

# Bluetooth Security Issues, Threats And Consequences

Ajay Sharma

USIT, Guru Gobind Singh Indraprastha University, Delhi

hotajay@gmail.com

*Abstract- Bluetooth is an open industry standard for the unlicensed short-range radio communication of voice and data between IT devices, eliminating any need for wires and cables and permitting ad hoc networking. it was thought that this type of networking will be the most secure in all but is it secure, through this paper we try to highlight the key areas of security architecture and also present a analysis of various threats and vulnerabilities present today which lead to spread of viruses and Trojans and also allow hacker to gain an insight into the so called secure network..*

## INTRODUCTION

Unlike 802.11, Bluetooth is a technology that operates solely in ad hoc networks. Infrastructure mode is absent from Bluetooth discussions, as are long ranges among stations. Interestingly, Bluetooth gets its name from a Danish Viking king named Blatand, who was king of Denmark around the late 900s. He was responsible for Christianizing Denmark and uniting it with part of Norway. His name indicates nothing about the technology but rather signifies the importance of countries in this region of the world in the wireless industry. In 1998, a little more than one thousand years after his death, five companies, following Ericsson's lead, founded the Bluetooth consortium. These companies, including Intel, IBM, Nokia, and Toshiba, directed the development of Bluetooth specifications with the intention of Bluetooth's being a low-cost wireless transmission standard. Many more companies joined what is now termed the Bluetooth Special Interest Group (SIG); the membership totals around 1,000.

Bluetooth is a de facto standard, as well as a specification for small-form factor, low-cost, short-range radio links among devices. The Bluetooth SIG drives the development of the technology and is attempting to push it to the general telecom, networking, and computer industry markets.

The Bluetooth SIG goal is to integrate Bluetooth in everyday devices, not just cell phones and laptops. SIG operates under the premise that adding Bluetooth technology to a device should increase its cost by only \$5 or so. Bluetooth should be capable of functioning in such basic implements as a pen and such complicated devices as a computer or PDA. Bluetooth spares expensive wiring and infrastructure costs but does require stations to be within close proximity of one another to communicate. It enables devices to interoperate with an approximate range of 10 meters. The Bluetooth SIG members intend for Bluetooth to be the dominant technology for connecting all consumer electronic devices. They envision the use of Bluetooth to connect a cordless handset to its phone, a peripheral to a computer, a PDA to a computer, two PDAs to each other, or perhaps even a remote control to a TV via a computer.

In general, devices similar to Bluetooth, which use infrared (IR) as a transmission medium, are reliable, and building the technology into a device requires little cost. These devices do, however, require a line of sight between them, which significantly limits their versatility. Bluetooth itself does not

have this same line of sight restriction because it operates over radio instead of light, like other IR-capable devices. Security A however, require a line of sight between them, which significantly *architechure*

The general architecture is shown in Figure 1. The key component is a security manager with the following tasks:

- Store security-related information on services
- Store security-related information on devices
- Answer access requests by protocol implementations or applications (access granted or refused)
- Enforce authentication and/or encryption before connecting to the application.
- Initiate or process input from an ESCE (“External Security Control Entity.”) to set-up trusted relationships on device level.
- Initiate pairing and query PIN entry by the user. PIN entry might also be done by an application.

