INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

GENERAL APPROACH FOR BLUETOOTH NETWORK SECURITY SYSTEM

[1]Shivappa M Metagar, [2]Dattatraya T Huvinahalli, [3]Theja N, [4]B.P.Savukar
[1&2] Assistant Prof, Department of CSE, SVERI's COE Pandharpur
[4]Prof. B L D Engg College Bijapur
[3] Raju Gandhi Institute of Technology Bangalore
[1]shivametagar@gmail.com [2]savukarbp@yahoo.co.in [3]thejan.hdk@gmail.com [4]datta111@yahoo.co.in

Abstract

Bluetooth provides a short range wireless communication between devices making it convenient for users and thus eliminating the need for messy cables. According to Bluetooth Special Interest Group Bluetooth wireless technology is the most widely supported, versatile, and secure wireless standard on the market today. Bluetooth operates in the open 2.4 GHz ISM band and is now found in a vast array of products such as input devices, printers, medical devices, VoIP phones, whiteboards, and surveillance cameras. However the proliferation of these devices in the workplace exposes organizations to security risks. Detecting Bluetooth Security Vulnerabilities, This paper will explain what Bluetooth is, how it works, and some of the vulnerabilities and risks associated with it. In the past, the only way to connect computers together for the purpose of sharing information and/or resources was to connect them via cables. This can be not only cumbersome to set up, but it can get messy real quick. Bluetooth provides a solution to this problem by providing a cable-free environment. The key features of Bluetooth technology are robustness, low power, and low cost. The Bluetooth specification defines a uniform structure for a wide range of devices to connect and communicate with each other.

Keywords: Bluetooth device; source device; destination device; user; connecting media; mobile phones; wireless media etc

I. INTRODUCTION

About Bluetooth

Bluetooth has emerged as a very popular ad hoc network standard today[1] The Bluetooth standard is a computing and telecommunications industry specification that describes how mobile phones, computers, and PDAs should interconnect with each other, with home and business phones, and with computers

using short-range wireless connections. Bluetooth network applications include wireless synchronization e-mail/Internet/intranet access using local personal computer connections,

hidden computing through automated applications and networking, and applications that can be used for such devices as hands-free headsets and car kits. The Bluetooth standard specifies wireless operation in the 2.45 GHz radio band and supports data rates up to 720 kbps.5 It further supports up to three simultaneous voice channels and employs frequency-hopping schemes and power reduction to reduce interference with other devices operating in the same frequency band. The IEEE 802.15 organization has derived a wireless personal area networking technology based on Bluetooth specifications v1.1.

How Bluetooth Works

Bluetooth can[2] be used to connect almost any device to another device. Bluetooth can be used to form ad hoc networks of several (up to eight) devices, called piconets Vainio, When Bluetooth devices first connect, there is a piconet master that initiates the connection, and the others are slave devices[5] .One piconet can have a maximum of seven active slave devices and one master device. All communication within a piconet goes through the piconet master. Two or more piconets together form a scatternet, which can be used to eliminate Bluetooth range restrictions. Haataja[6] It is not possible to be a master of two different piconets because a piconet is a group of devices all synchronized on a hopping sequence set by the master. For that reason, any devices that share a master must be on the same piconet .

Bluetooth Security

Security has played a major role in the invention of Bluetooth. The Bluetooth [3][7]SIG has put much effort into making Bluetooth a secure technology and has security experts who provide critical security information. In general, Bluetooth security is divided into three modes: (**1**) non-secure; (**2**) service level enforced security; and (**3**) link level enforced security. In non-secure, a Bluetooth device does not initiate any security measures.[11] In service-level enforced security mode, .two Bluetooth [8] devices can establish a non secure Asynchronous Connection-Less (ACL) link. Security procedures, namely authentication, authorization and optional encryption, are initiated when a L2CAP (Logical Link Control and Adaptation Protocol) Connection-Oriented or Connection-Less channel request is made. Haataja The difference between service level enforced security and link level enforced security is that in the latter, the Bluetooth device initiates security procedures before the channel is established. As mentioned above, Bluetooth's security procedures include authorization, authentication and optional encryption. Authentication involves proving the identity of a computer or computer user, or in Bluetooth's case, proving the identity of one piconet member to another. Authorization is the process of granting or denying access to a network resource. Encryption is the translation of data into secret code. It is used between Bluetooth devices so that eavesdroppers cannot read its contents. However, even with all of these defence mechanisms in place, Bluetooth has shown to have some security risks.

