البرامج الخبيثة تنتقل الى جهاز المحمول

رغد محمد هادي*

فاطمة حسن**

الهيئة العراقية للحاسبات والمعلوماتية-معهد المعلوماتية للدراسات العليا. *

كلية أدارة واقتصاد/الجامعة المستنصرية.**

تقديـــــم البحث 2010/ 9/6

قبول نشر البحث 2011/1/17

الخلاصة

على الرغم من أن أجهزة الموبايل ذات فائدة وإنتاجية كبيرة ألا أنها تتعرض لمخاطر البرامج الخبيثة لذلك فان النظام المقترح مصمم خصيصا من اجل اضافة تحسينات او امنية اعلئ للملفات المرسلة مع الهاتف الجوال (رسائل والاغاني وصور ...الخ) لضمان وصول هذه الملفات الئ اصحابها دون تغيير من قبل البرامج الخبيثة ، ومن اجل معرفة امكانية هذا النظام لقد تم اجراء بعض عمليات الفحص باكتشاف التلاعب او الاضافات التي قد تحدث للملفات المنتقلة عبر الهاتف الجوال من هذه الفيروسات وتم ذلك عن طريق النظام المقترح والذي صمم خصيصا لمكافحة الفيروسات لقد تم تصميم برنامج للكشف عن الشيفرات الخبيثة التي تهاجم الهاتف المحمول.

الكلمات المفتاحية :

اجهزة الموبايل، البرامج الخبيثة، فايروسات الحاسوب، فايروسات الموبايل،الخبيثة.

Abstract

While mobile handheld devices provide productivity benefit, they also pose new risks (Malicious code). So the proposed system specially designed for adding improvements or security for files that sent with the mobile phone (letters, songs, and pictures…etc) to ensure access to their files without change by malicious code, in order to determine the possibility of this system have been some checks discovering manipulation or additions that may occur by viruses, where it supervised the deletion of the signal via mobile phones by viruses. This is done by a proposed system which specially designed anti virus program to detect the malicious code that attack mobile phone device.

Keywords:

Mobile devices, malicious code, computer viruses, phone viruses, malware.

1. Introduction

With the trend toward a highly mobile workforce. The use of handheld device is growing at an ever-increasing rate. These devices are moderately inexpensive productivity tools that have become a necessity for government and industry. While such devices have their limitations, they are nonetheless extremely useful in managing appointments and contact information, accessing remote corporate data, and change it, making those resources a potential target of an attack.

One of the most serious security threats to any computing device is malicious code. Malicious software is defined as any software that attempts to subvert the confidentiality, integrity or availability of a system. The introduction of malicious software on the system from the internet and internal sources has become one of the most significant threats to information security.

The boundary between the different types of malicious software, such as computer viruses, logic bombs, trapdoors, Trojans, worms, and mobile phone viruses, is becoming increasing blurred [2]. Computer viruses are not much different than human viruses, they infect, replicate, and do damage. The spread of computer viruses is also aggravated by unsafe computing practices, just like human viruses. However, with a reasonable amount of care, we can reduce our chances of having data lost because of a viral infection [1]. In this paper we investigate the type of malicious software and propose a system for solving mobile phone viruses.

The paper organized as follows: section2 presents the general context of the presented work by exploring the type of malicious software and explain in details the mobile phone viruses. Section3 covers the structure of the proposed system and section4 presents an overview of related work. Section5 concludes the paper d presents suggestions for future work.

2. Theoretical background:-

2.1 type of malicious software:-

By familiarizing our self with the types of malicious software that exist, we'll be better able to prevent them.

A very simple definition of computer viruses is:" a program that modifies other programs by placing a copy of itself inside them. The damage caused by a virus may consist of the deletion of data or programs may be even reformatting of the hard disk, but more subtle damage is also possible. Some viruses may modify data or introduce typing errors into text. Other viruses may have no intentional effects other than just replicating.[1], like mobile devices, such devices which have communications and internet-access capabilities, have become popular only recently and thus have not been significant targets of Trojan horses, viruses, and worms, [6] three different

groups of viruses occur on PCs, boot sector viruses (**BSV**), program viruses, and application viruses (macro viruses) although a few viruses can belong to more than one group.

