Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Bluetooth: The Global Technology?

The purpose of the paper is to familiarize you with the Bluetooth specification, its capabilities, and associated security concerns with regards to implementation. The security features inherent to Bluetooth are adequate for ad hoc networks, and data transfer of non-sensitive information. Additionally, the 10 cm transmission range of Bluetooth devices operating with a maximum output power of 1 mW provides adequate security for money transfers, and transmission of sensitive data. Information integrity problems will prim...

Copyright SANS Institute
Author Retains Full Rights

AD

Bluetooth: The Global Technology?

Howard Johnson

Version 2.1

April 24, 2002

The purpose of the paper is to familiarize you with the Bluetooth specification, its capabilities, and associated security concerns with regards to implementation.

Introduction

As technology managers and technicians, we are constantly engaged in an ongoing struggle between functionality, usability, and security. To effectively balance our concerns, we must keep pace with changes in technology. The telecommunications and computing industries continue to create and market technologies designed to enhance mobility and functionality, both at home and at work. Any organization that desires to exploit opportunities must realize that greater mobility demands a global technology. Bluetooth provides mobility and will emerge as a scalable, economic global technology.

Why Bluetooth?

Bluetooth will become the short-range wireless technology of choice because it provides mobility, security and functionality in one small package. The small form factor of the Bluetooth radio also provides a unique balance of component cost, physical range, bandwidth, and power consumption. The Bluetooth specification is much more than just a cable replacement technology, because it is capable of wireless connections to a wide variety of portable electronic devices via one-to-one, and one-to-many device connections. Bluetooth enabled devices are also capable of simultaneous voice and data connections, as well as, ad hoc networking. All electronic devices that support Bluetooth, or the closely aligned IEEE (The Institute of Electrical and Electronics Engineers, Inc.) 802.15.1 standard for Wireless Personal Area Networks (PAN), will have a 1.5-inch transceiver chip that uses the globally available, unlicensed, Industrial, Scientific, and Medical (ISM) Band ranging from 2.4 GHz to 2.485 GHz (gigahertz). Future development of Bluetooth promises greater functionality and interoperability with other Bluetooth devices, as well as enhanced data transfer capabilities with IEEE 802.11 (Wireless Local Area Networks).

What is Bluetooth?

Bluetooth is an open-source standard that borrows many features from existing wireless standards such as IEEE 802.11, IrDA (Infrared Data Association), DECT (Digital Enhanced Cordless Telecommunications), Motorola's Piano, and TCP/IP to connect portable devices without wires via short-range radio frequencies (RF).

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

In doing so, Bluetooth inherits the following capabilities:

- Use of the ISM Band
- Frequency-hopping Spread Spectrum (FHSS)
- Authentication
- Privacy
- Power Management
- LAN Capabilities
- Object Exchange Capabilities
- Voice Data Transmission Capabilities
- Ad hoc Networking
- Circuit and Packet Switching

In order to accomplish this, developers purposely chose the free, worldwide available, ISM Band. Bluetooth utilizes an unlicensed portion of the RF spectrum beginning at 2.4GHz, therein providing a globally available communications channel free to all electronic devices, ranging from cellular phones to consumer electronics that support the Bluetooth specification. Bluetooth promises to allow both stationary and mobile electronic devices to communicate, with minimal user interaction, due to its "always on" state.

In order to seamlessly interconnect devices, each and every electronic device will require a Bluetooth chip. Try to imagine every electronic device you now posses enabled by Bluetooth Technology. Now imagine effortless connectivity between your computer, stereo, car, cell phone, and home environmental controls. The economics of producing a wireless technology that promotes, mobility, functionality, security, and interoperability is simply astounding. Bluetooth technology, and its potential, is virtually limitless. Bluetooth will commence a new era of human-machine interaction.

