Global Information Assurance Certification Paper

Brush up on Bluetooth

Jeffrey B. Hall
GSEC Practical Assignment
Version 1.4b
Option 1

08/21/2003

Abstract

This paper will attempt to provide a basic understanding of what Bluetooth is and how it works. It will then describe the critical elements of Bluetooth security as well as potential security weaknesses. Finally, it will provide some guidelines for using Bluetooth securely.

What is Bluetooth?

Bluetooth is a wireless radio specification designed to replace cables as the medium for data and voice signals between electronic devices. The specification is defined by the Bluetooth Special Interest Group (SIG) which is made up of over 1000 electronics manufacturers. Intended primarily for mobile devices, Bluetooth's design places a high priority on small size, low power consumption, and low costs. The Bluetooth specification seeks to simplify communication between electronic devices by automating the connection process.

Gartner research projects that 161 million Bluetooth devices will ship in 2003 and that number will rise to 362 million in 2004. (Cox 1) Bluetooth can currently be found in devices such as laptop computers, cellular phones, PDA's, headsets, printers, computer keyboards and mice, as well as digital cameras and other consumer electronic devices. Bluetooth connectivity is even finding its way into automobiles as some cars now come equipped with Bluetooth systems that facilitate hands-free calling via Bluetooth enabled cellular phones. (Bluetooth in Cars 1) The wide variety of products that will support Bluetooth technology combined with the convenience of automated communication promises to usher in a new era of connectivity among electronic devices.

How Does Bluetooth Work?

Bluetooth radios operate in the unlicensed 2.4GHz Industrial, Scientific, and Medical application (ISM) frequency range. This frequency is already widely used by devices such as microwave ovens, baby monitors, cordless telephones, and 802.11b/g wireless networking devices In order to avoid interference from these devices, Bluetooth uses a technology called spread spectrum frequency hopping. Spread spectrum frequency hopping changes the transmission frequency up to 1600 times per second across 79 different frequencies. As a result, interference on any one of those frequencies will only last a fraction of a second. (Franklin 4) This, coupled with the limited range of Bluetooth radio transmitters, results in a robust signal that is highly tolerant of other devices sharing the same frequency.

Bluetooth devices automatically attempt to communicate whenever one device comes within range of another. Bluetooth devices discover each other and initiate communication via inquiry and page transmissions. If device A would like

to connect to device B, it will broadcast a page message progressively across the Bluetooth frequency range. Before device B establishes a connection, it will wait in standby mode listening for page and inquiry messages. In order for the page message to succeed in establishing communications, device A must know device B's Bluetooth address and system clock settings. If device A does not have device B's address, it will broadcast an inquiry message requesting this information. Device B will respond with the correct information and communication is then initiated with a page message. (Bluetooth Technology, 11)

Bluetooth devices have the ability to form ad hoc networks. The topology of these networks is both temporary and random. (United 4-1) An ad hoc network of two or more Bluetooth devices is called a piconet. When two Bluetooth devices initiate a connection, they automatically determine if one device needs to control the other. Generally, the device that initiates the communication assumes the role of master and exercises certain controls over the other members of the piconet which are known as slaves. Upon establishing a piconet, the slave devices synchronize their frequency hopping sequence and system clock with that of the master in order to maintain their connection. A master device can have up to seven slaves. A slave in one piconet can also be the master in another, thus allowing piconets to overlap and interact forming what is known as a scatternet.

Bluetooth Security

Bluetooth security is based on three critical services: authentication, authorization, and encryption. The authentication service is tasked with ensuring that a device seeking a connection is indeed who it claims to be. Authorization is the process that determines whether or not a requesting device is allowed access to specific information or services. Encryption helps to ensure confidentiality by protecting private data from being viewed by unintended recipients.

Bluetooth devices can be set in one of three different security modes. In security mode 1, no security measures are utilized. Any other Bluetooth device can access the data and services of a device in security mode 1. Security mode 2 enacts security measures based on authorization. In this mode, different trust levels can be defined for each of the services offered by the device. Security mode 3 requires both authentication and encryption.

