IJETST- Vol.||03||Issue||01||Pages 3449-3457||January||ISSN 2348-9480 2016

Open access Journal International Journal of Emerging Trends in Science and Technology
DOI: http://dx.doi.org/10.18535/ijetst/v3i01.05

Connecting & Addressing Security Concerns of Bluetooth Technology in Current Scenario

Authors
Rajnish Mehra[1], Dr Pratima Gautam (Dean)[2]
[1]Department of Computer Sc. & Applications, M.phil (Comp Sc) AISECT University, Bhopal, India (M.P)
[2]Department of Computer Sc. & Applications, AISECT University, Bhopal, India (M.P)

Abstract- *In this paper we present a survey on Bluetooth technology regarding the threats and vulnerability attacks during data transfer on its security mechanism. Bluetooth technology uses the personal area network (PAN). It is the kind of wireless Ad-hoc network. Low cost, low power, low complexity and robustness are the basic features of Bluetooth. It works on Radio frequency. Bluetooth Technology has many benefits like replacement of cable, easy file sharing, wireless synchronization and internet connectivity. As Bluetooth Technology becomes widespread, vulnerabilities in its security protocols are increasing which can be potentially dangerous to the privacy of a user's personal information. Security in Bluetooth communication has been an active area of research for last few years. The article presents various security threats and vulnerability attacks on Bluetooth technology and also how to restrict them.*

Keywords- *Bluetooth security; security protocol; vulnerability; security threats; blue jacking; eavesdropping; malicious attackers.*

I. INTRODUCTION

Bluetooth is an open standard for short-range radio frequency (RF) communication. This allows users to form ad-hoc networks between a wide variety of devices to transfer voice and data. 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*. A piconet is composed of two or more Bluetooth devices in close physical proximity that operate on the same channel using the same frequency hopping sequence. An example of a piconet is a Bluetooth-based connection between a cell phone and a headset. Bluetooth piconets are often established on a temporary and changing basis, which offers communications flexibility and scalability between mobile devices. Some key benefits of Bluetooth technology are— **Cable replacement, Ease of file sharing**, **Wireless synchronization, Internet connectivity.** Bluetooth technology uses various types of protocol as key agreement protocol. Generating keys for Bluetooth technology is very decisive part, so our main focus is on functioning of key agreement protocol. For example if two devices want to communicate securely to each other first of all they want to generate a secret key because initially they do not have shared secret key, because of this they use the key agreement protocol. When this protocol performed the link key and encryption keys are generated. The encryption key is used in E0 stream cipher and the link key is used in challenge response technique which is used for authentication in Bluetooth. Link key is of two types: unit key and combination key. Unit key: same key is use for authentication for all the connection. Combination key: is specific to one pair of Bluetooth device.

II. PROTOCOL STACK OF BLUETOOTH

A protocol stack is a combination of software/hardware implementation of the actual protocols specified in the Bluetooth architecture standard. It also defines how the devices

should communicate with each other based on the standard. The Bluetooth protocol stack is shown in Fig. 1.

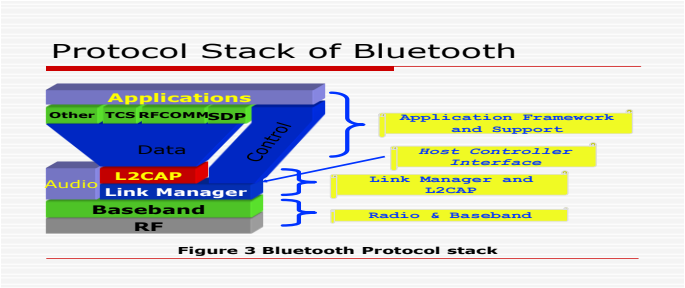

Fig. 1 Bluetooth architecture- Protocol Stack

1. Radio Frequency (RF) Layers

The radio frequency (RF) layer is the physical wireless connection. In order to reduce collisions with other devices using the ISM range, the radio uses frequency mapping to separate the range into 79MHz bands, starting at 2.402GHz and stopping at 2.480Hz and uses this spread spectrum to hop from one channel to another, up to 1600 times per second. Mainly sending and receiving modulated bit streams.