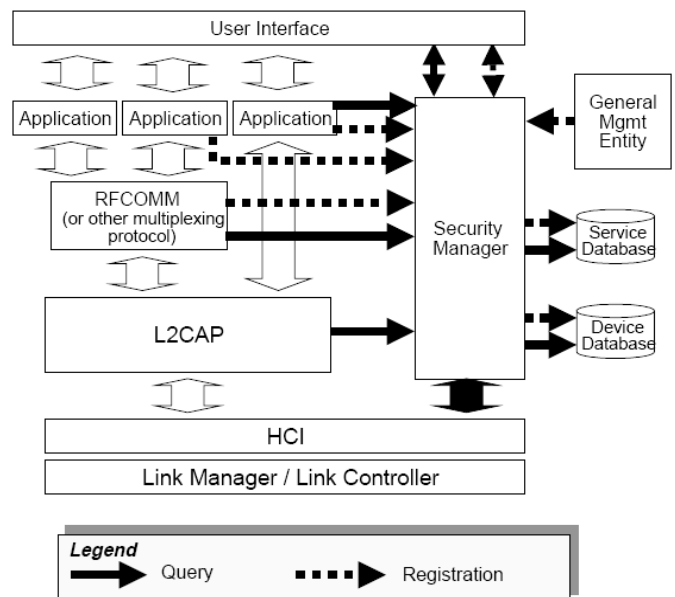


Figure 1: Security Architecture

Three security modes are possible under the instruction of the Generic Access Protocol:

- Security Mode 1. Non-secure. The device does not automatically initiate any security procedures.
- Security Mode 2. Service-level enforced security. The device does not automatically initiate security procedures before the L2CAP layer establishes a channel. This level facilitates ease of interaction with applications that have varied security requirements.

· Security Mode 3. Link-level enforced security. The device initiates security procedures before the link is established at the LMP level.

### *Bluetooth Vulnerabilities*

Having gone through the architecture of security in case of Bluetooth one can feel that he or she is the most secure person on the earth while using Bluetooth but that's not true let's look at the vulnerability issues in case of Bluetooth:

- 1) Encryption is not mandatory
- 2) Insecure default settings are not ruled out.
- 3) Weak PINs can be guessed.
- 4) Unit keys are insecure
- 5) Weak protection of integrity
- 6) Quality of the random number generator.

Now by seeing these vulnerabilities how many of you start thinking that why we have chosen the same PIN for connecting to each and every other device.

The following additional aspects should also be considered:

- 1) Mobile devices are exposed to a higher risk of theft than stationary devices.
- 2) All that is needed to use a Bluetooth device is for the device to authenticate itself; normally the user does not have to authenticate himself to the device. When a mobile , paired devices go missing, unauthorized third parties will thus normally be able to use them immediately.
- 3) Bluetooth device addresses can be manipulated with suitable equipment (flash memory).
- 4) Again, in ad hoc networks there exists a danger that computer viruses and Trojan horses could spread.

### *Bluetooth Threats*

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

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

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

### D. Virus: METAL Gear.a for Series 60

Dec 21 2004: Another new security notice for Series 60 owners--avoid a file claiming to be the game Metal Gear Solid with the file name METAL Gear.sis. According to security firm SimWorks, the virus looks for and then disables anti virus software. The METAL Gear trojan uses the same icon disabling technique pioneered by the recent Skulls trojan, this time to disable specific anti-virus and file browsing applications. Once on your phone, the METAL Gear trojan will install a version of the Cabir virus. Another file called SEXXY.sis is spread via Bluetooth to all phones in the area--this file in turn disables the Symbian application selection button on the target phone.

E. Bluetooth trojan leaves mobile users out of pocket \$5 charge for leaving your phone open to attack

"The trojan gets your phone to send an SMS to a premium rate number and then sends an authority that they can charge you without you knowing about it," said Richard Hales, country manager for UK and Ireland at F-Secure.

F-Secure warned that users are still leaving their mobile devices and laptops open to attack by using unsecured Bluetooth connections, despite the company's warnings at trade shows such as CeBIT. The security firm's honeytrap system at Infosec picked up 1,142 open Bluetooth products in the first three hours of the security show, and had 183 devices in range as it was demonstrated to vnunet.com. Hales said that the new attack is similar to the CommWarrior mobile virus which originally spread itself over mobiles without causing anything more than a higher bill for sending itself to contact via MMS as well as Bluetooth.

User ignorance is still the main reason for the spread of CommWarrior type viruses, according to F-Secure. "If someone's phone is infected with CommWarrior, all of these phones in range would be getting a message saying: 'Install CommWarrior, yes or no?'," said Hales.

"If you say no it immediately pops the message back up again if you're still within range. So you press no, no, no, oh for goodness sake, yes."

