Analysis of Smartphone Worms:
A Smart worm for Smartphones

Kayhan Ozturk Qaiser Munir
Email: {kayoz945, qaimu880}@student.liu.se
Supervisor: Anna Vapen, {annva@ida.liu.se}
Project Report for Information Security Course
Linköpings universitet, Sweden

Abstract

In this report, we discuss about mobile phone worms which are running on the Symbian operating system. We focused especially on the Cabir worm which is the first identified worm on mobile phones. We analyzed the Cabir worm to identify the flaws it uses to exploit in Symbian and how its spreading functionality works. We also compare Cabir with some other Smartphone worms.

1. Introduction

Mobile communication was a dream in 1800s but it became real in 1940s with cell based radio telephony service. Since the invention of the mobile phone, it is rapidly increasing in use of daily life. Its popularity came from the answering the need of daily life [1].

Nowadays, mobile phones are suited with advanced operating systems such as the Symbian OS, Windows Mobile, Palm OS and Apple OS X for Apple iPhone. Such mobile phones are also known as smartphones. They bring many features to mobile phones such as high resolution colour screens, built-in cameras for taking pictures, recording videos, wireless data access, web browsers, and e-mail client. Some smartphones are also equipped with Bluetooth and other wireless technologies for exchanging data and communication [10].

According to the statistics, there are 1.5 billion internet users in the world but there are 5 billion users of mobile phones in the world. So it makes mobile phones very attractive to write malicious software for. Although, bundled with an OS and multiple applications – just like PCs – the mobile phones are becoming more vulnerable to security threats like viruses, worms and Trojan horses. According to F-Secure, currently there are more than 200 mobile malwares in circulation [1] and over 200.000 for PCs until 2007 [2].

1.1 Problems

- Which Flaws in the Symbian operating system does the Cabir worm exploit?
- How does the Cabir worm works?
- How to mitigate the threats of a Cabir attack?

1.2 Aim

In our report, we focused on the Cabir worm which is the first identified worm is written for Symbian OS based phones. We explain how the Cabir worm works; try to find ways to mitigate its threats and explain which technology it uses to spread. Also we compare it with other worms for the Symbian operating system.

1.3 Expected Results

We expect to understand that how this worm works and how it is harmful for Smartphones. We will show a flash animation to demonstrate how it spreads from one phone to another.

1.4 Method of Work

For understanding the structure of Symbian OS and explaining how Cabir/Caribe worm works we need a systematic approach to accessing the knowledge. So in this report we focused on published research. This project avoided unsubstantiated conjecture as to the causes of the problem of lack of proven data. To examine the problems of Cabir/Caribe worm, this project relied on both published research and the observations of end-users who studied technology on universities computer science departments.

2. Background

Understanding the terminology of different mobile OSs and worms are little bit complicated. So in this section, instead of giving descriptions of all the mobile OS, we focused on giving the basics of Symbian OS, the Bluetooth stack in Symbian OS and Trojan horses that can carry the Cabir worm as a payload.

2.1 Symbian OS basics

Symbian OS is an operating system designed specifically for mobile devices. It is also offering complete interface and platform for developing mobile apps. A device based upon the Symbian OS has a number of software and hardware layers to handle different aspects of the device such as:

- User Interface(UI)
- Application Data Processing Engine
- Core System Functionality
- Process and Device Drivers
- Hardware Adaptation

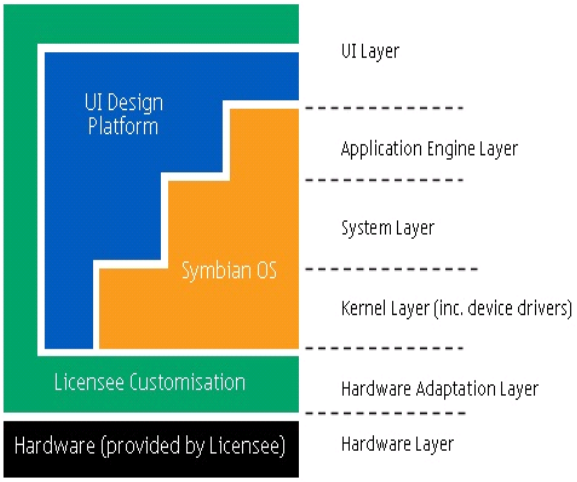


Figure 1: Layers of Symbian OS

As can be seen in the picture above (Figure 1), the software on a typical Symbian OS device is split into a number of layers. These layers are explained as below:

UI Layer – This contains software specific to the UI; including all the applications.

