UDC 621.395:004.491.23, DOI:10.2298/CSIS090330027F

Trojan horses in mobile devices

Daniel Fuentes[1], Juan A. Álvarez[1], Juan A. Ortega[1], Luis Gonzalez-Abril[2],
and Francisco Velasco[2]

[1] Departamento de Lenguajes y Sistemas Informáticos
Universidad de Sevilla
Avda. Reina Mercedes s/n, 41012, Seville, Spain
{dfuentes, jaalvarez, jortega}@us.es
[2] Departamento de Economía Aplicada I
Universidad de Sevilla
Avda. Ramón y Cajal 1, 41018, Seville, Spain
{luisgon,velasco}@us.es

Abstract. This paper focuses on the behavior of Trojan horses in mobile devices. This malicious software tries to steal information from a mobile device while the user is unaware. We describe the communication links through a Trojan horse installed into a mobile device. To demonstrate the effects of a Trojan horse infection we present a practical example on a PDA. Via SMS, the malicious user can access a user's contacts information through the previous installation of the Trojan horse. The results show that this process means a loss of information and a quantified cost to the attacked user too. This paper proposes different solutions to avoid this malware and its effects.

Keywords: Mobile security, Mobile Infections, Trojan horses.

1. Introduction

According to a study by the ITU (International Telecommunication Union) at the end of 2008, there were 4.000 millions of mobile phones in the world. A lot of people in the world are permanently communicated and can exploit the power of their terminals for advanced operations by the increased capabilities of these devices: via GPS navigation, Internet communication, photography, video, etc. According to Gartner Inc., in 2009 Smartphone sales surpassed 40 million units, a 27 per cent increase from the same period last year, representing the fastest-growing segment of the mobile-devices market. In addition, currently 33 millions of users already use mobile devices for shopping and are expected to be 103.8 millions in 2010. The increasing user base will influence collaboration and communication of enterprises more than ever: it is expected that more than 80% of the knowledge workers will receive and create information on notebooks and Smartphones by 2012 [1]. Communication, entertainment, exercising and travel are merely a few lifestyle improvements made possible with mobile technology. Moreover, the growing number of services and benefits, are becoming more essential in our daily life because they provide not only the basic voice communication service, but also contain other forms of communication such as instant messaging, multimedia messaging, Bluetooth, NFC (Near Field Communication) or e-mail. And all of these services can be an infection vector.

In this paper we explain a test program designed to study the behavior of a Trojan horse. Trojans, as well as viruses and worms, are known to create a backdoor that gives malicious users access to a system, possibly allowing confidential or personal information to be compromised. Due the growth of the personal information stored in mobile devices (location, mail, SMS, photos, etc.), we focus this work on one of its possible infections, the Trojans horses. We have demonstrated how Trojan horses can easily carry out the theft of the data contained in another user's phone book. Communication will be via SMS with predefined structures in which the attacker can send commands to the attacked PDA while the other user is aware of anything. The Trojan horse prototype for PDA will install into the attacked device and it will return user data from his contacts to the malicious user. The Trojan horse will be camouflaged inside an image (although it could also be implemented into an audio or video file).

The structure of this paper is as follows. In section 2 we present some related works. Section 3 describes different possible attacks on mobile devices and infection vectors. In particular, section 3.1 focuses on Skulls Trojan horse attacks whose main objective is, in addition to its own propagation, the theft of private user information while the victim is unaware. Section 4 describes the behavior of the Trojan horse in mobile devices through a practical experience where this infection is introduced on a mobile phone to obtain the user's contacts information stored in the terminal. In 4.3 we explain the results of the experiment and in 4.4 we propose different solutions to avoid the effects of the infection. Finally, in Section 5, we summarize our conclusions and present some lines of future work.

2. Background and related work

In the last years, many types of malware for mobile devices have appeared [2]. They can attack a device in many different ways, as we can see in Figure 1, and degrade mobile functions, delete or steal personal data, increase the victim's phone bill or disable the device completely. Each service that allows the user to connect to another device can be an infection for a virus intrusion or other threats [3-4].

