J Comput Virol (2006) 2:109–119
DOI 10.1007/s11416-006-0022-0

ORIGINAL PAPER

About malicious software in smartphones

Sampo Töyssy · Marko Helenius

Received: 10 March 2006 / Accepted: 10 June 2006 / Published online: 22 August 2006

Abstract Phones with some of the capabilities of modern computers also have the same kind of drawbacks. These phones are commonly referred to as smartphones. They have both phone and personal digital assistant (PDA) functionality. Typical to these devices is to have a wide selection of different connectivity options from general packet radio service (GPRS) data transfer to multi media messages (MMS) and wireless local area network (WLAN) capabilities. They also have standardized operating systems, which makes smartphones a viable platform for malware writers. Since the design of the operating systems is recent, many common security holes and vulnerabilities have been taken into account during the design. However, these precautions have not fully protected these devices. Even now, when smartphones are not that common, there is a handful of viruses for them. In this paper we will discuss some of the most typical viruses in the mobile environment and propose guidelines and predictions for the future.

1 Introduction

As mobile phones have evolved into fully fledged computers the problems associated with desktop systems are also creeping into the mobile domain. These advanced mobile phones will be referred here as smartphones. Wide spread operating systems such as Symbian and Microsoft Windows Smartphone make smartphones more vulnerable to malware epidemics. If a malware writer wants to leave a mark he needs a program which spreads as widely as possible. This postulates widely spread standardized platforms such as Windows operating system in desktop computers.

A review of malicious software in smartphones will be conducted and guidelines for minimizing the threat at personal and organisational level will be established. As worms are the most wide spread and most damaging type of malware we will concentrate on them.

This paper is divided into the following sections: smartphone operating systems, infection routes, malware written so far, smartphone malware prevention, new epidemiological models and smartphone viruses in a major Finnish newspaper called Helsingin Sanomat [16]. Finally, results will be discussed and conclusions will be presented.

2 Definitions

It is essential to know the meaning of the terms used. We will next propose definitions for a smartphone and a SIS-file.

2.1 Smartphones

First of all, we must note that the difference between a computer and a smartphone is an indeterminate area. It is difficult to make the distinction, because computers are getting the properties of phones and phones are getting the properties of computers. Moreover, there are properties that cannot be precisely classified.

S. Töyssy
10tons Ltd, Iidesaukio 1 A 52, 33100 Tampere, Finland
e-mail: sampo.toyssy@uta.fi

M. Helenius (✉)
University of Tampere,
Department of Computer Sciences,
Virus Research Unit,
Kanslerinrinne 1, 33014 Tampere, Finland
e-mail: cshema@cs.uta.fi

Nevertheless, a definition is needed for precise discussion and thus we will propose the following definition: A smartphone is a mobile phone that includes software that a user is able to modify and update. The user controlled software must be able to transfer information to and from external systems.

The idea is that a smartphone must include the calling properties of a phone and it must be mobile. In addition, there must be some software which can be updated and even modified or at least custom software can be installed. There must also be a way to transfer information. When these properties are fulfilled also viral programs are possible provided that there is no impeding security. For example, if program code is able to transfer a recursively replicating form of itself then the viral condition is fulfilled.

On the other hand non-replicating malware, like Trojan horses (referred as trojans later on), just need to be installed on the target device. They do not need spreading vectors to other devices to fulfill their malicious function. Trojans need a device to function on and a way to arrive to the device. Without connectivity the functionality is limited: malware cannot send information to anyone. For example, the two most known trojans RedBrowser [21] and FlexiSpy [23] need certain connectivity to fulfill their function. Trojans with no connectivity are limited to attacks which affect the phone itself. For example, a trojan masquerading as a file manager could wipe out the address book.

In this paper, when referring to smartphones in general the word smartphone will be written in lower-case. If referring to Microsoft Smartphone OS it will be written as "MS Smartphone" or "Smartphone 2002". This is because we need a clear distinction between the general concept of smartphones and a single product.

2.2 SIS-file

The SIS-file is defined here because most of the malware is for Symbian-based devices and it often arrives in SIS-files. A SIS-file is an installation package for the Symbian operating system. A user can easily install software from SIS-files. As a consequence they also make it easy to install malware provided that a user accepts the installation. The main safety mechanism against malware is the installation confirmation in Symbian based devices.

3 Operating systems

In order to analyze the threat of malicious software in smartphones we need to introduce the most common platforms. At the moment there are four competitors with more or less established markets. Linux seems to be coming up strongly and different sources give different numbers of market shares. The main point is that Symbian is the largest player. Also the trend seems to be that PDAs are losing to smartphones in sales.

According to IDC the Symbian OS (operating system) held the market share majority with 63% in 2003. Microsoft had 14% share and Palm OS 13%. IDC estimates that Symbian will have 61%, Microsoft 21% and Palm 11% in 2007. In year 2004 the numbers are following: Symbian 55.9%, Microsoft 12.7%, Linux 11.3% and others including Palm OS 20.1%. It is also stated that Microsoft has a larger share than Palm OS. This means the Palm OS may hold about 10–12%. This estimate is also presented in Fig. 1 [2,3].