Authentication

Bluetooth authenticates devices using secret keys called link keys. There are two different types of link keys: unit keys and combination keys. A device that uses a unit key uses the same link key for all of its connections. A combination key is specific to one pair of Bluetooth devices. Link keys can be generated

either dynamically or through a process called pairing. When a device is configured to generate link keys dynamically, it requires the user to enter the passkey each time a connection is established.

Pairing, on the other hand, generates a long-term, stored link key that allows for the simple automated connections that are the hallmark of the Bluetooth specification. In order to pair two devices, the user will set both devices in pairing mode and will then enter a shared passkey. This passkey is then used to generate an initialization key. The initialization key is based on the Bluetooth addresses of the two devices, a random number and the passkey. This initialization key is then used to authenticate each device as well as in the creation of the link key. Finally, the link key is stored locally on each device for future authentication. After the pairing process has completed, the devices will "automatically and transparently authenticate and perform encryption of the link."(United 4-8)

Bluetooth authentication is based on a challenge-response process and can be both unidirectional and mutual. The authentication process uses the E1 algorithm which is based on the SAFER+ block cipher. (Xydis, p.3) If device A were seeking to be authenticated by device B, it would begin the process by sending its 48 bit Bluetooth address to device B. Device B will then issue a 128 bit random number-based challenge to device A. At this point, both devices will compute an authentication response which is a function of the E1 algorithm and is based on device A's Bluetooth address, the random number challenge issued by device B, and the previously established link key. Device A will then transmit its authentication response and Device B will compare it to its own calculations. If the two agree, then the device is authenticated. If the authentication responses do not match, then the connection is refused. Once the authentication process has completed, device B generates a new random number for its next authentication session.

Authorization

Authorization is the process by which a Bluetooth device determines whether or not another device is allowed access to a particular service. Authorization incorporates two important Bluetooth security concepts: trust relationships and service security levels. Authorization is dependent on authentication as the authentication process establishes the device identity which is used to determine access.

The Bluetooth specification allows for three different levels of trust between devices: trusted, untrusted, and unknown. If device A has a trusted relationship with device B, then device B is allowed unrestricted access to device A. If device B is untrusted, then device B has been previously authenticated, but its access to services on device A is restricted by service security levels. An

unknown device has not been authenticated and it is considered untrusted. (Bluetooth Technology 18)

Service security levels control access to a device's services on a per service basis. The first security service level requires both authentication and authorization in order to grant access to a service. In other words, the identity of the requesting device has to be confirmed and the requesting device has to be granted specific permission to access the service. The second level of service security requires authentication only. At this security level, the identity of the requesting device need only be judged genuine in order to be granted access to the service. The third level requires encryption only. At this level, access to the service will be granted to any device that is encrypting its communications. The last level is open to all devices. An example of a use for this security level would be if a user wanted to grant unrestricted access to a business card stored on the device while restricting access to other, more sensitive services.

Encryption

Bluetooth strives to maintain confidentiality by offering a 128 bit encryption service. By encrypting its transmissions, a Bluetooth device ensures that only a recipient with the proper decryption key can view the data. Bluetooth's encryption uses an algorithm called E0. A device's encryption key is based on its link key. This simplifies the key generation process as both the sender and receiver have shared secret information upon which to key their encryption. Bluetooth's encryption service has three different modes. In mode 1, no encryption is performed. In mode 2, communication with individual devices is encrypted, but broadcast traffic is not. In mode 3, all communications are encrypted.

In addition to reducing interference, Bluetooth's limited range and spread spectrum frequency hopping help to ensure confidentiality by reducing the possibility of eavesdropping. According to Widcomm, a leading developer of Bluetooth software:

> "The use of fast frequency hopping, at 1600 hops per second, represents an important barrier to interception. Since the transmitter only dwells on a specific frequency for 625 microseconds, it is difficult to even detect the presence of a Bluetooth device unless it is in the process of actively paging another device." (Widcomm 6)

Most Bluetooth devices are equipped with radios which have a range of 10 meters. Potential eavesdroppers would have to be within this range to intercept a Bluetooth device's transmissions.

