Scientific Research and Essays Vol. 6(30), pp. 6254-6261, 9 December, 2011
Available online at http://www.academicjournals.org/SRE
DOI: 10.5897/SRE10.1098
ISSN 1992-2248 ©2011 Academic Journals

*Full Length Research Paper*

# Direct attacks on mobile phones by bluetooth for forensic analysis

**Beatriz López Martínez, Marcos Arturo Rosales García, Gabriel Sánchez Pérez*, Gualberto Aguilar Torres and Linda Karina Toscano Medina**

Instituto Politécnico Nacional, Av. Santa Ana 1000, Col. San Francisco Culhuacan C.P. 04430, México City, USA.

Accepted 18 November, 2011

**Nowadays users demand sophisticated applications and services on their mobile phones since they have become a basic necessity for everyday life. The Symbian operating system has the features outlined earlier and provides a security and data protection module, besides it is one of the world market leader in mobile phones. The attacks described here were made through 'Bluetooth technology', and its importance lies in the ease of operation for any user, but this also represents risks and vulnerabilities that threaten the security mechanisms offered by different mobile phones. This research used direct attacks on Bluetooth communication to violate such mechanisms. The techniques used are well-known hacking practices like Bluejacking, Bluebug, Bluesnarfing and Blueprinting for Nokia GSM smartphones. The results show evidence that can be obtained from mobile phones which allows the forensic investigator to have solid basis to determine that an attack was successfully done and what kind of information was removed or copied from the mobile phone. The main purpose of this research is to provide forensic investigators with evidence to detect mobile phones violated by direct attacks using a methodology for forensic analysis based on NIST SP 800-86.**

**Key words:** Mobile, bluejacking, bluebug, blueprinting, bluesnarfing, forensics pairing, Symbian OS, bluetooth.

## INTRODUCTION

Nowadays, the mobile phone handset manufacturers are offering affordable and reliable data services in addition to their traditional voice services. They have to provide timely production of feature-rich, innovative and fashionable handsets to the mass market. Symbian OS is an advanced data-enabled operating system for mobile phones and is structured to ease the integration of hardware and software (Pavlaković, 2002). The architecture of a system is the vehicle through which its design goals are realized (Rodríguez, 2005). Architecture intelligence of mobile phone is based on three logical layers: a CPU core (Central Processing Unit), a SoC (system-on-chip) which contains the CPU core and other peripherals; all of them on a phone PCB (printed card board). Symbian OS is designed for the mobile phone environment. It addresses constraints of mobile phones by providing a framework to handle low memory process, a power management model, and a rich software layer implementing industry standards for communications, telephony and data rendering. Even with these abundant features, Symbian OS puts no constraints on the integration of other peripheral hardware. This flexibility allows handset manufacturers to pursue innovative and original designs (Pavlaković, 2002). However, there are also vulnerabilities on those operating systems, on the mobile devices by their own features. Part of the technology that supports Symbian OS is Bluetooth communication. Bluetooth technology is a short-range wireless communication. In this communication, a device pairing is necessary as a prerequisite for such *in-situ* device-to-device connectivity –the first time introduction and association between two devices, often without prior context. Such a connection must be set up before the two

*Corresponding author. E-mail: caaann@gmail.com, gasanchezp@ipn.mx. Tel: 91183664, 57296000, Ext: 73207.

phones can engage in an interaction like the above applications (Torres and Bernal, 2006). This paper focuses on identifying some registers from a forensic analysis made to a mobile phone safety device that has been attacked.

In a further research we intend to complete the data about digital evidence stored in a smart phone to determine the type of attack, the module violated, and what information was obtained, with different techniques, as well as the behavior on different systems operating speed to a digital forensics on mobile phones. However, it is also necessary to implement protection measures and to have skilled personal with the proper abilities to be able to recognize an attack on mobile phones for an efficient forensic investigation.

## MATERIALS AND METHODS

### Symbian OS

Symbian OS is a 32-bit, little-endian operating system (Pavlaković, 2002). It is the largest and most advanced operating system in the industry for next generation mobile phones. It was designed to meet the requirements of phones that support 2.5 and 3G, because it offers good performance in processing, multimedia, application services, communications and security. Symbian OS certainly aims at unequaled robustness, making strong guarantees about the integrity and safety of user data and the ability of the system to run without failure. From the beginning, it has also aimed to be easy and intuitive to use and fully driven by a graphical user interface (GUI) (Rodríguez, 2005). For a forensic investigation it is important to generate a certain level of confidence and have an ease of operation. The security features are:

1) Encapsulation of data by applications.
2) Using cryptographic algorithms such as DES, 3DES, RC2, RC4, RC5 and AES.
3) Support for IPsec and VPN clients.
4) Setting user permissions.
5) Persistence of data through and embedded SQL database.
6) Support of MIDP 2.0 (mobile information device profile).
7) Using secure protocols such as HTTPS, SSL and TLS.
8) Application monitoring capacity.