II RELATED WORK

Wireless Networks

Wireless networks serve as the transport mechanism between devices and among devices and the traditional wired networks (enterprise networks and the Internet). Wireless networks are many and diverse but are frequently categorized into three groups based on their coverage range: [14][15]Wireless Wide Area Networks (WWAN), WLANs, and Wireless Personal Area Networks (WPAN). Frequency is increased beyond the RF spectrum, EM energy moves into the IR and then the visible spectrum.

Ad Hoc Networks

Ad hoc networks such as Bluetooth are networks designed to dynamically connect remote devices such as cell phones, laptops, and PDAs. These networks are termed “ad hoc” because of their shifting network topologies. Whereas WLANs use a fixed network infrastructure, ad hoc networks maintain random network configurations, relying on a master-slave system connected by wireless links to enable devices to communicate. In a Bluetooth network, the master of the piconet controls the changing network topologies of these networks. It also controls the flow of data between devices that are capable of supporting direct links to each other. As devices move about in an unpredictable fashion, these networks must be reconfigured on the fly to handle the dynamic topology. The routing that protocol Bluetooth employs allows the master to establish and maintain these shifting networks.

Figure 1 illustrates an example of a Bluetooth-enabled mobile phone connecting to a mobile phone network, synchronizing with a PDA address book, and downloading e-mail on an IEEE 802.11 WLAN.

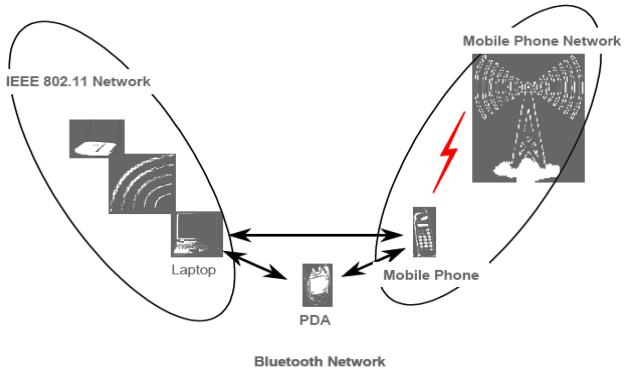

Fig 1. Notional Ad Hoc Network

Wireless Devices

A wide range of devices use wireless technologies, with handheld devices being the most prevalent form today. This document discusses the most commonly used wireless handheld devices such as text messaging devices, PDAs, and smart phones.

Personal Digital Assistants

PDAs are data organizers that are small enough to fit into a shirt pocket or a purse. PDAs offer applications such as office productivity, database applications, address books, schedulers, and to-do lists, and they allow users to synchronize data between two PDAs and between a PDA and a personal computer. Newer versions allow users to download their e-mail and to connect to the Internet. Security administrators may also encounter one-way and two-way text-messaging devices. These devices operate on a proprietary networking standard that disseminates e-mail to remote devices by accessing the corporate network.