Application Engine Layer – Provides access to data that is required by applications.

System Layer – Provides all the core functionality of the system. This is usually in the form of system servers.

Kernel Layer – Software that provides kernel services such as process and thread creation.

Hardware Adaptation Layer – Software required so the upper software layers will run on the chosen hardware. This layer is dependent on the hardware. All upper layers are independent of the hardware.

Hardware – The actual hardware on which the software will run. This is either supplied by the licensee themselves or licensed from an Original Design Manufacturer (ODM).

Symbian OS has evolved rapidly since its creation and has been developed into multiple interface versions such as S40, S60 and S80. However, it is not completely an open operating system but some parts of it are shared with the community which enables third-party developers to write and install applications independently from device manufacturers. It helps developers by providing an extensive C++ API which allows access to services such as telephony and messaging, in addition to basic operating system functionality. Today, Symbian OS has a 46.6% share of the smart mobile devices market [3].

It has small memory footprint and low power consumption. This is very important since users do not want to recharge their phone every day. Although, some devices that run Symbian OS may not be switched off for years; therefore, the operating system was designed so that applications could run for years without losing user data. The operating system can run on more than one hardware platform, so it can be used on a variety of different device types including those with touch screens and with pens or keyboards [10].

2.2 Bluetooth in Symbian OS

Symbian OS is an operating system for mobile phones, which includes a bluetooth stack. All phones based on Nokia's S60 platform and Sony Ericsson/Motorola's UIQ platform use this stack. The Symbian bluetooth stack runs in user mode rather than kernel mode, and has public APIs for L2CAP, RFCOMM, SDP, AVRCP, etc. Profiles supported in the OS include GAP, OBEX, SPP, AVRCP, GAVDP, PAN, PBAP Additional profiles supported in the OS + S60 platform combination include A2DP, HSP, HFP1.5, FTP, OPP, BIP, DUN, SIM access device ID [4].

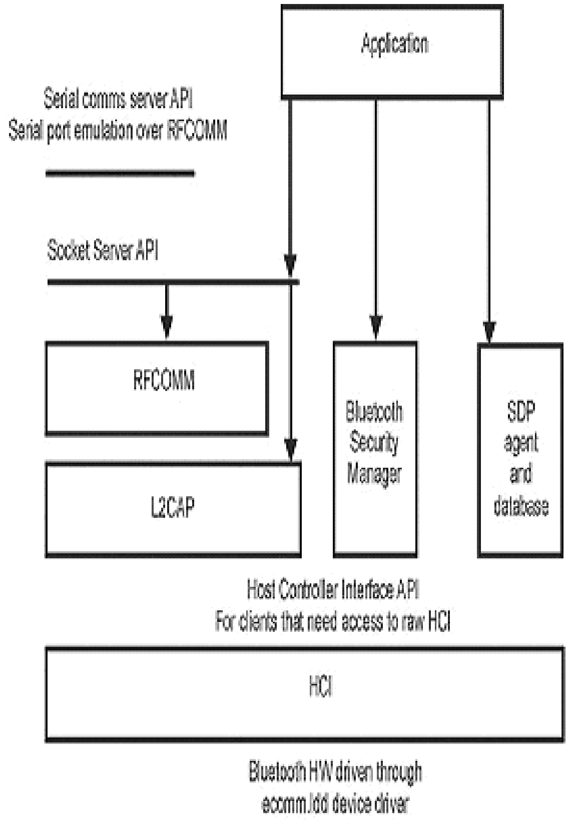

Application
Serial comms server API
Serial port emulation over RFCOMM
Socket Server API
RFCOMM
Bluetooth Security Manager
SDP agent and database
L2CAP
Host Controller Interface API
For clients that need access to raw HCI
HCI
Bluetooth HW driven through ecomm.ldd device driver

Figure 2: Bluetooth Stack in Symbian OS

Symbian OS has supported Bluetooth technology since the version 6.0 of operating system.

In the Symbian OS Bluetooth Architecture, the core stack functionality is implemented by two components (Figure 2), Host Controller Interface (HCI.DLL) and the Bluetooth Protocol module (BT.PRT). The Host Controller Interface module encapsulates the set of BT HCI commands and events. Bluetooth Protocol Module (BT.PRT) encapsulates L2CAP and RFCOMM layers. As a Symbian OS protocol module, it provides a Socket API to these protocols [5].

BT.PRT module also contains the Bluetooth Manager and Service Discovery Protocol servers (Figure 2). The Bluetooth Manager abstracts e.g. all User Interface (UI) interactions according to BT. The Bluetooth Security Manager enables Bluetooth services to set appropriate security requirements for incoming connections [5].