3.1 Symbian OS

The Symbian OS was developed in 1998 and the owners are the biggest handset makers in the world. They include: Ericsson, Motorola, Nokia, Panasonic, Psion, Samsung Electronics, Siemens, and Sony Ericsson. The Symbian OS is the most common OS in smartphones at the moment. Symbian OS can handle the normal task expected from a smartphone: video, audio, instant messaging and multi threading. It also supports open standards such as Java, Bluetooth and SyncML. In addition, the Symbian OS does not display Symbian logos or texts on the user interface, which is a desired feature for some manufacturers and operators who may want to brand their phone exclusively [1].

At the moment of writing (the first half of 2006) there are several viruses for the Symbian platform. This is expectable as it is the most common smartphone OS. In May 2005 the web page of F-Secure listed 39 different

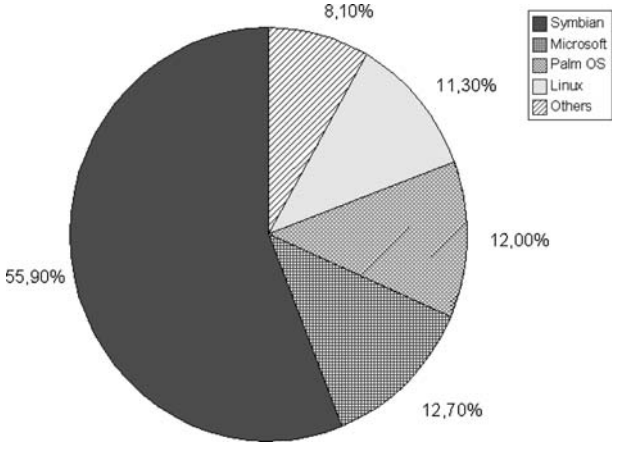

Fig. 1 IDC's estimate of smartphone OS marketshares in 2004

Symbian OS viruses including variants and the standard EICAR test file [14]. In February 2006 this number has grown to 125. Most of the growth is probably due to variants as, for example, there were totally 26 variants listed for the Cabir virus.

3.2 Palm OS

The Palm OS was first used in 1998 in PDAs. Since then it has changed towards a more smartphone friendly operating system. The current version is 5. It can also handle the most common tasks expected from a smartphone such as time management, notes and telephony features. A new version of Palm OS will be released in the near future with more emphasis on smartphones. This version is called Palm OS 6 [1].

So far, Palm OS has been rarely targeted by virus writers. The first virus for the Palm OS platform is called Phage and it was discovered on the 22 September 2000 [10]. In addition, F-Secure lists 2 Palm OS trojans (Liberty and Vapor) and one Palm greeting card application dropped by a Windows virus (Palm/MTX II.A).

3.3 Microsoft smartphone 2002

Microsoft's Smartphone OS has been derived from the Microsoft Pocket PC Phone Edition. It uses less memory and it has less features compared to the Microsoft Pocket PC platform. Microsoft works directly with the service providers instead of handset manufacturers [1].

At the moment there are no specific viruses for the Microsoft Smartphone. However, there are at least two viruses for the Microsoft Pocket PC. This indicates that it is probably only a matter of time when a specific MS Smartphone virus surfaces.

3.4 Linux

Linux is used as a smartphone OS but so far only by a few manufacturers. This is because current implementations require more memory and lack features compared to other operating systems. If Linux were to be used as an OS a handset manufacturer should probably invest some development capital to make it a viable competitor. At the moment Linux based smartphones remain a curiosity which means that there are no known viruses for Linux based smartphones as the number of these devices is small. However, when the processing power and the amount of memory increase Linux becomes more viable [1].

3.5 Java

Java is not an operating system but a cross-platform programming language. However, since Java is an inherent part of smartphones and it can be used as a virus platform it is mentioned here. So far Java viruses have not appeared for smartphones. Nevertheless, there is a possibility that while the Java API used in smartphones grows more powerful also Java viruses may become more feasible and powerful. Although viruses have not appeared so far trojans have appeared that, for example, make unauthorised connections (e.g. RedBrowser discussed in Sect. 5.4).

3.6 Summary

In the summer of 2006 the Symbian platform seems to be the most popular platform for smartphone virus authors. This may be anticipated since it is the most common smartphone OS. Palm OS also has a limited amount of viruses and trojans. MS Smartphone OS has yet to be targeted by any viruses but since MS Pocket PC already has viruses it is likely that the smartphone platform will be targeted also.