III PROBLEM STATEMENT

Wireless Security Threats and Risk Mitigation The Introduction to Computer Security [9][11] generically classifies security threats in nine categories ranging from errors and omissions to threats to personal privacy. Authorized and unauthorized users of the system may commit fraud and theft; however, authorized users are more likely to carry out such acts. Since users of a system may know what resources a system has and the system’s security flaws, it is easier for them to commit fraud and theft. Malicious hackers, sometimes called crackers, are individuals who break into a system without authorization, usually for personal gain or to do harm. Malicious hackers are generally individuals from outside of an agency or organization (although users within an agency or organization can be a threat as well). Such[10] hackers may gain access to the wireless network access point by eavesdropping on wireless

device communications. Malicious code involves viruses, worms, Trojan horses, logic bombs, or other unwanted software that is designed to damage files or bring down a system. Many of the services offered over Bluetooth can expose private data or allow the connecting party to control the Bluetooth device. For security reasons it is necessary to be able to recognize specific devices and thus enable control over which devices are allowed to connect to a given Bluetooth device. At the same time, it is useful for Bluetooth devices to be able to establish a connection without user intervention (for example, as soon as they are in range). To resolve this conflict, Bluetooth uses a process called *bonding*, and a bond is created through a process called *pairing*. The pairing process is triggered either by a specific request from a user to create a bond (for example, the user explicitly requests to "Add a Bluetooth device"), or it is triggered automatically when connecting to a service where (for the first time) the identity of a device is required for security purposes. These two cases are referred to as dedicated bonding and general bonding respectively. Pairing often involves some level of user interaction; this user interaction is the basis for confirming the identity of the devices. Once pairing successfully completes, a bond will have been formed between the two devices, enabling those two devices to connect to each other in the future without requiring the pairing process in order to confirm the identity of the devices. When desired, the bonding relationship can later be removed by the user.

IV PURPOSE AND SCOPE OF THE PAPER

The purpose of this document is to provide agencies with guidance for establishing secure wireless networks[12]. Agencies are encouraged to tailor the recommended guidelines and solutions to meet their specific security or business requirements. Wireless technologies are changing rapidly. New products and features are being introduced continuously. Many of these products now offer security features designed to resolve long-standing weaknesses or address newly discovered ones. Yet with each new capability, a new threat or vulnerability is likely to arise. Wireless technologies are evolving swiftly. Therefore, it is essential to remain abreast of the current and emerging trends in the technologies and in the security or insecurities of these technologies. Again, this guideline does not cover security of other types of wireless or emerging wireless technologies such as third-generation (3G) wireless telephony.

This document covers details specific to wireless technologies and solutions.

The key-scheduling algorithm (KSA)

The key-scheduling algorithm is used to initialize the permutation in the array "S". "keylength" is defined as the number of bytes in the key and can be in the range $1 \leq \text{keylength} \leq 256$, typically between 5 and 16, corresponding to a key length of 40 – 128 bits. First, the array "S" is initialized to the identity permutation. S is then processed for 256 iterations in a similar way to the main PRGA algorithm, but also mixes in bytes of the key at the same time.

```
for i from 0 to 255
   S[i] := i
endfor
j := 0
for i from 0 to 255
   j := (j + S[i] + key[i mod keylength]) mod 256
   swap(S[i],S[j])
endfor
```

Combination keys are the safer method of authenticating a device because these keys are

only used between a pair of devices. This means that each connection using combination keys in a Bluetooth network has a distinct link key.

On the other hand, unit keys are simpler to maintain, but offer less security. Unit keys are link keys that are used by a device for each connection it makes. However, in order to add some small sense of security, only one device in a pair is allowed to use a unit key.

The other device must use a combination key. Unit keys are typically used by devices which are unable to maintain large amounts of unique key pairs. Because unit keys are shared by all devices connected to the unit key device, it is possible for other devices in the network to eavesdrop on traffic intended for the unit key device. This could allow an attacker to gain privileged information or impersonate a device. This also means that unit keys offer no protection from other pair devices. In fact, the Bluetooth SIG has released an official recommendation that unit keys be used as little as possible. Sometimes, the device classified as the "master" device wants to transmit data to more than one recipient. To do this, something called a master key is created which temporarily replaces the link key. The master key informs the receivers that the data being transmitted to them is being sent to multiple devices as well as stating who the information is from.