Background

In 1994, Ericsson, a Swedish Telecommunications Firm, began research on cable-less connections in order to integrate their cellular phones with Internet enabled devices via RF. Originally designed by two Ericsson Telephone employees, Sven Mattison (Swedish) and Jaap Haartsen (Dutch), their research produced a small, cheap radio chip that could be placed in almost any electronic device. Since its initial development, over 2,000 companies worldwide have signed on as members of the Bluetooth Special Interest Group (SIG). The SIG is an industry group that consists of leaders from the telecommunications and computing industries that are driving the development of the wireless specification. Furthermore, the SIG is also responsible for promoting the technology in the marketplace. The potential of Bluetooth technology has attracted unprecedented interest and financial investment by companies from the telecommunications, computing, networking, consumer, automotive, military, industrial, semiconductor and other industries.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

There are three categories of involvement with the Bluetooth SIG: Promoter, Associate, and Early Adoptor. The top-level group is the Promoter group. It consists of companies responsible for the developing and marketing the Bluetooth technology. Current members are:

Bluetooth Promoter Group

Founding Members	Additional Members
• Ericsson	• 3Com
• Nokia	• Lucent
• IBM	• Microsoft
• Intel	• Motorola
• Toshiba	

Membership within this group is exclusive and there are no plans to expand the membership.

At the mid-level is the Associate group. Associate members can be any company that has signed the Early Adoptor 1.1 contract and the Associate Member Amendment. There is a membership fee associated with this level based on the annual revenue of the applying company.

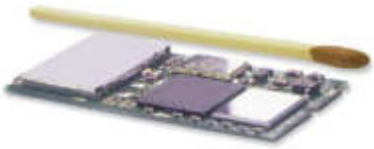
The bottom-level group is the Early Adoptor group. Early Adoptor members can be any company that has signed the Early Adoptor 1.0 contract. There is no fee for this level of membership. Additionally, there are also working groups, expert groups, and marketing subgroups.

In order to appreciate the financial commitment to the development and marketing of the Bluetooth standard, HomeRF (specification for wireless digital communications between PCs and consumer electronics), a competing wireless standard, currently has less than eighty member companies. No other wireless standard has the support and commitment given to Bluetooth. An up-to-date list of the Bluetooth SIG membership can be found at www.bluetooth.com/sig/memberlist/memberlist.asp.

Bluetooth Components

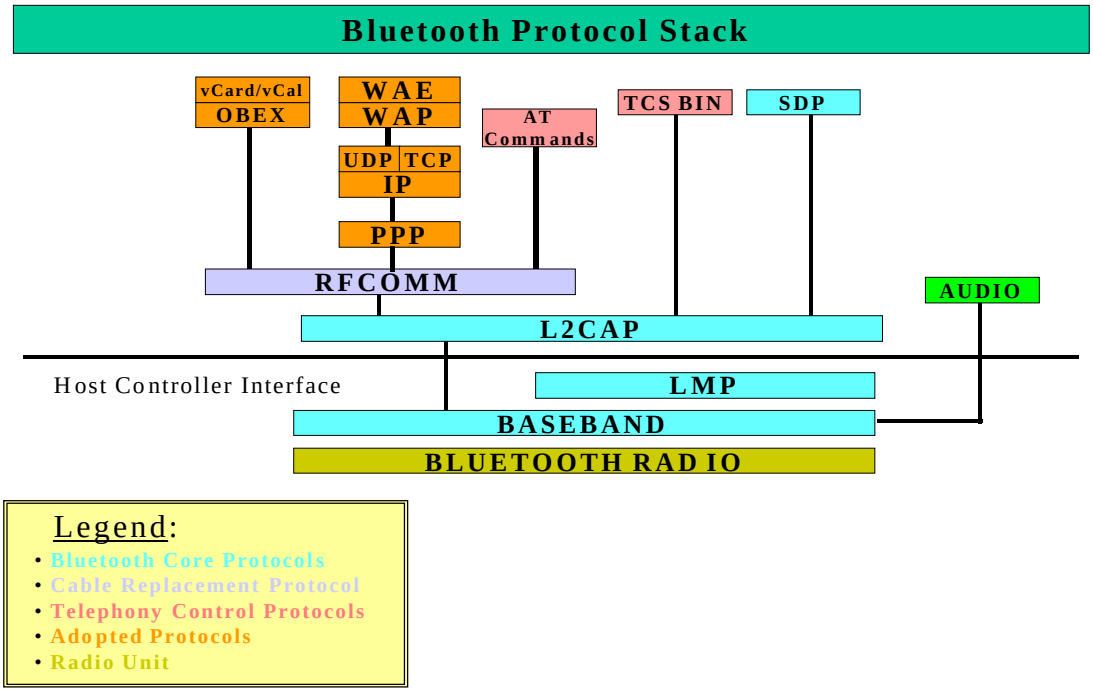
Any electronic device incorporating Bluetooth technology will consists of four major components:

- Radio Unit
- Baseband Unit
- Software Stack
- Application Software



Bluetooth Module

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.



