

INTRUSION AND PROTECTION OF MOBILE DEVICES

I. Mobile Devices

There are more and more mobile devices without which we may lose "connections" in our daily life. We use mobile phones to communicate with our friends, use PDAs to manage our personal affairs, and PSPs and iPods to play games and music. With smart appearance and usages mobile devices free us from the limitations of fixed devices.

Let's first go through the simple classification of mobile devices from Wikipedia.

Due to the varying levels of functionality associated with mobile devices, in 2005 T38 and the DuPont Global Mobility Innovation Team proposed the following standardized definition of mobile devices:

Limited Data Mobile Device: *devices that have a small, primarily text-based screen, with data services usually limited to SMS (Short Message Service) and WAP access. Typical examples of these devices are cellular phones.*

Basic Data Mobile Device: *devices that have a medium-size screen (typically between 120 x 120 and 240 x 240 pixels), menu or icon-based navigation via a thumb-wheel or cursor, and which offer access to e-mail, address book, SMS, and a basic web browser. Typical examples of these devices are BlackBerry and Smartphone.*

Enhanced Data Mobile Device: *devices that have medium to large screens (typically above 240 x 120 pixels), stylus-based navigation, and which offer the same features as the "Basic Data Mobile Devices" plus native applications such as Microsoft Office applications (Word, Excel, PowerPoint) and custom corporate applications such as mobilized versions of SAP, intranet portals, etc. Typical devices include those running Windows Mobile 2003 or version 5, such as Pocket PCs.*

With degrading of the mobile devices software cost and upgrading of its performance, we could actually regard a high-end mobile device as a PC with more diversified functions. The high-end mobile phones, for instance, integrate the image-shooting, radio station, game playing, PDA, Bluetooth, infrared transmission and WiFi all-in-one devices while providing basic phone functions. At the same time, the software designed exclusively for mobile devices also multiple. Many PC programs are transplanted to the mobile devices. Through mobile devices we can surf the internet, check emails, and chat online with friends. With mobile devices, we can edit word files and schedule our life, and, of course, with these little magic gadgets on the palm, we can listen to the music, watch TV and play games playing wherever we go.

II. Mobile Device Viruses

All you 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.

Let's run back over the history of mobile viruses.

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.

The situation when Pocket PC antiviruses detect only EICAR file had to end

...

As a verse by William Blake depicts "if the doors of perception were cleansed every thing would appear to man as it is, infinite." new viruses and their variants begin to propagate. 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.

SymbOS/CommWarrior and its variants integrate some regular technologies used by PC viruses. These worms are capable of spreading both over Bluetooth and MMS messages, and the numbers of phones where they send the MMS messages are read from the phone address book, just like the PC worms read Outlook contacts to get email addresses. New Commwarrior variants can terminate the most common antivirus processes, and reset the mobile randomly.

SymbOS/Redbrowser is a J2ME based Java Midlet that sends SMS messages to premium rate numbers. It affects Symbian S60 devices, apparently works on most phones with J2ME support (ie. hundreds of different phones), and sends SMS messages to Russian premium rate numbers to steal money from the user.

Redbrowser pretends to be a WAP browser that offers free WAP browsing using free SMS messages to send the WAP page contents. Actually Redbrowser.A sends SMS messages to expensive numbers, causing an increased phone bill to the user. After Redbrowser, another proof of concept virus named "CrossOver" was announced. It is a multiplatform virus targeting Windows desktop OS's, Windows CE, and Windows Mobile with .NET CF 1.1. It is the first malware to cross-infect a handheld phone or PDA from a desktop PC binary file. It spreads from a Windows-based desktop PC to a Windows CE-based handheld device via an ActiveSync connection.

According to statistics from Fortinet, there have been more than 40 virus families and more than 300 mobile viruses since the first mobile virus was identified in 2004. The number is keeping increasing.

We can see that the mobile virus technologies are evolving through the typical mobile viruses I mentioned above. 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. So, how will mobile viruses develop in the future? Will they skyrocket to be rampant and devastating or grow slowly and finally disappear?

Let's first examine 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.

Let's see the factors affecting the future development of mobile phone viruses. Here are the negative factors on mobile phone virus increasing:

1. No overwhelming Mobile Device and OS

So far, the smart phone market is shared by many Operation Systems, and the largest share of about 50 percent belongs to Symbian. However, it is a quite different story in the desktop Operation System market where Microsoft holds the lion's share of more than 95 percent. Even for mobile phones using the same Operation System, it could be difficult for the same virus to run universally because of the different types of mobile phones.

2. New Mobile OSs support build-in platform security module

Currently, security is a main focus of mobile Operation System. The newly released Symbian 9.0 OS and the coming Window Mobile 6.0 OS are all equipped with a security management mechanism in Operation System level. Although the mechanism can not prevent viruses coming up in new platform, it could restrict and weaken the performance of viruses to some extent.

Let's 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. The wireless revolution is driving consumer and enterprise applications increasingly closer to the mobile space. We could image that mobile devices in 3G network are just laptops which are always online, they have to face to the security threatens from the network.

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.

Part III: Mobile Virus Technologies

All major PC virus technologies are transplanted to mobile device platforms, and mobile viruses also have their own features.

Basic technologies

1. Infect executables as **classic virus**

WinCE/Duts is the first virus infecting Windows CE executables, and it was proved that Symbian executables could be infected too, at least on Symbian OS 7.0 & 8.0.

2. Spread itself via network as **worm**

Currently, mobile worms spread copies of themselves via Bluetooth and SMS/MMS, and I think there will be worms spread via mail or just network when 3G network is popular.