F. Cabir virus: is the first verified example. The virus was created by a group from the Czech Republic and Slovakia called 29a, who sent it to a number of security software companies, including Symantec in the United States and Kaspersky Lab in Russia. Cabir is considered a "proof of

concept" virus, because it proves that a virus can be written for mobile phones, something that was once doubted.

Cabir was developed for mobile phones running the Symbian and Series 60 software, and using Bluetooth. The virus searches within Bluetooth's range (about 30 meters) for mobile phones running in discoverable mode and sends itself, disguised as a security file, to any vulnerable devices. The virus only becomes active if the recipient accepts the file and then installs it. Once installed, the virus displays the word "Caribe" on the device's display. Each time an infected phone is turned on, the virus launches itself and scans the area for other devices to send itself to. The scanning process is likely to drain the phone's batteries. Cabir can be thought of as a hybrid virus/worm: its mode of distribution qualifies it as a network worm, but it requires user interaction like a traditional virus.

G. Gavno. a virus disables calls on Symbian phones Jan 24 2005

Symbian security firm SimWorks has sounded the warning for a new mobile phone virus, Gavno.a. Gavno.a is the first mobile virus to cause serious damage--Gavno leaves Symbian 7 handsets unable to make calls. The threat, Gavno.a is spread via a file called patch.sis and induces mobile phone users to install it on their devices by masquerading as a patch for their phone, a concept familiar to mobile phone users from other computing platforms such as Microsoft Window

Gavno affects Series 60 phones using Symbian OS v7 such as the Nokia 6600 and 7610, not popular models like the Nokia 3650 that use Symbian 6.

H. Symantec warns of three new Symbian Trojans Jan 20 2006

Symantec has issued an alert over three new trojan horse applications for Symbian powered phones. These will affect Nokia's S60 line of Smartphones. The trojans are being called: SymbOS.Bootton.E, SymbOS.Pbstealer.D and SymbOS.Sendtool.A. To be affected you will have to install an application, so use general precautions before installing software on your phone (e.g. know who it's from). Filenames to watch out for include: Fspreader.SIS, ChattingYuk.SIS, PBCompressor.SIS and Restart.S60.SIS.

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

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

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

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

#### *SECURITY TIPS*

- Enable Bluetooth only when you need it.
- Keep the device in non-discoverable (hidden) mode.
- Use long and difficult to guess PIN key when pairing the device (key such as 12 is unacceptable).
- Reject all unexpected pairing requests.
- Update your mobile phone firmware to a latest version,
- Enable encryption when establishing BT connection to your PC.
- Update your mobile antivirus time to time to keep pace with the new emerging viruses and Trojans.

#### *CONCLUSION:*

Bluetooth wireless is constantly growing in popularity because of the convenience of exchanging information between mobile devices. As Bluetooth usage rises, so do the security risks associated with the technology. While Bluetooth technology itself is relatively secure, the problems mentioned in this paper are primarily to do with various implementations by software developers and phone manufacturers. However, with the improvements in security we will also see improvements in hacker knowledge of Bluetooth security. New attacks affecting both old and new Bluetooth specification will undoubtedly emerge. In general, the risk of security incident while using Bluetooth technology can still be considered low, as long as users are following the simple Bluetooth security tips as listed in the paper.

#### *REFERENCES:*

- 1) Bialoglowy, Marek. 2005. Bluetooth Security Review, Part 1. Security Focus.
- 2) Bialoglowy, Marek. 2005. Bluetooth Security Review, Part 2. Security Focus.
- 3) Haataja, Keijo M.J. 2006. Security in Bluetooth, WLAN and IrDA: a comparison.
- 4) Korzeniowski, Paul. 2005. Bluetooth Security Threats Starting to Spread. TechNewsWorld.
- 5) Bluetooth SIG <http://www.bluetooth.com>
- 6) Research of trinite group - <http://trifinite.org>
- 7) Research of Ollie Whitehouse - <http://www.blackops.cn>