluetooth specification requires that the wait interval between attempts to exponential growth in continues identity verification however, it does not require the kind of waiting interval of authentication the suspect requests, so the attacker can collect a large number of suspected response(which the confidential link key

encryption),may leak information about the secret link key information.

- Broadcast Secret Sharing: for broadcast encryption master key is shared between all the micro-network equipment. secret key shared between two or more of the parties to provide favorable conditions for the simulated attack
- Equipment certification attack: device authentication is simple shared key suspect in the response. One-way-only suspect that the response to the authentication part of MITM attacks. Bluetooth provides mutual authentication , it should be used as s verification device and network legitimacy.

2.5 BLUETOOTH SPEED BAESD ON DEVICE

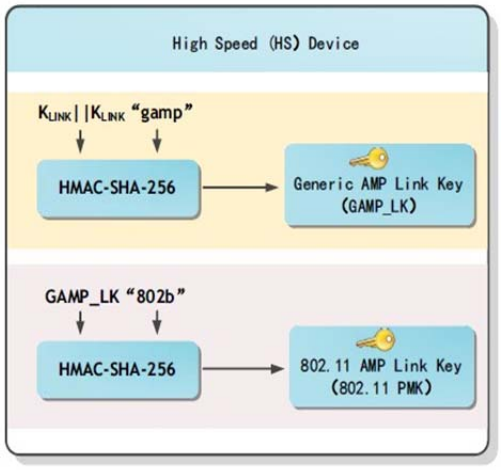
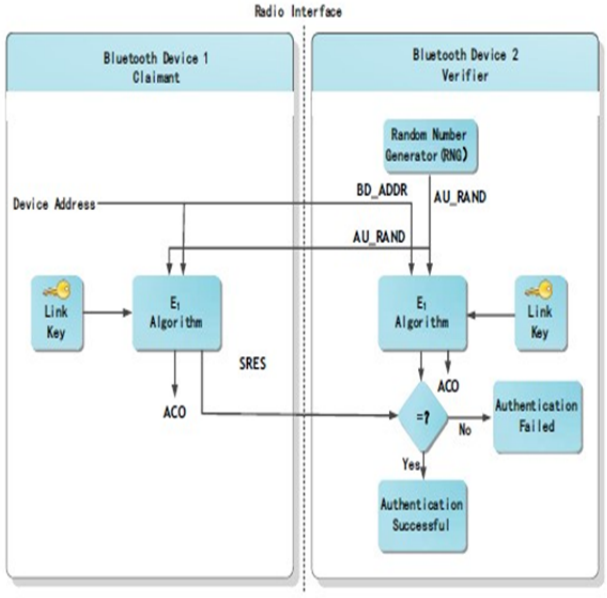


Figure 2. $(GAMP\_LK)$ using Bluetooth link key series and extended the ascii code key identifier (keyID).

[PairingandAuthenticationSecurityTechnologiesinLow-PowerBluetooth, June 2013]



[PairingandAuthenticationSecurityTechnologiesinLow-PowerBluetooth, June 2013]

3.0 ADVANTAGE OF BLUETOOTH

Cable Replacement: Bluetooth technologies overcome cables at a great extent, such as those that were previously used for secondary devices like mouse, keyboard, printers, etc.

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

Wireless synchronization: Bluetooth can provide auto-synchronization involving Bluetooth-enabled devices. For example, synchronization of electronic contacts and calendar using Bluetooth.

Internet connectivity: Internet may well be shared on or after one Bluetooth enabled device to the other.. For example, a laptop can use a Bluetooth connection to direct a cell phone to establish a dial-up establish so that the laptop can use the Internet through the phone.

Table 1. Different version:

versions	Basic rate	Approximately speed
1.1 and 1.2	1 Mbps	720 Kbps
2.0	3 Mbps	2.1 Mbps
3.0	4 Mbps	2.8 Mbps
4.0	4.2 Mbps	3.7 Mbps

3.1 BLUETOOTH THREATS

Bluesnarfing: Bluesnarfing enable attackers to increase right to use to a Bluetooth-enabled device by exploit a firmware error in older devices. This attack services a link to a Bluetooth device, allowing access to data stored on the device as well as the device's international mobile equipment identity . The IMEI is a matchless identifier for all device that an enemy might potentially use to route all inward calls from the user's device to the attacker's device. Bluesnarfing is the burglary of information from a wireless device during a Bluetooth link. Bluetooth is a speedy but very limited wireless technology for exchange data between desktop and cellular phone computers, personal digital assistants, and other devices. By exploit a susceptibility in the way Bluetooth is implemented on a mobile phone, an mugger can access information -- such as the user's calendar, contact list and e-mail and text messages -- without departure any proof of the attack. Other devices that make use of Bluetooth, such as laptop computers, may also be weak, even if to a lesser extent, by virtue of their more difficult systems. working in unseen mode protects a number of devices, but others are weak as long as Bluetooth is enabled.

Blue jacking: Blue jacking is an attack conduct on Bluetooth-enabled cell phone devices, such as cell phones. An attacker initiate blue jacking by transfer unwanted messages to the client of a Bluetooth-enabled gadget. The real messages do not reason damage to the user's gadget, but they may tempt the user to react in some fashion or add the new contact to the device's address book. This message-sending assault resemble spam and phishing attacks conducted against e-mail users. Blue jacking can reason damage while a user initiate a answer to a blue jacking message sent with a damaging plan.

