Analysis of Malicious Detection in Bluetooth Enabled Devices Exploiting Wireless Personal Area Networks

GJCST Computing Classification
D.4.6, K.6.5 & C.2.1

M.Latha[1] S.Arockiasamy[2]
1. Asst.Prof, Department of Computer Applications, SNR Sons College, Coimbatore.
Email:lathamurali@yahoo.com
2. Head, Department of Information Systems, University of Nizwa, Sultanate of Oman.
Email : arockia99@gmail.com

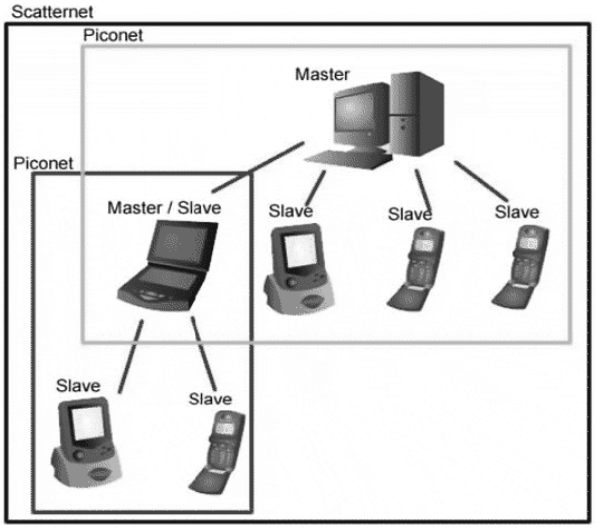
***Abstract*- The growing popularity of mobile devices (smart phones, handsets, PDAs) along with 3G technology brings the mobile internet services on these devices. The wireless devices with messaging capabilities attracted the malware writers to target the hand held devices. Even though the mobile device have numerous benefits like mobility, compact size and ease of their connectivity, the open nature increases the threats and risks being posed. The mobile viruses so far discovered exploited vulnerabilities in Bluetooth by infecting nearby devices and then propagate through SMS to other devices in the mobile network. The problem becomes worse with the growth of MMS (Multimedia Messaging Service), mobile game, and mobile commerce in near future. This paper investigates the propagation of mobile worms and viruses that spread primarily via SMS/MMS messages and short range radio interfaces – Bluetooth.**

Keywords- Bluetooth, Bluetooth Security, Mobile Threats, Radio frequency, and Worms.

I INTRODUCTION

A. *Bluetooth Architecture*

Bluetooth technology is a low cost and low power technology. It is primarily used in short-range radio frequency (RF) communication. It is a protocol used for connecting set of wireless devices, ranging from PDAs, Mobile phones, Notebook computers, Microwave ovens, Refrigerators etc,. The Bluetooth specification was developed by the Bluetooth Special Interest Group (SIG), an industry consortium founded by Ericsson, IBM, Intel, Nokia, and Toshiba. Bluetooth radio operates in the 2.4 GHz unlicensed ISM band (Industrial, Scientific, and Medical). Two or more devices sharing the same channel form a piconet. There is one master device and upto seven active slave devices in a piconet. The
devices can be in any one of the state action, shift, hold, and park. Multiple piconet with overlapping coverage areas form a scatter net. Bluetooth Network – piconet and scatter net is shown in figure1 [8].



The Bluetooth supports both point-to-point connection and point-to-multipoint connection. In point-to-multipoint connection, the channel is shared among several Bluetooth devices. The channel is divided into time slots, each 625µs in length where each slot corresponds to an RF hop frequency. The hop rate is 1600 hops/s, Bluetooth uses frequency hopping for low interference and fading, uses TDD (Time-Division-Duplex) scheme for full duplex transmission and transmits using GFSK (Gausian Frequency Shift Keying) modulation.

