Enhancing Security and Usability for Bluetooth Discovery and Pairing

Benjamin Arrington, Jayme Thysell, Josh Ramsden, Thuy Tran, Penelope Skordalakis
INFS 612 – Summer 2008 - PGN #6

Abstract

Over the past several years, Bluetooth technology, and Bluetooth enabled devices specifically, have become a large part of the mobile device landscape. With Bluetooth, users are able to perform tasks such as connecting mobile phones to wireless headsets, connecting computers to printers, and sending images from one mobile device to another. This is all done wirelessly and with the click of a few buttons. The benefits of Bluetooth are undeniable, but so are the security concerns associated with the technology. Many of these concerns, we argue, are the result of weak specifications and implementations with regard to mobile device discovery. We suggest two possible enhancements to the current Bluetooth device discovery process: implementing White List functionality, and the ability to pass Bluetooth tokens with text messages. These enhancements would provide greater security, with the added benefit of increased usability, with regard to device discovery. In addition, we suggest enhancements to certain aspects of the current Bluetooth specification, which will ultimately lead to more secure implementations by mobile device vendors, enhancing the overall security of the Bluetooth specification.

1. Introduction

This paper describes the current Bluetooth landscape, describing what Bluetooth is and does, as well as listing the security issues associated with it. Additionally, this paper attempts to address security issues specifically related to Bluetooth device discovery, providing potential solutions that will allow for added security as well as enhanced usability, attempting to improve the overall user experience.

1.1 History of Bluetooth

1.1.1 Origin of the Name

Bluetooth technology is named after the 10th century Danish King, Harold "Bluetooth" Blåtand. King Blåtand, also known as King Bluetooth, is known for uniting the warring factions of Scandinavian Europe and establishing Christianity as the primary religion in the countries of Denmark, Norway, and Sweden. Due to the Bluetooth founder's Scandinavian roots, and the goal to unite different technologies into one network, Harold was the perfect candidate to honor with this new technology [18][19][20]. The Bluetooth logo is Harold Blåtand's initials using the runic alphabetic characters "H" and "B" forming a bind rune; runes are indigenous to Scandinavia [3].

1.1.2 Development of the Technology

In 1994, Ericsson Mobile Communications initiated a study to find a way to eliminate wire clutter in homes and offices. At the time, the goal was to replace cables with a low-power radio chip to connect devices. They developed the specifications for a wireless frequency-hopping technology which would create a personal area network (PAN) [4][18][19].

In 1998, the Bluetooth Special Interest Group (SIG) was formed by 5 companies: Ericsson, IBM, Intel, Toshiba, and Nokia. The group's mission statement, "Strengthen the Bluetooth brand by empowering SIG members to collaborate and innovate, creating the preferred wireless technology to connect diverse devices," infers that the Bluetooth SIG was created to promote, develop, and control the new technology, but it does not manufacture or sell Bluetooth products [4]. Four hundred companies had joined the Bluetooth SIG by the end of 1998. As of 2008, the Bluetooth SIG has over 10,000 members. In ten years, Bluetooth wireless technology has grown to include nearly two billion products [4][18][19].

In 1999, the specification for Bluetooth 1.0 was first released. There were versions 1.0 and 1.0B, which contained interoperability problems between different manufacturers. Version 1.1 was soon released to correct the errors with version 1.0B and contained

support for signal strength and non-encrypted channels [4].

The Institute of Electrical and Electronics Engineers (IEEE) ratified the 802.15.1 specification as the standard for Bluetooth in 2002. The standard was again modified in 2005 to support Bluetooth 1.2. Following the publication of this standard, the IEEE voted to discontinue their support of future Bluetooth versions [15] [16].

The Bluetooth 1.2 core specification was adopted in 2003 as the first major enhancement of the technology. Improvements to this technology included faster connections, faster transmission speeds, improved voice quality, Host Controller Interface support, and resistance to radio frequency interference. This version was also backwards-compatible with version 1.1 [4] [15] [16].

Backwards-compatibility to Bluetooth 1.1 has been supported by the recent Bluetooth versions. Bluetooth 2.0 introduced the Enhanced Data Rate (ERD) improvement in 2004 and version 2.1 appeared in 2007 with even more functionality. ERD provided three to ten times the transmission speeds of previous versions in addition to lower power consumption and simplified multi-link scenarios. Bluetooth 2.1 expanded on ERD by further reducing power consumption and improving the pairing procedures and security.

Security is also improved with version 2.1. Extended Inquiry Response is used to filter devices more efficiently before creating a connection. Encryption Pause Resume increases security for connections of long duration times. Near Field Communication (NFC) creates automatic secure connections when the NFC radio interface is available by bringing devices physically close to each other for secure data transmissions [4].

1.1.3 Future Enhancements

The future of Bluetooth is expected to include additional functionality while still improving data-transfer rates, power consumption, and the user experience of making simple connections among their devices. Broadcast channels will allow Bluetooth enabled devices to pull from information points. This advancement will lead to less power consumption and increased security for portable devices. Alternating MAC/PHY connections will be used for data transport, while radio is still used for connections, which will allow for a more efficient use of power. The inclusion of Topology Management would be invisible to users, but will allow the technology to work better [22].

The next version of Bluetooth, presumably version 3.0, is expected to include improved audio and video quality of service using Ultrawide Bandwidth (UWB) radio technology; UWB has high speeds which can support applications such as VoIP. This specification will also include Wibree's technology which will become the Bluetooth Low Energy Wireless Technology. [4]

"Bluetooth 3.0" will also include Wibree, an ultra-low-power digital radio technology. Wibree will be included in future Bluetooth specifications due to an agreement made by the Bluetooth SIG for Wibree to become the Bluetooth Low Energy Wireless Technology [4].

