Mobile Phones: The Next Frontier for Hackers?

Neal Leavitt

Security experts are finding a growing number of viruses, worms, and Trojan horses that target cellular phones. Although none of the new attacks has done extensive damage in the wild, it's only a matter of time before this occurs, noted Aaron Davidson, CEO of SimWorks International, a New Zealand-based antivirus company.

Security researchers' attack simulations have shown that before long, hackers could infect mobile phones with malicious software that deletes personal data or runs 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, said Davidson.

Smart phones represent a particular risk. They offer Internet connectivity, function like minicomputers, and can download applications or files, some of which could carry malicious code.

Market research firm IDC predicts that by 2008, vendors will sell more than 130 million smart phones, representing 15 percent of all mobile phones. ARC Group, another market research firm, said 27 million smart phones were sold worldwide in 2004, accounting for about 3 percent of the total global handset market.

Mobile-device technology is still relatively new, and vendors have not developed mature security approaches, according to Matias Impivaara, director of mobile security services for antivirus-software vendor F-Secure. "The most worrying scenarios are not coming from stereotypical virus writers such as teenagers but from more organized [criminal groups]."

To counter the growing threat, antivirus companies have stepped up their research and development. In addition, vendors of phones and mobile operating systems are looking for ways to improve security.

DRIVING THE MOBILE ATTACK

Financial gain is perhaps the principal driving force behind mobile malicious code, said Joshua Wright, deputy director of training for the SANS Institute, a research and education organization that operates the Internet Storm Center early-warning system.

Viruses can let intruders 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*.

Users are just beginning to make purchases and conduct financial transactions over mobile devices, particularly in Europe and Japan. Many industry observers expect such activity to increase dramatically during the next few years. Even now, some mobile-phone users store their credit card numbers and other financial information in electronic wallet software.

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.

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," noted SimWorks' Davidson. "Phone users want to communicate, and viruses want to be communicated."

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, said Vanja Svajcer, principal virus researcher for SophosLabs, a global network of virus and spam analysis centers overseen by antivirus company Sophos.

Cell phones use a variety of processor platforms, including those from ARM, Motorola, and Texas Instruments.

The three dominant mobile-device OSs are Symbian, Palm, and two Windows CE versions: Pocket PC Phone Edition and Smartphone Edition. According to Canalys, an industry-analysis research firm, Symbian's market-leading share rose to 53 percent in 2004 from 38 percent in 2003. Thus, Symbian phones have become malware writers' favorite target.

"If a generic language such as Java is used for creating the malicious code,

Published by the IEEE Computer Society

it could affect devices that support Java," noted Impivaara.

NEW MOBILE MALICIOUS CODE

Because mobile malware is relatively new, virus writers have released it primarily as proof-of-concept code so far, according to Wright.

F-Secure found the first mobile virus—designed for Palm devices—in 2000. The company estimates hackers released about a dozen mobile viruses between 2001 and 2003. In 2004, security researchers discovered 21. And F-Secure already identified 10 in the first two months this year.

Several recent mobile viruses have been particularly noteworthy.

Cabir

The well-known 29A Eastern European hacker group, which specializes in creating proof-of-concept viruses, sent the first version of the Cabir worm, known as Cabir.A, to a number of antivirus firms.

Cabir runs on smart phones from vendors such as Motorola, Nokia, Panasonic, and Sony Ericsson that support the Nokia-licensed Symbian Series 60 platform.

Cabir can be acquired via a shared infected application or it can replicate via Bluetooth, a short-range, radio-based, wireless connectivity technology. The worm arrives on victims' phones as an .SIS (Symbian installation system) application-installation file.

Target devices display a message asking users if they want to receive a message via Bluetooth and then ask for further confirmation if the application is not digitally signed by an authorized Symbian authority. If the user chooses to receive the file, it installs and then sends itself to other Bluetooth-enabled devices within the technology's 10-meter range.

After infecting a phone, Cabir.A displays the text "Caribe VZ/20a"and Cabir.B displays "Caribe" on the victim's screen. The worm also interferes with a host device's normal Bluetooth system by forcing it to constantly scan for other enabled devices. This reduces a device's battery life and either makes Bluetooth unavailable to legitimate applications or degrades Bluetooth performance, explained Davidson.

A few users of sites that distribute *warez*—software stripped of copy protection and placed on the Internet for downloading, generally illegally—have reported accessing Cabir-infected applications.

"We recently reported its arrival in Australia and in other countries including China, the Philippines, Singapore, and the United Arab Emirates," Davidson said.

Security experts are finding more malicious code that targets mobile devices.

