IJCSC International Journal of Computer Science and Communication Vol. 2, No. 1, January-June 2011, pp. 211-213

BLUETOOTH QUALITY ISSUES, THREATS AND SECURITY TIPS

PAWAN KUMAR

Lord Krishna Institute, Karontha, Rohtak *E-mail: pawanpruthi@rediffmail.com*

ABSTRACT

The Bluetooth, LAN's and IrDA technology is a boon of the present era. It's a part of wireless communication as well as mobile communication. Bluetooth use low power and generally do not require a license for spectrum use LAN is a technology for data transfer providing data rates up to 54 Mb/s. Infrared data association (IrDA) is a non profit organization whose goal is a develop specifications for infrared wireless communication and is cheap and reliable for short range wireless communication.

This paper is an attempt to study various technical aspects of Bluetooth its Quality/Security issues, threats and consequences.

1. INTRODUCTION

Bluetooth is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers (desktop and laptop), cameras, printers, coffee makers, and so on. A Bluetooth LAN is an ad hoc network, which means that the network called piconet. A Bluetooth LAN can even be connected to the Internet if one of the gadgets be large. If there are many gadgets that try to connect, there is chaos. Bluetooth technology has several applications. Peripheral devices of a computer can communicate with the computer through this technology (wireless mouse of keypad).

Monitoring devices can communicate with sensor devices in a small health care centre. Home security devices can use this technology to connect different sensors to the main security controller. Conference attendees can synchronize their palmtop computers at a conference.

1.1 Security Features in Bluetooth

Security beings when a user decides how a Bluetooth device will implement its connectability and discoverability options. The different combinations of connectability and discoverability capabilities can be divided into three security levels.

Silent: The device will never accept any connections. It simply monitors Bluetooth traffic.

Private: The device cannot be discovered. Connections will be accepted only if the devices Bluetooth address is known to prospective master.

Public: The device can be both discovered and connected. Security within Bluetooth has three major areas namely: authentication, authorization and encryption. Authentication is used for proving the identity of one piconet member to another. The results of authentication are used for determining the client's authorization level. Encryption is used for encoding the information being exchanged between Bluetooth devices. Usually a PIN is provided for providing trust between two devices.

An initialization key is generated when Bluetooth devices meet for the first time and is used for securing the generation of other more secure 256-bit keys which are generated during nest phases of the security chain of events. We can also add unique word in the initialization phase for unique identity of the devices. An initialization key is derived byte PIN code and a Bluetooth devices address. A combination key is always dependent on two devices and therefore derived for challenge response authentication in which a claimant's knowledge of a secret link key is checked. During each authentication a new 128 bit unencrypted random number is exchanged. The claimant returns a 32-bit result (SRES, signed response) to the verifier. The verifier also calculates the same SRES value and compares it to the received SRES. If the SRES value match, the authentication is completed successfully. The SRES value can be continuously varied in case information is more critical for providing higher level of security. Usually this type of variation demands extra bandwidth and adds time delays on the cost of high level of security. Bluetooth security can be enhanced by using some standard third party certificate based encryption methods at software level as extra security in addition to Bluetooth built in security. Devices may use digital signatures to add extra level of authorization security.

Quality of services (QoS) is an internetworking issue that has been discussed more than defined. We can informally define of service as some thing a flow seeks to attain.

1.2 Flow Characteristics

Traditionally, four types of characteristics are attributed to a flow: reliability, delay, jitter, and bandwidth, as shown in Fig. 1.