Bluetooth Security Weaknesses

The security features of the current Bluetooth specification provide for secure communication at the link level. However, there are some weaknesses that need to be addressed. These weaknesses arise from the specification's heavy reliance on device authentication for security services as well as the level of control that the user has over Bluetooth devices and their configuration. The current Bluetooth specification does not provide any means of user authentication. The lack of any means of user authentication coupled with the reliance on device authentication leaves Bluetooth particularly vulnerable to spoofing attacks and the misuse of authenticated devices.

The pairing process is a particularly vulnerable point for Bluetooth. The Bluetooth Security Expert Group writes, "The user should be aware that when using the pairing procedure from the Bluetooth Baseband specification, the initial exchange of keys using non-encrypted channels is the weakest part of the security procedure." (Gehrmann 19) If an attacker could intercept the transmissions of the pairing process, he could then derive the initialization key by calculating initialization keys for every possible passkey and comparing the results to the intercepted transmissions. The initialization key could then be used to compute the link key. The link key calculated by the attacker could then be compared to the intercepted transmission to see if it is correct. It should be noted that one of the reasons for this vulnerability is the fact that Bluetooth allows for the use of short passkeys. Short passkeys significantly reduce the complexity of initialization and link keys thus making it easier for an attacker to derive these keys from intercepted pairing transmissions.

The use of unit keys is another cause for concern. A device that uses a unit key is a security risk because it uses the same link key for each device that it establishes a secure connection with. As a result, any one of the devices that has the unit key can use it to eavesdrop on secured connections that use that link key. In its white paper on Bluetooth security, the Bluetooth SIG Security Expert Group points out that "when using a unit key there is no protection from trusted devices."(Gehrmann 7) Bluetooth security does not take into account the identity or the intent of the user. As far as Bluetooth's link level security is concerned, a device with the proper unit key is secure.

The loss or theft of a Bluetooth device can give an attacker access to sensitive data or services. The mobile devices that are most commonly equipped with Bluetooth are at a high risk of theft or loss. In the United States, over 350,000 laptops, 35,000 PDA's, and 232,000 cell phones were lost or stolen in 2001.(Girard 1) The security services of Bluetooth are based on the authentication of devices. The Bluetooth specification does not provide any means of protection from a malicious user operating an authenticated device. Assuming there are not higher level security measures in place and that there is no response to the theft, an attacker could use a lost or stolen device as if he

were the intended user. That is, the device would have access to the same level of services and devices it had been previously authorized to use.

"The goal of wireless communications security is to keep the air link from being the weakest link." (Widcomm 5) In the case of Bluetooth, the user is the weakest link. The combination of mobility and limited administrative controls that can be found on many Bluetooth enabled devices means that such devices are only as safe as their user. On many devices, users will be able to configure the security settings and establish their own connections. The link layer security measures built into the specification can be effective in securing Bluetooth communications, but only if they are utilized and configured correctly.

Bluetooth enabled cellular phones are an excellent example of how the burden of security falls upon the user. For the most part, users' cellular phones fall outside the purview of corporate IT departments. As a result, potentially unwary users are left to fend for themselves when it comes to the security of their Bluetooth enabled cellular phones. If not configured properly, an attacker could access that phone to make phone calls, to access the internet, to access sensitive information stored on the phone or even to gain access other Bluetooth devices. As more and more cellular phones and other user-managed devices begin interacting with corporate networks, the need for security policies and measures will increase.

Bluetooth is designed to make connections more convenient. Users who purchase Bluetooth products are likely to be put off by the inconvenience of Bluetooth's security services. A recent Gartner report suggests that "users will rebel against having to frequently use PINs and other identity mechanisms and will attempt to switch such features off." (Girard 6) In the case of Bluetooth, this means that users are likely to opt for paired link keys instead of more secure dynamic link keys. They are also likely to use unit keys instead of more secure combination keys. Users that are in pursuit of maximum convenience may go so far as to configure their devices for security mode 1 turning off security services altogether.