2. **Base band layer**

The base band allows the physical connection between devices. It is responsible for controlling and sending data packets over the radio link. When a Bluetooth device connects to another Bluetooth device, they form a small network called a piconet. A piconet is a small network of Bluetooth devices, where every device in the network can be in one of the following states. Mainly defines the timing and framing also flow control on the link.

Master: The Bluetooth device that initiates communication. The master sets the time and broadcasts its clock to all slaves providing the hopping pattern, in which they hop frequency at the same time.

Slaves: The state given to all devices that are connected to another. The device can be an active slave if it actively transmits or receives data from the master, or a passive slave if it is not currently sending or receiving any information. The passive slaves check if there is a connection request from the master by enabling their RF receivers periodically.

All devices that are not connected to a master (i.e. not slave) are called 'standby' devices. When searching for other devices, a device enters the inquiry state. When a device starts creating a Bluetooth link, it enters the page state. Also a device can go to a low power mode to save power.

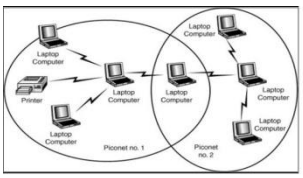

Fig 2: Typical Scatternet

3. Link 2 Manager Protocol (LMP) The LMP protocol uses the links set up between devices by the base band to establish logical connection responsibilities of the LMP. It also includes security aspects and device authentication. Mainly managing the connection states, enforcing fairness among slaves and power management.

4. Logical Link Control and Adaptation Protocol (L 2CAP) The L2CAP is responsible for receiving applicative data from the upper layers and translates it to the Bluetooth format so that it can be transmitted to the higher layer protocol over the base band. Mainly handles multiplexing of higher level protocols,segementation & reassembly of large packets and device discovery of QOS.

5. Radio Frequency Communication Protocol (RFCOMM) The RFCOMM is used to emulate serial connections over the base band layer to provide transport capabilities for upper level services and avoiding direct interface of the application layer with L2CAP. Mainly cable replacement protocol, emulation of serial ports over wireless network.

6. Service Discovery Protocol (SDP) The SDP protocol is used to discover services, providing the basis for all the usage models. Mainly means for applications to discover device information, services and its characterstics.

7. TCP/IP layer The TCP/IP protocol defines the call control signaling for the establishment of

voice and data calls between Bluetooth devices. TCP/IP signaling messages are carried over L2CAP. Mainly network protocols for packet data communication and routing.

8. Application Layer The application layer contains the user application. The applications interact with the RFCOMM protocol layer to establish an emulated serial connection. Mainly consists of Bluetooth aware as well as un-aware applications.

9. Host Controller Interface (HCI) Layer The HCI layer provides a command interface to baseband controller and link manager, also to hardware status, control and event register.

III. BLUETOOTH SECURITY ARCHITECTURE

Security for Bluetooth is provided on the radio paths, which means that link authentication and encryption may be provided, but true end-to-end security is not possible without providing security solutions for the higher layers of Bluetooth. Basically, Bluetooth addresses the three security services:

Confidentiality: Firstly, Bluetooth provides confidentiality or privacy. This prevents an information compromise caused by eavesdropping by ensuring that only authorized devices can access and view transmitted data.

Authentication: Secondly, Providing verifying the identity of communicating devices based on their Bluetooth device address. Bluetooth does not provide native user authentication. Authentication allows the communicating devices able to recognize each other; hence communication aborts if the user is not authorized.

Authorization: Thirdly, allowing the control of resources by ensuring that a device is authorized to use a service before permitting it to do so.

Keys used in Bluetooth security

Unit Keys: The authentication and encryption mechanisms based on unit keys are the same as those based on combination keys. However, a unit that uses a unit key is only able to use one key for all its secure connections. Hence, it has to share this key with all other units that it trusts. Consequently, all trusted devices are able to eavesdrop on any traffic based on this key. A trusted unit that has been modified or tampered with could also be able to impersonate the unit distributing the unit key. Thus, when using a unit key there is no protection against attacks from trusted devices.