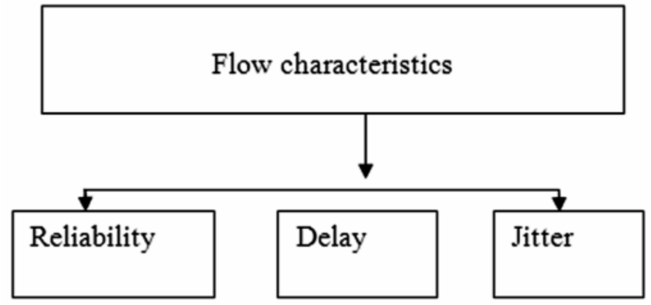

Fig. 1: Flow Characteristics

2. RELIABILITY

Reliability is a characteristic that a flow needs. Lack if reliability means losing a packet or acknowledgement, which entails retransmission. However, the sensitivity of application program to reliability is not the same. For example, it is more important that electronic mail, file transfer, and Internet access have reliable transmission than telephony or audio conferencing.

3. DELAY

Source - to destination delay is another flow characteristic. Again application can tolerate delay in different conferencing, and remote log-in need minimum delay, while delay in file transfer or email is less important.

4. JITTER

Jitter is the variation in delay for packers belonging to the same flow. Real time audio and video cannot tolerate high jitter. For example, a real- time video broadcast is useless is there is a 2-ms delay for the first and second packets and a 60-ms delay for the third and fourth. On the other hand, it does not matter if packets carrying information in a file have different delays. The transport layer at the destination waits until all packets arrive before delivery to the application layer.

5. IMPROVEMENT IN QOS WITH THE HELP OF JINI

Jini is a Java technology centered distributed system conceptualizing the unification of user groups of services required by them. Jini architecture attempts to represent the dynamic nature of user groups and their computational needs. Its overall goal is to realize a flexible, easily administrable network on which user can dynamically discover resources. Resources may be software programs, hardware devices or both. The major goals of Jini are:

- Enabling users to share services over the network.
- Providing users easy access to resources anywhere on the network while allowing the network location of the user to change.
- Simplifying the task of building, maintaining and altering a network of devices, software and users.

6. COMBINATION OF BLUETOOTH AND JINI FOR IMPROVEMENT IN QOS

With Jini discovery-join-lookup protocol and leasing transportation mechanism, Service discovery protocol (SDP) of bluetooth can be used to send notification of the occurrence of an event and the information that must be contained in such a specification. It also allows various degrees of assurance on delivery of notification, suppose for different policies of scheduling notification and explicitly allows the interposition of objects that will collect, hold, filter and forward notifications. Therefore, with Jini, SDP can provide an event notification when services or information about services become unavailable. However, with Jini, SDP can provide an event notification when attribute of services is modified.

7. BLUETOOTH THREATS

(*a*) Bluesnarfing is a method of hacking into a Bluetooth-enabled mobile phone and copying its entire contact book, calendar or anything else stored in the phone's memory. By setting the device in non-discoverable, it becomes significantly more difficult to find and attack the device. However, the software tools required to steal information from Bluetooth-enabled mobile phones are widely available on the Web, and knowledge of how to use them is growing. (Kotadia, 2004) Companies such as Nokia and Sony Ericsson are making sure new phones coming to market will not be susceptible to Bluesnarfing.

(*b*) Man in the Middle Attacks In a man in the middle attack, an attacker seeking (unauthorized) access to a Bluetooth device inset himself "in between" two authorized devices communications between the two devices then pass through the man in the middle, who intercepts and manipulates data packets.

(*c*) First Bluetooth virus, Series 60 affected Jun 15 2004. Symantec warns for Series 60 mobile phones that transmits itself through Bluetooth. It's just a proof-of-concept (doesn't do any damage), but it's a scary concept. The worm spreads as a SIS file, which is automatically installed into the "APPS" directory when the receiver accepts the transmission. Upon execution, it will display a message then copy itself to a directory that is not visible by default. The worm runs from this directory whenever the phone is rebooted, so it continues to work even if the files are deleted from the APPS directory.