Range

The reliable coverage range for 802.11 WLANs depends on several factors,[21] including data rate required and capacity, sources of RF interference, physical area and characteristics, power, connectivity, and antenna usage. Theoretical ranges are from 29 meters (for 11 Mbps) in a closed office area to 485 meters (for 1 Mbps) in an open area. However, through empirical analysis, the typical range for connectivity of 802.11 equipment is approximately 50 meters (about 163 ft.) indoors. A range of 400 meters, nearly ¼ mile, makes WLAN the ideal technology for many campus applications. It is important to recognize that special high-gain antennas can increase the range to several miles.

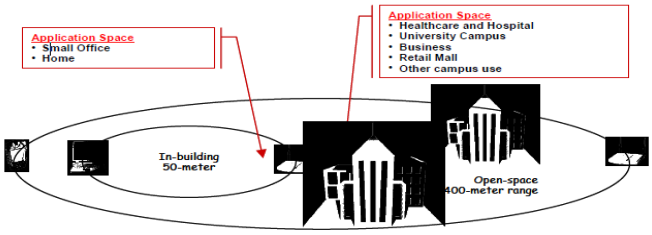

Fig: 2 Typical Range of 802.11 WLAN

AP's may also provide a "bridging" function. Bridging connects two or more networks together and allows them to communicate[22] to exchange network traffic. Bridging involves either a point-to-point or a multipoint configuration. In a point-to-point architecture, two LANs are connected to each other via the LANs' respective APs. In multipoint bridging, one subnet on a LAN is connected to several other subnets on another LAN via each subnet AP. For example, if a computer on Subnet A needed to connect to computers on Subnets B, C, and D, Subnet A's AP would connect to B's, C's, and D's respective APs. Enterprises may use bridging to connect LANs between different buildings on corporate campuses. Bridging AP devices are typically placed on top of buildings to achieve greater antenna reception. The typical distance over which one AP can be connected wirelessly to another by means of bridging is approximately 2 miles. This distance may vary depending on several factors including the specific receiver or transceiver being used.*13* Fig 2 illustrates point-to-point bridging between two LANs. In the example, wireless data is being transmitted from Laptop A to Laptop B, from one building to the next, using each building's appropriately positioned AP. Laptop A connects to the closest AP within the

building A. The receiving AP in building A then transmits the data (over the wired LAN) to the AP bridge located on the building's roof. That AP bridge then transmits the data to the bridge on nearby building B. The building's AP bridge then sends the data over its wired LAN to Laptop B.

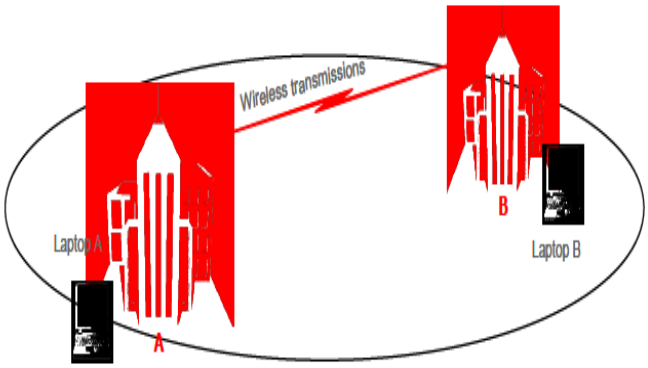

Fig:3 Access Point Bridging

V BENEFITS WLANs offer four primary benefits

User Mobility: Users can access files, network resources, and the Internet without having to physically connect to the network with wires. Users can be mobile yet retain high-speed, real-time access to the enterprise LAN.

Security Features of 802.11 Wireless LANs per the Standard The three basic security services defined by IEEE for the WLAN environment are as follows:

Authentication: A primary goal of WEP was to provide a security service to verify the identity of communicating client stations. This provides access control to the network by denying access to client stations that cannot authenticate properly. This service addresses the question, "Are only authorized persons allowed to gain access to my network?"

Confidentiality: Confidentiality, or privacy, was a second goal of WEP. It was developed to provide "privacy achieved by a wired network." The intent was to prevent information compromise from casual eavesdropping (passive attack). This service, in general, addresses the question, "Are only authorized persons allowed to view my data?"