Combination Keys: The combination key is generated during the initialization process if the devices have decided to use one. Both devices generate it at the same time. First, both of the units generate a random number. With the key generating algorithm E21, both devices generate a key, combining the random number and their Bluetooth device addresses. After that, the devices exchange securely their random numbers and calculate the combination key (K_{ab}) to be used between them as shown in Fig 3.

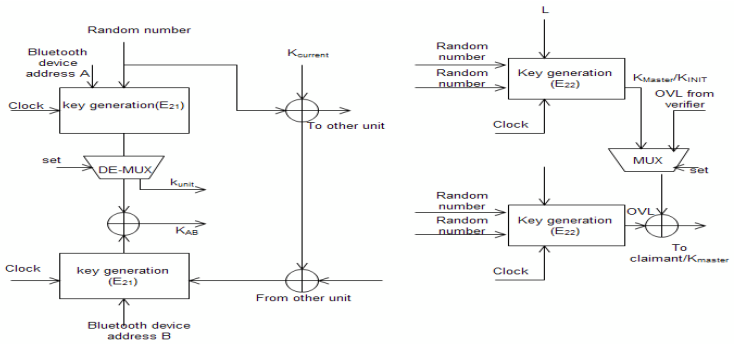

Fig 3: Link Key generation

Encryption keys: The encryption key is generated from the current link key, a 96-bit Ciphering Offset Number (COF) and a 128-bit random number. The COF is based on the Authenticated Ciphering Offset (ACO), which is generated during the authentication process. When the Link Manager (LM) activates the encryption, the encryption key is generated. It is automatically changed every time the Bluetooth device enters the encryption mode.

IV. SECURITY CONCERNS

Bluetooth technology is not without its problems. The biggest concern revolves around security issues with Bluetooth devices. Currently, the protocol is vulnerable to various types of attacks.

These attacks, when properly exploited, can have serious consequences on the users of Bluetooth-enabled devices. The most high-profile exploits include Bluejacking, Bluebugging, Bluesnarfing, the Cabir Worm, and Denial of Service attacks, which are described below

V. VULNERABILITY ATTACKS ON BLUETOOTH

Now a days, Bluetooth devices are frequently used, malicious security violations are common events now and it will be increased in future. So Bluetooth architecture needs to be constant upgrading to prevent new unknown threats. Bluetooth attacks depend on exploiting the permission request/grant process that is the backbone of Bluetooth connectivity. Here are a few examples of the mobile security threats in which Bluetooth makes us vulnerable, along with tips to secure your mobile workforce devices.

1. Bluejacking- Bluejacking is an attack conducted on Bluetooth-enabled mobile devices, such as cell phones. An attacker initiates bluejacking by sending unsolicited messages to the user of a Bluetooth- enabled device. The actual messages do not cause harm to the user's device, but they may entice the user to respond in some fashion or add the new contact to the device's address book. This message- sending attack resembles spam and phishing attacks conducted against e-mail users. Bluejacking can cause harm when a user initiates a response to a bluejacking message sent with a harmful intent.

2. The Car Whisperer- Car Whisperer is a software tool developed by European security researchers that exploits a key implementation issue in hands-free Bluetooth car kits installed in automobiles. The Car Whisperer software allows an attacker to send to or receive audio from the car kit. An attacker could transmit audio to the car's speakers or receive audio (eavesdrop) from the microphone in the car.

3. Bluebugging- Bluebugging is a bit more dangerous than the first two, allowing attackers to remotely access a user's phone and use its features, including listening to calls, forwarding incoming calls, placing calls and sending text messages — and the user doesn't realize what's happening. This can result in expensive phone bills if it's used to make premium or international calls.

4. General software vulnerabilities- Software in Bluetooth devices – especially those using the newer Bluetooth 4.0 specification – will not be perfect. It's unheard of to find software that has zero security vulnerabilities.

To restrict this threat: Switch off your Bluetooth when you're not using it.