4 Infection routes

4.1 MMS

The name multimedia messaging service (MMS) implies that there are only media files in MMS messages but in reality the situation is different. Malicious software can spread via MMS messages by attaching a copy of itself on to a MMS message and sending it to some other device capable of receiving MMS. This can be seen as a flaw in MMS systems as the procedure of embedding an infected SIS file is very simple. SIS files are essentially python scripted installer files. A good example of a worm which can browse the phone book and then spread via MMS messages is a worm called Commwarrior.A [8].

4.2 Bluetooth

The first smartphone viruses spread via Bluetooth. Spreading via Bluetooth requires two premises: There is a suitable Bluetooth device in range and that the device is in discoverable mode. Even after this the user typically has to accept the incoming infected file and install it. This limits the viability of this spreading route but it is still effective as the device goes where the user goes.

For example, a smartphone worm called Lasco. A spreads via Bluetooth [9]. Bluetooth has no

intermediaries between the victim and the infecting device. This means on the one hand that network operators or other services cannot monitor this infection route or use any countermeasures and on the other hand the connections are temporary. Also as the infection requires relatively close proximity the ordinary epidemiological models do not give accurate results on viruses spreading via Bluetooth as discussed in Sect. 6.5.

The viruses written so far do not seem to use any actual vulnerabilities in Bluetooth. The viruses depend on user interaction: the user sets the device to be discoverable to other Bluetooth devices, then deliberately accepts the incoming files and installs the incoming file. Finally, the autorun feature is able to run the malware. It seems that if the virus could make itself a part of a file often exchanged via Bluetooth it could spread quite efficiently. Infected files could come from a trusted source and seem like authentic.

There are actually some vulnerabilities in Bluetooth but they may require custom hardware and at the moment they seem unpractical for smartphone viruses [4,5]. Nevertheless, it is possible that viruses will employ vulnerabilities in the Bluetooth protocol itself some day.

4.3 IP connections via GPRS/EDGE/UMTS

Usually Internet connections made by smartphones are temporary and the connectivity is only used by explicit request. An IP connection is opened only when it is needed and it seldom runs in the background. However, this might change in the future if WLAN connections and 3G services with flat pricing models will become more common. In addition, the bandwidth available via a GPRS or even EDGE connection is limited to speeds comparable to ISDN modems. Even though the speeds are low they are sufficient for worms if the connection is always available. IP radio connections such as GPRS, EDGE or UMTS have their technical limits which are a hindrance to the spreading of the worm. Phones do not form a similar network as computers in a LAN environment and the addresses of other phones are not as easy to acquire as addresses from a LAN. Also the availability of other accessible devices is much lower than suitable desktop computers in a LAN. Still a mobile worm spreading efficiently trough a VPN is a possibility.

4.4 WLAN

At the moment WLAN abilities are relatively uncommon in smartphones and therefore no viruses are known to spread through wireless networks. In the future if WLAN access points will become more common and the number of WLAN enabled devices will increase the wireless networks may become a viable infection route.

4.5 Copying files

Many viruses spread themselves to other files upon infection. These files can be copied to other devices and the virus spreads. This requires more active participation from the user so it is not as effective as automatic methods where the victim only has to accept the file which has been sent automatically. This could be compared to the classical scenario where the user would deliberately insert a possibly infected floppy into a diskette drive without exact knowledge of the actual contents of the floppy.

4.6 Removable media

It is also possible for a virus to spread explicitly over removable media much like in the old days with floppy diskettes. So far the removable media has not been used to transport files from a system to another in a large scale but in the future this will probably change if people start to use their phones more like digital cameras.

One simple example scenario is an infected self-service photo printing machine which installs a virus on the removable media and this way infects all the compatible devices which have come in contact with the machine. This scenario is not very likely, but the removable media nonetheless is an infection vector and it must be treated accordingly [18].

A virus which actually plants Windows malware on the memory card of the smartphone has been written and it is called CardTrap [6]. The virus is described in Sect. 5.

4.7 Summary

In a nutshell it seems that MMS messages and Bluetooth are the most viable infection routes since they provide the addresses and contact methods easily. Also MMS and Bluetooth are favorable over WLAN at the moment since they are more common. Considering the facts it can be said that spreading via MMS messages is the most efficient way since the requirements of spreading are lowest. WLAN is hindered by the small number of enabled devices, Bluetooth is crippled by the proximity requirements and the IP connections are usually temporary and therefore the probability of contacting a suitable device is small. A worm can send itself via MMS automatically to all entries in the phone book. The victim needs to have a MMS enabled phone and a suitable platform. The victim might eventually notice the unusual MMS traffic but at that point it will be too

late. In the future if persistent wireless IP connections will become more common the smartphone viruses will probably use them also.

5 Existing smartphone malware

We will next discuss some of the current malware for smartphones. This section is not supposed to be the most up to date catalog on smartphone viruses but a general description which gives a brief image of the field. This section reflects the time of writing in first half of 2006.