The protocol uses a combination of circuit and packet switching. Bluetooth protocol stack can support asynchronous connection-less (ACL) link for data and up to three simultaneous synchronous connection oriented (SCO) links for voice or a combination of asynchronous data and synchronous voice (DV packet type). There are Transport Protocol group, Middleware protocol group and Application group in the protocol stack. The Transport group protocols are used to manage physical and logical links with higher layer protocols and applications and allow Bluetooth device to locate each other. The Radio, Baseband, Link Manager, Logical link control and Adaption (L2CAP) layers and the Host controller and Interfaces (HCI) are included in the transport protocol group. Third party industry standard protocols and Bluetooth SIG developed protocols are included in middleware protocol group. Industry standard protocols include point-to-point, Internet protocols. TCP, WAP and Object Exchange Protocol, RFCOMM, Telephony

control signaling protocol and service discovery protocol comes under Bluetooth SIG developed protocols. The Bluetooth protocol stack is shown in Figure 2 [15]. The IEEE standard 802.15.1 standard for Bluetooth was published in 2002. The IEEE standard defines only the physical (PHY) and MAC (Medium Access Control) layer in its standards.[7]

B. *Device Discovery in Bluetooth*

In Bluetooth environment before a connection is established, device discovery procedure has to be performed before packets start flowing in the wireless links between the master and slave devices and vice versa. When a Bluetooth device wants to find other devices in its vicinity, it broadcast inquiry packets by hopping 3200 times per second along a 32-channel inquiry hopping sequence. A nearby device in the discoverable mode listens on the same frequency sequence but moves

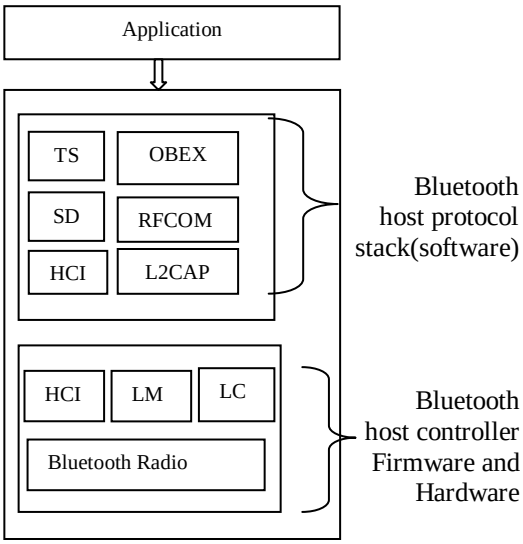


Figure 2: Bluetooth Protocol stack

forward its listening carrier every 1.28 seconds. When a device hears an inquiry packet it backs off for a random period of time and then reenters the scanning state. When it receives another inquiry packet, it responds with a frequency hop synchronization (FHS) packet. On the arrival of this packet, the inquirer device discovers the responders. Once a device has discovered its neighboring devices, it may want to establish a connection with one or more of them. In order to set up a Bluetooth link with a neighbor device, it goes through the paging process. This process is similar to the inquiry process, except that the paging device explicitly specifies the receivers address to indicate which device it wants to set up a connection with. After a connection is established, the pager device and the paged device are called the master and slave of the new link respectively. In the connected state, the master and the slave can exchange normal data packets by hopping 1,600 times per second along a 79-channel frequency sequence decided by the master's local clock and its device address. [12]

C. *Bluetooth Security*

Bluetooth provides security in three ways:

i. It uses pseudo-random frequency hoping to solve the problem of interference from other signals after transmitting or receiving a packet.
ii. Authentication to restrict connectivity to devices. Authentication is initiated when the device is in security mode 2 or in security mode 3.
iii. It uses encryption to employ secret keys, where only authorized users can make data intelligible again.

Frequency –hopping scheme

Bluetooth users use Frequency Hopping Spread Spectrum (FHSS) when transmitting signals. A channel is used for a very short period (e.g. 625μs for data/voice links) followed by a hop marked by a predetermined pseudo-random sequence to another. The frequency-hopping scheme enables the Bluetooth device to avoid interference with other devices. Bluetooth also allows for radio link power control, a low power consumption adaption output scheme, where devices can negotiate and adjust their radio link power consumption relative to the transmitted signal intensity. The combinations of a frequency hopping scheme and radio link power control provide Bluetooth with some additional protection from eavesdropping and malicious access. Spread spectrum transmission are less affected by outside signal interference since any noise interference is likely to affect only a small portion of the signal and not impact the entire signal.

Security Modes

All Bluetooth enabled device implement the Generic Access profile. The profile defines a security model that includes three security modes:

Security Mode 1

i. Mode 1 is as insecure mode of operation. It provides no security.
ii. When a Bluetooth device is in security mode 1, no security procedure is initiated.
iii. Device operating in this mode are able to pair with devices operating in the same mode because neither device implements security controls.