## VULNERABILITIES IN MOBILE PHONES

Here describes the major security failures “mutually exclusive” identified in the mobile devices according to Hoffman (2007).

### Malware

The malicious code is commonly called malware which is a portion of additional data joined to a program. By the time the user runs the program, it automatically loads additional code, infecting the device. Such attacks can be done via Bluetooth, MMS or Internet malware (Evans, 2010).

### Direct attacks

Direct attack is called when an intruder enters into the device and makes deliberate actions to make some damage (Sales, 2005).

One way to perform this attack is social engineering, through simple observation of the target; it suffices to identify the device when it has asset infringing services. With the aforementioned, the hacker determines the best exploit to use against that device. One of the methods used to locate devices is through the signals they emit such as Bluetooth which will be used to exemplify this type of attack in this paper. After locating the device and accessing it, the hacker can perform various actions that can break the stability of the device, such as delete, edit, upload data, change settings or use the device in an unauthorized manner.

### Interception of communication

A simple way to attack a device is doing it indirectly. Currently, there are a variety of devices that are able to connect to other devices or networks through many methods; it is during this process in which it may be violated and used for malicious purposes.

### Authentication attacks

The authentication process verifies the identity of a person that is trying to access. This method is present in a variety of systems, from e-mail access to the establishment of an Internet connection. The reason for this mechanism is simple: privacy. One of the main features of the information is confidentiality, which is, that only authorized personnel must know the information, so any unauthorized access to a mobile device may represent an attack authentication.

## ATTACKS ON MOBILE PHONE WITH SYMBIAN OS

There are two ways to perform an attack: protected and non protected form. Unprotected and protected (Evans, 2010), by the way it communicates in the exchange of data. In the first case, the devices do not require pairing, that is, that the communication is transparent to the user under attack; this attack was common at the onset of mobile phones in the market. Protected attack refers to spend a few levels of security, in addition to require pairing between devices, which imply that the user accepts the request victim incoming transmission. This document was used in a protected form. The attacks made through Bluejacking, BlueBug, BlueSnarfing, and BluePrinting, were chosen for their ease of reproduction and acquisition, as well as its development under J2ME (Java Micro Edition), platform that allows its implementation on Windows environments. Mobile phones attacked equipment manufacturers are Nokia (Jansen and Ayers, 2004) while the native operating system is Symbian.

### Bluejacking

Bluejacking is a spam attack similar to Bluetooth by which unsolicited messages are sent to nearby devices. Bluetooth pairing is a process by which two devices are able to send messages to each other (Evans, 2010). For forensic analysis purposes, the attack was simulated with the tool Bluejacking Super Bluetooth Hack. The process consisted in installing the tool, only in the attacking equipment, and then doing a search for active devices (with Bluetooth turned on). So, having located a device and setting the pairing (social engineering or without security), we proceed to obtain user data transparently (Figure 1).

### BlueBug

BlueBug exploits a vulnerability caused by a bug in the


**Figure 1.** Bluejacking, spam on mobile phone.

implementation of the Bluetooth stack of the memory through which you can connect to RFCOMM serial port of the mobile phone and send AT (attention telephone or attention terminal) commands. AT commands allow giving instructions to both mobile devices and ordinary landline telephones, to be executed in the GSM terminal. By exploiting this vulnerability, exploiting an attacker could make calls, get the address book and calls, access to the SMS service and set call forwarding (Dunham, 2009). This tool allows the attacker to create a serial connection with a cell phone via Bluetooth interface. With this type of connection, a variety of commands can be executed on the device. It is also possible among other things as reading text messages and intercepting calls (Moreno, 2006). To simulate this type of attack, the tool used was 1.0 of trifinite.groupBloover, which was introduced to read the address book, as well as some SMS messages, and add an entry to the phonebook (Bluehack, 2010). Figure 2 shows the unauthorized access to a device with Symbian OS (Nokia Xpress Music 5610), through the attack obtained of a Phonebook user, the change of the language settings, and making phone calls from the attacker (Figure 2).