5.1 Lasco and Cabir families

Cabir is a worm which spreads itself via the Bluetooth connection. The latest variants have better spreading capabilities compared to the earlier ones. The worm searches nearby Bluetooth enabled phones in discoverable mode and sends itself to the target device. The victim needs to accept the transmission. The virus does not use any actual vulnerabilities since the user can set the discoverability on or off. The user needs to accept the incoming file and install the program. Only after the installation the autostart feature will infect the device.

Lasco resembles Cabir, but in addition to spreading via Bluetooth, it also infects all SIS-files available. When these SIS-files are copied to another suitable device and activated the device becomes infected. This makes the spreading easier since the device can be infected with a file from a trusted source. For example, a trusted party (e.g. a friend) could send infected software. The next victim may install the software without hesitation thus activating the virus.

5.2 Commwarrior and Mabir families

Commwarrior was discovered on the 7th of March 2005 and it is the first worm capable of infecting other devices via MMS messages. The Commwarrior virus uses the local address book and sends MMS messages including the infected SIS file to the recipients. Real life situations have been reported where a user has installed the software which was received as an MMS message and after that the virus started sending messages to recipients picked up from the address book [17]. The infected files sent via MMS use a predefined subject such as: "Norton AntiVirus Released now for mobile, install it!". It uses Bluetooth in a similar way to Lasco and the infected files sent via Bluetooth have randomly generated filenames. The only function of the worm is to spread itself. Nevertheless, as MMS messages can be expensive this behavior certainly is harmful to the bill payer [8].

Just a month after the discovery of Commwarrior.A a new virus called Mabir.A emerged. It resembles Cabir-family but it employs MMS messages as a spreading vector just like Commwarrior. It has some additional functionality, which can be seen as an automatic social engineering attack. The virus reads the local address book and also monitors incoming messages. If the infected phone receives an MMS message the virus sends a fake reply to that message including a copy of the virus [13].

5.3 Phage

Phage is a Palm OS virus first discovered in September 2000. The virus spreads to a Palm OS based device when synchronizing it with a PC or when transferring infected files via the infra red connection. The virus is classified as a low threat as it spreads very slowly. However, the virus carries a nasty payload which aims to destroy all installed programs by overwriting the beginning of the Palm executables.

5.4 RedBrowser

RedBrowser is a Java based trojan. It runs on J2ME enabled devices and masquarades as a WAP browser with free browsing using SMS. Actually the program sends SMS messages to a certain number which may cause financial losses to the victim.

This virus uses social engineering to get access to the messaging services. If the user gives the program the required permissions it asks to send the messages. Social engineering messages of the trojan are in Russian, which hinders the functionality outside Russia [21].

5.5 FlexiSpy

FlexiSpy is a Symbian-based trojan or toolkit depending on the viewpoint. FlexiSpy is a commercial program [24] and it must be intentionally installed [23]. The program is marketed as a way to catch cheating spouses or protect children. The program sends all usage information to the FlexiSpy server, where the one who installed the program on the monitored device can see the logs. The program can be accessed on the phone with special codes only known to the installer.

FlexiSpy is installed on the phone as a background service. There are no obvious visible clues about the program when it is running. The user can see, however, an application named "Phones" and it can be removed. Most users will not uninstall this since many devices have a background service called "Phone" which provides

the basic functionality. Furthermore, removing an application called "Phones" from a cellphone might seem unwise to many users.

5.6 CardTrap

CardTrap [6] is a cross-platform virus which tries to disable the system and third party applications on the device. It also infects the memory card with malware infecting Windows. However, according to F-Secure the windows malware failed to autorun when the infected memory card was introduced to Windows 2000 or Windows XP systems. It is still a proof of concept that cross-platform malware that includes Symbian is possible.

6 Prevention and countermeasures

It is important to prevent smartphone malware. Therefore we will propose measures that will make malware prevention feasible. We will discuss user education, antivirus software and the roles of network operators and phone manufactures.

6.1 User education

At the moment of writing no smartphone virus can activate itself when it arrives to a device. This means that a user has to accept the installation and/or transfer in order to activate/receive the virus. Thus it may be that currently the most efficient way to hinder the spreading of smartphone viruses is to educate users. Users should not install or transfer any suspicious programs or programs of non-trusted origin. This applies especially to organisations with high information exchange rates and cross-device operations since a virus with multi-platform capabilities could transfer itself to critical systems from a smartphone.

If a virus with abilities to install itself automatically surfaces the situation gets much worse. Therefore it is of great importance to make sure that security holes allowing this kind of behavior are corrected and that these kind of security flaws do not come into existence in the first place.

Many of the viruses depend on social engineering to spread. They can, for example, pretend to be something else or promise the user something for free. User education would most likely make users more resistant to social engineering. For example, a trojan called Skulls (variant D) pretends to be a cracked version of a game or an application [25].

For example, the Finnish Communications Regulatory Authority (FICORA) has already taken steps to educate the users about the security of mobile devices. FICORA and several other organisations and companies such as FiCom, DNA, Elisa, Ericsson, F-Secure, Nokia and TeliaSonera have collaborated to produce the material which can be acquired at http://www.ficora.fi/mobiiliturva/english/index.html. Below are the guidelines that FICORA provides concerning installation of software on mobile phones [7].