5. Pairing Eavesdropping- PIN/Legacy Pairing (Bluetooth 2.0 and earlier) and LE Pairing (Bluetooth 4.0) are susceptible to eavesdropping attacks. The successful eavesdropper who collects all pairing frames can determine the secret key(s) given sufficient time, which allows trusted device impersonation and active/passive data decryption. Just like with Wi-Fi, Bluetooth encryption is supposed to stop criminals listening in to your data or phone calls. In other words, eavesdropping shouldn't be a problem. However, older Bluetooth devices use versions of the Bluetooth protocol that have more security holes. Even the latest specification (4.0) has a similar problem with its low-energy (LE) variant.

To restrict this threat: Ban devices that use Bluetooth 1.x, 2.0 or 4.0-LE.

6. Denial of Service- Like other wireless technologies, Bluetooth is susceptible to DoS attacks. Impacts include making a device's Bluetooth interface unusable and draining the device's battery. Malicious attackers can crash your devices, block themfrom receiving phone calls and drain your battery.

To restrict this threat: Again, switch off your Bluetooth when you're not using it.

7. Bluetooth range is greater than you think- Bluetooth is designed to be a "personal area network." That is to say, devices that are more than a few feet away should not be accessible via Bluetooth. However, you're not safe if you simply ensure there's distance between you and a potential attacker; hackers have been known to

use directional, high-gain antennae to successfully communicate over much greater distances.

To restrict this threat: Once again, switch off your Bluetooth.

8. MAC Spoofing Attack- Among all passive attacks, the most frequently reported attacks are classified as MAC spoofing and PIN cracking attacks. Malicious attackers can perform MAC spoofing during the link key generation while Piconets are being formed. Assuming the attack is made prior to successful pairing and before encryption is established attackers can easily intercept data intended for other devices. Attackers, with specialized hardware, can easily use spoofing to terminate legitimate connections or capture and/or manipulate data while in transit.

To restrict this threat: Bluetooth SIG did not provide a good solution to prevent this type of attack. They only advised the users to do the pairing process in private settings. They also suggested that a long, random, and variable PIN numbers should be used.

9. PIN cracking attack- Using a Bluetooth frequency sniffer (or protocol analyzer) and acquisition of a FHS packet, attackers can attempt to acquire IN_RAND, LK_RAND and the initialization key during the entire pairing and authentication processes. The attacker would have to list all of the possible permutations of the PIN. Using the acquired IN_RAND and BD_ADDR they would need to try possible permutations as input in the E22 algorithm. Eventually they would be able to find the correct initialization key. The next step is to hypothesize and test possibilities of the shared session link key using all of the previous data. Assuming the right information is collected, the proper equipment is used, and enough time is allowed, PIN cracking becomes a fairly simple task. **To restrict this threat**: The proposed solutions for these types of attacks involve different pairing and authentication schemes that involves using a combination of public/private keys.

10. Man-in-the-Middle/Impersonation Attack- Man-in-the-Middle and impersonation attacks actually involve the modification of data between devices communicating in a Piconet. A Man-in-the-Middle attack involves relaying of authentication message unknowingly between two devices in order to authenticate without knowing the shared secret keys. By forwarding the message of two devices trying to pair, an attacker will relay two unique link keys. By acting between two devices an attacker can trick two devices into believing they are paired when in fact they have paired with the attacker.

To restrict this threat: The suggested solutions to this kind of attack involve incorporating more Piconet specific information into the pairing process. For example, timestamps and nested mutual authentication can be used to determine the legitimacy of a device's challenge before responses are sent in return.

11. Blue Printing Attack- A Blue Printing attack is used to determine the manufacturer, device model and firmware version of the target device. An attacker can use Blueprinting to generate statistics about Bluetooth device manufacturers and models, and to find out whether there are devices in the range of vulnerability that have issued with Bluetooth security, for example. BluePrint 0.1 is a tool for performing Blue Printing attack. It runs on Linux and it is based on the BlueZ protocol stack.

To restrict this threat: Blue Printing attacks work only when the BD_ADDR of the target device is known.

12. Blueover attack

Blueover and its successor Blueover II are derived from Bluetooth. However, because they run on handheld devices such as PDAs or mobile phones and are capable of stealing sensitive information by using a BlueBugging attack. A Blueover attack can be done secretly, by using only a Bluetooth mobile phone with Blueover or Bluover II installed. Bluleover and Bluover II run on almost every J2ME (Java 2 Micro Edition) compatible handheld device.