1.1.4 Exposing the Vulnerabilities

There have already been some famous and mocked situations in the world of Bluetooth security. Paris Hilton, as an example, was misreported to have had her Sidekick hacked through Bluetooth, only later to have that claim refuted as the device wasn't even Bluetooth capable. Some experts in the past have in fact made light of some of the earlier attempts to crack Bluetooth security. As a proof of concept, a brute force tool called Redfang was created, which some seemed to take as a clumsy brute force attack rather than a proof of concept of theoretical weaknesses in Bluetooth. Although the run time for it to legitimately open a hidden Bluetooth device was not an immediate threat, (in the years initially), due to the brute force nature of the attack, there are implications. Any brute force attack that can theoretically be successful simply requires time, technology and creativity to eventually become a true threat. [27], [29]

Manufacturers themselves have certainly had some problems with specific devices and the particulars of being able to get into those devices. As an example, with two commands on a Linux machine, some models of Nokia and Ericsson phones produced in 2003 were able to have their entire address books downloaded without authorization. These types of manufacturer specific problems have been fairly consistent as the authorization and authentication of Bluetooth hasn't historically been implemented correctly by manufacturers. [26]

More recently and far reaching in 2005, a team of cryptographers discovered that getting past Bluetooth security in general wasn't nearly as difficult as one might think. During the pairing process it has always

been possible to catch the key that was passed between devices on an initial pairing. The real threat however, was that the ID could be obtained by spoofing the pair device and sending a "forget" message to the device one wished to hack. By doing so it created a new session and the hacker could gain control of the device [28].

Bluetooth sniping was also later revealed where the range of attackers could be extended up to a mile to attack vulnerable Bluetooth devices. The latest concerns about vulnerability stem from the possibility of a worm exploiting the vast number of new Bluetooth services and the volume of Bluetooth devices left in a visible state [3][5].

1.1.5 Comparing the Competition

Over the last ten years, Bluetooth has successfully established itself in the market. Skeptics predicted that Bluetooth was a fad or would "fail to be relevant" [14] and suggested that it would be surpassed by other emerging technologies. While other wireless devices do exist, none of them have experienced the same amount of growth as Bluetooth [4].

The most direct competitors of Bluetooth are those which are designed to establish a wireless PAN, such as Infrared Data Association (IrDA), Zombie, and Body Area Network (BAN). IrDA exchanges data over infrared light for a short range with a direct line of sight. It is very effective at transporting data and has an extremely low power usage, but other technologies are favored in practice due to the line of sight limitations. Zombie is a low-cost, low-power alternative to Bluetooth, using the IEEE 802.15.4 standard. Since it has lower power consumption than Bluetooth, its ideal use is in warning device sensors and automation control devices. A BAN attempts to create a low-power, low-frequency short-range network around a person's body; its primary application is for healthcare. Currently, it has been assigned the IEEE 802.15.6 standard [15] [16].

Other types of Bluetooth competitors are Wife, Wireless USB, and Sony's "Transfer Jet". Wife, including the 802.11 wireless Ethernet standards, provides a wireless network to connect devices to the internet, which is designed to have a much greater range than Bluetooth. Wireless USB is designed to have high data transfer rates between devices. When "Bluetooth 3.0" is released with UWB, there will be more direct competition between Wireless USB and Bluetooth. Sony's "Transfer Jet", which connects devices using an electric induction field coupler, will be a direct competitor of both Wireless USB and "Bluetooth 3.0". The existence of three viable wireless formats could potentially lead to wireless format war [21].

1.2 Technical Information

Bluetooth operates on any device that can have short range radio frequency at 2.4 GHZ by using the Industrial-Scientific-Medical (ISM) radio band. It is free and unlicensed, and it operates on a single chip. It uses the Frequency-Hop spread spectrum which divides the frequency into a number of hop channels. A transceiver is applied to combat interference and fading.

Robust data transfer rates up to 721 kbps can be achieved in Bluetooth. Full-duplex synchronous and asynchronous data transfer is supported. Bluetooth can support an asynchronous data channel, three simultaneous synchronous voice channels, or a synchronous channel that simultaneously supports synchronous voice and asynchronous data. It uses a time-division multiplexing scheme; Diagram 1.2a illustrates the Bluetooth protocol stack.

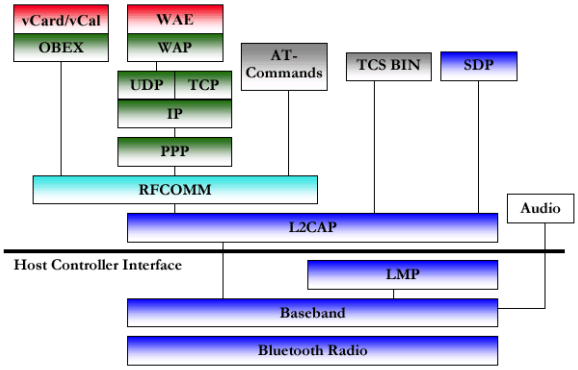

Diagram 1.2a: Complete Bluetooth protocol stack

At the start of a connection between devices, the initializing unit is assigned as the master. The master initiates the connection and can control up to seven slave units. For example, a wireless handset can act as a master while a Bluetooth headset and a car speaker system can both act as slave devices. Collectively, these ad-hoc devices on a Bluetooth network create a piconet. Piconets can communicate with one another via the ISM radio band.

The baseband layer of the protocol is a combination of circuit and packet switching. Slots can be reserved for synchronous packets, and a packet can span one to five

slots. The synchronous switching, Synchronous Connection Oriented (SCO), is used for voice communication and is a point to point link between a master and slave device. The access code section of the packet format identifies all the packets of a channel in a piconet (see Diagram 1.2b).

The asynchronous packet switching, Asynchronous Connectionless (ACL), is used for data transmissions. The master device can support multiple ACL links to slave devices. Data can be retransmitted when necessary to ensure reliable delivery. Asynchronous packets not addressed to a specific slave are read by all devices and considered broadcast messages.