Radio Unit

The radio unit is a transceiver that facilitates the wireless link between Bluetooth enabled devices operating in the ISM Band. Although the ISM Band does not require an operator's license from any regulatory agency, there are international regulations that limit power output. By limiting power output and using frequency-hopping spread-spectrum, Bluetooth is able to co-exist with other technologies that operate in the ISM Band like microwave ovens, Wireless LAN (IEEE 802.11a, b, and g), cordless phones, baby monitors, and HomeRF. Bluetooth is designed to operate in noisy RF environments. To accomplish this, Bluetooth radios use fast acknowledgement and frequency-hopping after each packet is transmitted and received to minimize interference from competing signals. The Federal Communications Commission (FCC) mandates that FHSS systems spend no more than 0.4 seconds on any single channel every 30 seconds in the 2.4 GHz ISM band. These same systems are also required to hop through at least 75 channels in order to reduce the likelihood of packet collisions. The Bluetooth SIG has taken the FCC mandate, along with the operation output power limit of 100mW, and pushed its standard to accommodate an US/European standard that hops through 79 channels displaced by 1MHz, with a maximum frequency-hopping rate of 1600 hops/s. In France and Spain however, regulations limit the number of hops to 23 channels, which limits the range of available frequencies. In order to limit the number of frequency hops available to the Bluetooth transceiver, an internal software switch is used. Bluetooth also supports three power classes that provide varying distances of link establishment. When the maximum output power of 100mw (milliwatts) is employed, Bluetooth enabled devices can communicate at ranges up to approximately 100 meters.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

The charts provided below show the interrelationships between the Bluetooth specification, transmitter characteristics, and ISM band usage.

Radio Bands and Channels

Country	Frequency Range	RF Channels
USA/Europe	2.4000 – 2.4835 GHz	79
Japan	2.4710 – 2.4970 GHz	23
Spain	2.4450 – 2.4750 GHz	23
France	2.4465 – 2.4853 GHz	23

Transmitter Characteristics

Power Class	Maximum Output Power	Distance
1	100 mW (20 dBm)	~ 100.0 m
2	2.5 mW (4 dBm)	~ 10.0 m
3	1 mW (0 dBm)	~ 0.1 m

Transceiver Specifications

- 1600 hops per second
- 79 (or 23) channels displaced by 1 MHz
- 220 micro-second Time Division Duplex (TDD) guard time
- Covers entire 2.4 GHz ISM Band
- Transmit power ranges from –30 to +20 dBm
- Modulation scheme – GFSK (Gaussian Frequency Shift Keying)
- Receiver sensitivity – -70 dBm
- Circuit and Packet Switching

Baseband Unit

The Baseband unit, also called the Link Control Unit, is the physical hardware that facilitates the RF link among Bluetooth devices. To better understand this, think of the Baseband Unit as a virtual serial cable physically connecting two devices. Once connected, there are two types of links associated with the Baseband packets: Synchronous Connection-Oriented (SCO) and Asynchronous Connectionless (ACL). An SCO link provides circuit-switched, point-to-point connections, usually for voice, data, and streaming content. SCO links are symmetrical. The maximum data rate for both sending and receiving is 433.9 Kbps. Conversely, an ACL link provides packet-switched, point-to-multipoint connections, usually for data. ACL links are asymmetrical. The maximum data rate for receiving is 723.2 Kbps, while sending is limited to 57.6 Kbps. Bluetooth enabled devices can support three types of connections:

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- One ACL Channel
- Three simultaneous SCO Channels
- One simultaneous ACL and SCO Channel

This virtual RS-232 cable consists of at least one antenna and one RF transceiver bundled with the low-level radio controller software. The Baseband module consists of flash memory and a central processing unit that is responsible for controlling timing, frequency hopping, data encryption, and error correction functions in conjunction with the Link Manager Protocol (LMP). LMP, one of the core Bluetooth protocols, is responsible for control and setup of data and audio links between Bluetooth devices. LMP is also responsible for the control and negotiation of the Baseband packet size. As depicted in the diagram, the Bluetooth Radio, the Baseband controller, and the Link Manager Protocol are normally referred to as the Bluetooth Hardware or the Host Controller Interface. The Host Controller Interface provides all required functionality for establishing and maintaining all communications links.