To Restrict this threat: A Blueover attack is dangerous only if the target device is vulnerable to Blue Bugging. Moreover, an attacker has to know the BD_ADDR of the target device.

13. Off-Line PIN Recovery Attack- An off-line PIN recovery attack is based on intercepting the IN_RAND value, LK_RAND values, AU_RAND value and SRES value, and after that trying to calculate the correct SRES value by guessing different PIN values until the calculated SRES equals the intercepted SRES. It is worth noting that SRES is only 32 bits long. Therefore, a SRES match does not necessarily guarantee that an attacker has discovered the correct PIN code, but the chances are quite high especially if the PIN code is short.

14. Brute-Force Attack- A brute-force BD_ADDR scanning attack uses a brute- force method only on the last three bytes of a BD_ADDR, because the first three bytes are publicly known and can be set as fixed. A brute-force BD_ADDR scanning attack is perhaps the most feasible attack when target devices are Bluetooth mobile phones, because millions of vulnerable Bluetooth mobile phones are used every day all over the world.

15. Reflection Attack- Reflection attacks (also referred to as relay attacks) are based on the impersonation of target devices. An attacker does not have to know any secret information, because the attacker only relays (reflects) the received information from one target device to another during the authentication. Hence a reflection attack in Bluetooth can be seen as a type of a MITM attack against authentication, but not against encryption.

16. Backdoor Attack- The backdoor attack involves establishing a trust relationship through the pairing mechanism, but ensuring that it no longer appears in the target's register of paired devices. The attacker may continue using the resources that a trusted relationship with that device grants access to until the users notice such attacks. The attacker can not only retrieve data from the phone, but other services such as modems, Internet, WAP and GPRS gateways may be accessed without the owner's knowledge or consent.

To restrict this threat:A backdoor attack works only if the BD_ADDR of the target device is known. Moreover, the target device has to be vulnerable to a backdoor attack.

VI. COUNTER MEASURES

Table 1 : Problems with Native Bluetooth Security

Security Issue or Vulnerability		Remarks/Description
Versions Before Bluetooth v1.2		
1	Link keys based on unit keys are static and reused for every pairing.	A device that uses unit keys will use the same link key for every device with which it pairs. This is a serious cryptographic key management vulnerability.
2	Use of link keys based on unit keys can lead to eavesdropping and spoofing.	Once a device's unit key is divulged (i.e., upon its first pairing), any other device that has the key can spoof that device or any other device with which it has paired. Further, it can eavesdrop on that device's connections whether they are encrypted or not.
Versions Before Bluetooth v2.1		
3	Security Mode 1 devices never initiate security mechanisms.	Devices that use Security Mode 1 are inherently insecure. For v2.0 and earlier devices, Security Mode 3 (link level security) is highly recommended.
4	PINs can be too short.	Weak PINs, which are used to protect the generation of link keys during pairing, can be easily guessed. People have a tendency to select short PINs.
5	PIN management and randomness is lacking.	Establishing use of adequate PINs in an enterprise setting with many users may be difficult. Scalability problems frequently yield security problems. The best alternative is for one of the devices being paired to generate the PIN using its random number generator.
6	The encryption keystream repeats after 23.3 hours of use.	The encryption keystream is dependent on the link key, EN_RAND, Master BD_ADDR, and Clock. Only the Master's clock will change during a particular encrypted connection. If a connection lasts more than 23.3 hours, the clock value will begin to repeat, hence generating an identical keystream to that used earlier in the connection. Repeating a keystream is a serious cryptographic vulnerability that would allow an attacker to determine the original plaintext.