**BlueSnarfing**

Bluesnarfing is the unauthorized access of data that typically occurs over a link between the system paring hacker and the target device. If the device is enabled to be viewed publicly or to allow pairing, Bluesnarfing is not possible. Bluetooth flow previously existed so it could be exploited for Bluesnarfing against declared private phones, but it is a vulnerability that has been repaired. You can make Bluesnarfing against non-active devices if you know its Bluetooth MAC address (Stewart, 2008). Bluesnarfing successful attacks against PDAs, cell phones, and notebooks have been able to extract the agenda, list of contacts, text messages, e-mails, images, videos and more. This technique is illegal in many countries because it represents data theft. The tool used to simulate this attack was BlueScanner Aruba Networks (Figure 3) installed in a computer, which shows the list of Bluetooth devices functioning, even if that service is down. Thus, it is possible to know the MAC address of the manufacturer, where the first three bytes are associated with the chip manufacturer and the last three identify the device. Figure 3 shows the interface of the BlueScanner with a list of all detected devices, with and without Bluetooth enabled.

**BluePrinting**

It is a technique aimed to obtain information from cell phones without additional connections and using it to determine the manufacturer, version, model, inter alia, through knowledge of the MAC address (Kumar, 2010) (Figure 3). The device identification is possible through the use of the database stored in BD_ADRR. The Bluetooth device address, BD_ADDR, is used to identify a Bluetooth enabled device. The list of services can be obtained from the SDP (service discovery protocol). The simulation of the attack was carried out with the tool BlueScanner. Figure 4 illustrates the identification of devices BlueScanner, their services and a brief description of their characteristics on Protocol SDP. So you can use