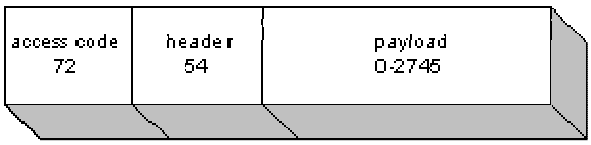

Diagram1.2b: General Bluetooth packet format (with # of bits per section)

Bluetooth devices establish network connections in the STANDBY mode. It is in this mode that devices 'listen' periodically (every 1.28 seconds) for an incoming message. When an address is known, the connection is initiated with a PAGE message. In the case of an unknown address, a connection is initiated by an INQUIRY message, which is followed by a PAGE message. The purpose of the INQUIRY message is to find other Bluetooth devices that do not have an address.

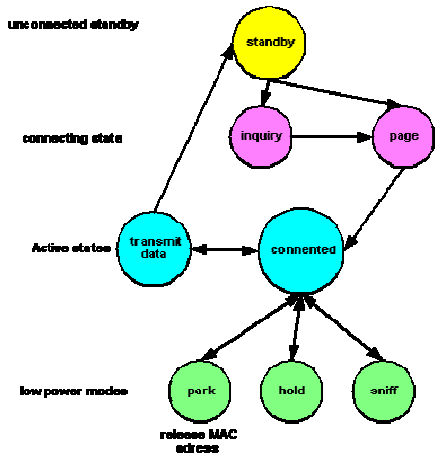

Diagram 1.2c

There are three power saving modes, HOLD, SNIFF, and PARK. If there is nothing to transmit, master devices can put slaves into HOLD mode. A slave unit can request to be put into HOLD mode, and then transmissions can resume when the slave unit is out of HOLD mode. The SNIFF mode is when a slave device listens at a reduced rate. To enter SNIFF mode the master and slave negotiate a sniff interval and offset. The PARK mode keeps the device synchronized in the piconet, but disables its participation in the traffic. Slave devices can still listen periodically for the master to re-synchronize and check on broadcast messages. [1][2]

Once Bluetooth devices have agreed to communicate, they are said to be 'paired'. For two devices to pair, they must be set to discoverable mode and have exchanged passkeys. Discoverable mode allows a user to see other users who are also in discoverable mode within a distance of approximately 10 meters from one another. Normally devices in discoverable mode will be identified to one another by the factory name of the device or a user generated name. A passkey is a password that is shared between two devices that the users have agreed upon. Once both users have entered the correct passkey they are said to have formed a 'trusted' pair.

It is recommended that Bluetooth devices not in use turn their discoverable mode to "off." When the discovery setting is set to "off" on a particular device, no other Bluetooth devices will be able to find or connect to it. [3]

1.3 Current Uses

Undeniably, Bluetooth is a specification that has opened up a variety of functionalities and capabilities for devices. It addresses a need which no technology to date has had the ability to do. The promise and capabilities with regards to ad-hoc networking, device synchronization, and extensibility for a non-technical consumer base has been embraced.

Since this specification is designed with both voice and data in mind, it allows for a variety of capabilities. Setting up and discovering devices are very easy to do. Using Bluetooth enabled devices usually requires only a moment of configuration or discovery at most to get them operational. It doesn't suffer from some of the shortcomings of infrared technology; the signals are very adaptive to the real world and don't require line of sight.[23]

Since the receivers are small and inexpensive, they have made their way into plenty of devices already. Many devices in the voice world are also using Bluetooth to unify lines of communication. One device, for example, allows the combination of a land

line and a cellular line into one wireless phone system. Several automobile manufacturers now equip their vehicles with Bluetooth so that a user's cellular phone can be used hands free style through the car's built in speakers and microphones.

Obviously, one of Bluetooth's greatest strengths is unifying devices and information. Unifying can happen instantaneously between devices for an indefinite amount of time, such as a PDA & a cell phone or a cell phone & a laptop. Many cameras now allow for automatic wireless transfer of images from the camera to a laptop or other Bluetooth enabled storage device. Even speakers and other multimedia equipment have been wirelessly teamed together [23].

The technology is now also being discussed and implemented in ways that may have broader reaching implications as well. Many companies have an interest in using variations of the technology for easy financial transactions. The idea is tempting, because easy synching with a checkout could allow for automated quick transactions, which may not require the overhead of employees to process. Some have even discussed potential uses of the technology in ways of coordinating or controlling devices en masse. For example, what would the implications be if the technology could be used at entrances to hospitals to turn off particular services on devices or the devices themselves for all guests to ensure hospital policies are obeyed?[23]

2. 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 [4][5][6].

2.1 Specific Bluetooth Attacks

2.1.1 Bluejacking

Bluejacking is the process of sending a phone book contact, along with a message, from one mobile phone to another. From a general security standpoint, this vulnerability seems relatively harmless. The major concern with Bluejacking, however, lies in privacy issues. Victims of Bluejacking attacks receive these contacts and the messages associated with them. An attacker can choose to send out these contacts to any device within range. This can be considered a type of spamming, where messages are sent to users' phones, potentially overloading their contacts with unwanted and unnecessary information. In addition, the messages associated with these contacts could contain inappropriate, and even potentially threatening, information. As the average age of cell phone users becomes younger and younger, issues like Bluejacking can become more and more of a concern.

Diagram 2.1.1 Bluejacking attack

2.1.2 Bluesnarfing

Bluesnarfing is one of the more serious attacks that Bluetooth-enabled devices may be susceptible to. This attack occurs when an attacker gains access to the data, such as calendar, contact information, text messages and pictures, on another user's phone. Obviously, this type of attack could cause serious problems for the user being attacked, depending on what type of information is stored on the phone. For example, an attacker could gain access to a user's calendar, discovering where the user will be on a given date at a given time.