SMS, MMS and Bluetooth [5] are together the most common ways for a possible infection. The small size of SMS (only 160 bytes, 168 characters) is the main disadvantage and the reason why there has not yet been a large-scale infection via SMS. However, MMS is one of the most used routes of infections. The maximum size of the MMS is imposed by the service provider and depends on the device. For example, in India it's common for mobile videos to be 100kb and however in Sweden, the network Telia restricts MMS size to 300kB. All 3G compatible phones can receive/send 300kb MMS and most older phones may only allow 100kb, whilst even older phones may only allow 50kb. Today, the most extended size is 300KB which seems an appropriate size to accommodate the malware. Bluetooth technology develops different levels of security based on the identification of the devices involved but, in spite of that, the number of vulnerabilities via Bluetooth has increased considerably. One of the most dangerous vectors is e-mail [6], since there are no size restrictions and they can spread more easily to other tools, mainly PCs. Other ways, like USB connections, allow an infection to move from one device to another. Finally, WI-FI networks provide interoperable wireless access but sometimes the network origin and reliability is unknown.

Mobile malware detection [7-8] is a new area and almost all solutions that currently exist for mobile devices were originally created for PCs and they do not approach the key challenges of the mobile environment such as limited processing power as important issues. Recently, products like Flexilis [9] or Airscanner [10], which are dedicated exclusively to mobile devices security, protect mobile devices against threats including viruses, malwares or spam.

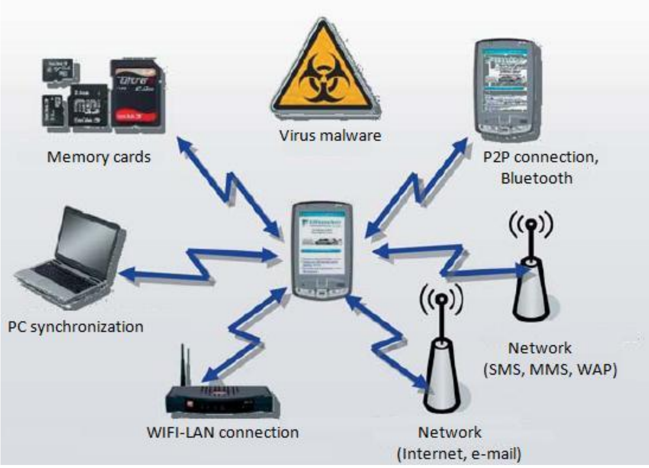

Fig. 1. Virus malware routes in mobile devices

2.1. Trojan horses in mobile devices

What happens if your mobile phone or PDA is lost or stolen? The device may contain confidential data and legal liabilities could arise if it contains confidential information such as medical records. We have already seen that there are many ways in which a mobile device can be attacked, but this article focuses on attacks with specific Trojans horses whose primary goal is, in addition to its own propagation [11], getting information in a maliciously way while the attacked user is unaware of the theft.

Nowadays, when users download a song, video, image or video game in his terminal, the data necessary for the download has been seen in an advertisement on TV, Internet website, magazine or newspapers. These downloads are usually done by sending SMS messages to telephone numbers that do not guarantee the safety of what the user will receive in his mobile phone. We could think that since we are paying for the download service, this may not prove to be an infection vector and, however, it is not too difficult to send a Trojan horse in a file of this type. As we will see in the demonstration, the Trojan horse will be camouflaged inside an image, but it can be introduced in any file so that when the infection arrives to the terminal, its malicious software will be installed.

One clear example of a Trojan horse is the Mosquito Trojan 2.0 [12], which accompanied the pirated version of the game for mobile devices with the same name. The Trojan did not affect the functionality of the device, but sent SMS messages to premium services (1 €/SMS approximately) while the user was playing with an illegal copy of the game. In fact, it is very probable that there are still websites where a user can download the game and, although there are two warnings before installing it, some users may be tempted to install it. Despite everything, this Trojan horse disappeared when the mobile game was deleted.