- At the stage programs are being installed, the mobile phone always requests user permission or that the installation be confirmed.
- Use only reliable sources for program downloading.
- Remember that a multimedia message or an e-mail message with an installable program from a familiar number or address could also be produced by a malicious program.
- There is anti-virus software available for smartphones. This can be separately obtained from a store or as an anti-virus service offered by the operator.
- If a malicious program accesses your mobile phone, free cleansing tools from the Internet can normally be used to get your mobile phone to work properly again.
- Part of the applications developed for mobiles phones are digitally secured, but this is still rare.
- If you receive a multimedia message on your phone, which has a file name ending with .SIS, the message could include a malicious program. If you are not sure that the message is uninfected, it is recommended that you delete such a message immediately.

Although the information is readily available from the Internet and in printed form, it would probably do no harm to include this information also with every mobile phone sold.

6.2 Antivirus software

Although antivirus software for smartphones is likely to suffer from the same kind of deficiencies than antivirus software with personal computers, antivirus software is likely to restrain the problem. We will next discuss some antivirus software developed so far.

There is a varying selection of antivirus programs for major platforms. MS Smartphone antivirus programs are not as common as programs for Symbian and Palm operating systems. The amount of available programs seems to depend on the level of threat. Even though there are no MS Smartphone 2002 specific viruses there are at least two antivirus programs, one from Kasperky Labs [12] and one from AirScanner [11]. The software

from AirScanner is an on-demand scanner and it must be activated by the user.

The antivirus software from Kaspersky Labs monitors connections which can be used as infection vectors. On PDAs this usually means infrared and other proprietary connections to other devices, which are usually desktop computers. On-demand virus scanning is also available and the program updates itself automatically via the Internet. Kaspersky's antivirus program is available for the Microsoft Pocket PC and Palm OS.

At the moment F-Secure provides an antivirus solution for Symbian platform devices. The range includes both Symbian Series 60 and the Nokia Communicator 9500/9300 series. The program can monitor the device in real time and it can update itself via HTTPS data connection. F-Secure has solutions also for MS Pocket PC 2003 and MS Smartphone 2003 [15].

6.3 Network operators

One way to prevent an epidemic is to use filtering within the network infrastructure. This could be similar to spam filtering in e-mail. One interesting single point in the infrastructure is the Multimedia Messaging Service Center. This facility stores and forwards MMS messages. It could be easy to implement a simple filtering service at this point. The filter would check every message for virus signatures and typical virus-like behavior of messages. If a message with a virus is discovered the sender could be notified. Depending on how strict policies were conducted the facility could filter out explicitly known viruses or even all suspicious messages such as ones including installable SIS-files. In fact, some operators actually indicate that they are filtering network traffic and it seems like a very wise thing to do [17].

6.4 Phone manufacturers

At the moment the user of a Symbian based smartphone needs to go to a store to update the operating system. This means that the users will not probably do that unless there is something clearly wrong with the phone or the new version offers some beneficial features which are obvious to the user. If a security hole would be found and even corrected in time, many users would not go to a store and update their phone. If the update could be done by the users themselves via the Internet the threshold for updating the OS would be much lower. Even better would be automatic updating mechanism without costs to a user. This would keep more phones up to date and thus make it more difficult to exploit security holes.

On the other hand the system updates made by the user open a new security whole. What if a virus could pretend to be an update and get the same permissions on the device as the actual update program?

As with other platforms the rules of diversity and depth apply. Phone manufactures should avoid a situation where a single program is able to cause damage. If an intruder or malware penetrates to a phone it should face additional security mechanisms built inside the system. For example, the possibilities to make unauthorized external connections could be prevented. This seems to be the case so far and most of the viruses need user interaction in order to work effectively.

Furthermore, it would be feasible to implement phone architecture solutions supporting security. For example, if a program tries to make a phone call or network connection it could be physically prohibited. Only when there is a valid permission the connection is established. Please note that the idea is that the prohibition is not based merely on software which might be vulnerable. Hardware level solution would implement a new security layer.

For example, Nokia has tightened the security procedures with their Series 60 third edition. The programs need to be signed if they need to have connectivity or some other features without user acceptance. If the Symbian software is not signed the following need to accepted by the user: reading user data, writing user data, using local services, using environment, using network services (asked each time) and using location services (asked each time). Basic signing provides blanket permissions for these services. Extended signing provides the same but also the access to multimedia device drivers, DRM (Digital Rights Management), power management and generation and capture of system events [22].

6.5 New epidemiological models

Epidemiological models are used to forecast if a virus which has been detected will form an epidemic. They can also tell more about the nature of the epidemic. Usually a virus dies out quietly or it causes an epidemic. The basic models take the connectivity, virus birth rate and disinfection rate as input attributes [20]. This may be insufficient when modeling the spreading of smartphone viruses.