**Figure 2.** Getting an address book on a mobile phone with Symbian OS.

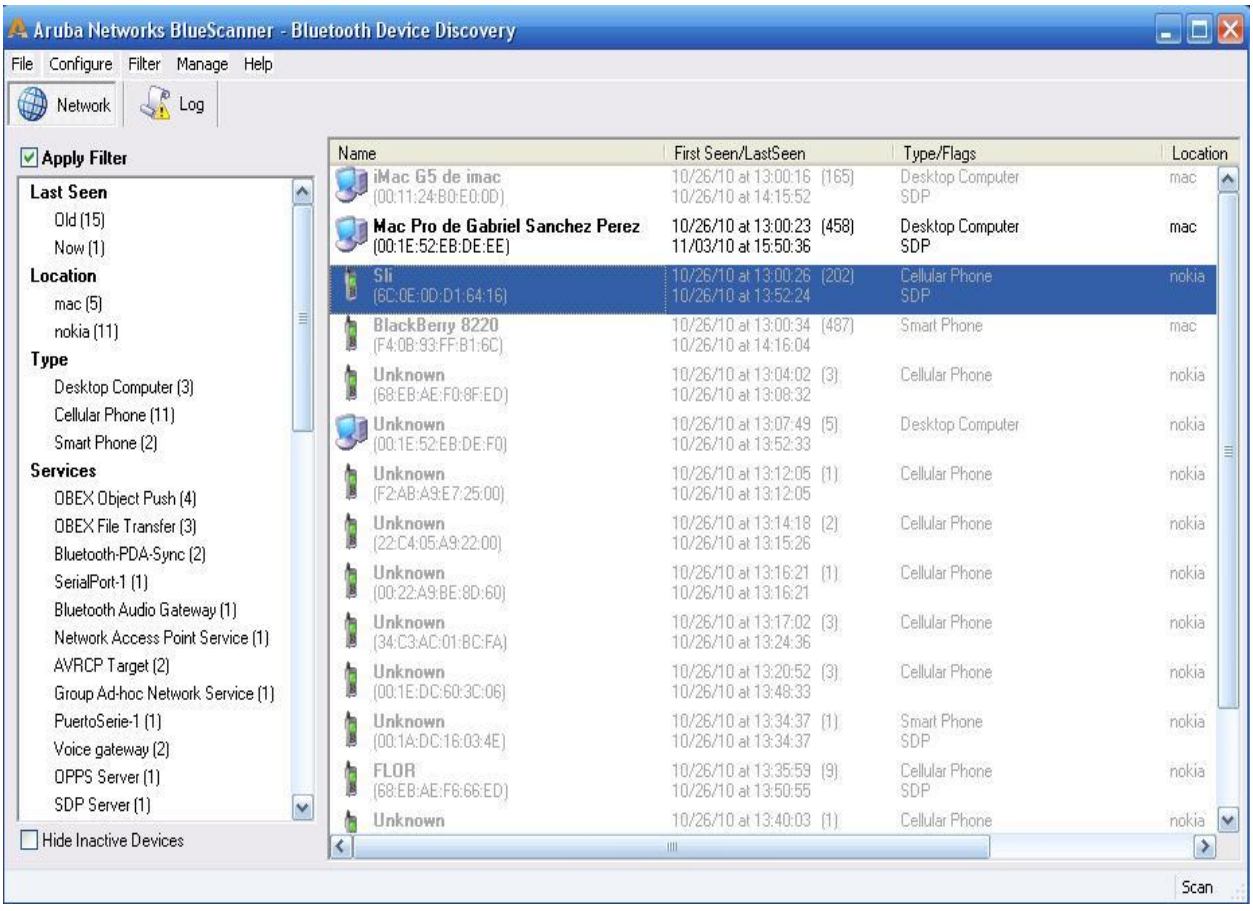


**Figure 3.** BlueScanner list from a nearby device with Bluetooth.

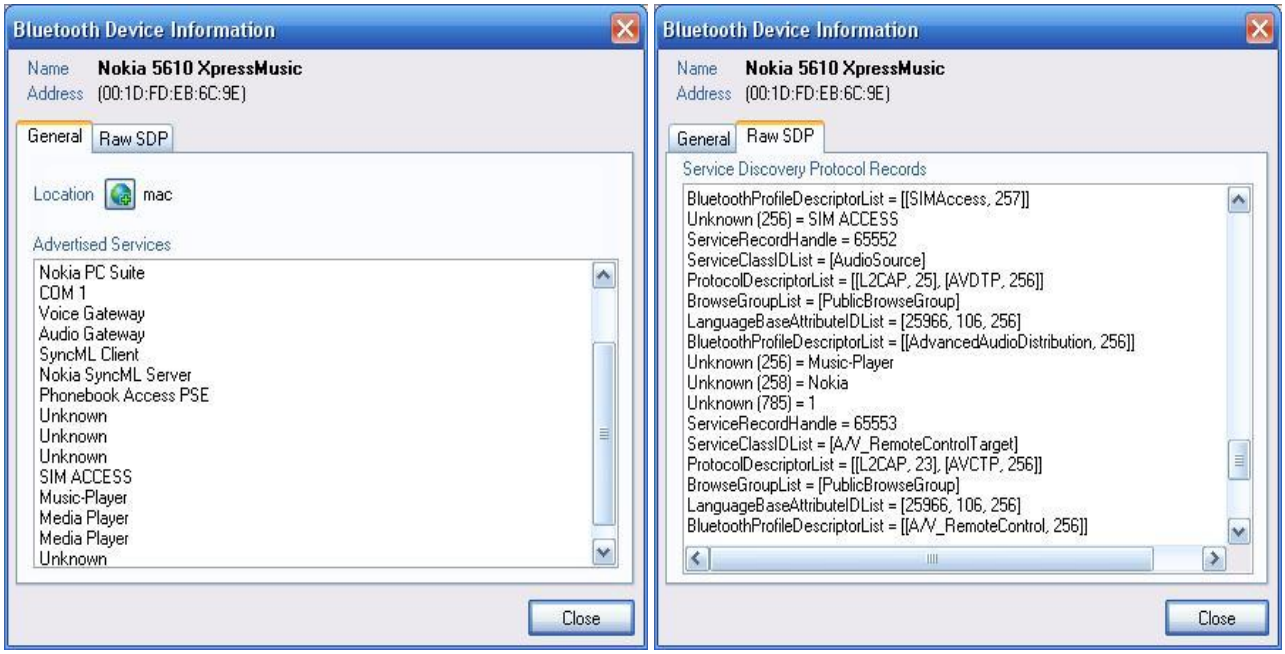


**Figure 4.** Identifing services on mobile phones with Bluetooth from BlueScanner.

that information to guide and refine certain types of attacks and known vulnerabilities (Arroyo, 2005).