Service Discovery Protocol server handles SDP queries and appropriate responses.

Symbian OS also supports Serial port emulation (Bluetooth Comms server moduleBTCOMM.CSY), which provides a number of virtual serial ports for different services running over RFCOMM socket functionality [5].

2.3 Trojan Horses

A Trojan horse is a type of malware that appears to perform a desirable function but in fact performs undisclosed malicious functions that allow unauthorized access to the host machine, giving them the ability to save their files on the user's computer or even watch the user's screen or control the computer.

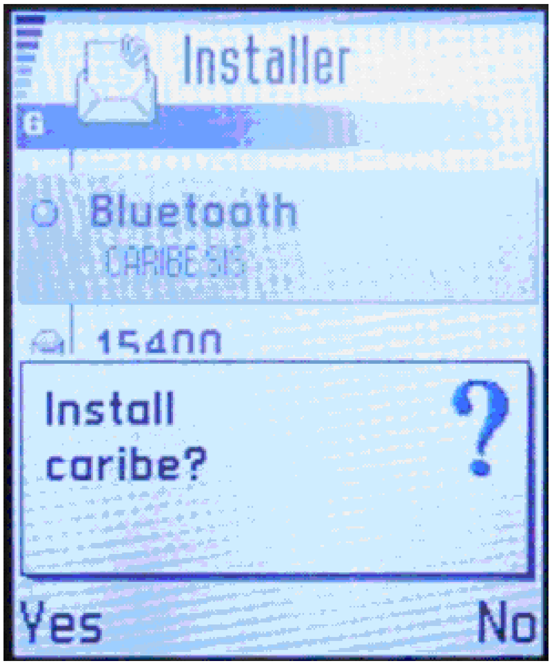
However, hand-held devices are vulnerable to malicious code in many of the other ways that PCs are also susceptible. For example, the major mobile operating systems such as Symbian OS provide reading, writing, and other standard file operation functions. "Such functionality is all that's needed for a viral threat to spread" said Symantec's Chien. And unlike some desktop platforms, he said, mobile operating systems don't limit the ability of code to modify system files. Because hand-held devices with communications capabilities are relatively new, vendors are still discovering and trying to solve security problems. In addition, when vendors rolled out the first wave of intelligent hand-held devices, security wasn't a top issue. Even now, said Giga analyst Jan Lundgren, "most vendors are focused more on functionality than security."

But some mobile OS (Symbian OS) has implemented the security tracking code to control the signature of executable files before they are executed. However, this is not a permanent solution because it does not prevent the execution of file if the user wants to execute and install the file.

The Cabir worm sometimes also brings or calls Trojan horses to infected mobile phones. It also disables the mechanism of running of security code for the device to understand if the application is healthy or harmful. Some of the mentioned Trojan horses are; MetalGear (XX), Skull.DD, and Gavno.a/Gavno.b.

3. Cabir/Caribe Worm

Cabir is a worm that runs in Symbian operated mobile phones using Bluetooth, that support Series 60 platform. Cabir replicates itself over Bluetooth connections and arrives to the phone messaging inbox as a file named caribe.sis that contains the worm's main executable caribe.app, system recognizer flo.mdl and resource file caribe.rsc. The caribe.sis file contains auto start settings that will automatically execute caribe.app after the sis file is installed. However, the caribe.sis file will not arrive automatically to the target device, so the user needs to answer `Yes` to the transfer question while the infected phone is still in range. The question will be repeated to the user if they select `No`. If user clicks yes the phone will ask normal installation question and then the worm will activate [4].



Installer

Bluetooth
CARIBE.SIS

15400

Install caribe?

Figure 3: Attempt to install itself (Caribe worm)

When user clicks the caribe.sis and chooses to install the caribe.sis file the worm activates and starts looking for new devices to infect over Bluetooth. When Cabir worm finds another Bluetooth device it will start sending infected SIS files to it, and lock to that phone so that it won't look other phones even when the target moves out of range. Please note that the Cabir worm can reach only mobile phones that support Bluetooth, and are in discoverable mode. Setting up the phone into hidden Bluetooth mode will protect the phone from the Cabir worm [6].

When the phone is infected, the phone's screen displays the word "Caribe". The worms also modify the Symbian OS on the phone so that Cabir is activated each time the phone is switched on.

The infected mobile phones also scan for vulnerable phones using Bluetooth. Finding a target, the phone then sends the caribe.sis file that contains the Cabir worm. Cabir/Caribe does not destroy data on the phones they infect. Instead, it blocks legitimate Bluetooth wireless connections and rapidly consumes the phone's battery [4].