2.1.1 BSV (boot sector viruses)

Infects the boot sector on a diskette or hard disk. Normally the boot sector contains code to load the operating system files. The BSV replaces the original boot sector with itself and stores the original boot sector somewhere else on the diskette or simply replaces it totally. When a computer is then later booted from this disk, (or the diskette is in the drive when the computer is turned on, even if it is not strictly speaking a "boot disk") the virus takes control and hides in RAM. It will then loads and execute the original boot sector, and from then on everything will be as usual. Except, of course, that every diskette inserted in the computer will be infected with the virus, unless it is write-protected. [1]

2.1.2 Program viruses

Attach themselves to executable programs, usually .COM and .EXE files but sometime also overlay files. An infected program will contain a copy of the virus, usually at the end, but in some cases at the beginning of the original program. When an infected program is run, the virus may stay resident in memory and infect every program run. Viruses using this method to spread the infection are called "Resident viruses"[1]

2.1.3 Application viruses (macro viruses)

Are contained in the macro language for programs such as Microsoft word and Excel. Perhaps the most prevalent type of virus; they attach themselves to files (as opposed to programs) and are some of the hardest viruses to detect.

Macro viruses are not specific to an operating system and spread with ease via email attachments, floppy disks, web downloads, file transfers, and cooperative applications. Microsoft word and excel files are affected by such viruses. Word macro viruses can infect at different points during a file's use, such as when is opened, saved, closed or deleted.[2]

2.1.4 Logic bomb

(Also known as a backdoor) is code inserted into legitimate software which is designed to produce a result unintended by a legitimate user of the software. (A fragments, which triggered by some event. Often the time or logic bomb inserted to modify the program in some way and malicious acts when some predefined condition occurs. Time bombs activate on after a specific date. Logic bombs can be triggered by any event the program chooses such as the addition or deletion a specific file. When time or logic bomb is triggered, it will usually do something unpleasant. This can range from changing a random byte of data some where on the disk to make the entire disk unreadable.[2]

2.1.5 Trojan horses

Trojan horses programs are a common way for intruders to trik victim into installing "back door" programs that allow intruders easy access to victim system without victim knowledge change system configurations or infect victim computer with a computer viruses.[3]

2.1.6 Worm

A worm is self replicating program. Unlike a virus, a worm does not require any action from a user to spread. It is a program that runs independently, and it consumes the resources of its host from within in order to maintain itself,

and can propagate a complete working version of itself on to other machine. Unlike a virus, a worm makes copies of itself without needing to modify the host. Like viruses worms may (or may not) do things other than replicating.[5]

2.2 Mobile phone viruses

Mobile devices are the next frontier for hackers and virus writers. All mobile devices that access the internet and receive or send text messages are vulnerable to malware. Some devices known as smart-phone, can obtain viruses from downloading and installing an application. Mobile viruses can spread to contacts have stored on user mobile phone. [4]

Mobile phones could eventually be susceptible to viruses because they use operating system that turns them into minicomputers.

The user that can look at the phones that runs Microsoft applications, like Excel these can be e-mailed from a computer to a phone or a PDA(personal digital assistant) and that opens the risk to a virus on the phone.