Security Mode 2

i. Mode 2 is known as service level enforced security, provides security at the service level after the channel has been established. This mode enables applications to run in parallel and have different access policies.
ii. When a Bluetooth device is in security mode 2 no security procedure is initiated before a channel establishment request has been received or a channel establishment procedure has been initiated by itself.
iii. Device operating in this mode enforce service level security at the L2CAP layer and above by involving authorization and authentication scheme.

Security Mode 3

i. Mode 3 known as link level enforced security provides security at the link level before the channel is established.
ii. Link encryption is enforced by devices operating in mode 3 at the LMP layer.[10]

II BACKGROUND STUDY

A. *Bluetooth Security Issues*

Bluetooth protocol is a PAN protocol used by devices that communicate wirelessly with one another within 300 feet. Bluetooth is designed to run in a peer-peer short-range wireless network. If the security of Bluetooth is compromised and if one or more devices in the network are used as gateways to other connected network, it could expose the devices or their attached networks. If the network is adhoc there is no access point, there is no centralized mechanism for security administration as there with a WAN where MAC address filtering and other security mechanisms are used to provide protection against rogue access.

Additional to this there are security concerns for Bluetooth mobile phones, where information stored on them such as the addresses and phone numbers of contacts, calendar information and Emails can be stolen. Blue bugging in a hacking technique that access the phone's commands, allowing the hacker to make phone calls, and delete contact information or eavesdrop on the phone owner's conversation. Cell phone worms take advantage of the Bluetooth technology to propagate to other Bluetooth devices.

Everyday more and more viruses and worms have been surfaced on the mobile devices. Bluetooth worms are significantly different from Internet worms in three ways. A Bluetooth enabled device controlled by the worm can only infect neighbors within its radio range. This differs from Internet worms that often scan the entire IP address space for susceptible victims. Second the bandwidth available to Bluetooth devices is much narrower that those of Internet links. Finally the mobility of Bluetooth worm is dynamic when compared with Internet worm. In future the attack on the Bluetooth enabled devices may be severer in the form of handset downtime, service description due to Denial of Service (DoS) attacks, physical damage in device hardware and theft of sensitive data on the device [3][4][5][6][9][11].

B. *Study On Mobile Malwares*

The earliest versions of malicious codes are harmless and they didn't spread from device to device. The recent malicious malwares are capable of spreading to nearby devices via Bluetooth and pose serious threats on enterprise networks. The Table.1 shows the classification of Malwares, its spreading mechanism, target platforms etc.[1][2][13][14][16][17][18].

III RESULTS AND ANALYSIS

This study focuses on the initial investigation of the Bluetooth worm's nature and its characters. The main difference between Blue tooth worm and the Internet worm is the mechanism adapted by the worms to infect the devices. The Blue tooth worm uses proximity scanning process to infect the nearby devices.

A simulation environment is setup with the basic RWP (Random Way Point) mobile model. It is a simple model in which an entity randomly selects a destination in the rectangle area. It moves straight from the current position towards the destination at a uniform speed. When it reaches the destination, it is idle for a period of time, which is again uniformly distributed. Once it enters into active state from idle state, it chooses another destination and the process repeats.

Cabir & Comwarrior are the most popular worms that affects Bluetooth enabled devices.Cabir replicates over Bluetooth connection and install its payload as Symbian System Installation file(SSI).It drains the power of infected phones and starts scanning for next Bluetooth devices for infection. Comwarrior spreads through the messages sent, in which the payload is attached. When it reaches a MMS enabled phones it randomly choose a phone number from the device address book and resets the infected device on the 1st hour of 14th of any month. After infecting a phone, it searches for nearby Bluetooth enabled devices for sending infected files.

The simulation window is set for 3600 seconds. The first worm is chosen randomly for a set of 200 devices and the infection starts at simulation time of 0 seconds. Fig.3 shows the Cabir worms attack ratio. With increase of time (seconds) the graph shows the increase of attack vector created by the Cabir worm. Fig.4 shows the Comwarrior attack ratio. With increase of time (seconds) the graph shows the increase of attack vector created by the Comwarrior worm.Fig.5 shows the average infection caused by the Cabir worm. The infection rate is higher or lower according to the number of Bluetooth enabled devices / applications that are within the affected device vicinity.Fig.6 show the average infection caused by the Comwarrior worm. The infection rate increases with time.

The simulation result shows the impact of Cabir worm and Comwarrior worm on Bluetooth enabled applications.