Viruses which spread via Bluetooth connections behave in a profoundly dissimilar way to conventional viruses which use fixed network connections. This is because of the temporary nature of connections to other devices and the varying amount of available connections. Also the geographical location of the phone is

important as there are places where there are lots of phones around and places where there are none. Therefore for a worm to successfully spread via Bluetooth, a device in close proximity is required. According to Mickens and Noble [19] the traditional models (Mickens and Noble refer to the Kephart–White model [20]) are not accurate and may, for example, forecast an epidemic while the virus will die out in reality. Mickens and Noble define two main reasons for this inaccuracy: the status of connectivity varies in mobile networks and the node velocities vary. Because of this Mickens and Noble propose a new model in their article. Mickens and Noble focus around the Bluetooth as the spreading vector. Because of that, a virus with several spreading vectors such as MMS, Bluetooth, removable media and e-mail, would not probably act according to the predictions from their model.

One of the most interesting claims in their article is the estimate that viruses in class 2 Bluetooth devices are unlikely to spread via Bluetooth. This is because the range of class 2 devices is about 10 m and they have a maximum power of 2.5 mW. (There are three classes and the other two are class 1 devices which can use up to 100 mW and reach 100 m and class 3 with power of 1 mW and a range of 1 m.) They state that if a hundred class 2 devices would travel randomly in a 1,000 m^2 area, the device would have zero neighbors 96.2% of time. Even if the number of devices would be 1,000, they would be alone 69.4% of time. Finally Mickens and Noble state: "These Class 2 networks will be impervious to all but the most virulent malicious code. Such code would have to be extremely aggressive in scanning for vulnerable neighbors and exceptionally difficult to purge. For these reasons, effective viruses in Class 2 networks will likely eschew point-to-point contact as the primary infection vector."

The model could be extended to account for different vectors as many of the viruses have multiple vectors. Also some research could be done about current vectors used by smartphone viruses. Many of them spread via multimedia messages and they do not have any proximity requirements: As long as there is a GSM/3G network available, the virus can spread globally. Spreading via MMS messages depends on the phone numbers stored: The more numbers the user has, the more potential targets the virus has. The whole concept of these new vectors affects the epidemiological models and it would be an interesting subject in a more thorough study.

7 Smartphone viruses and media

Like ordinary biological viruses the computer viruses also have a great impact on media. Their uncontrollable nature and spreading are excellent material for newspaper articles. All journalists are not specialists in the area so the information is sometimes questionable or even completely inaccurate. Also there have been claims that the companies producing anti-virus software could raise unnecessary hype about smartphone viruses and that could boost software sales. For example, WDSGlobal (a company which handles support operations for several major phone manufacturers) claimed that the results published by Symantec (anti-virus software producer) on awareness about smartphone viruses do not reflect reality that well. Symantec claimed that 73% of smartphone users are aware of the attacks and viruses aimed at the device [27]. On the other hand only 0.0036 percent of all support inquiries placed at WDSGlobal were about smartphone viruses (May 2005)[26]. Because of such disputes we wanted to see how the media impact of smartphone viruses has developed during the last few years.

We made a small study on the media presence of smartphone viruses in order to see how smartphone viruses and similar appear in a major Finnish newspaper called "Helsingin Sanomat". This way we can see how the general media awareness has developed even though user awareness was not studied in this case.

The study was made using the archives of "Helsingin Sanomat", the largest newspaper in Finland. The timespan was from 2000 to the end of 2005. Articles mentioning virus and cellphone or smartphone were searched. The search term used was: virus AND (cellphone OR smartphone OR cell). The original search term was in Finnish and the word "kannykka" which is a short version of the word "cellphone" and in here it is translated to "cell". The search produced some articles which were not clearly related to the subject in question and only articles which were primary about phones and viruses were counted. The total number of articles returned by the search was 51 and of them only 14 were actually about our subject and most were about viruses in general. The number of occurrences have been compiled in Table 1.

The first reference to a cellphone virus was found on 28 December 2000. The article was about the F-Secure company starting a new mobile phone

Table 1 Number of articles about mobile phone viruses in Helsingin Sanomat

Year	Number of articles
2000	2
2001	0
2002	1
2003	0
2004	3
2005	8

antivirus program. At that time WAP (Wireless Application Protocol) was the most advanced protocol for browsing online content with a phone. Through years 2000 to 2004 there were from none to very few occurrences of cell phone/smartphone viruses. It was not surprising that in the year 2005 the amount of articles was considerably higher since the impact of the smartphone viruses was already seen by the normal consumer. Smartphone viruses are still not a large issue in the media but they have made themselves known. Also the language was quite colorful in many cases and especially one headline stood out: "A Killer SMS Threatens Nokia Cellphones" (published in 21 January 2002).