Now that you are familiar with the Bluetooth protocol and its technical specifications, let's explore some of the capabilities this technology will provide.

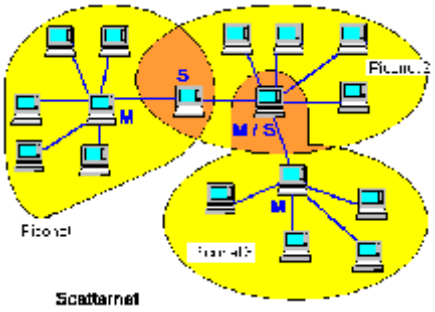
Wireless electronic devices promise greater freedom at home and in the office. They promise the freedom of greater mobility, information exchange, synchronization of applications, and effortless networking. The functionality of Bluetooth will enable humans to make more efficient use of space when using electronic equipment because unsightly, cumbersome cables will no longer be required.

The Bluetooth wireless system supports point-to-point and point-to-multi-point connections. An ad hoc Bluetooth scatternet may be established by linking several piconets together. A piconet is defined as a group of devices consisting of at least one master and one slave unit which all share the same frequency-hopping sequence. A scatternet is a collection of interlinked piconets with each piconet maintaining its unique frequency-hopping sequence. A Bluetooth device may link two piconets by being a slave in two different piconets. Additionally, it may be a slave in one piconet while being a master in another. At present, a device may not participate in more than two piconets at the same time. The current specification also limits the number of piconets within a scatternet to 10 piconets. Within a scatternet of 10 fully loaded piconets, a full-duplex data rate of more than 6 Mb/s is possible.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Bluetooth Ad Hoc Networking

Bluetooth enabled devices promise ad hoc networking. Ad hoc networking is the capability to quickly establish and dissolve small groups of devices with little user interaction, and no requirements for permanent address assignment among connecting devices. When two Bluetooth enabled devices come within range of one another, one device becomes the Master and the other, a slave. The Master device establishes synchronization among all slave devices by using its clock and hopping sequence. Once connected, the devices form a Piconet. A Piconet can have a total of eight devices, one master and seven active slaves. A Piconet can also include as many as 255 parked slaves, which are devices synchronized with the Piconet but not actively sending or receiving any signals.



When two or more independent and non-synchronized Piconets communicate with one another, they form a Scatternet. In order to facilitate communications between the separate Piconets, a single device being either a master or slave, must become a slave in the other Piconet. Once this is accomplished, the shared device will relay all communications between Piconets as required.

In an ad hoc network, there is no fixed infrastructure. The network is established on the fly, via wireless links. Individual devices act as routers when relaying data from one device to other when the two devices are too far from one another for direct communications. Since ad hoc networks are mobile and constantly changing in topology, ad hoc networking presents intriguing security challenges.

Bluetooth Security

Bluetooth supports several security features depending on the application, and user requirements. These features range from the protection against eavesdropping, inherent to the frequency-hopping spread-spectrum technology, to the use of keys or Personal Identification Number (PIN), and password combinations. With the use of PINs (alphanumeric strings of up to 16 characters), the 128-bit SAFER+ encryption algorithm is used to create very strong security and encryption between devices. If required, additional security can be added in the application software.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

The Bluetooth specification defines three security modes:

- Non-secure
- Service-level Security
- Link level Security.

In non-secure mode, a Bluetooth device does not initiate any kind of security procedures.

In the service-level security mode, security policies are allowed, based upon the access requirements of the application in use. This is especially useful when running several applications that require different security modes.