Other threat come from Bluetooth, which lets users connect their phones and send messages, the technology is handy for those who want to use wireless headsets with their phones or send data from a phone to Bluetooth enabled printers. [6]

Antivirus experts believe that the problem of mobile viruses is more likely to happen when user connects their phones to their computer to personally upload data or connect to the web and download content. This method makes more susceptible to security threats, because it opens phones up to internet viruses and hackers. [7]

The mobile phone has quickly evolved from a simple black box to something more akin to a mini multimedia center. However, like with the PC, as these

devices become more advanced, with increased connectivity, the potential for security threats from viruses and hacks become greater. [7]

Security researchers attack simulations have shown that before long, hackers could infect mobile phone with malicious software that delete personal data or run up a victim's phone bill by making toll calls. The attacks could also degrade or overload mobile networks. Eventually causing them to crash and they could be even more insidious in the future by stealing financial data. [8]

A mobile phone virus is basically the same thing as a computer virus an unwanted executable file that "infect" a device and then copies itself to other devices. But whereas a computer virus or worm spreads through e-mail attachments and Internet downloads, a mobile phone virus or worm spreads via Internet downloads, MMS (Multimedia Messaging Service) attachments and Bluetooth transfers. The most common type of mobile phone infection right now occurs when a mobile phone downloads an infected file from a PC or the internet, but phone to phone viruses are on the rise. [9]

The three dominant mobile device OSs are symbian plam, and two windows CE versions: pocket PC phone edition and smartphone edition. [8]

Current phone to phone viruses almost exclusively infect phone running the symbian operating system. The large number of proprietary operating system in the mobile phone world is one of the obstacles to mass infection.

Infected files usually show up disguised as applications like games, security patches add on functionalities and, of course, pornography and free stuff. Infect text message sometimes steal the subject line from a message victim has received from a friend, which of course increases the likelihood of operating it but operating the message isn't to get infected. The victim has to choose to open the message attachment and agree the program, which is another obstacle to mass infection: to date, no reported phone virus's auto installs. [9]

The user can see the favorable factors for mobile viruses:

1. Mobile devices are becoming popular and powerful Smart devices become more and more popular. When smart devices become smart enough to run various applications, the virus will seize this opportunity to intrude these smart devices.

2. 3G Network is coming Next-generation 3G technologies are taking wireless communication to the next level, offering people an 'always-on' connection, and the ability to send and receive information in almost any form - voice, text, image, or video -- irrespective of place and time.

3. Mobile device programming becomes easy either the Symbian or the Windows Mobile provides development tools, development documents and demos to help developers to do further research, and the third-party vendor also provides assistant tools to enhance the efficiency of developers. All these efforts make mobile phone software developing easier, and at the same time facilitate the mobile phone virus programming.

4. Mobile virus technology is evolving with the development of PC viruses, mobile phone virus technologies also upgrade. PC viruses are directly or indirectly transplanted to the programming of mobile phone viruses. I will give further information of current mobile phone virus technologies later.

5. No perfect Mobile OS although the mobile Operation System has been equipped with a security management mechanism, there would be no OS perfect enough to stop the potential threat accompanying every bug existing in the Operation System or at the application level.[2]

3. General system structure

Although there have been some recent reports of attackers and viruses plaguing handheld PCs, the problem is not widespread. It's always possible to get mobile viruses, but right now we need to be very unlucky to get one.

Some mobile viruses spread in the same way as traditional computer viruses, namely when we download programs or files that are already infected. In the case of mobile phones, that might mean downloading photos, video clips, ring tones, cell phone themes, or other programs. Currently, we are not aware of any viruses that can be transferred from laptop or desktop to windows mobile based device. Other mobile viruses can spread like human viruses do by close contact in the presence of the right host. Some cell phones are equipped with Bluetooth, a technology that allows transferring data between different devices, such as sending photos from cell phone to printer or transferring addresses stored on windows mobile device to laptop. This handy technology comes with a few risks if don't use it correctly. If the Bluetooth enabled on the mobile device and in "discoverable mode", and come within 30 feet of another infected device that also has Bluetooth enabled and is running the same operating system as the mobile device, then we might get infect.