Bluetooth device manufactures are also a source of concern. In late 2002, computer security firm RSA issued a warning that some cell phone and PDA manufacturers were shipping Bluetooth devices with the security features disabled. This would allow anyone within range unrestricted access without requiring a pairing code for authentication. (Judge 1) Bluetooth devices that come out of the box set to security mode 1 would grant unrestricted access to any Bluetooth device they come in contact with.

In June of 2003, Bluetooth security was put under the microscope with the release of Redfang. Developed by Ollie Whitehouse of computer security firm @Stake, Redfang is the first hacking tool to target Bluetooth devices. One of the security measures of the Bluetooth specification is a stealth mode where a

device will ignore any inquiry broadcasts it receives. By ignoring these broadcasts, the device keeps its Bluetooth address a secret and communication links cannot be established. Redfang gets around this security measure by using a brute force attack to determine device ID's of any Bluetooth enabled devices within range of the attacker. Assuming Redfang could determine a target device's Bluetooth address, it could then transmit a page message and attempt to establish a connection. While the practical use of Redfang has been called into question, it has succeeded in proving a theoretical weakness in Bluetooth security and focusing the attention of the security community on Bluetooth. (Bluetooth Hacking 1)

How Can Bluetooth be Used More Securely?

Understanding how Bluetooth works and its inherent vulnerabilities is the first step toward developing a secure approach for using these devices. IT security professionals will have to evaluate how Bluetooth will be used and what level of security will be required before they decide what additional steps need to be taken to secure Bluetooth in their organization.

The Bluetooth specification only provides services to secure the link level. The availability of these measures may not provide the depth of security that some organizations will require. In order to bolster the security that is built into Bluetooth, IT departments will likely look toward application level security measures. Application level security measures can provide an additional layer of security for Bluetooth devices through services such as user authentication, virtual private networking, logging, and end to end encryption.

IT departments will need to maintain stringent inventory controls to track Bluetooth devices. The loss or theft of a Bluetooth device could allow an attacker access to sensitive data or services. It is imperative that IT departments be able to detect and react to such situations quickly. Any devices that make use of unit keys should be thoroughly documented in order to facilitate a rapid response to loss of a Bluetooth device.

Over time, vulnerabilities in the Bluetooth specification will undoubtedly be discovered. It is reasonable to expect that the SIG will update the Bluetooth specification as these weaknesses are identified. Manufacturers will similarly issue product updates to address security concerns and changes in the Bluetooth specification. Bluetooth devices must be kept up to date with product revisions so that they are not vulnerable when flaws or weaknesses are discovered.

The Security Expert Group has made several recommendations on how to use the current Bluetooth specification securely. As mentioned earlier, the initial pairing of devices is considered one of the weakest links in the Bluetooth specification. In order to reduce the risks that are intrinsic to the pairing process,

the Security Expert Group recommends pairing in a known, secure environment. Pairing in a private, secure environment instead of a public place significantly reduces the threat of eavesdropping. Risks can further be reduced by the use of long passkeys. Longer passkeys increase the difficulty of deriving the passkey from captured initialization transmissions.

The Security Expert Group also recommends that the use of unit keys be avoided in favor of more secure combination keys. Avoiding the use of unit keys will reduce the risk of eavesdropping from a trusted device as well as reducing the potential harm that could result from a device with a unit key being lost or stolen. These recommendations from the Security Expert Group highlight the need for effective security policies and Bluetooth security training.

IT professionals need to familiarize themselves with Bluetooth specification and its security provisions so that they can formulate comprehensive Bluetooth security policies. Organizations need to have policies in place that address issues such as the use of personal Bluetooth devices in the workplace, required security settings, and who is authorized to configure devices. It is important that IT departments be proactive in establishing their policies as the explosive growth of Bluetooth and its widespread distribution in electronic devices puts IT departments in the position of having to address Bluetooth before it makes its way into their organizations.

User training is perhaps the most significant step to be taken towards securing Bluetooth in a corporate IT environment. The shifting of administrative control from IT departments to the users means that users will need to be trained on the secure use of their Bluetooth devices as well as how to configure them properly. The more the users understand the risks involved with Bluetooth, the more likely they are to use their Bluetooth devices in a secure fashion. IT professionals should lead the way in the pursuit of Bluetooth knowledge but the users should not be far behind.