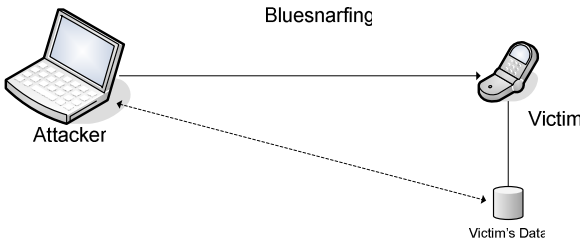

Diagram 2.1.2: Bluesnarfing attack

2.1.3 Bluebugging

Possibly the most serious of the current Bluetooth attacks is Bluebugging. Bluebugging is when an attacker gains unauthorized access to an unsuspecting user's mobile device along with the data that resides on it, and can execute internal commands on the user's phone. With this access, the attacker can perform actions on the user's behalf, such as making phone calls, sending and receiving text messages, and viewing contact information. In addition, the attacker may eavesdrop on any phone conversations involving the unknowing users. Again, depending on the type of information stored on the phone, and the types of conversations of unsuspecting users, this type of attack could have serious consequences.

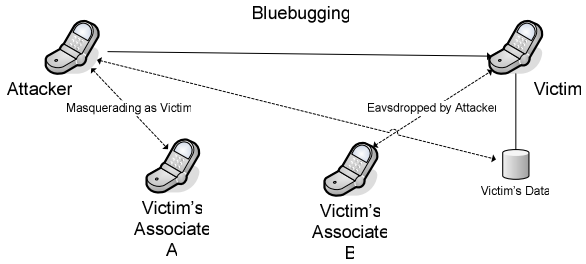

Diagram 2.1.3: Bluebugging attack

2.1.4 Cabir Worm

The Cabir Worm is a form of malware. When installed on a vulnerable mobile device, the Cabir Worm uses Bluetooth technology to the self-replicate itself on to other mobile devices.

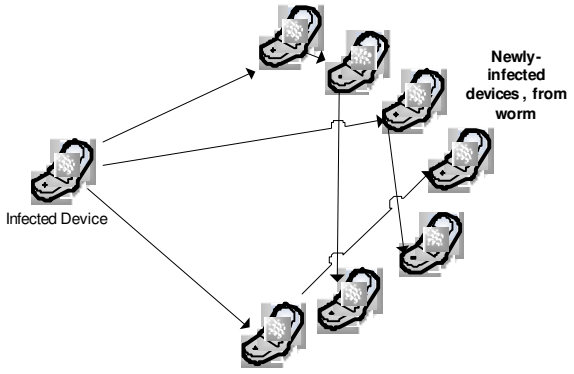

Diagram 2.1.4: Cabir Worm

2.1.5 Denial of Service

All Bluetooth enabled devices are potentially susceptible to Denial of Service attacks. In this type of attack, an attacker could send Bluetooth requests to the device being attacked. If numerous requests are sent over and over, the battery life of the mobile device can be weakened to the point that the phone is no longer usable, until recharging, without an alternate form of power.

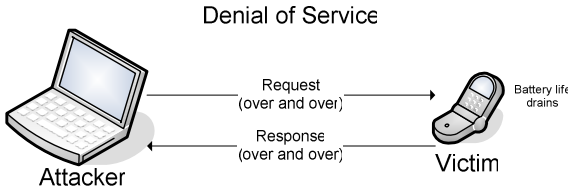

Diagram 2.1.5: Denial of Service

It should be noted that, due to the limited range of the Bluetooth technology, all of these exploits need to be performed in close proximity to the mobile device(s) being attacked. While this seems to be an advantage for the victims, attackers have been known to use Bluetooth-enabled devices to discover the location of expensive equipment, such as laptop computers in cars for example. With this information, thieves have broken into the cars in order to steal the equipment [7].

2.2 General Bluetooth Security Concerns

In general, much of the Bluetooth security concerns revolve around the intended openness of the technology. If users so chose, they can place their mobile device in a discoverable mode, allowing other nearby Bluetooth-enabled devices to locate, or see, the device. This allows for greater convenience, making it much easier for users to find and pair with other devices. This convenience comes with a cost, however, as this is how Bluejacking is made possible – a Bluejacker scans for nearby devices and sends, or spams, contacts to these devices. Users can chose to accept or reject the contact information, but if they accept, they may be surprised at what they find in the message. At the very least, it's a nuisance for the receiving device to have to respond to these unsolicited attempts at contact. Just imagine having to accept or deny each piece of spam you receive in your email inbox!

3. Bluetooth Security Enhancements

For the benefit of the reader, we now provide a more detailed view of the Inquiry process, used by Bluetooth devices wishing to discover, and be discovered, by other devices. This will be broken into two sections: the view from the inquiring device perspective, as well as that of the device being discovered.

3.1 Inquiring Device Process

When a device wishes to discover other Bluetooth-enabled devices, it enters the inquiry substate. When in this substate, the inquiring device sends a broadcast inquiry message over and over, which any other discoverable Bluetooth device within range may receive. This broadcast message contains no information about the source device. It may, however, indicate in the message that only certain types of devices should respond. As discoverable devices respond, the inquiring device keeps track of the addresses and clocks of these devices, as well as specific services supported. The inquiring device does not, however, acknowledge the receipt of these responses. With this information, the inquiring device may initialize the Paging, phase of the overall process to establish a paired connection with one of the responding devices.

3.2 Discoverable Device Process

Any device wishing to be discoverable will enter the inquiry scan substate. When in this state, the discoverable device may respond to any inquiry message being broadcast from an inquiring device. It is important to point out that the response is optional. If a device does decide to respond, it enters the inquiry response substate. From this substate, the responding device provides its address, clock, and potentially, a list of available services and other device information. With this information, the inquiring device may initiate the Paging phase of the overall process to establish a paired connection with the responding device.