Bluetooth v2.1 and v3.0		
7	Just Works association model does not provide MITM protection during pairing, which results in an unauthenticated link key.	For highest security, devices should require MITM protection during SSP and refuse to accept unauthenticated link keys generated using Just Works pairing.
8	SSP ECDH key pairs may be static or otherwise weakly generated.	Weak ECDH key pairs minimize SSP eavesdropping protection, which may allow attackers to determine secret link keys. All devices should have unique, strongly-generated ECDH key pairs that change regularly.
9	Static SSP passkeys facilitate MITM attacks.	Passkeys provide MITM protection during SSP. Devices should use random, unique passkeys for each pairing attempt.
10	Security Mode 4 devices (i.e., v2.1 or later) are allowed to fall back to any other security mode when connecting with devices that do not support Security Mode 4 (i.e., v2.0 and earlier).	The worst-case scenario would be a device falling back to Security Mode 1, which provides no security. NIST strongly recommends that a Security Mode 4 device fall back to Security Mode 3 in this scenario.
Versions Before Bluetooth v4.0		
11	Attempts for authentication are repeatable.	A mechanism needs to be included in Bluetooth devices to prevent unlimited authentication requests. The Bluetooth specification requires an exponentially increasing waiting interval between successive authentication attempts. However, it does not require such a waiting interval for authentication challenge requests, so an attacker could collect large numbers of challenge responses (which are encrypted with the secret link key) that could leak information about the secret link key
12	The master key used for broadcast encryption is shared among all piconet devices.	Secret keys shared amongst more than two parties facilitate impersonation attacks.
13	The E0 stream cipher algorithm used for Bluetooth BR/EDR encryption is relatively weak.	FIPS-approved encryption can be achieved by layering application-level FIPS-approved encryption over the Bluetooth BR/EDR encryption. Note that Bluetooth LE uses AES-CCM.
14	Privacy may be compromised if the Bluetooth device address (BD_ADDR) is captured and associated with a particular user.	Once the BD_ADDR is associated with a particular user, that user's activities and location could be tracked.
15	Device authentication is simple shared-key challenge/response.	One-way-only challenge/response authentication is subject to MITM attacks. Bluetooth provides for mutual authentication, which should be used to provide verification that devices are legitimate.
Bluetooth v4.0		
16	LE pairing provides no eavesdropping protection. Further, the Just Works pairing method provides no MITM protection.	If successful, eavesdroppers can capture secret keys (i.e., LTK, CSRK, IRK) distributed during LE pairing. Further, MITM attackers can capture and manipulate data transmitted between trusted devices. LE devices should be paired in a secure environment to minimize the risk of eavesdropping and MITM attacks. Just Works pairing should not be used.
17	LE Security Mode 1 Level 1 does not require any security mechanisms (i.e., no authentication or encryption).	Similar to BR/EDR Security Mode 1, this is inherently insecure. LE Security Mode 1 Level 3 (authenticated pairing and encryption) is highly recommended instead.
All Versions		
18	Link keys can be stored improperly.	Link keys can be read or modified by an attacker if they are not securely stored and protected via access controls.
19	Strengths of the pseudo-random number generators (PRNG) are not known.	The Random Number Generator (RNG) may produce static or periodic numbers that may reduce the effectiveness of the security mechanisms. Bluetooth implementations should use strong PRNGs based on NIST standards.
20	Encryption key length is negotiable.	The v3.0 and earlier specifications allow devices to negotiate encryption keys as small as one byte. Bluetooth LE requires a minimum key size of seven bytes. NIST strongly recommends using the full 128- bit key strength for both BR/EDR (E0) and LE (AES- CCM).
21	No user authentication exists.	Only device authentication is provided by the specification. Application-level security, including user authentication, can be added via overlay by the application developer.
22	End-to-end security is not performed.	Only individual links are encrypted and authenticated. Data is decrypted at intermediate points. End-to-end security on top of the Bluetooth stack can be provided by use of additional security controls.
23	Security services are limited.	Audit, non-repudiation, and other services are not part of the standard. If needed, these services can be incorporated in an overlay fashion by the application developer.
24	Discoverable and/or connectable devices are prone to attack.	Any device that must go into discoverable or connectable mode to pair or connect should only do so for a minimal amount of time. A device should not be in discoverable or connectable mode all the time.