Conclusion

Bluetooth exemplifies the timeless struggle between user convenience and information security. Bluetooth seeks to provide automatic connections between electronic devices; however this convenience is not without some compromise in security. Mitigating the resulting security risks comes at the expense of convenience. The conveniences offered by Bluetooth could make it a worthwhile endeavor, yet the security risks could make it a security professional's worst nightmare. It falls on the IT security professional to weigh the benefits of Bluetooth's convenience against the costs of Bluetooth's security risks and to seek some sort of balance between the two.

Security professionals need to consider what role Bluetooth will play in their IT structure and how best to secure it for that task. These decisions need to be made quickly as Bluetooth is rapidly making its way into the mainstream. Bluetooth radio sales are projected to increase by 74 percent per year over the next four years. (Smith 1) Bluetooth seems well on its way to becoming the next ubiquitous technology. Bruce Potter, a security expert with the Shmoo Group, predicts that "Bluetooth security will become a real issue in the next year or two. There are currently more Bluetooth radios in existence than 802.11 radios, but most corporate security departments don't know the first thing about Bluetooth security." (Knight 1) IT security professionals need to work quickly to improve their understanding of Bluetooth so they can make informed decisions regarding how they will use Bluetooth and how to use it securely.

Works Cited

"Bluetooth in Cars". 10 July 2003. http://www.webdesk.com/bluetooth-in-cars/ (18 August 2003).

"Bluetooth Technology Overview". Version 1.0. 4 April 2003. http://ncsp.forum.nokia.com/downloads/nokia/documents/Bluetooth_Technology_Overview_v1_0.pdf?ref=wdn (19 August 2003).

"Bluetooth Hacking Tool Released". Bluetoothnews.com. 24 June 2003. http://bluetoothnews.com/industrynews/hacking_tool.htm (17 August 2003).

Cox, John. "Study: Bluetooth Security Should Raise Red Flags". Network World Fusion. 9 September 2002. http://www.nwfusion.com/news/2002/0909bluetooth.html (14 August 2003).

Franklin, Curt. "How Bluetooth Works" . http://electronics.howstuffworks.com/bluetooth.htm (17 August 2003).

Gehrmann, Christian. "Bluetooth Security White Paper". Version 1.0. 19 April 2002. www.bluetooth.com/upload/24Security_Paper.PDF (14 August 2003).

Girard, John. "Mobile Device Security: Don't Be at Risk". 6-11 October 2002. http://symposium.gartner.com/docs/symposium/itxpo_orlando_2002/documentation/sym12_26g.pdf (15 August 2003).

Judge, Peter. "RSA Issues Bluetooth Security Warning". 11 October 2002. http://www.zdnet.com.au/reviews/coolgear/wireless/story/0,2000023546,20268990,00.htm (14 August 2003).

Knight, Will. "Many Bluetooth Gadgets Open to Wireless Snooping." New Scientist. 11 August 2003. http://www.newscientist.com/news/news.jsp?id=ns99994041 (August 16 2003).

Smith, Tony. "Bluetooth Chip Sales to Hit 17.7bn in 2007". The Register. 29 July 2003 http://www.theregister.co.uk/content/68/32044.html (17 August 2003)

United States Dept. of Commerce. National Institute of Standards and Technology. Technology Administration. Special Publication 800-48: Wireless Network Security: 802.11, Bluetooth and Handheld Devices. By Tom Karygiannis and Les Owens November 2002. http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf (18 August 2003).

Widcomm, Inc. "Bluetooth Security Solutions". 2001. www.widcom.com/bluetooth/pdfs/BluetoothSecurityWP.pdf (14 August 2003).

Xydis, Ph.D., Thomas G. and Simon Blake-Wilson. "Security Comparison: Bluetooth Communications vs. 802.11" 10 November 2001, revised 15 May 2002. http://www.bluetooth.com/upload/14Bluetooth_Wifi_Security.pdf (17 August 2003).