3.3 Best Practices

It should be noted that the Bluetooth designers/developers have made some simple suggestions and recommendations to improve the overall security of the technology [4]:

- Keep the device in non-discoverable mode when possible.
- Only pair with known devices
- Pair your device(s) in private

3.4 Enhancements to current model

We will now describe the current security model, with regard to device discovery, and propose enhancements to this model.

3.4.1 Normal discovery/pairing scenario

One of these recommendations is for users to keep their devices in non-discoverable mode, only switching to discoverable mode when actively attempting to pair with a known device, preferably in a non-public place. Thus, the steps involved in order to pair two devices would ideally follow these steps:

- Exchange PIN, preferably out of band
- From a private location,
- Place device A in discoverable mode
- Place device B in discoverable mode
- Device A broadcasts inquiry messages to all devices within range
- All devices within range, including B, respond to the inquiry, providing their information to the inquiring device
- User of Device A enters the pairing PIN in his/her device and initiates the pairing with Device B
- User of device B enters the matching PIN in his/her device to accept the pairing
- Place device A in non-discoverable mode
- Place device B in non-discoverable mode

It's quite plain to see that the steps involved just to pair two devices, according to the Bluetooth SIG's security best-practices, are extensive. This appears to go against the desired ease and openness of the technology. Even more concerning, the designers of the Bluetooth specification have placed much of the security burden associated with the technology squarely on the users' shoulders. It addition, these best-practices do not solve any real security concerns. Looking back to the known, specific Bluetooth attacks, virtually every one of them is predicated on the fact that in order to perform an attack, the attacker(s) first need to be aware of (discover) the devices they are going to be attacking. Working under the assumption that these attackers are opportunistic, one could argue that the less prone a device is to being attacked, the less likely that device is actually going to be attacked. Essentially, the attackers are going to focus on easy prey. If this is the case, then in order to truly mitigate these risks, we must focus on the virtual open door of these attacks – the Discoverable mode.

3.4.2 Enhanced discovery/pairing scenario

Instead of this binary approach for discovering devices – Discoverable and Nondiscoverable, we argue that there can be a compromise – one that allows devices to discover or be discovered by friendly or known devices, while remaining hidden from unknown devices. We propose two such methods. The first of these methods is a white list of allowable devices, requiring devices to use an alternate form of Discovery mode. The other approach, passing Bluetooth credentials when passing text messages, would allow devices to locate each other without having to rely on the current Discovery mechanism.

3.4.2.1 White List

Using a mechanism such as a white list could accomplish the compromise discussed above. With this approach, users could place the required information of known devices for which they are willing to be discoverable to into a list, and the device will be discoverable by only the devices on the list, while remaining hidden from all other devices. This approach is essentially a third option to the existing discover modes – a Discoverable-by-Known-Devices mode. The general process would be as follows:

Assume devices A and B are in discoverable-by-known-devices mode

- Device A broadcasts inquiry messages to all devices within range
- Each device within range validates Device A against its white list. Any device whose white list contains A responds to the inquiry, providing their information to the inquiring device
- User of Device A enters the pairing PIN in his/her device and initiates the pairing with Device B
- User of device B enters the matching PIN in his/her device to accept the pairings

There are two main differences between this process and the initial process outlined above. The first difference is that the inquiring device is required to provide identifying information in its broadcast message. The second is that instead of having to respond, each device only responds if the inquiring device exists in its white list. Additionally, since each device is only responding to those inquiry broadcasts initiated by known devices, they may remain in the more secure discoverable mode, as opposed to turning discovery off completely. This addresses the usability problem posed by the Bluetooth SIG's #1 best practice recommendation above; users would no longer have to keep toggling between discoverable and non-discoverable modes just to initiate pairings. This enhancement would require modifications to the specification to allow source devices to include identifying information in the inquiry broadcast message.

It should be pointed out, however, that this approach still requires that the devices be placed in *a* Discovery mode; a better approach would be to provide a mechanism that allows for devices to locate each other without using any sort of Discovery mode. In addition, a burden is placed on the users of the devices, as they will be required to manually enter the necessary information for any device they wish to add to their white list. Both of these concerns can possibly be addressed by allowing users to pass a Bluetooth token when sending text messages to other users.

3.4.2.2 Bluetooth token provided with text message

This approach would allow devices to contact other devices it has had previous contact with – specifically, with which they've received a text message from. The general idea is that when a user sends a text message to an associate, they can choose whether to provide a Bluetooth token containing their Bluetooth information – hardware address, clock, services - along with the text message. Piggybacking off of the white list approach, the receiving user could then choose whether to add this device, based on the token, to its white list. In this manner, both the sender and receiver have acknowledged that they are friendly devices, which will allow us more freedom with the initial discovery process. Instead of relying on even a discoverable-by-known-devices model, neither device would technically have to be in discoverable mode in order to initially locate one another. Instead, the connecting and connected devices can both bypass the Inquiry step altogether, and begin their process straight with the Paging (or Connecting) process (refer back to Section 1.2 for details). Those familiar with wireless LANs will notice the similarities between how mobile devices connect to an access point that is not broadcasting its SSID, and this approach. In both cases, the connecting device needs prior information about the device being connected to, as this device is not broadcasting this information out to the world. The general steps are as follows:

Time N:
Assume Device A exists in Device Bs white list

- Device B sends Device A a text message, passing its Bluetooth token with the message

- Device A accepts Device Bs token, adding B to its white list – it now has the information needed to send a Page request to Device B

Time N+1:

- Device A sends a page request to Device B.
- Device B responds to Device As page request.
- Exchange PIN, preferably out of band
-
    - Device A provides a PIN and sends a Page request specifically to device B
    - Device B is Page scanning, specifically for device A. Provides PIN to establish connection
- Connection established

Overall, this is quite an improvement over the initial outline of steps showing the current process. As can been seen, neither device is required to go through the Discovery mode of the connection operation. Thus, instead of being discoverable by *ALL* Bluetooth devices within range, each device is discoverable only by devices that it has a known relationship with, based on the token passed with the text message. Another benefit of this approach is that, unlike the White List approach outlined above, users are not required to manually enter the information of known devices into the list; the information is provided by the text message sender and automatically added to the list, if the receiver of the text message chooses to do so.