Integrity: Another goal of WEP was a security service developed to ensure that messages are not modified in transit between the wireless clients and the access point in an active attack. It is important to note that the standard did not address other security services such as audit, authorization, and non repudiation. The security services offered by 802.11 are described in greater detail below.

VI More prevalent applications of Bluetooth include

- ☑ Wireless control of and communication between a mobile phone and a hands-free headset. This was one of the earliest applications to become popular.
- ☑ Wireless networking between PCs in a confined space and where little bandwidth is required.
- ☑ Wireless communications with PC input and output devices, the most common being the mouse, keyboard and printer.
- ☑ Transfer of files between devices with OBEX.
- ☑ Transfer of contact details, calendar appointments, and reminders between devices with OBEX.
- ☑ Replacement of traditional wired serial communications in test equipment, GPS receivers, medical equipment, bar code scanners, and traffic control devices.

- ☑ For controls where infrared was traditionally used.
- ☑ Sending small advertisements from Bluetooth enabled advertising hoardings to other, discoverable, Bluetooth devices.
- ☑ Two seventh-generation game consoles, Nintendo's and Sony's PlayStation 3 use Bluetooth for their respective wireless controllers.
- ☑ Dial-up internet access on personal computer or PDA using a data-capable mobile phone as a modem

VII CONCLUSION

Bluetooth wireless is constantly growing in popularity because of the convenience of exchanging information between mobile devices. As Bluetooth usage rises, so do the security risks associated with the technology. Advantages to Bluetooth include .the ability to simultaneously handle both data and voice transmissions which enables users to enjoy variety of innovation solutions such as a hands-free headset for voice calls, printing and fax capabilities, and synchronizing PDA, laptop, and mobile phone applications Bluetooth SIG Bluetooth users should familiarize themselves with Bluetooth security issues before using Bluetooth devices, and especially before they bring these devices. For now, Bluetooth offers convenience and access to a broader base of information, but one must remember that there are people out there with malicious intent, and they can violate Bluetooth security. As long as everyone is aware of this and does their best to maintain some security, then Bluetooth can act as a sufficient step towards a world of secure ad hoc networks.

REFERENCES

[1] Bluetooth Special Interest Group, “Specification of the Bluetooth System,” 5 November 2003

[2] Gehrmann, Christian *et al*, “Bluetooth Security White Paper,” Bluetooth SIG Security Expert Group, 19 February 2002

[3] Kardach, James, “Bluetooth Architecture Overview,” Intel Technology Journal, 2000

[4] Kurose, James F. and Keith W. Ross, “Computer Networking: A Top-Down Approach Featuring the Internet, 3rd ed. (Boston: Addison Wesley, 2005)

[5] Laurie, Adam and Ben Laurie, “Serious flaws in Bluetooth security lead disclosure of personal data,” TheBunker

[6] Newitz, Annalee, “They’ve Got Your Number…”Wired December 2004, 92.

[7] Vainio, Juha T. “Bluetooth Security,” Helsinki University of Technology, 25 May 2000

[8] Wikipedia.org, “Bluetooth,” Wikipedia.org, 5 March 2005,

[9] NIST Special Publication 46, Security for

[10] Norton, P., and Stockman, M. Peter Norton’s Network Security Fundamentals. 2000.

[11]Wack, J., Cutler, K., and Pole, J. NIST Special Publication 41, Guidelines on Firewalls and Firewall Policy, January 2002.

[12] Gast, M. 802.11 Wireless Networks: The Definitive Guide Creating and Administering Wireless Networks, O’Reilley Publishing, April 2002.

[13] Arbaugh, W.A., Shankar, N., and Wan, Y.C.“Your 802.11 Wireless Network Has No Clothes.”March 30, 2001.

[14] Basgall, M. “Experimental Break-Ins Reveal Vulnerability in Internet, Unix Computer Security.”

[15] Cam-Winget, N., and Walker, J.“An Analysis of AES in OCB Mode.” May 2001.