3. Development

There are programs like Windows Mobile Pro-X FlexiSPY [13] which performs mobile espionage. This application allows you to control all sent and received SMS messages and all call records and their duration, listen to telephone conversations, remote control software functions using SMS, or download directly into the device without a PC or cables. Moreover, if the device has a GPS function, it can be used as a crawler to get the coordinates to locate the device. It works with all versions of Windows Mobile 2003, except with Pocket PC, and it costs approximately 350 US$.

We have carried out a simulation of a Trojan horse infection. This software allows a malicious user to steal all the contacts information. Then, we describe the Trojan horse implementation and the results, quantify the damage and take measures to prevent it.

3.1. Implementing a Trojan horse malware

Windows Mobile 6 Professional Software Development Kit was installed on the Microsoft Visual Studio 2008 programming environment to implement the

Trojan horse prototype. The attacked user will be played by the Visual Studio Simulator and when the program begins, it will emulate the installation of a malicious software running in the background while the user will only see a picture.

Moreover, the Microsoft Tool Cellular Emulator v1.43 was used to enable the malicious user to send and receive SMS messages and make calls (including other services) to the Visual Studio's emulator. Thus, the simulation of information exchange via SMS between mobile devices has been done in an efficient manner without using the services of any company. The main objective is to obtain private data from the attacked phone. In this application that information will consist of the contacts' names and telephone numbers.

The main Windows Mobile 6 SDK classes used for the demonstration were:

OutlookSession: It allows, among other functions, to access and modify data in the Contacts. In this case, it uses the nickname and the phone number.

MessageInterceptor: Personalized message receiver. It implements the channel that allows the infection to remain pending for an incoming SMS. The purpose of the *MessageInterceptor* class will be a key factor in the implementation of the Trojan horse and the proposed solution (as we shall see below), because it contains the event which receives SMS messages (*MessageReceived())*.

SmsMessage: It implements the creation and sending of SMS.

3.2. Information flow

The operation on the user's attacked device is shown in the pseudocode:

1. The attacked user receives the picture where the Trojan horse infection is packed. The file can be transferred from the Internet through MMS or via Bluetooth to the terminal.
2. Once the virus reaches the mobile phone, it automatically installs itself.
3. The malicious program awaits orders. The attacker's instructions are introduced by means of a SMS with a default structure.
4. If the received SMS is in the correct format, in this case with the head *@spy@*, the content processing begins. Otherwise, the message goes to the user's inbox.
5. Then, the Trojan horse checks the label-value pairs. The parser recognizes the pairs <*sms*>*telephone_number*.
6. The program automatically sends the Contacts data in the Phonebook to each phone <*sms*>*telephone_number* pair which appears in the SMS received (stage 3). In the demo, it was sent via SMS to each contact

name and phone number with the format *contact_name:telephone_ number*, but different data could also be sent.

7. Once every SMS is sent, the Trojan horse infection awaits new orders.

The pseudocode of the Trojan horse behavior on the attacked device is:

```
image_download();
trojan_horse_installation();
execution_in_background();
if (sms_received ())
      if(is_malicious_user(SMS_recieved))
             while(is_all_information_contacts_sent())
                  SMS_send(information_contacts,
                  SMS_received .telephone_number);
            end_while
      else
            send_SMS_to_inbox();
      end_if
end_if
```

Now, the Trojan horse is installed in the victim's mobile phone. In turn, the Trojan horse behavior on the attacker device is described in detailed in the next process.

1. The malicious user sends an order to the Trojan horse by a SMS to the user under attack in an appropriate format, which in the test application is *@spy@<sms>telephone_number<sms>telephone_ number<sms>…*
2. Awaits the response of the Trojan horse.
3. Begins to receive SMS messages to the structure *contact_name:telephone_number-contact_name:telephone_number-* …The messages are processed through a second parser in which the malicious user decides how to process information.