The main issue with this approach is the actual passing of the Bluetooth token as part of the text message. Obviously, text messages are not part of the Bluetooth technology, so it would require the Text Messaging specification to be modified to include the Bluetooth token. Additionally, mobile device vendors would have to implement this feature in their devices in order for users to take advantage of it. Also, while neither of the connecting devices ever enters the Discovery process, they are still vulnerable to attacks. Specifically, attackers can technically spoof the hardware address of the Paging device, and send a Page request to the receiving device. This would require prior knowledge, on the attacker's behalf, of both the sender and receiver's information. So, while these types of attacks are *possible*, they are not *probable*.

Both of the approaches listed above would allow for enhanced security with regard to discovering, and being discovered by, other Bluetooth devices. The second approach, passing the Bluetooth token as part of a text message, has the added benefit of enhancing overall usability as well. Both enhancements would require changes to the current standard vendor implementation, so the benefit of added security and enhanced usability must be weighed against the cost of possibly having to modifying specification(s), and vendors having to implement such features into their products. It must also be assumed that the cost of these changes will be pushed to consumers, as the price of devices and services will ultimately be affected for these added benefits.

3.4.3 Broadcast Encryption No Longer Optional

Currently, the Bluetooth specification allows encryption to be an option rather than a requirement for the communication of devices. Some have argued that the channel hopping nature itself is a form of protection; however this is not the case.

Channel hopping is something that can be observed and recorded. Seventy nine channels are available during the hopping sequence, recording and playback of that sequence is potentially possible. If recording and playback occurs, then unencrypted data would not be protected from malicious intent. [24]

Although the lack of encryption can be useful for some devices, security would be improved if all devices had built in Bluetooth encryption. If all traffic were encrypted, then even if channel hopping were observed, captured data would be more difficult to use.

3.4.4 Do Not Allow Users to Generate Passkeys

Users currently are responsible for generating their own passkeys when pairing with devices. This is convenient because users can simply enter in a number into their own device, and verbally relay that to their pairing partner to enter when information is to be exchanged.

The problem with this, unfortunately, is that users may choose to create very short, easy to remember, keys. These keys often can be a variation on something simplistic such as 0000, and can be easily guessed or retrieved via social engineering. Instead, the keys themselves, as part of the application level specification, should be generated with an appropriate length, at random, for the users during the pairing process. This would ensure additional security and only cause a little work up front for a more secure transaction between the users. [24]

Alternatively, a new option may be available in the latest specification of Bluetooth 2.1. Near Field Communication could either increase the security of key generation or decrease it. In this form of

communication, proximity alone is enough for two devices to perform all key matching activities and communication initiation. If this form of communication can be enforced for the pairing process of all devices, inherently, the key generation process could be more secure. This is because no verbal or manual processes are taking place to generate and exchange a key. If manufacturers implement the technology in a device, at the application level, no interaction from the device owner is required. Thus implications of accidentally brushing up against someone on the subway or in a crowd could drastically change.

3.4.5 Application Level Specifications

The Bluetooth specification is designed around the transport layer and the layers below it that allow the radio communication to work appropriately. Although there are generic profile recommendations for implementation in the application layer, this is something that should be specified to a much greater degree. As manufacturers are left to their own best practices for some parts of implementation, those that do not fully understand the specification are bound to make missteps with it. With that in mind there are three up-front recommendations in the application level that could help, and in general, these types of specifications should vastly be expanded. These three recommendations are described in the following sections.

3.4.5.1 Key Database Storage Specifications

Bluetooth awaits link keys to perform its security tasks. "The Bluetooth specification does not contain any recommendations for how a host should handle the key database." [24: 62] This means host manufacturers are left to determine how this database is to be stored, secured, and implemented; keys are sent into the Bluetooth system only when needed. [24]

That being the case, manufacturers can store the key database in any fashion they like (plain text for example). At a bare minimum this database should be encrypted, and ideally it should require credentials for it to be accessible. For example, think about what the implications would be if a manufacturer decides to do key storage for their device on a local unsecured PC, on a network accessible drive, as they download their spam ridden email.

Since the specification does not have this type of requirement built in, manufacturers are going to implement this functionality in different ways. The implication is that those manufacturers will implement this without a necessarily unified view of Bluetooth security in their implementation. The security of these keys, ultimately, determines the security of the Bluetooth enabled device, which must be considered as a serious matter with regards to Bluetooth.

3.4.5.2 When Discovering Devices, Show Real Designations.

When auto discovering devices are nearby, the distinguishing information shown to the user is minimal. Usually a designation of the phone information is shown, as many users never customize their device name. Even in the case where a device name is customized, that same device name can be spoofed as the initiator attempts to pair with that device [32].

Instead, connectable devices should be shown and should have a unique ID appended onto the end of the generalized identifier. If two devices appear and have the same or significantly similar unique identifier, neither should appear, nor be connectable. This way, device names can't be spoofed preventing unauthorized access to the telephones.

3.4.5.3 Add an Application Level DMZ

Manufacturers are allowed to define behavior past the transport layer with regard to functionality with applications. This can lead to unwanted access to data and information by devices connected via Bluetooth. As a response to that, an in depth specification should be researched to define a DMZ for applications and data which are shareable and those which aren't for each device. This specification would allow users to very specifically point out the information that they don't mind sharing, and should shield the rest of the system from items that are brought in via Bluetooth as well.