8 Discussion

Smartphone malware written so far is mostly harmless compared to widespread worms from the conventional environment. This could change instantly if a really nasty worm should arise. In order to prevent this the smartphone operating systems could use more security. For example, the ability to send MMS messages automatically by the virus itself is very alarming. It seems that while the developers have taken care that the phone cannot open IP connections without the acceptance of the user, the conventional messaging system seems insecure as Commwarrior is able to transmit itself via MMS messages without the user noticing.

We should also remember, that if there will be vulnerabilities in smartphone software a worm in smartphones could cause the same kind of epidemics as we have seen in personal computers. Therefore prevention at the smartphone design level is required. This issue has been partly addressed by digitally signing the software.

The most unsettling scenario would include multiplatform viruses which could infect several platforms and spread through them. Imagine a virus which infects the phone through MMS and installs itself automatically. After that when the user synchronizes his mail the virus would spread into a more conventional corporate network. This way the virus could go through all security without anyone noticing. Backdoors could be installed or business systems could be harmed. Maybe also the layer where hand held devices and the conventional corporate networks intertwine should be taken into account. Furthermore, there are several other methods which smartphone malware can use like denial of service attacks, data theft and modification of personal data. A paper discussing the current Symbian malware techniques has been written by Niemelä [18].

So far the average smartphone user has probably been a technically minded person with at least some basic knowledge about viruses and the nature of the device. When smartphones penetrate the mainstream market and most of the phones in use can be classified as smartphones the user base will be much more diverse and the users may not be so aware of smartphone malware. Most computer users have encountered information about viruses, antivirus software and firewalls with their desktop systems but if the user regards the smartphone more like a conventional cellphone he might not be so careful with software from unknown source. Therefore the user should be made aware that he is using a small computer which can become infected and inoperative with malicious software. Maybe the OS should warn the user about the possibilities of malware when the user installs new software on the device.

Another very disturbing scenario is mobile spam. In this case the attacker would take in control several phones and use them like captured PCs to send MMS and SMS spam to all users in the phone book. This is very similar to e-mail spamming. When using a random infected phone to send the spam, it will be the owner of the phone who pays the costs, while the identity of the spammer is hidden. The spammer could use a trojan similar to RedBrowser [21].

Due to the limited nature of the media study in Sect. 7 the conclusions drawn are restricted. It can be said that the year 2005 has been a great year for smartphone viruses in media as they have gained a foothold as a concept. On the 14 May 2005 it was stated by Nokia, Symantec and the Office of Telecommunication that the smartphone viruses are no threat at all. Also on 29 April 2005 ZDNet reported research results from Symantec which stated that 73% of the smartphone users participating in their study knew about the different threats [27]. The last two articles in 2005 (October and December) were about the Commwarrior virus spreading and about the costs which virus inflicted while spreading via MMS messages paid by the victim. There might be a small threat after all. The scale is still small but it seems that in 2005 there was no consensus about the true level of the threat among the major players in the industry.

In the future a more extensive study about the media presence of computer viruses, and maybe even smartphone viruses in detail, would be interesting. Furthermore, correlation between the actual virus threat and the media hype could be researched. The research could be conducted also with scientific newspapers and journals. It might yield quite similar results, but we would expect more criticism and neutral viewpoint. Moreover, the different aspects of social engineering and smartphone malware would be an interesting topic. This is because smartphones are primarily "social devices" as they are mostly used to communicate with other people.

9 Conclusions

Even though the situation seems to be in control at the moment it cannot be said that it will surely remain that way. It is not wise to spread panic or make up threats but on the other hand it is necessary to research the smartphone malware to build better technology and safer systems now and in the future. Probably it is just a matter of time when the majority of phones can be classified as smartphones. It is also likely that all smartphones run only on a handful of platforms and there will probably be a single dominant platform.

It has to be noted that this field advances very fast. During the writing of this article from the spring of 2005 to summer of 2006 many new types of threats have surfaced such as the J2ME-based trojan RedBrowser in the beginning of 2006 and the cross-platform virus CardTrap. Entirely new kinds threats will probably surface in the future also and we cannot prepare ourselves for every possible threat. This means the defenses should be built also on general methods such as user education, in addition to anti-virus technology. Of course, user education is harder to monetize than technology which can be sold as software. At the moment user education seems to be the most effective countermeasure since most of the viruses need user interaction to function. Only after a virus has penetrated to the device real time virus monitors and disinfection tools come into play.

Also the connectivity gets better. Therefore it is crucial that organisations are aware of the possible infection route through the hand-held devices. Smartphones have better integrated base-level security than conventional desktop computers because of their operating system architecture. The current situation being, that all installed software needs to be accepted by the user in the Symbian environment, hinders virus epidemics effectively. If virus authors can go around this obstacle, a widespread outbreak is possible. This also produces the need for new epidemiological models, like the one by Mickens and Noble [19], and the research of new kinds of spreading vectors.