## FORENSIC ANALYSIS

The forensic process is made in the following phases:

### Verification

During this stage, the forensic examiner called on duty takes a careful look at the information logged by the system, by the applications and by the network devices to be sure the incident effectively occurred. For this case study, in this phase analyses, the state of cell phones, watching their status and the active services is isolated to obtain their volatiles data (Figure 4).

### System description

Once the verification task is successfully completed and the security incident occurred, the forensic examiner has to fill in a detailed system description: the information ranges from the hardware and software system characteristics, the hard disks geometry (useful for the following media analysis phase), its utility, the list of users and other useful information. During this phase, a detailed report of the features of hardware and software of the mobile phone were obtained and accurately documented as shown in Table 1.

### Acquisition of evidence

All data from the mobile phone must be transferred to an external media or to a forensic workstation in order to perform the analysis tasks. This operation is critical because the examiner needs to be sure that only the original data is transferred and taken into account. In this case, the Paraben´s Device Seizure V. 4.0 for Windows platform is the perfect tool design for forensics motives, which lets us browse the phone's internal memory.

### Timeline analysis

This is a complete image file list associated with the MAC times info; it is very useful to trace back the system activity; (the timeline file prints out the last time an executable file was run, the last time a file or a directory were created/deleted and it could also prove the presence of scripting activity. This is shown in Figure 5.

### Device analysis

The toolset available to the forensic analyst depends on several variables:

i) The software platform used in the forensic workstation.
ii) The software platform used in the system target of the analysis.
iii) If the analysis has to be performed on a live system.
iv) The network configuration.

In this stage, the forensic analyst has to examine thoroughly the media layers [physical, data, metadata, file system (Nokia, 2009) and file name] searching for evidence of suspicious binary installations, files, and directories added, removed and so on. At this phase records found synchronization files (Nokia, 2010) (Figure 5).

### Search string

With this deep knowledge of the system, the analyst can now begin searching for specific strings contained inside files to reveal useful

**Table 1.** Features from the mobile phones used, supported by Bluetooth and Symbian OS.

| Phone | Operating system and data | Memory/battery | Network | Dimensions/weight/features |
|---|---|---|---|---|
| Nokia Xpress Music 5610 | Symbian OS 7.2.<br>GPRS: Class 10 (4 + 1/3 + 2 slots), 32 - 48 kbps.<br>EDGE: Class 10, 236.8 kbps.<br>3G: Yes, 384 kbps.<br>WLAN: No.<br>Bluetooth: Yes, v2.0 with A2DP.<br>Infrared port: No<br>USB: Yes, v2.0 microUSB. | Phonebook: 2000 entries, Photocall.<br>Call records: Yes.<br>Internal: 20 MB.<br>Card slot: microSD, up to 8 GB.<br>Standard battery, Li-Ion 900 mAh (BP-5M).<br>Stand by: Up to 320 h.<br>Talk-time: Up to 6 h. | 2G - GSM 850/ 900/1800/1900 .<br>3G - UMTS 850/2100.<br>UMTS 850/1900- American version. | 98.5 x 48.5 x 17 mm, 75 cc 111 g.<br>Messaging: SMS, MMS, e-mail, instant messaging.<br>Java: Yes, MIDP 2.0. |
| Nokia 6131 | Symbian OS.<br>GPRS: Class 10 (4 + 1/3 + 2 slots), 32 - 48 kbps.<br>EDGE: Class 10, 236.8 kbps.<br>3G: No.<br>WLAN: No.<br>Bluetooth: Yes, v2.0.<br>Infrared port: No.<br>USB: Yes, pop-port. | Phonebook: 1000 x 15 fields, Photo call.<br>Call records: 20 dialed, 20 received, 20 missed calls.<br>Standard battery, Li-Ion 820 mAh (BL-4C).<br>Stand by: Up to 240 h.<br>Talk-time: Up to 3 h 20 min. | 2G - GSM 850/900/1800/ 1900. | 92 x 48 x 20 mm 112 g.<br>Messaging: SMS, MMS, e-mail, instant messaging.<br>Java: Yes, MIDP 2.0. |