3.5 Other Related Research & Future Work

As technology advances, applications improve as well and Bluetooth technology is no exception. Nonetheless, vulnerabilities have always been a security concern in the industry. Being wireless, Bluetooth is potentially vulnerable to many attacks, because it is very difficult to prevent Bluetooth signals from leaking outside the desired boundaries. However, the security of the whole system relies on the user choice of a secret Personal Identification Number

(PIN) - which is often much too short [8]. There have been numerous studies about Bluetooth vulnerabilities, and the different ways that these devices can be hacked into.

3.5.1 Cracking the Bluetooth PIN

An article that was written on Bluetooth vulnerability techniques stated that two security researchers found a method for taking control of Bluetooth-enabled mobile phones, even when the handsets have security features switched on. This is a practical implementation of a technique described by Ollie Whitehouse, which allows an attacker with specialized equipment to connect to a Bluetooth handset without authorization. The possible wireless attack starts with the ability to eavesdrop on the data transferred during the communication of two devices, and ends with the ability to fully impersonate other devices. Once the connection is established, the attacker could make calls on the target's handset, siphon off data, or listen in on data transfers between the device and a PC. They have demonstrated that a 4-digit PIN can be cracked in less than 0.3 second on an old Pentium III 450 MHz computer and in 0.06 second on a Pentium IV 3GHz HT computer [8]. As a result, security firms have recommended to financial traders that they should avoid the usage of the Bluetooth handsets.

3.5.2 'Sniffs' Vulnerability in Bluetooth Devices

A student at the University of Southern California has developed the BlueSniper rifle, a tool that looks like a big gun which can "attack" wireless devices from more than a mile away. This raises a bold statement, "If you've used your cell phone today -- or any other wireless device that uses Bluetooth technology -- someone could be watching you." [9] Luckily, the founder's purpose is to only use it for determining security vulnerabilities, not to actually hack wireless devices to obtain personal information. However, that doesn't guarantee that the rifle can't fall into the wrong hands.

The Bluetooth Special Interest Group says that no security holes have been discovered in the Bluetooth specification itself, however, the vulnerabilities comes from the implementation of the Bluetooth devices much like the internet to a PC vulnerability[9].

3.5.3 Case Study on Bluetooth Vulnerabilities in Mobile Devices

This paper discusses security vulnerabilities and privacy issues inherent in the use of Bluetooth devices. This case study was conducted by the faculties of engineering at the University of Ulster in Derry, Northern Ireland that looked at a five day period during a teaching semester. Over the five day period, there were over 340 Bluetooth devices detected. Specific manufacturers and models using only default Bluetooth friendly names; and ten were found to be vulnerable to Bluesnarf or Bluebug attacks. The specific manufacturer detected devices are broken down as such: 30% were Sony Erickson, 60% were Nokia, and 10% were Motorola. [12]

3.5.4 Bluetooth Vulnerability Future Work

Little can be implemented on Bluetooth devices to eliminate the inherent vulnerability that the devices possess. What can be done is to educate the users of its vulnerabilities and advise them of preventive measures. Some manufacturers like Nokia, and Sony Erickson, advise users to set their Bluetooth devices to "undiscoverable" or to simply turn the Bluetooth functionality off as a preemptive measure. Nokia stated they will not be releasing a fix for vulnerable devices as potential attacks are limited, and not expected to be a regular occurrence. Sony Erickson advised their customers to upgrade their phones through the Sony Erickson service center [12].

In the short term this problem may continue to be an issue. The problem of user tracking is more complex and it is not clear how this issue could be resolved given that unique and invariant Bluetooth addresses are the fundamental prerequisite for establishing device connection. It comes down to a tradeoff between the potential sacrifice of personal freedom, and the flexibility and functionality offered by Bluetooth technology [12]. In the future, Blueprinting may be used to increase the percentage of device models which can be identified. The idea is similar to IP fingerprinting techniques as used in tools like nmap, where it is possible to determine a host's operating system by specific behaviors of the IP stack. With Blueprinting, it is possible to determine the manufacturer, the device model, and the firmware version of the respective device. In order to communicate security issues to the respective manufacturers, it is important to know about the properties of the concerned device [13]. Blueprinting can contribute positively to the efforts to make Bluetooth devices more secure.

4. Recommendations/Conclusion

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.

Removing the users' need to generate a passkey, and instead putting passkey generation into the application layer specification would force Bluetooth device manufacturers to standardize this process Not only would this enhancement reduce or eliminate passkey spoofing, it gives users the peace of mind that the devices they pair with are using the same level of security as their own devices. Additionally, there is no procedural impact to the user. This approach should not be considered without providing some level of encryption for passing the passkey, as plain text can be intercepted even if the application is generating the passkey. Mandatory encryption, together with automated passkey generation, could be successful in deterring a Bluesnarfing or Bluebugging attack. These attacks both require a malicious user to gain access to one's Bluetooth device, namely, via interception of the plain text passkey.

Further security measures can be implemented at the network level to hide data behind a DMZ. By limiting access to data, predators would have limited capabilities even with a Bluebugging or Bluesnarfing attack, because very little or no data would be accessible without the user's express desire to expose that information to others. However, this would require a lot of user involvement; requiring them to identify each piece of data they would like exposed to other devices, and may deter users who are not technically savvy.

In conclusion, 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. After having compiled information on the current Bluetooth security threats for this research project, most group members felt uncomfortable in the George Mason University Johnson Student Center setting their mobile phones and PDA's to Discoverable mode, even if just for a short time.