So, the proposed system is designed to protect from mobile phone viruses that comes from internet or from another infected mobile device or from Bluetooth device, the first part in the proposed system is to send all suspect file from infect mobile device to computer device by using Bluetooth, and then generate temporary file in the computer device and add the suspect file from infected mobile device in this temporary file, then check the temporary file from viruses, by anti virus program that illustrate below, if its contain the some type of viruses the proposed system kill it, the proposed system uses multiple scanning engines, each relying on a malicious code signature database, to find Trojan horses, viruses, and worms. The code is then isolated so that it can't reach the handheld device. The second part in the proposed system is if it

cant kill virus the proposed system delete all contain of the temporary file and show message on the screen on computer device say "the temp file is infect", if no mobile phone viruses found the proposed system send the file checking to the temporary file to send it to the mobile device the diagram in figure (1) represent the mechanism of the proposed system.

Its true that numerous companies are developing security software for cell phones, some for free download, some for user purchase and some intended for cell phone service providers. But my proposed system is designed to simply detect and then remove the virus once its received and installed, or it may protect our phone from getting certain viruses in the first place.

3.1 Anti virus program

All users have seen are the beautiful sides of mobile devices, however, wherever there is software application there is virus. When the virus breaks out and the damages follow, all the beautiful glory of mobile devices ends up being a nightmare. And the history of mobile viruses are: the first mobile worm capable of spreading to cell phones named Worm.Cabir was found at June 2004. Cabir is a proof of concept virus running on Symbian operating system which spreads between Symbian mobile phones using a specially formatted Symbian operating system distribution (or SIS) file disguised as a security management utility. When Cabir infects a mobile phone, it scans for other vulnerable phones using Bluetooth, and then sends a copy of itself to the first vulnerable phone it finds. After Cabir, first Windows CE virus named WinCE/Duts occurs at July 2004. Duts, a 1520 bytes long program hand written in assembly for the ARM processor, is a proof of concept virus running on Windows CE Operating System written by 29A. When an infected file is executed the virus pops up a message box: ***Dear User, am I***

allowed to spread? When a user presses "Yes", Duts will attempt to infect all EXE files in the current directory. Duts contains two messages that are not displayed: *This is proof of concept code. Also, i wanted to make avers happy.* SymbOS/Skull and its variants take advantage of a design fault of Symbian OS(OS vulnerability), change the icons of most applications to a skull icon, and lead to function failures of these applications. Once his mobile is infected the victim user can only do hard reset if he has no specific removal tool in hand. Basic principles and development patterns of PC viruses have been widely used in mobile viruses. And at the same time, some features unique to mobile phones enable mobile phone viruses to do special damages. The reasons for the current small number of mobile viruses:

1. **Smart mobile devices** are not very popular Smart mobile device accounts for a small portion of the total mobile market, though its market is increasing very quickly.
2. **Mobile developing is relatively difficult** because of a shortage of development tools and documents
3. **Comparing with PC viruses** that have existed for more than 20 years, mobile virus of two years' history is something comparatively new.
4. **Most of mobile virus writers** compose viruses only for fun, not for profit. In other words, there is no enough profit to drive virus writers and spammers to create more viruses.

So for all the reason above the current mobile antivirus technologies are still very simple. A simplest mobile antivirus software consists of only pattern matching scanning engine, virus definition file and a GUI, while a "complicated" one includes some more functions such as file monitor, simple firewall and software update module, which are a piece of cake in contrast to the rich security functions of PC security software. It's because the mobile antivirus software developing is just beginning, and the technologies are

relatively simple. So we used in this research our basic components of a complete mobile security system with reference to PC security software which are designed for adding improvements or security for files that sent with the mobile phone (letters, songs, and pictures…etc) to ensure access to their files without change by malicious code, in order to determine the possibility of this system have been some checks discovering manipulation or additions that may occur by viruses, where it supervised the deletion of the signal via mobile phones by viruses**.**
And this can dawn it by these rules:

1. First rule is Monitor mobile securit**y** by file system monitor and firewall. File system monitor checks whether a file is valid or not (its damage by malicious code) when it is opened, closed or renamed; network firewall examines the network traffic to detect attacks from network. Additional to the above two monitors, there are some other monitors for mobile devices should be mentioned here: SMS/MMS monitor Mail monitor Bluetooth/Infrared monitor.
2. Second rule is to looking for certain types of instruction or certain ordering of instructions e.g (format, delete, remove....).
3. Third rule is Pattern Matching in the technique of pattern matching; the anti virus program knows the particular sequence of code and is looking for an exact match which will identify the code as a virus. More often, the anti virus program is looking for sequences of code which are similar, but not necessarily identical, to the known sequences of virus code. Pattern matching is the mostly used method in the antivirus engine. In the proposed system we use database, that its filed are virus name, signature, characteristic, and behavior structure, that contents information about

virus, and we can update it to develop the proposed system in the future to detect new viruses daily.

4. fourth rule is Heuristics the anti virus program can combine basic pattern matching techniques with heuristics - a technique using general rather than specific rules - to detect several viruses in the same family. The technique allows a single description to be created which will catch several variants of one virus. The anti virus flowchart represent in figure (2).

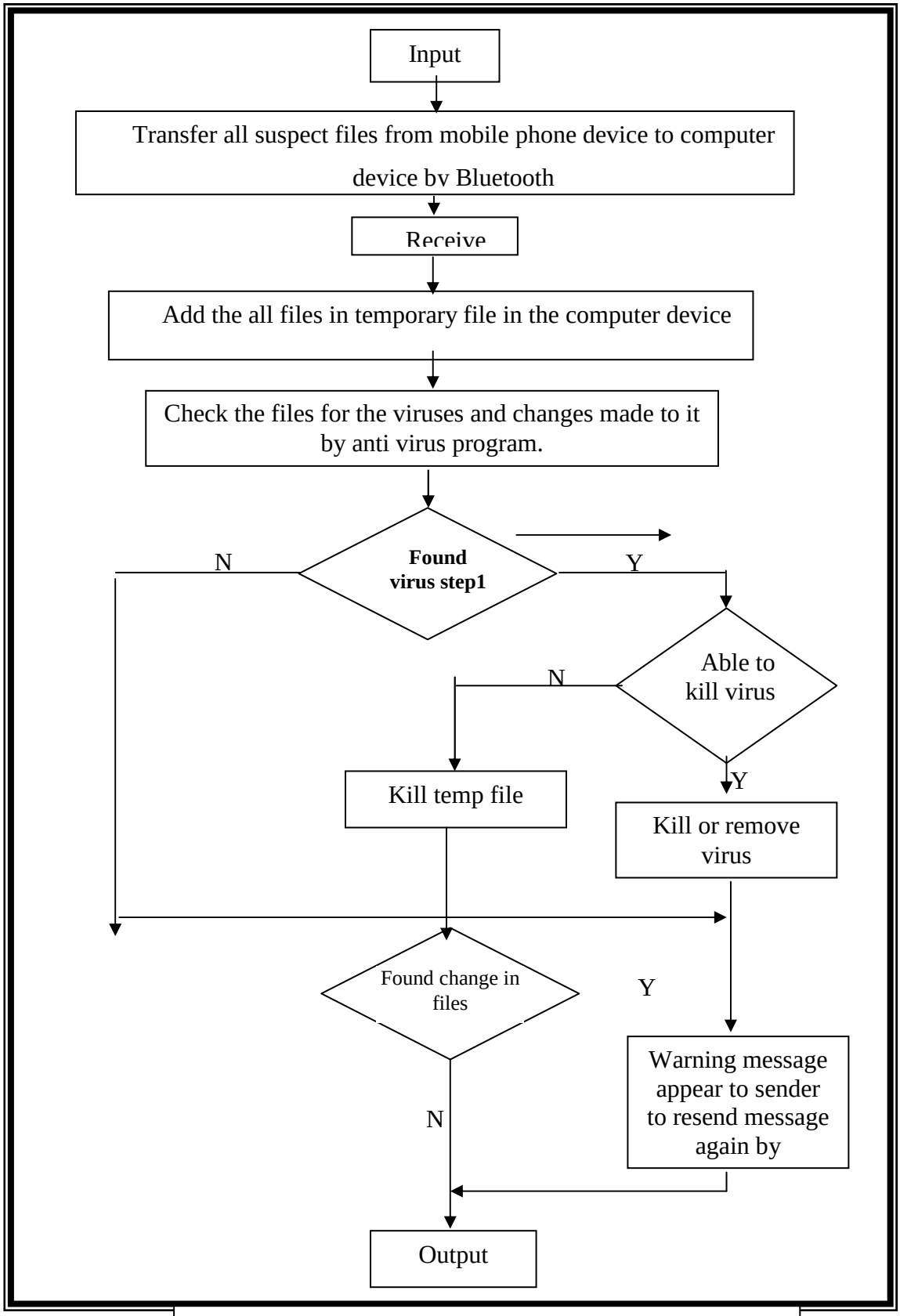

Figure 1: General system software architecture

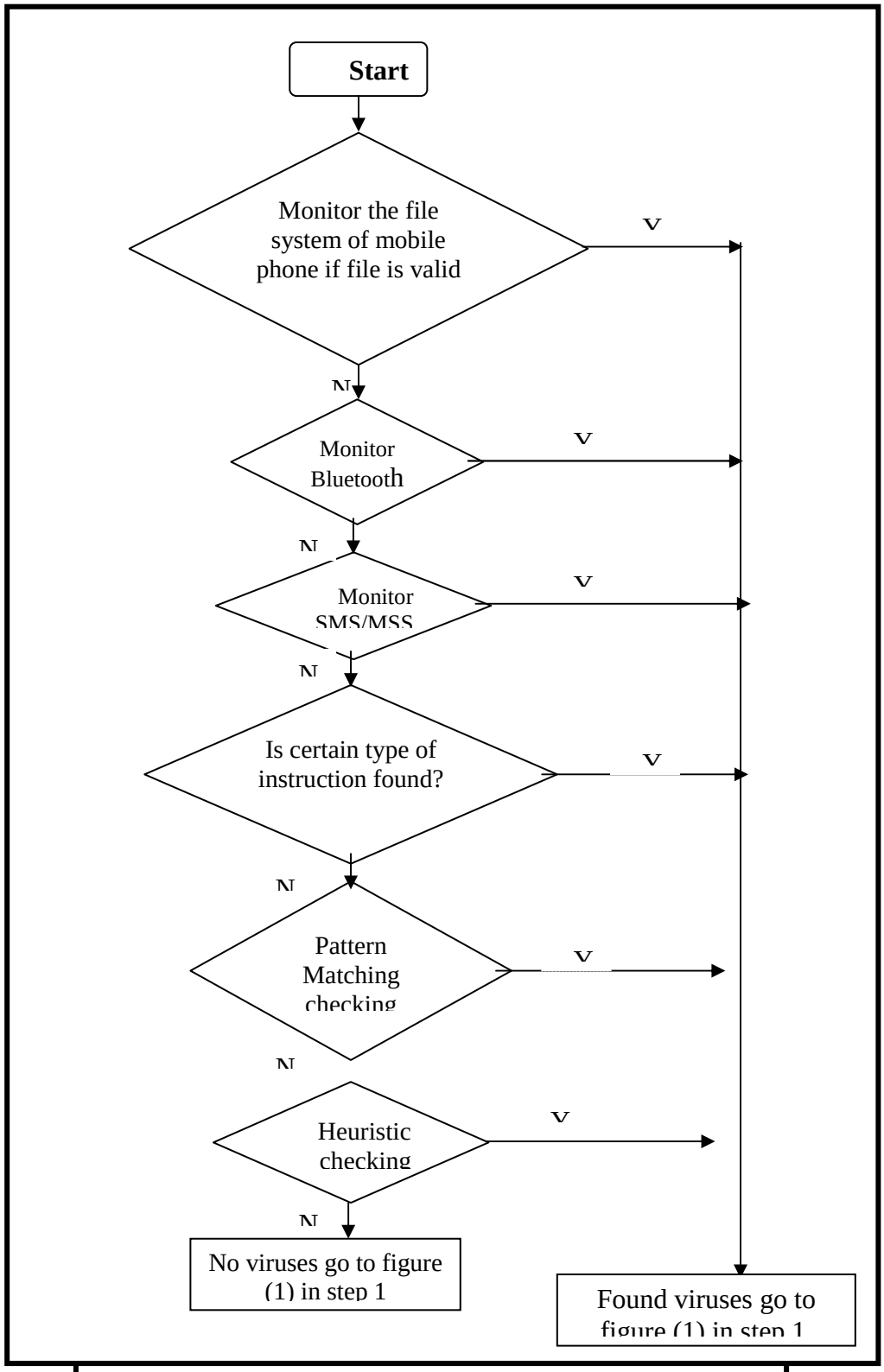

Figure (2): Anti virus programs flowchart

From the figure (1) we can see general system software architecture and the algorithm are explained as:

3.1 Algorithm (1)

Input: Suspect files from mobile phone.

Output: No infect file.

Step1: Transfer all suspect file from mobile phone device to computer device by Bluetooth.

Step2: Add the file in temp file in computer device.

Step3: Open the temp file a file of string to prevent viruses from operation.

Step4: Scanning the temp file for viruses' special strings by anti virus program if found go to step6.

Step5: Check if the change in files is found go to step9.

Step6: Able to kill virus if yes go to step8.

Step7: kill temp file.

Step8: Delete and remove virus.

Step9: Appear the warning message to user to resend message again by Bluetooth.

Step10: End.

4. Conclusions

1. Although mobile viruses are not currently a serious threat, some experts predict that the problem is on the rise and may become more widespread in the future.
2. Mobile phone viruses which attack mobile device by create unnecessary files in mobile device, so our solution is to design checking software procedure implemented and up to date for newer mobile phone viruses.
3. Viruses can let intruder's access passwords or corporate data stored on a cell phone. Also, attackers can manipulate a victim's phone to make calls or send messages, a crime called theft of service.