The process is completed when the user decides to send an SMS with new orders that lead to begin the process of reattacking. In pseudocode, the Trojan horse behavior on the attacker device is:

```
send_SMS();
while(no_response_recieved())
      if(SMS_recieved())
            processing_contacts_information();
      end_if
end_while
```

3.3. Results of the experiment

Obviously, the whole process takes place without the user's awareness of the attack because the Trojan horse remains running in the background. In addition, messages sent from the device to the attacked phone do not arrive to the mailboxes, so they do not arouse suspicion. Furthermore, sending SMS messages entails an economic cost. For a possible estimation, we will assume that the average length of the contact's name or nickname is ten characters approximately and we know that mobile phone numbers consist of nine characters. If we add the spaces, a contact's information consumes twelve characters. An average user may have one hundred contacts stored in his phone book and an SMS costs 0.15€ on average in Spain (according to Viviane Reding, European Commissioner for Information Society). Therefore, whenever a malicious user requests data from the contacts in the agenda of the attacked device it will cost the attacked user 8.62€ approximately and the malicious user can begin this process whenever he wants.

In tests carried out on a HTC 3300 PDA, it has been found that when the device is in any way attacked (after the Trojan horse was installed) it is not aware of the entry or exit of information via SMS, which the Trojan horse uses in the process. Moreover, the device does not save copies of those SMS messages in inbox or outbox. However, when the user receives a message with the malicious Trojan horse the screen light turns on but still nothing happens.

3.4. Proposed solutions

A Trojan horse that has easily allowed the obtaining of information from the Contacts of an infected device has been implemented. It has been also found that the theft of information goes completely unnoticed by the user of the attacked terminal.

Therefore, one possible solution is a service that uses the Event Listeners (for SMS, MMS, GPS, Bluetooth...), which are provided by the specific programming language to detect access to a list of potentially dangerous resources in the event the terminal is the target of an attack. In the case of our demonstration activities, the *MessageReceived()* event is used to receive SMS. This event is provided by Microsoft Windows Mobile 6 SDK (*MessageInterceptor()* method) to detect any access via SMS that occurs in our system (in PDAs the test program reports no information for in/out SMS), and thus the system can alert the user that a new message has .been received, regardless of its content or origin.

When a new SMS arrives, the user will be alerted of the arrival by the PDA, providing additional information as to the identity of the sender or the first characters of the message. In turn, the user can accept it (go to inbox) or delete it, as appropriate.

This is undoubtedly a simple and flexible solution that can contribute to a more comprehensive control of entry and exit information from our device. However, the user will make the final decision, helped by his experience and the content of the SMS, to allow sending or receiving a message.

Another solution would be including a signature in outgoing SMSs, but this procedure shows several disadvantages, for example, the origin of the SMS is not one hundred per cent ensured; in addition, it does not work with incoming messages and reduces the free space for writing messages. However, with this method, only signed messages could be sent and the problem caused by the infection could be solved.

Moreover, another solution for incoming messages would be the implementation of a new parser to check these messages. First, the sender's phone number is checked and if it does not belong to a known contact, the contents would be checked again by the parser. The main problem, however, is the parser design and which characters are to be included.

4. Conclusions and future work

Currently most mobile users, unlike PC users, do not feel the need to install on their mobile terminals an antivirus program or other devices to protect them from potential infections. However, due to the growth of services, capabilities and stored data of these devices, it is almost indispensable to take any measure against a possible attack.

In this article we have discussed the attacks on mobile terminals by Trojan horses, through which new vulnerabilities can be installed on the attacked device, capturing and sending some of the private information for future misuse, taking into account that throughout the process the user is unaware of the theft and the device functionality is not damaged at all.

We have developed a demonstration to show the theft of part of the contact information contained in the mobile device phonebook. This experiment was conducted on a simulator provided by Microsoft Windows Mobile 6 SDK and then ran on a PDA. The solution proposed in the article provides a further control on the flow of information sent and received from the device.

As future work, we plan to study the behavior of Trojan horses when they attack other terminal services such as Bluetooth, GPS or e-mail. And not just Trojan horses, but other types of vulnerabilities such as worms or viruses that could affect the operational ability of the device (software or hardware).