5. References

[1] What is Bluetooth? 2000. Rad Data Communications. <http://www.pulsewan.com/data101/bluetooth_basics.htm>

[2] Bluetooth Protocol and Security Architecture Review. April 20, 2000. Korak Dasgupta <http://www.cs.utk.edu/~dasgupta/bluetooth/>

[3] The Comprehensive Guide to Everything Bluetooth. 2008 SP Commerce LLC. <http://www.bluetomorrow.com>

[4] Bluetooth.com. Bluetooth Special Interest Group (SIG). Wireless Security. Copyright© 2008 Bluetooth SIG.
<http://www.bluetooth.com/Bluetooth/>
<http://www.bluetooth.com/Bluetooth/SIG>
<http://www.bluetooth.com/Bluetooth/Technology/Works/Security/>

[5] Essential Bluetooth Hacking Tools, May 27. 2007 <http://www.security-hacks.com/2007/05/25/essential-bluetooth-hacking-tools>

[6] A Menu of Bluetooth Attacks, May 7, 2005. Carlos A. Soto.
<http://www.gcn.com/print/24_20/36437-1.html>

[7] "Phone Pirates In Seek and Steal Mission". Cambridge News, Royston & Saffron Walden. August 18, 2005. <http://www.cambridge-news.co.uk/cn_news_royston/displayarticle.asp?id=209574>

[8] Cracking the Bluetooth PIN. Avishai Wool. May 02, 2005. <http://www.eng.tau.ac.il/~yash/shaked-wool-mobisys05/>

[9] Cheung, Humphrey. "'Rifle' Sniffs Out Vulnerability in Bluetooth Devices." NPR 13 April 2005. <http://www.npr.org/templates/story/story.php?storyId=4599106>

[10] The Bluejacking, Bluesnarfing, Bluebugging Blues: Bluetooth Faces Perception of Vulnerability. Legg, Gary. 04 August 2005. <http://www.wirelessnetdesignline.com/showArticle.jhtml?articleID=192200279>

[11] Haataja, MJ Keijo, "Detailed descriptions of new proof-of-concept Bluetooth security analysis tools and new security attacks", REPORT B/2005/1, University of Kuopio, Kuopio FINLAND

[12] Solon AJ, Callaghan MJ, Harkins J, and McGrinnity TM, "Case Study on the Bluetooth Vulnerabilities in Mobile Devices", IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.4, April 2006

[13] Herfurt, Martin and Mulliner, Collin, "Blueprinting – Remote Device Identification based on Bluetooth Fingerprinting Techniques", White Paper (version3), December 20, 2004.

[14] "Perspective: Bye-bye, Bluetooth". CNET News.com, J. William Gurley. August 13, 2001. <http://news.cnet.com/2010-1071-281535.html>

[15] "IEEE 802.15 WPAN Task Group 1 (TG1)". IEEE 802, Copyright© 2003, IEEE. <http://www.ieee802.org/15/pub/TG1.html>

[16] IEEE Wireless Standards Zone, Copyright © 2008 IEEE <http://standards.ieee.org/wireless/> <http://standards.ieee.org/wireless/overview.html#802.15>

[17] "Serious flaws in Bluetooth security lead to disclosure of personal data." The Bunker, Copyright (c) 2003, 2004; Adam Laurie, Ben Laurie, all rights reserved. Last updated 14th October, 2004 <http://www.thebunker.net/resources/bluetooth>

[18] "Bluetooth History". Bluelon, Copyright© 2002-2007 Bluelon, Nattergalevej 6, DK-2400 Copenhagen NV, Denmark. <http://www.bluelon.com/index.php?id=411>

[19] "Introducing Bluetooth". The Wireless Directory, Copyright © 2001-2003 WTIS Ltd, Wireless Telecommunications Information & Services. <http://www.thewirelessdirectory.com/Scripts/Downloads/Bluetooth%20End%20to%20End.pdf>

[20] "Brief history of Bluetooth Technology". University of Denver, Catherine Ferguson. July 19, 2005. <http://mysite.du.edu/~ccfergus/bluetoothweb/history.htm>

[21] "Sony's 'TransferJet' to take on Bluetooth 3.0". ARS Technica, News Desk. Nate Anderson. January 07, 2008. <http://arstechnica.com/news.ars/post/20080107-sonys-transferjet-to-take-on-bluetooth.html>

[22] "With UWB uptake slow, Bluetooth hops on Wi-Fi". EETIMES, Rick Merritt. February 11, 2008. Copyright © 2008 TechInsights, a Division of United Business Media Limited. All rights reserved. <http://www.eetimes.com/news/latest/showArticle.jhtml?articleID=206401864>

[23] Nathan J. Muller, Bluetooth Demystified, New York, McGraw Hill, 2001, pp. 1-308

[24] Christian Gehrmann, Joakim Persson, Ben Smeets, Bluetooth Security, Boston, Artech House, 2001, pp. 3-182

[25] Specification of the Bluetooth System Volume 0, Covered Core Package Version 2.1 +EDR, 07/26/2007, http://www.bluetooth.com/

[26] Bluetooth Security Review, Part 1, Security Focus, Marek Bialogowy, 2005-04-25, <http://www.securityfocus.com/infocus/1830>

[27] Hacking Bluetooth, Government Computer News, Carlos A. Soto, 07/25/05, <http://www.gcn.com/print/24_20/36432-1.html>

[28] New Hack Cracks "secure" Blutooth Devices, Newscientest.com, 06/3/05, <http://www.newscientist.com/article.ns?id=dn7461>

[29] Red Fang "Bluetooth hack" not much use, newswireless.net, Guy Kewney, 09/10/2003, <http://www.newswireless.net/index.cfm/article/924>

[30] The Bluetooth Car, Bill Howard, 01/30/2004, <http://www.pcmag.com/article2/0,1759,1473715,00.asp>

[31] Bluetooth, Wikipedia, 06/30/2008, <http://en.wikipedia.org/wiki/Bluetooth>

[32] "Security of Wireless Technologies: 802.11 Wireless LAN and IEEE 802.15 Bluetooth", Michael Spence, Nikesh Patel, Anish Patel, Daniel Layden, Andrew Hinton, Derek Bartram, 7/12/2008, <http://www.cs.bham.ac.uk/~mdr/teaching/modules04/security/students/SS1A-wireless.pdf>