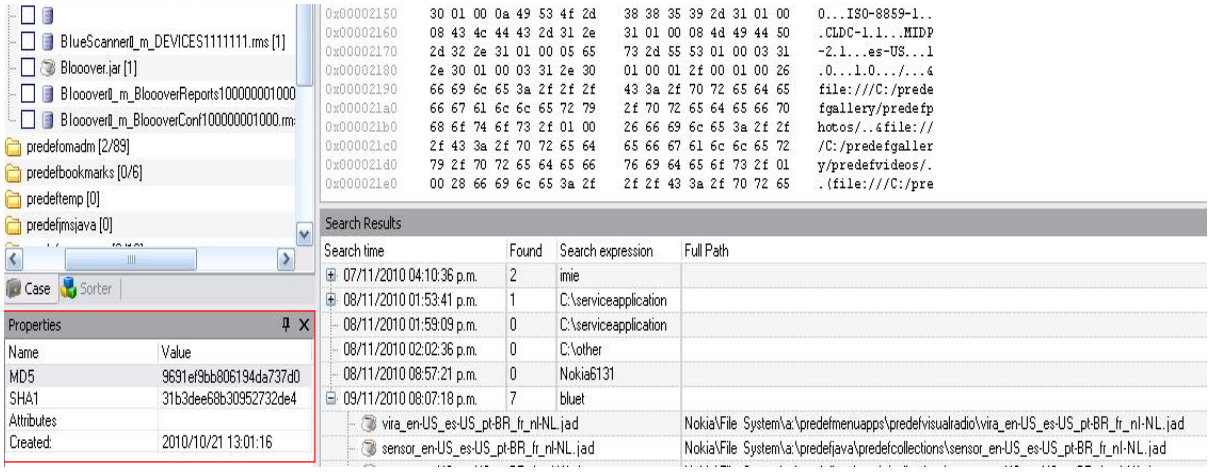


**Figure 5.** Timeline analysis.

information. A list of standard “dirty words” could be very useful to pull out relevant information about the compromise of the system. Figure 6 shows the search string with the word “blue”.

### Data recovery

The forensic examiner can take a thorough look at the media, extracting the unallocated data in order to recover any deleted files.

## RESULTS AND DISCUSSION

Table 2 shows the relationship between the mobile phone and the attacks. The attack route of the vulnerable telephones with BlueJacking and BlueBug was C:\OTHER in the memory telephone. The system file was Nokia 6131, all which is located in the file system of the

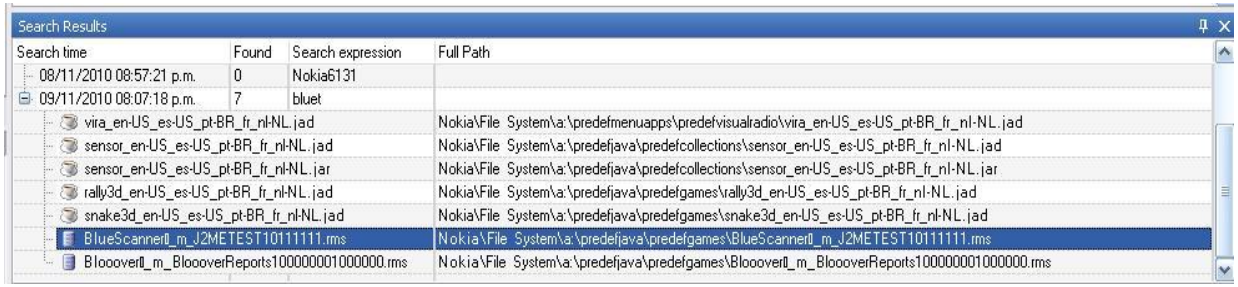


**Figure 6.** Strings search by word “blue”.

**Table 2.** The relationship between attacks and telephones.

| Mobile phone | Bluejacking | BlueSnarfing | BlueBug | BluePrinting |
|---|---|---|---|---|
| Xpress music 5610 | X | X | X | X |
| Nokia 6131 | X | X | X | X |
| Motorola WX295 | | X | | X |
| Blackberry 8220 | | X | | X |

**Table 3.** Comparison of the actions taken by each attack.

| Bluejacking | BlueBug | BlueSnarfing/BluePrinting |
|---|---|---|
| Access to the address book. | Access to the address book. | Scan mobile phones and PCs with Bluetooth on and off. |
| Read messages SMS from phone memory and SIM. | Read messages SMS from phone memory and SIM. | Get address MAC. |
| Send spam. | Add records to address book. | Get information on the services supported. |
| Add records to address book. | Set call forwarding. | Get information transmission from the protocol SDP. |

Symbian operative system. The path phones attacked and violated with Bluejacking and BlueBug were C:\OTHER in the phone memory and the file Nokia 6131 in the file system of the Symbian OS. The record of the attacks detected are synchronization and Java applications:

a) Nokia\Filesystem\a:\predefsyncml\

b) Nokia\Filesystem\a:\predefjav

Only the mobile phone with Symbian OS was analyzed; the others were auxiliary to attacks. From design, Bluetooth technology presents vulnerabilities as the separation of the protocol stack of a security policy suggested, since in the absence of a rule defining how and when to transmit certain protocol we can find faults, and it is presented as a failure, the ability to support any compatible software, leading to support multiple applications for malicious purposes as exemplified in this document. Table 3 shows a comparison of the actions taken by each attack.