F-Secure researchers believe the author of the Cabir worm released the source code of the worm in 2004 [7]. They believe that the reason of the fast spreading faster between mobile phones is that Cabir has a specially-formatted Symbian Installation System (SIS) file.

4. Evaluation and Comparison

Symbian is the leading OS in the smart mobile device market. It is designed for the specific requirements of advanced 3G mobile phones. Symbian OS combines the power of an integrated applications environment with mobile telephony, bringing advanced data services to the mass market. The growing use of these technologies has made them become an important attack vector for the malware industry.

The Cabir worm does not modify or attach itself to existing files. It simply makes copies of a .SIS archive. Other than the propagation routine, the first variant, Cabir.a, has no additional payload. There are at least 15 variants of Cabir that may be found spreading in over 35 countries worldwide. Once installed to a phone, Cabir works endlessly to find additional victims [8].

There is another worm which is similar to the Cabir worm named Comwar. Comwar also targets the Symbian operating system. Like Cabir it is also able to spread using the phone's Bluetooth connection but this worm does not rely only on the bluetooth technology to propagate. It can also be spread via MMS (multimedia messaging service) from one phone to another. By using the phone's internal telephone contact list, the Comwar can transmit itself to another Symbian-based Smartphone located anywhere in the world [8].

5. How to mitigate its threats

Now that we know how to identify these threats, what can we do to protect our phones from them?

Today, most of the Smartphone worms and Trojan horses have failed to spread. In a few cases, Cabir.a managed to spread from one phone to another using Bluetooth. However, the spreading of Cabir is severely curtailed by the need to accept and install the programs.

Users can prevent attacks by disabling Bluetooth and declining to accept and install any new software from the networks, especially pirated software. Even if the Bluetooth is turned on, visibility can be set up as hidden on the OS menu to avoid making the mobile phone discoverable.

According to industry experts, users most likely to be hit by Trojan horse programs such as Skulls and MetalGear are typically users who like to download new software from Symbian freeware sites or peer-to-peer networks.

The only way to get rid of Trojans is to reset the infected phone to its default factory settings [9]. However, this means all the data and configuration will also be lost.

6. Conclusions

Cabir was the first identified worm which brought a threat for the Symbian based mobile phones. The worm uses the Bluetooth technology to spread from one mobile phone to another. Comwar is another piece of malware for Symbian based mobile phone which uses Bluetooth and MMS (Multimedia Messaging Service) technology to propagate itself from one device to another. A mobile phone which is affected by this worm consumes the battery so much because it turns on the Bluetooth even if user tries to turn off it. It also opens a back door for Trojan horses which cause privacy leakage. By keeping the Bluetooth in hidden mode, an infection from this worm can be avoided, and there is also a need to educate the people about the security issues, to not accept any file or data for which they did not make a request. Also there are some commercial mobile antivirus software which can be used to get rid of Trojan horses.

References

[1] Niemela J. Virus Descriptions: Cabir http://www.f-secure.com/v-descs/cabir.shtml, 2004

[2] Oers, van Marius OSX Malware not taking off yet, http://www.avertlabs.com/research/blog/index.php/2007/03/20/osx-malware-not-taking-off-yet/

[3] Zeman E. Apple Beats RIM, Microsoft try to Become No. 2 Smartphone Provider in the market http://www.informationweek.com/blog/main/archives/2008/11/apple_beats_rim.html

[4] Shaharudin Ismail, Zahri Hj Yunos, “Worms and Trojans Go Mobile”, 2005

[5] Forsman S. Reusable Bluetooth Networking Component for Symbian Operating System,

Lappeenranta University of Technology, Finland, April 2002.

[6] Symbian Foundation Publish, “Introduction to The Symbian OS Architecture”, 2008

[7] Mosquito Born Malware and Cabir, http://www.informit.com/articles/article.aspx?p=327991&seqNum=3, 2008

[8] Coursen Shane, The future of mobile malware, August 2007 http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6VJG-4PFN9PR-5&_user=650414&_rdoc=1&_fmt=&_orig=search&_sort=d&view=c&_acct=C000034998&_version=1&_urlVe sion=0&_userid=650414&md5=41fdc127fda8f7a9d3925515480d4b0b

[9] Lemos, R. Skulls program kills cell phone apps. http://news.zdnet.com/2102-1009_22-5460194.html

[10] J. Kumar Gandhi, Symbian OS Layers, http://www.jkg.in/category/symbian/ , 2006