3. Have a second, non obvious malicious effect as **Trojan** in addition to its primary effect,

4. Set trapdoor in a program to gain access illegally as **backdoor**

5. Exploit OS vulnerabilities as **harm or joke program**

Advanced technologies

Beside to these basic technologies, some other typical technologies are used in the mobile virus area.

1. Social engineering

Social engineering is a collection of techniques used to manipulate people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery for information gathering or computer system access and in most (but not all) cases the attacker never comes face-to-face with the victim. Social engineering is wildly used in the computer security field, and also virus field. Most of worms and Trojans use this technology to induce victims running virus executables or installing virus packages.

2. Basic armoring

The purpose of armoring is primarily to protect virus process from being killed or detected by antivirus software or hinder virus analysts reaching a complete understanding of the virus' code. Such as:

Scan memory for common antivirus processes and terminate them, or even delete

the executable files.
Encrypt the important code and data

3. Buffer overflow exploit

Buffer overflow exploit is one of the major technologies for a remote hacker to penetrate a potential victim system in a user unconscious way. We could notice that a vulnerability in MMS processing in Windows CE 4.2x was found by Collin Mulliner at DefCon in August 2006. A simple script could crash any Nokia device even the latest Nokia N70 and Nokia 3250.

```
<html><body><script>
function crash()
{
    alert('Nokia Browser Crash by Qode');
    shellcode = unescape('%ucccc');
    fill = unescape('%ucccc');
    addr = 0x02020202;
    var b = fill;
    while (b.length <= 0x400000) b+=b;
}
</script>
Nokia Browser Crash by Qode<br>
<input type='button' onClick='crash()' value='Crash'>
</body></html>
```

All of these lead to one conclusion that there are lots of potential bugs on the current mobile Operation System. The virus does not break out just because there are quite few virus writers interested in the vulnerabilities of mobile Operation System. These hidden bugs are still threats to the security of mobile devices, for mobile devices enjoy long lifespan and it is difficult to upgrade the firmware. Once a virus or malicious code completes the buffer overflow exploit, the speed mobile viruses spread and the damages they cause will escalate.

More advanced technologies

I think the following technologies will be used in the mobile virus area sooner or later.

1. Mobile OS rootkit

Like Windows and Linux, once the kernel mechanism of mobile operating system is revealed, Mobile OS rootkit will be released.

2. Advanced armoring

Like Windows viruses, Mobile viruses will begin to use packers or other tools to encrypt and compress virus bodies to make tracing them in a debugger and/or disassembling them difficult.

3. Advanced network technologies

If the 3G Network is wildly used, and mobiles become real internet client, mobile viruses will take advantage of the network and fully use the PC virus experience.

4. Blended attacks

"Blended attacks" is also called "Combined attacks" or "mixed attacks", it

integrates hack methods, such as exploits, vulnerabilities, buffer overflow exploits, etc., and virus technologies, such as infection, spreading, etc.

Additional technologies for mobiles

The following are some special technologies which could be used only under mobile devices.

1. Dial premium rate numbers to steal money from the user.
2. Send SMS/MMS as spam
3. Spread via Bluetooth
4. Infect other OS via memory card

Part IV: Mobile Antivirus Technologies

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.

Let's see the basic components of a complete mobile security system with reference to PC security software:

1. Mobile Security Monitor System
2. Mobile Security Scanning System
3. Mobile Security Update System

Mobile Security Monitor System

Basically, mobile security monitor system should include file system monitor and firewall. File system monitor checks whether a file is valid or not 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

Mobile Security Scanning System

A powerful virus scanning engine is the heart of a security system. Our experience from PC antivirus developing could be totally reused in the mobile antivirus field. Underlying all methods is the basic concept of looking for certain types of instruction or certain ordering of instructions.

Pattern Matching

In the technique of pattern matching, the engine knows the particular sequence of code and is looking for an exact match which will identify the code as a virus. More often, the engine 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.

Heuristics

The virus engine 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.

Emulation

Emulation is a technique applied by the virus engine to polymorphic viruses. Executables that are sent to the engine for scanning are run inside the emulator which tracks the decryption of the virus body as it is written to memory. Normally the virus entry point sits at the front end of a file and is the first thing to run. In most cases, only a small amount of the virus body has to be decrypted in order for the virus to be recognized. Most clean executables stop emulating after only a few instructions, which reduces overheads. Because the emulator runs in a restricted area, if the code does turn out to be a virus, it does not infect the computer.

Mobile Security Update System

There are more ways for mobile devices to keep their security software or virus definition files up-to-date than PCs. The followings are some possible ways for the security software to update.

1. Regular online update

Mobile security software pulls latest update pack from a specific web site, manually or automatically. It is the most commonly used way to update.

2. WAP Push update

WAP Push, has been incorporated into the specification to allow WAP content to be pushed to the mobile handset with minimum user intervention. A WAP Push is basically a specially encoded message which includes a link to a WAP address. Mobile users could simply click the WAP address to get updated.

3. SMS/MMS update

We could use SMS and MMS to get instant updated, and an simple example is that we could send an outbreaking virus update signature in encoded format as a short message to let our clients get updated.

We learn from the PC antivirus software developing experiences that antivirus technologies always lag behind the virus technologies. However, if we get a profound understanding of how viruses were written and how they function, and attempt to work out solutions in advance, we will no longer panic or become bewildered upon the breakout of new viruses. Fortinet will say our solution is to face it with a sober mind and fix it with a quick hand.