## Conclusions

Bluejacking, Bluebug, Bluerpinting and Bluesnarfer are an example of the kind of attacks that can be performed under simple J2ME and Bluetooth devices scan on. The path infringed is C:\OTHER file and Nokia 6131, Nokia 5610, respectively, used mobile phones Symbian OS. There are paths that contain information related to an attack or intrusion scanning performed by those who hold information about the J2ME platform the file system of Symbian OS, Fylesystem \ a: \ predefsyncml and information relating to the timing of equipment, Nokia \ Fylesystem \ a: \ predefjava \ predefgames. It is possible to notice that both attacks, Bluejacking and Bluebug offer high probabilities of success because it is easy to obtain information from the main attacked user, and because there are J2ME applications that left visible records with regard to support of this platform applications (predefjava). The execution of techniques as BlueSnarfing and Blueprinting require a more skillful analysis for the interpretation of the data, but they are useful enough to identify the target attack, returning information from the mobile phone features. The records left by these tools to run are located in the path of the file system regarding the timing that should exist between the mobile communications Bluetooth (predefsyncml).

### REFERENCES


Pavlaković Z (2002). “Symbian Operating System for Mobile Phones.” Online: http:// hrcak.srce.hr/file/10154/ atm3_4_02_pavlakovic_168_kraj.pdf. Last consulted: June 30, 2010.

Rodríguez J (2005). Operating Systems in the Belt. UNAM, DGSCA, 4(38): 9-17.

Torres J, Bernal A (2006). “Implementation of Network Topology Bluetooth Devices Capable of Accessing the Internet through a LAN.” Av. Sist Inf., 3(2): 37-41.

Hoffman D (2007). Blackjacking: Security Threats to Blackberry Devices, PDAs, and Cells Phones in the Enterprise. Wiley Pub., 115-204.

Evans J (2010). “Hacking Practical Protection, Mobile Malware – The New Cyber Threat.” IT Security Magazine, 5(8): 1733-1786.

Sales J (2005). Symbian OS internals, Real Time Kernel Programming. John Wiley & Sons, Ltd: pp. 315-386.

Jansen W, Ayers R (2004). “Guidelines on Cell Phone and PDA Security.” Forensics National Instit. Standards Technol., 12-22.

Dunham K (2009). “Mobile Malware Attacks and Defense.” Syngress, pp. 197-329.

Moreno A (2006). *Bluetooth Security*. Universidad Pontificia Comillas, pp. 53-114.

Bluehack (2010). “Bloover, Vulnerabilities and Attacks Bluebug from J2ME.” Spanish Bluetooth Security Group. Online: http://bluehack.elhacker.net/proyectos/vulnerabilidades/bluebug/desdeJ2ME/desdeJ2ME. Last consulted: July, (2010).

Stewart J (2008). *CompTIASecurity + Review Guide: SY0-201*. Wiley, pp. 3-24.

Kumar A (2010). “Bluetooth Hacking.” Online: http://hak50.blogspot.com/2009 /04/bluetooth-hacking.html. Last consulted

Arroyo JP (2005). Bluetooth Security. “Texts, Digital Security Research.” Online: http://www.digitalsec.net/stuff/texts/Seguridad_Bluetooh.ppt. Last consulted: June, (2010).

Nokia (2009). “Symbian OS Change for Platform Security: File Server (F32).” Symbian Developer Library Online: http://library.forum.nokia.com/index.jsp?topic=/S60_5th_Edition_Cpp_Developers_Library/GUID-35228542-8C95-4849-A73F2B4F082F0C44/sdk/doc_source/guide/platsecsdk/PlatformSecurity-F32.doc.html. Last consulted: June 17, 2010

Nokia (2010). “Synchronization Markup Language.” Forum Nokia. Online: http://www.developer.nokia.com/Community/Wiki/Syncml/. Last consulted: June 19, 2010.