VII. BLUETOOTH SECURITY RECOMMENDATIONS & PRECAUTIONS

Both users and Bluetooth application developers have responsibilities and opportunities to minimize the risk of compromise via Bluetooth. **Users should follow these best practice security guidelines:**

1. Never use standard commercial Bluetooth headsets.
2. Enable Bluetooth functionality only when necessary.
3. Require and use only devices with low-power Class 2 or 3 Bluetooth transceivers.
4. Keep devices as close together as possible when Bluetooth links are active.
5. Independently monitor devices and links for unauthorized Bluetooth activity.
6. Make devices discoverable (visible to other Bluetooth devices) only if/when absolutely necessary.
7. Make devices connectable (capable of accepting and completing incoming connection requests) only if/when absolutely necessary and only until the required connection is established.
8. Pair Bluetooth devices in a secure area using long, randomly generated passkeys. Never enter passkeys when unexpectedly prompted for them.
9. Maintain physical control of devices at all times. Remove lost or stolen devices from paired device lists.
10. Use device firewalls, regularly patch Bluetooth devices, and keep device anti-virus software up to date.
11. Comply with all applicable directives, policies, regulations, and guidance.
12. Subject Bluetooth solutions and deployments to independent security audits by qualified evaluators.

VIII. SECURITY TIPS

- Enable Bluetooth only when you need it.
- Keep the device in non-discoverable (hidden) mode.
- Use long and difficult to guess PIN key when pairing the device.
- Reject all unexpected pairing requests.
- Update your mobile phone firmware to a latest version.
- Enable encryption when establishing BT connection to your PC.
- Update your mobile antivirus time to time to keep pace with the new emerging viruses and Trojans.[3]

IX. CONCLUSIONS

This paper proposes enhancements to the existing security model in order to decrease the vulnerabilities of the Bluetooth technology. The risks of Bluetooth vulnerabilities are largely accepted by today's users in order to preserve its current ease of use; additional security typically means additional complexity. However, these vulnerabilities can be addressed with minimal impact to the user's current Bluetooth experience. These enhancements include increased security during the pairing/discovery process, mandatory encrypted transmission, manufactured passkeys, standard practices, and application layer authentication. Implementing a Discoverable-by-Known-Devices Mode, via a White List, would arguably deter predators from random attacks to Bluetooth devices. This can be accomplished by limiting the use and exposure of devices by reducing the time spent in Discovery Mode. By trading a Bluetooth token in a text message between devices, the need for a device to enter Discovery mode could be eliminated altogether; however trading Bluetooth tokens via text message is not without its own limitations. There are security implications, and unfortunately, text messaging interfaces are typically only available to mobile phones and Personal Digital Assistants, leaving other Bluetooth enabled devices unable to implement this approach.

Finally, we feel that the benefits provided by Bluetooth must be weighed against the security vulnerabilities when pairing two smart devices together. Its primary functionality is also the source of its troubles. Implementing enhanced

security measures, such as those which have been proposed in this paper, would reduce the risks of the current model. Technological improvements leading to lower power consumption and higher connection speeds should allow enhanced security implementations without degrading the current level of performance. In turn, Bluetooth technology's adoption would increase by businesses, universities, and other organizations with particular concerns about security.

REFERENCES

1. Nateq Be-Nazir Ibn Minar, Mohammed Tarique, "Bluetooth Security Threats and Solutions: A Survey" International Journal of Distributed and Parallel Systems, volume 3, No. 1, January 2012
2. Christian Gehrmann, Bluetooth™ Security White Paper, Bluetooth SIG Security Expert Group.
3. " The Blue Bug ", a Bluetooth virus, available at: http://trifinite.org/trifinite_stuff_bluebug.html
4. "A Review of Bluetooth Attacks and How to Secure Mobile Workforce Devices"
5. "Bluetooth Connectivity Threatens Your Security" available at: http:// blog.kaspersky.com/bluetooth security/
6. Robayet Nasim ,"SECURITY THREATS ANALYSIS IN BLUETOOTH-ENABLED MOBILE DEVICES" International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.3, May 2012
7. Guide to Bluetooth Security, US National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/ 800-121/SP800-121.pdf.
8. Antnan, Bluetooth Security, Communication Security Department, Ruhr University, Bochum.