Sophos advises users to protect themselves against Cabir and other Bluetooth-based threats by simply turning off the Bluetooth settings in their phones that let other devices recognize and contact them via the technology.

There have been several Cabir variants. Cabir.H, for example, attaches itself to applications' installation files on a phone. Victims who download and install the application can unknowingly infect their devices with Cabir.

Skulls

Skulls is a Trojan horse and thus masquerades as a useful application to convince users to install it. Its authors wrote Skulls to appear to be an application that lets users preview, select, and remove design themes for their phone screens.

Hackers deliberately—and file sharers inadvertently—uploaded Skulls to several shareware sites, from which unsuspecting users have downloaded the application.

Skulls targets the Nokia 7610 phone, although some other Symbian Series 60 phones can also install it.

According to SophosLabs' Svajcer, Skulls makes the original Symbian binaries for everyday functions—such as file management, Bluetooth control, messaging, Web browsing, and application installation and removal—useless by replacing them with nonfunctional binaries. The phones can then only make and receive calls.

Because Skulls disables Symbian applications, only phones with third-party file managers can remove the Trojan. Those using Symbian's file manager must perform a hard reset, thereby erasing all stored data. Skulls also replaces each application icon with a skull and crossbones.

Each of several Skulls variants and hybrids has a slightly different effect. For example, Skulls.D—posted to several Web discussion forums and warez sites—pretends to be a Macromedia Flash player for Symbian Series 60 devices. The variant replaces system binaries related to application uninstall and Bluetooth control with nonfunctional binaries, installs the Cabir.M worm, and disables antivirus programs and third-party file managers.

Mquito

Mquito is a version of the popular Mosquito game whose copy protection crackers have broken. Once the game is installed on a Symbian Series 60 device, it surreptitiously sends unauthorized SMS text messages to high-cost toll phone numbers in Germany, Holland, Switzerland, and the UK.

Reportedly, said Vincent Weafer, senior director of Symantec Security Response, game-maker Ojom deliberately added Mosquito's hidden SMS functionality as a copy-protection technique. He said that Ojom, which declined to comment for this article, wanted the program to send an SMS message alerting the company if someone was using an unlicensed copy.

"The Symbian OS provides the functionality required for any application to send and receive SMS messages with or without user intervention," said

Symbian spokesperson Peter Bancroft.

Current versions of the game no longer have the hidden SMS functionality, but cracked versions with the capability are still available online for downloading.

Potential Future Attack Approaches

In the future, mobile viruses will likely try to spread by using the Short Message Service or Multimedia Messaging Service, according to Joshua Wright, deputy director of training for the SANS Institute, an information-security research and education organization.

A fast-spreading SMS or MMS mobile virus could send huge numbers of messages and inundate a carrier's service center or mobile infrastructure, noted John Girard, vice president and research director of security for Gartner, a market research company.

Security vendor SimWorks International recently identified the first Symbian virus capable of spreading via MMS messages. The CommWarrior.a virus scans an infected phone's address book. Using the addresses, it sends itself via MMS to Symbian Series 60 cell phones anywhere in the world, not just within the 10-meter range of Bluetooth, a wireless technology used by some mobile viruses.

SMS and MMS

SMS—a paging-like service for cell phones that use the Global System for Mobile and Code-Division Multiple-Access technologies—is used to send brief text messages to mobile phones. "At 168 characters, the data capacity is very small. It [thus] may not be a useful mechanism for spreading mobile viruses but could let a virus cause harm by generating enormous quantities of SMS traffic," said Aaron Davidson, CEO of SimWorks International.

MMS—an advanced type of SMS for phones that are based on General Packet Radio Service technology—carries up to 50 Kbits of data, large enough for many viruses.

Other approaches

Many cell phones run e-mail applications. However, a virus author probably would not write mobile malware that uses e-mail attachments to transmit itself to wireless devices, as occurs with PCs, according to Wright.

The damage would not be sufficiently great because, unlike SMS and MMS, not many people use cell phones exclusively to read e-mail, explained Vanja Svajcer, principal virus researcher for SophosLabs, a global network of virus and spam analysis centers overseen by antivirus company Sophos. Virus writers would prefer to send malicious code via approaches used primarily by cell phones, he said.

"As mobile instant messaging's popularity grows, the same sorts of attacks seen on PCs are likely to appear, such as hijacking lists of IM names and sending links to recipients to direct them to malicious sites," said Girard. Mobile viruses could also send out IM messages with the malicious code attached, he noted.