(*d*) Cabir virus: is the first verified example. The virus was created by a group from the Czech Republic and Slovakia called 29a, who sent it to a number of security software companies, including Symantec in the United States and Kapersky Lab in Russia. Cabir is considered a "proof of concepts" virus, become it proves that a virus can be written for mobile phones, something that was once doubted. Cabir was developed for mobile phones running the Symbian and Series 60 software, and using Bluetooth. The virus searches within Bluetooth's range (about 30 meters) for mobile phones running in discoverable mode and sends itself, disguised as a security file, to any vulnerable devices. The virus only becomes active if the recipient accepts the file and then installs it. Once installed, the virus displays the file word "Caribe" on the device's display. Each time an infected phone is turned on, the virus launches itself and scans the area for other devices to send itself to. The scanning process is likely to drain the phone's batteries. Cabir can be thought of as a hybrid virus / worm: its mode of distribution qualifies it is a network worm, but it requires user interaction like a traditional virus.

(*e*) Symantec warns of three new Symbian Trojans Jan 20 2006. Symantec has issued an alert over three new trojan horse applications for Symbian powered phones. These will affect Nokia's S60 line of Smartphones. The Trojans are being called:

SymbOS. Bootton.E, SymbOS. Pbstealer.D and SymbOS. Sendtool A. To be affected you will have to install an application, so use general precautions before installing software on your phone (e.g. know who it's from). Filenames to watch out for include: Fspreader. SIS, Chatting Yuk. SIS, PB Compressory. SIS and Restart. S60. SIS.

(*f*) Bluebugging: It involves accessing the phone's commands so that the hacker can actually make phone calls, add or delete contact info, or eavesdrop on the phone owner's conversations. This vulnerability too, is being addressed by phone manufactures. Thus if you own a BT-enabled phone, it's important to keep the software updated or upgrade to the latest phone models frequently.

(*g*) Bluetooth devices can also be targets of Denial of Service (DoS) attacks typically by bombarding the device with requests to the point that it causes the battery to degrade.

(*h*) Mabir A.: Uses both Bluetooth and MMS to replicate which is quite an improvement. The worm also sends an MMS in a reply to any received SMS, which is clever technique to fool the user into installing the received application.

(*i*) "Backdoor" hacking. This is where a device which is no longer trusted can still gain access to the mobile phone and gain access to data as with Bluesnarfing, or also use service like WAP etc.

8. SECURITY POINTS

- 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 (key such as 12 is unacceptable).
- 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 Trojans.

9. CONCULUSION

This paper was intended as a brief introduction to the many challenges that the Bluetooth technology has to face while used for building Adhoc networks. We have described many of the issues that need to be tackled and that have been left unspecified in the current standards. We identified a number of objectives that any solution should aim at meeting, and provided an initial investigation of some of these problems.

REFERENCES

[1] Bluetooth Specifications 1.0, 1.1, 1.2 and Technical Specifications on www.bluetooth.org.

[2] Wireless Communications and Networks. By Stallings, Pearson Publication.

[3] Roch Guerin, Enyoung Kim and Saswati Sarkar, Bluetooth Technology: Key Challenges.

[4] Data Communications and Networks by Stallings, Pearson Publication.

[5] Dr Vikram Singh, Pawan Kumar, and Subham Gandhi, Quality Security Issues in Bluetooth, LAN's and IrDA.

[6] Nathan J Muller, Bluetooth Demystified, TMH Publication.

[7] Keijo M.J., Evaluation of the Current State of Bluetooth Security.

[8] www.google.com.

Security mode 3 has device level security, and security is also enforced on every low level connection. In addition, Bluetooth is based on two main architectures in its protocol stack: HCI [3] and LZCAP [4]. HCI stands for Host Controller Interface and provides a command interface to the baseband controller and link manager, and also access to configuration parameters.Â 2. BACKGROUND Bluetooth technology has been accepted by many instead of having problems regarding security issues. Different types of vulnerabilities have been discovered since 2001 onwards [5-10]. Some researchers from Bell labs discovered some problems in Bluetooth pairing protocol in 2001.