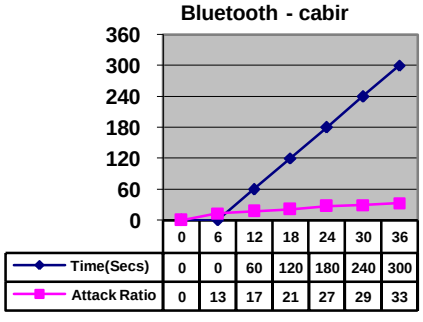


Figure 3. Attack Ratio

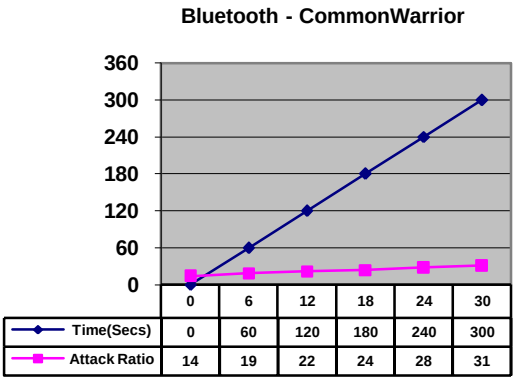


Figure 4. Attack Ratio

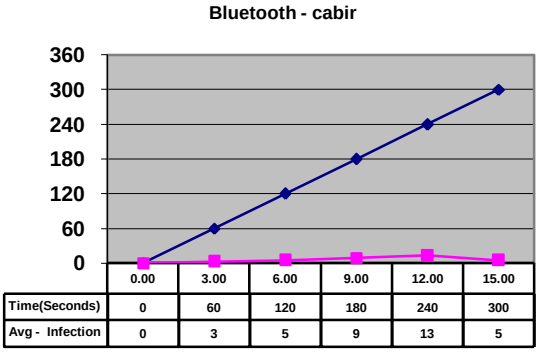


Figure 5. Avg – Infection

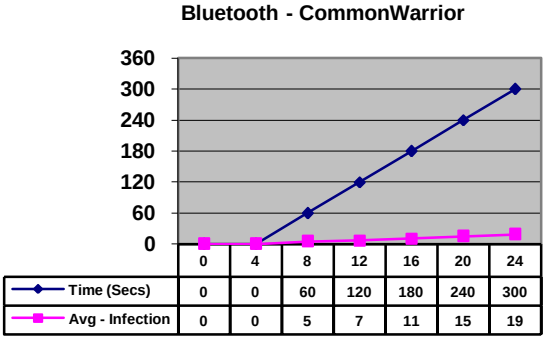


Figure 6. Avg – Infection

Table1. Year wise findings of Malwares in Bluetooth enabled devices

Year	Malware Type	Malware Name	Vulnerabilities
2000 [1]	Virus	Phage	Spreads from PDA to PDA if infected files are shared
2000 [1]	Worm	The Spanish Timophonica	It sends message to random GSM phone numbers via SMS gateway. It modifies MS outlook settings and device registry of an infected device. It also deletes CMOS memory and Master boot records of the device. It propagates through email.
2000 [1]	Worm	The Japanese 110	Affects .NIT DO CO MO i-mode mobile phones. Individual phone numbers in the address book can become victims of Dos attack.
2001 [1]	Virus	Liberty A	It affects hand held devices like palm PDAs, palm OS. To activate this virus it has to be manually installed. It deletes all applications and databases on palm OS-compatible device.
2004 [1]	Worm	Mabir	Spreads by selecting addresses of newly received MMS messages. It transmits MMS messages.
2004 - 2005 [1]	Worm	Cabir	Its variants replicate over Bluetooth connections and install the worm payload as a symbian system Installation (SSI) file.
2005 [1]	Worm / Virus	Lasco	It propagate by transferring its payload to any device in range. It combines the self replication of virus with the self propagation capability of worms.
2005 [1]	Worm	Commwarrior	Propagate by sending messages (along with the payload) to an MMS-enabled phone number randomly chosen from the compromised device's address book and resets the infected device on the first hour of 14th of any month.
2005 [1]	Trojan	Skulls	Propagates by sending both SMS and MMS messages and overwrites address books, e-mail viewer etc.
2005 [1]	Trojan	Drever	Propagates by prompting a user to install an update for symbian OS. Its primary damage is to disable symbian antivirus programs.
2005 [1]	Trojan	Locknut	It propagates like Lasco and overwrites ROM binaries and may crash the OS.
2005 [1]	Trojan	Cardblock	It attacks multimedia cards flash memory of mobile phones.
2005 [1]	Virus	WinCE.Duts	Protect Pc Virus infecting ARM based device. It appends itself to the executable files in the root folder and modifies the program execution leader.
2006 [1]	Virus	Crois over	Spreads from windows desktop PCs to mobile devices running on windows mobile pocket Pc.
2007 [16][17]	Worm	Cabir,I,cabir.H	Spread through specially formatted symbian OS distribution file distinguished as a security management utility. When the infected file, is launched the mobile phone's screen displays the word "velasco".
2008 [16][17]	Worm	Boselo.A	This worm is transmitted thru MMS users are deceived by the extension and unknowingly install the piece, the worm. A targets symbian s60-enabled/malicious device includes Nokia-6600, 6630, 6680, 7610, N70 and N72 handsets.
2009 [16][17]	Worm	Yxes.A	Gathers mobile phone nos and repeatedly send sms. The message feature a web malicious web address (URL) upon clicking of the address in the received message, the recipients will download a copy of the worm.