4. Cell phones are becoming targets largely because of their widespread use, providing millions of potential targets. They also have numerous vulnerabilities. For example, they generally don't come with antivirus software.
5. In addition, mobile devices are much more connected to the outside world than PCs. "phones are primarily used to communicate. They are built to make communication as easy as possible, phone users want to communicate, and viruses want to be communicated".
6. Some hackers may be discouraged from targeting wireless devices because to reach a large number of victims, they would have to design separate sets of malicious code for each mobile operating system and each processor platform.

5. References

[1] Health sciences library, "**Fact sheet: computer viruses**", st. francis medical center Pittsburgh, PA.

[2] Australian communications, "**handbook12 malicious software version 1.0**", electronic security instruction 33(ASCI 33).

[3] CERT coordination center, "**windows 95/98 computer security information**", carngie mellon university, 2006.

[4] Anti virus software for the mobile phone, "**McAfee virus scan mobile**", McAfee, Inc,2005.

[5] Antsar shaded,thesis,"**virus Eradication**",2007.

[6] KOMO staff and news services, "**security experts warn of cell phone viruses**", Internet paper, http://www.securiy week.com/viruses.threat, December 2004.

[7] Tara settembre**, "the future of cell phone viruses article",** internet paper,http://www.bonafidereviews.com/article.php=93, audust 2005**.**

[8] Leavitt communications**, "mobile phones: the next frontier for hackers",** internet paper, http://www.computer.org/portal/web/csdi/doi/mc. 2006.

[9] Julia Layton**, "how cell phone viruses work",** internet paper, 2009.