The possibility for malware to cause charges raises a difficult question: Who pays the charges or should be responsible of a malware incident, when the malware creator is not caught? Is it, for example, the user, network operator, phone manufacturer or the software manufacturer? Maybe some conventions could be found from the cases where a malicious program has installed a dialer on a computer. The dialer dials a number with a modem in the computer and the number usually has a cost per minute and the payments go to organisation or person who created the dialer. The RedBrowser J2ME-trojan is very similar to the dialers from the modem age. Even though this is not analogous to the situation described above, there are some similarities. This question becomes valid the moment a major outbreak occurs and the costs to consumers become major. At that point the code of conduct for this issue should be clear.

References

1. Vaughan-Nichols, S. J.: OSs Battle in the Smart-Phone Market. IEEE Comput. Soc. **36**(6), 10–12, ISSN: 0018-9162 (2003)
2. ZdNet Research: IDC: smartphone OS market shares. http://www.itfacts.biz/index.php?id=P323 (29.6.2006) (2003)
3. Ziff Davis Media Inc.: Linux trails Windows, Symbian in converged mobile devices. http://linuxdevices.com/news/NS4058662049.html (29.6.2006) (2005)
4. Wong, F.-L., Stajano, F., Clulow, J.: Repairing the Bluetooth pairing protocol. (2005)
5. Shaked, Y., Wool, A.: Cracking the Bluetooth PIN. http://www.eng.tau.ac.il/~yash/shaked-wool-mobisys05/index.html (29.6.2006) (2005)
6. F-Secure: CardTrap. http://www.f-secure.com/v-descs/cardtrap_a.shtml (20.6.2006) (2006)
7. Finnish Communications Regulatory Authority: Be Careful When Installing Programs. http://www.ficora.fi/mobiiliturva/english/8.html (20.6.2006) (2006)
8. F-Secure: Commwarrior.A. http://www.f-secure.com/v-descs/commwarrior.shtml (28.3.2005) (2005)
9. F-Secure: Lasco.A. http://www.f-secure.com/v-descs/lasco_a.shtml (28.3.2005) (2005)
10. Symentec: Palm.Phage.Dropper. http://securityresponse.symantec.com/avcenter/venc/data/palm.phage.dropper.html (28.3.2005) (2005)
11. Airscanner Corp.: Airscanner Mobile Antivirus for Windows Mobile Smartphone. http://airscanner.com/downloads/smartphone/smav.html (28.3.2005) (2003)
12. Kaspersky Lab: Kaspersky Anti-Virus Mobile. http://www.kaspersky.com/ beta?product=159494805 (28.3.2005) (2005)
13. F-Secure: Mabir.A. http://www.f-secure.com/v-descs/mabir.shtml (13.4.2005) (2005)
14. EICAR: The Anti-Virus test file. http://www.eicar.org/anti_virus_test_file.htm (25.4.2005) (2003)
15. F-Secure: F-Secure Mobile Anti-Virus. http://www.f-secure.co.uk/products/fsmav.html (11.6.2006) (2006)
16. Sanomat, H.: Helsingin Sanomat. http://www.helsingin-sanomat.fi/ (28.6.2006) (2006)
17. Valtovaara, M.: Kannykkaan tullut multimediaviesti aiheutti isot kulut. Helsingin Sanomat. **22**, A8 (2005)
18. Niemelä, J.: What Makes Symbian Malware Tick. In: Proceedings of the 15th Virus Bulletin Conference. Virus Bulletin Ltd., England. pp. 314–322 (2005)
19. Mickens, J.W., Noble, B.D.: Modeling epidemic spreading in mobile environments (2005)
20. Kephart, J., White, S.: Directed-graph epidemiological models of computer viruses. In: Proceedings of the IEEE Computer Symposium on Research in Security and Privacy, pp. 343–359. May 1991
21. F-Secure: RedBrowser. http://www.f-secure.com/v-descs/redbrowser_a.shtml (20.6.2006) (2006)
22. Nokia: Series 60 Platform 3rd Edition: What's New for Developers. http://sw.nokia.com/id/738fd4e2-aa2b-4722-b3b9-25ed7b6858f5/S60_3rd_Edition_What's_New_for_Developers_v1_3_en. pdf (20.6.2006) (2005)

23. F-Secure: FlexiSpy. http://www.f-secure.com/v-descs/flexispy_a.shtml (20.6.2006) (2006)
24. FlexiSpy: FlexiSpy - Spy Software for mobile / cell phones. Protect your children, catch cheating spouses!. http://www.flexispy.com/index.html (20.6.2006) (2006)
25. F-Secure: Skulls.D. http://www.f-secure.com/v-descs/skulls_d.shtml (20.6.2006) (2006)
26. Will, S.: Smartphone virus hype dismissed. http://news.zdnet.co.uk/hardware/mobile/0,39020360,39197468,00.htm (7.3.2006) (2005)
27. Matt, H.: Smartphone users 'aware of the growing threat'. http://news.zdnet.co.uk/hardware/mobile/0,39020360,39196753,00.htm (7.3.2006) (2005)