References

1. Beurer-Zuellig, B. and Meckel, M., “Smartphones Enabling Mobile Collaboration”, in Proceedings of the 41st Hawaii International Conference on System Sciences, pp. 49-49, 2008.
2. Gostev, A., “Mobile Malware Evolution: An Overview”, [Online]. Available: http://www.viruslist.com/en/analysis?pubid=204792080, Sept. 2009
3. Van Ruitenbeek, E., Courtney, T., Sanders, W.H. and Stevens, F., “Quantifying the Effectiveness of Mobile Phone Virus Response Mechanisms”. In Proceedings of the 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, pp. 790–800, 2007.

4. Ganesh, A. J., Massoulie, L., and Towsley, D., "The effect of network topology on the spread of epidemics". In Proceedings of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies. vol. 2, pp. 1455-1466, 2005.
5. Bose, A., and Shin, K. "On mobile viruses exploiting messaging and bluetooth services". In International Conf. on Security and Privacy in Comm. Networks (SecureComm'06)", pp. 1-10, Sept. 2006.
6. Newman, M., Forrest, S., and Balthrop, J., "Email networks and the spread of computer viruses", Phys. Rev.E 66, 3, Sept. 2002.11.
7. Pradip, D., Liu, Y. and Das, S.K., "An Epidemic Theoretic Framework for Vulnerability Analysis of Broadcast Protocols in Wireless Sensor Networks", in IEEE Transactions on Mobile Computing, vol. 3, pp. 413-425, 2009.
8. Bose, A., Hu, X., Kang, G., Shin, K.G. and Park, T." Behavioral detection of malware on mobile handsets", in Proceedings of the 6th international conference on Mobile systems, applications, and services, pp. 225-238, 2008.
9. Flexibilis, http://www.flexibilis.com
10. Airscanner, http://www.airscanner.com
11. Fleizach, C. B., "Can You Infect Me Now?. A Treatise on the Propagation of Malware in a Cellular Phone Network". Tech. Rep. CS2007-0894, UCSD, June 2007.
12. Flexi SPY, http://www.flexispy.com/
13. Kim, S. h. and Leem, C. S., "Security Threats and Their Countermeasures of Mobile Portable Computing Devices in Ubiquitous Computing Environments". In Proceedings of the International Conference Computational Science and Its Applications (ICCSA 2005), pp. 79-85, 2005.

Daniel Fuentes Brenes received his bachelor degree in Computer Science in March 2008. Since June 2008, he is a Lecturer in the Department of Languages and Computer Systems at the Seville University. His main research interests are mobile computing and machine learning.

Juan Antonio Álvarez García received his bachelor degree in Computer Science in 2003. He is a Lecturer since 2003 in the Department of Languages and Computer Systems at the Seville University. His main research interests are ubiquitous, mobile and urban computing. He is also interested in healthcare systems.

Juan Antonio Ortega Ramírez obtained the Ph.D. degree in Computer Science in 2000 at the Seville University in Spain. He is a Lecturer since 1992 in the Department of Languages and Computer Systems at the Seville University. His research interests are: the temporal series and the global information systems and specifically the domotic and assistencial systems. He is Head of the Centre of Computer Scientific in Andalusia (Spain).

Luis González Abril is a Lecturer in the Dep. Of Applied Economy I at the University of Seville (Spain). He obtained his graduate in Mathematics in 1986 from the University of Sevilla and his Ph. D. degree in Economy in 2002 from the University of Seville. Hisˇ researchs are:Similarities, Support vector machines, machine learning and bifurcations of dynamical systems applied to economic problems. e-mail: luisgon@us.es.

Francisco Velasco Morente is a Lecturer in the Dep. Of Applied Economy I at the University of Seville (Spain). He obtained his graduate in Mathematics in 1979 from the University of Sevilla and his Ph. D. degree in Mathematics in 1991 from the University of Seville. His researchs are: similarities, Support vector machine, bifurcations of continuous and discrete dynamical systems and optimal control problems, both applied to economic problems.

Received: March 30, 2009; Accepted: August 09, 2010.