Blue jacking is a hack technique that allows an person to send unidentified messages to Bluetooth-enabled devices inside a confident radius. First, the hacker scan his surrounds with a Bluetooth-enabled device, pointed for extra devices. The hacker then send an unwanted message to the detect devices.

Blue jacking exploit a basic Bluetooth characteristic that allow devices to send messages to contacts inside range.

Blue jacking does not engage device hijack, in spite of what the name imply. The blue jacker may send only unwanted messages. hijack does not really happen because the attacker not at all has manage of the victim's gadget. At worst, blue jacking is an exasperation. Blue jacking can be banned by setting a gadget to secreted, unseen or non-discoverable mode.

Blue bugging: Blue bugging exploit a safety fault in the firmware of a number of older Bluetooth devices to increase right to use to the device and its guidelines. This attack uses the guidelines of the device not including informing the user, allowing the enemy to access data, place cellular phone calls, overhear something on phone calls, send messages, and use other services or skin accessible by the gadget.

Blue bugging allows expert persons to right to use the mobile phone guidelines use Bluetooth wireless knowledge without notify or alert the phone user. This weakness allow the hacker to start phone calls, send and study SMS, read and write phonebook contacts, overhear something on phone conversations, and join to the Internet. As through all the attack, the hacker must be inside a 10 meter range of the cellular phone. This is a part weakness starting bluesnarfing and does not have an effect on all of the same phone as bluesnarfing. for example, after which the cellular phone machinery as a bug device, alternative up conversation in the phone's direct area. also, a blue bugger can set call forward and then receive calls future for the blue bug victim. Blue buggers also have bluesnarfing ability, so they be able to read phonebooks and calendars and more. They be able to even read a phone's call list to observe who their dead called or who called them. They be able to even change those list.

Car Whisperer: Car Whisperer is a software instrument developed by European security researchers that exploit a key execution problem in hands-free Bluetooth car kits install in automobile. The Car Whisperer software allow an enemy to send to or get audio from the car kit. An enemy can broadcast audio to the car's speakers or get audio (listen in) from the microphone in the car.

Using a unique directional antenna that allowable him to expand the usually small range of his Bluetooth associations to about a mile, Hertfort was capable to listen and send audio to regarding 10 cars over a one-hour stage recently.I could listen to voices from cars temporary by, he said. "If I had been following the car, I would have been able to listen in for a longer time."Though some Bluetooth users may be surprised to study that all they say through their next car ride can be overhear, fault for the problem lies directly with the Bluetooth system manufacturer, not with Bluetooth itself, Heft believed. Producer are dependability something incorrect with this. Bluetooth is a very excellent thing, once all is right.

Trifinite is at here study whether banned Bluetooth intruder could do everything more serious than listen in or suggest driving tips. Heft said it's not possible for an attacker to do something actually serious such as disable airbags or brakes, but he believe there may be other implication to his group hack.

It's achievable, for example, that an enemy could right to use a cell phone address book once he has linked with the Bluetooth system, but Trifinite will have to perform more study before it be able to say for sure whether this can occur, he said.

Denial of Service: Like other wireless technology, Bluetooth is vulnerable to DoS attack. impact include creation a device's Bluetooth boundary not viable and difficult the device's battery. These type of attack are not important and, because of the closeness necessary for Bluetooth make use of can regularly be simply avert by simply affecting out of range.

DoS/DDoS attacks is planned electronic incursions. Their reason is to disturb an organization network operation by deny right to use to its user. In other words, DoS and a DDoS attacks leave network resources out-of-the-way to individuals by deny right to use to those network resources. In our case, the attack were planned to severely maximum the access and make use of of online games and e-mail, but they can involve any online movement.

Network operations by deny right to use to its users. In other words, DoS and a DDoS attacks provide network resources unapproachable to individuals by denying access to that network property. In our case, the attacks were planned to severely limit the access and use of online games and e-mail, but they can involve any online movement.

Making matter bad, the reason, or **attacker**, can take manage of your computer or terminal and apply it to infect thousands of extra computers, referred to as **zombies**. The attacker then use these zombies to produce millions of **data packets** - requests for service - which finally overwork e-mail, web, and network servers. In this situation, as more than one processor was mixed up and dirty zombies were used, this type of attack is careful a scattered attack.

4. CONCLUSION

Bluetooth is not a frequently used technology; as many alternatives have been upcoming with the increase in technology. But still for small amount of data sharing and transferring the data; bluetooth technology is used. The data shared with this technology can be confidential and hence need to be protected.

Hence, algorithms can be generated through which a safer transmission can be done between the devices without any data theft or any attack between the sharing process. So, Bluetooth Hacking is a major problem for those who share their confidential or important datas through this technology; data such as contacts, images, documents and other personal as well as office based stuffs.

REFERENCES

[1]- Guide to Bluetooth Security, Recommendations of the National Institute of Standards and Technology, Overview of Bluetooth Technology(June 2012)

[2] PairingandAuthenticationSecurityTechnologiesinLo wPowerBluetooth (2013 ieee)

[3] Kathrine Aguilar Masagca, An Investigation of Bluetooth Security Threats , BlueBugging: (2011)

[4] HariharanRajasekaran, A Leaky Bucket called Smartphone ,2012 IEEE (19 March 2012)