[16] Ismadi, A., and Sukaimi, Y.B. Smart Card: An Alternative to Password Authentication. SANS, May 26, 2001.

[17] Lucent Technologies. ORINOCO Manager Suite Users Guide. November 2000.

[18] Menezes, A. “Comparing the Security of ECC and RSA.” January 2000.

[19] Cagliostro, C. Security and Smart Cards. www.scia.org, 2001.

[20] Cardwell, A., and Woollard, S. "Clinic: What are the biggest security risks associated with wireless technology? What do I need to consider if my organization wants to introduce this kind of technology to my corporate LAN?" www.itsecurity.com, 2001.
[21] Ewalt, D. M. "RSA Patches Hold in Wireless LANs: The fix addresses problems with the Wireless Equivalent Privacy protocol, which encrypts communication over 802.11b wireless networks." Information December 2001.
[22] Leyden, J. "Tool Dumbs Down Wireless Hacking." The Register, www.theregister.co.uk, August 2001.
[23] S. Craver, N. Memon, B. L. Yeo, and M. M. Yeung, "On the invertibility of invisible Watermarking techniques," in Proc. IEEE Int.Conf. Image Processing (ICIP'97), vol. 1, Santa Barbara, CA, Oct. 1997, pp. 540–543.
[24] N. Nikolaidis and I. Pitas, "Copyright protection of images using robust digital signatures," in Proc. IEEE Int. Conf. Acoustics, Speech, Signal Processing (ICASSP '96), vol. 4, Atlanta, GA, May 1996, pp. 2168–2171.
[25] X.-G. Xia, C. G. Boncelet, and G. R. Arc, "A multiresolution watermark for digital images," in Proc. ICIP '97, vol. 1, Santa Barbara, CA,Oct. 1997, pp. 548– 551.
[26] A. Piva,M. Barni, F. Bartolini, and V. Capellini, "DCT based watermark recovering without resorting to the uncorrupted original image," in Proc. IEEE Int. Conf. Image Processing (ICIP'97), vol. 1, Santa Barbara, CA, Oct. 1997, pp. 520–523.
[27] J. O'Ruanaidh and T. Pun, "Rotation, scale and translation invariant digital image watermarking," in Proc. ICIP '97, vol. 1, Santa Barbara, CA, Oct. 1997, pp. 536–539.

BIBLIOGRAPHY

SHIVAPPA M METAGAR received B.E. degree (Computer Science & Engineering) in 2010 from KBNCE, Gulbarga and M.Tech (Digital Communication and Networking) in 2012 from BTLIT, Bangalore. He is presently Working as Assistant Professor in the department of CSE, SVERI College of Engineering Pandharpur, Maharastra. His research interests are in the area of Networks, Network Security, Data Mining, Web Technology and Image Processing.

DATTATRYA.T.HUVINAHALLI received B.E. degree (Computer Science & Engineering) in 2008 from GIT , Belgum and M.Tech(Pursuing) (Network Engineering) in 2012. He is presently Working as Assistant Professor in the department of CSE, SVERI College of Engineering Pandharpur, Maharastra. His research interests are in the area of Networks,Network Security, Data Mining, Web Technology, Artificial Intelligance and Image Processing.

THEJA N received B.E. degree (Computer Science & Engineering) in 2009 from Sri Jayachamarajendra College of Engineering, Mysore and M.Tech (Computer Science & Engineering) in 2012 from BTLIT, Bangalore. He is presently working as lecturer in the department of ISE, RGIT, Bangalore. His research interests are in the area of Networks, Network Security, Data Mining, Web Technology and Image Processing.

B.P.SAVUKAR received B.E. degree (Electronics &communication Engineering) in 2000 from BLDEAS, Bijapur and M.Tech (Computer Science & Engineering) at KBNCE Gulbarga. He is presently working as professor in department of ECE, BLDEAS Bijapur. His research interests are in the area of Networks, Network Security, Data Mining, Web Technology and Image Processing Microcontroller, Microprocessor etc .