IV CONCLUSION & FUTURE WORK

The RWP model takes time (seconds) as a control parameter. It takes more time for propagation and less time for infection. The study of mobile virus / worms exploiting Bluetooth and messaging networks needs an enhanced model. Agent based Malware Model (AMM) is the most popular mobility model for analyzing the epidemic growth rate of Bluetooth worms. AMM focuses on the worm that spreads only with the help of human intervention. Further study has to be focused on the propagation speed and infection rate caused by the worms that spreads automatically in the Bluetooth network.

V REFERENCES

1) Abhijit Bose and Kang G. Shin, On Mobile viruses Exploiting messaging and Bluetooth services, IEEE, 2006.
2) Ahonen et al, Information security Threats and solutions in Mobile world, The service Developer perspective 2005, VTT, Espoo, VTT Research notes 2308.
3) Guanhua yan and S.Eidenbeny, "Bluetooth worms, Models, Dynamics, and Defense implications", proc. 22nd Ann. Computer security Applications conf (ACSAC) 2006.
4) Guanhua yan, L.Cuellar, S.Eidenbeng, H.D.Flores, N.Hengartner and V.Vu, "Bluetooth worm Mobility pattern Matters", Proc. Acm symp, Information, computer and communication, security (ASIACCS'07) Mar, 2007.
5) Guanhua yan and S.Eidenbeng, "Modeling propagation Dynamics of Bluetooth worms", Proc.27th IEEE, International conference Distributed computing systems (ICDCS'07) June 2007.
6) Guanhua yan and Stephan Eidenbenz, Modeling propagation dynamics of Bluetooth Worms (Extended version), IEEE, Mar 2009.
7) Guide to Bluetooth security (http://www.bluetooth.com/)
8) Jasonlam, Introduction to Bluetooth & J2ME, contributing writer, 2004
9) Jingsu, A.G.Miklas, K.K.W.Chan, K.PO, A.Akhavan, S.Saroiu, E.d.Lara and A.Goel, "A preliminary Investigation of worm Infections in a Bluetooth Environment", Proc.Fourth ACM workshop Recuring Malcode (WORM) 2006.
10) Marium Jalal Chaudhry, Sadia Murawwat, Farhat Saleemi, Sadaf Tariq, Maria Saleemi, Fatima Jalal chuadgry, "Power optimized secure. Bluetooth communication", IEEE 2008.
11) W.Mickens and B.D.Noble, "Modeling Epidermic Spreading in Mobile Environment", Proc.Fourth ACM Workshop wireless security (Wise'05) sept, 2005.
12) Rajeev sharey, Brent A.Miller, "The Bluetooth Technology: Merits and Limitations", IEEE, 2000.
13) PC QUEST, A CYBERMEDIA publications, January 2008
14) PC QUEST, A CYBERMEDIA publications, , July 2008.
15) Vincenzo Auletta, Carlo Blundo & Emiliano DeCristofaro,A J2ME transparent middleware to support HTTP connections over Bluetooth.
16) http:// www.F-secureu.com./2009
17) http:// www.mobiletor.com
18) http://www.microsoft.com/technet/secutity/altert/info/malware.mspx.