When using link level security mode, Bluetooth enabled devices set up security procedures before the link set-up is completed. Link level security requires that applications know who is at the other end of the link, in order to, provide authentication, authorization, and encryption services. Information integrity is vital to Bluetooth's future. As a result, developers have incorporated random number generation, encryption, encryption key management, and authentication. Authentication is an important element in any Bluetooth system that enables a user to develop a domain of trusted devices. Once established, authentication services allow the host controller interface to decide if a connection is to be formed based on the available identification at the hardware level. Upon link establishment, additional security may be applied to the data transmission using encryption. Encryption is applied to an existing connection, while authentication procedures dictate whether or not a connection will ever be formed. The security mechanisms inherent into the Bluetooth specification are secure enough for most applications. If not, stronger encryption schemes may be added to Bluetooth products at the software application level.

Potential Health Concerns

As wireless communications make there way into our homes and offices, more and more attention is being given to potential side effects of repeated exposure to microwave frequencies. To date, scientific studies indicate that current output power is too weak to harm humans since the radiation is omni-directional. Another concern focuses on whether Bluetooth RF emissions heat the human body. Studies in this area indicate that the output power of Bluetooth devices is insufficient to cause any detectable temperature increase. As more wireless devices are deployed at home and in the office, studies regarding prolonged exposure to electromagnetic radiation should be conducted. At present, some scientific studies indicate that certain individuals are more sensitive to prolonged exposure. Additionally, some people that claim that they can no longer be near such fields without considerable discomfort.

Conclusion

The simplest way to understand Bluetooth is to think of it as the cables that are connected to your PC. Bluetooth technology is the physical RF link between your computer and

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

your peripheral devices. It is the cable that connects your Palm Pilot to your laptop. It is the cable that connects your MP3 player to your headphones. Bluetooth represents all the cables that are currently attached to your computer, and to your printer, keyboard, mouse and monitor. Bluetooth enables the user to effortlessly connect devices anywhere within its operational range. Once this technology grows in popularity, manufacturing costs of Bluetooth chips are projected to cost approximately five dollars per device. Market researchers predict that over one hundred million Bluetooth enabled devices will be operational by the end of 2002. Furthermore, by the year 2005, over 1.4 billion products are expected to be in use worldwide. If these numbers are even close to being accurate, it appears that it will be difficult to purchase any item not equipped with Bluetooth technology.

The security features inherent to Bluetooth are adequate for ad hoc networks, and data transfer of non-sensitive information. Additionally, the 10 cm transmission range of Bluetooth devices operating with a maximum output power of 1 mW provides adequate security for money transfers, and transmission of sensitive data. Information integrity problems will primarily result from users using the wrong maximum output power.

Christina Bjorknader, marketing and communications manager for L.M. Ericsson Telephone, a major Bluetooth backer says, "You could have a pair of mufflers – the headphones over your ears – and be mowing the lawn outside, listening to your Walkman when your phone rings inside and automatically stops the music to tell you that there is a call which you can then take." Her scenario continues: Depending on whether your PDA has voice capabilities, you could even check your calendar while on the phone call and add an appointment or make a change. "Once you're done with the call, you can tell the headset to hang up the phone, which will simply restart the music from where you left off and you then finish mowing the lawn, all without taking your hands off the mower."[1]

References:

1. "Bluetooth"
http://www.anywhereyougo.com/bluetooth/ (April 2002)

2. "Palowireless Bluetooth Resource Center"
http://www.palowireless.com/bluetooth/ (April, 2002)

3. Johnson Consulting "Bluetooth – An Overview"
http://www.swedetrack.com/images/bluet00.htm (May 17, 2000)

4. Vainio, Juha T. "Bluetooth Security"
http://www.niksula.cs.hut.fi/~jiitv/bluesec.html#chap1 (May 25, 2000)

5. Saltzstein, William E. "Bluetooth: The Future of Wireless Medical Technology?"
http://www.devicelink.com/mddi/archive/02/02/001.html (February, 2002)

[1] Rohde

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

6. "Bluetooth"
http://www.ericsson.com/technology/Bluetooth.shtml (January 24, 2002)

7. "Bluetooth: The Official Website"
http://www.bluetooth.com/ (April, 2002)

8. Kardach, James. "Bluetooth* Architecture Overview"
http://www.intel.com/technology/itj/q22000/articles/art_1.htm (April, 2000)

9. Rohde, Laura. "Analysis: Can Bluetooth live up to the hype?"
http://www.cnn.com/2000/TECH/computing/07/12/bluetooth.idg/ (July 12, 2000)

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 26th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**