The community that develops *warez*—software stripped of copy protection and placed on the Internet for downloading, generally illegally—could make infected mobile games available online to unsuspecting users, added Matias Impivaara, director of mobile security services for antivirus-software vendor F-Secure.

Windows CE virus

The 29A hacker group has written the first proof-of-concept virus for Microsoft's mobile operating system.

Razcan Stoica, spokesperson for BitDefender, a Romanian security company, said the WinCE.Duts.A virus sends recipients a message asking for permission to download.

When granted permission, the virus tries to infect all executable files bigger than 4,096 bytes. During the infection process, the virus appends itself to a file. If a victim tries to run an infected file, the virus will function but the application won't. The virus then attempts to spread, looking for new files to infect.

"When files are exchanged between devices, the virus spreads along with them," said Stoica. "Being a proof-of-concept virus, it has no payload. However, it could be easily adapted."

Metal Gear

Metal Gear is a Trojan camouflaged as a mobile version of the *Metal Gear* Solid video game. To get infected with the Trojan, users must open and install the fake Metal Gear game.

According to SimWorks' Davidson, designers often port PC games to mobile platforms, so *Metal Gear* fans might believe the Trojan actually is a mobile version of the game.

The *Metal Gear* Trojan disables antivirus programs and installs the Cabir.G worm, which tries to spread a second Trojan program, SEXXXY, to nearby phones via Bluetooth.

"Users will have difficulty repairing their phones because the *Metal Gear* Trojan effectively disables all tools on the phone necessary to undo the damage," said Davidson.

Lasco

Lasco.A, a proof-of-concept program, uses Bluetooth to infect mobile phones running on the Symbian Series 60 platform. Lasco can create its own .SIS installer file, which lets the application load itself onto other Bluetooth-enabled devices within range. It can also insert itself into other .SIS files and thereby spread during file sharing. According to the SANS Institute's Wright, Lasco is the first mobile malware that can use both methods to infect devices, thereby increasing its ability to spread.

Once installed, Lasco changes a phone's file directory to include the appended file. It also sets up the .SIS file to tell the target phone's application manager to run Lasco during installation.

The file arrives in the phone's messaging inbox and asks, "Install Velasco?" If the user gives permission, the worm activates and looks for new devices to infect.

Gavno

Gavno, a Trojan reported to SimWorks but not yet found in the wild, contains an application file that hackers have deliberately rendered invalid by, for example, removing critical data. When the Symbian OS tries to use it as the type of file it is supposed to be, problems arise that cause a series of cascading errors in Nokia 6600 and 6630 phones.

The errors cause the OS to become unstable, limiting infected phones to receiving calls. Gavno then makes the phone reboot, which produces similar errors.

One of two variants, Gavno.B, includes a Cabir version.

SimWorks' Davidson predicted that mobile malware will become more sophisticated as virus writers gain more experience and hackers publish the source code for various viruses, worms, and Trojans. The "Potential Future Attack Approaches" sidebar provides more information.

However, Wright said, device vendors and service providers will also increasingly provide better antivirus and other security applications for cell phones, as the "Response and Prevention" sidebar explains.

John Girard, vice president and research director of security for Gartner , a market research company, said, "Antispyware and antivirus functionality will help mobile users be more resistant, but like in the PC world, there will always be hackers who want to rise to the challenge. Mobile device users will have to learn to be more vigilant to ensure that their data and communications stay secure." ■

Response and Prevention

While users now often protect their PCs with antivirus software, such measures are not so widespread in cellular phones. Most users aren't aware of potential mobile malicious code problems and thus aren't vigilant in preventing or avoiding attacks on their phones, said Vanja Svajcer, principal virus researcher for SophosLabs, a global network of virus and spam analysis centers overseen by antivirus company Sophos.

Also, few mobile phones currently have antivirus software, although companies are starting to install it. For example, Japan's NTT DoCoMo now provides buyers of its new Symbian-based FOMA 901i phones with McAfee's VirusScan technology.

Nokia has introduced two phones with Symantec Client Security software, which is preloaded on the memory card and can be updated wirelessly through Symantec LiveUpdate.

Antivirus-software vendor Trend Micro recently rolled out Trend Micro Mobile Security, which provides antivirus and antispam protection for mobile devices' SMS applications.

Mobile antivirus programs are similar to those used for PCs in that they scan files for code strings associated with viruses or watch for potentially harmful activities like those that viruses frequently undertake. Although they must be simpler than PC antivirus programs because mobile devices offer less memory and performance, the OSs and viruses they deal with are also simpler, explained Razcan Stoica, spokesperson for BitDefender, a Romanian security company.

Meanwhile, Symbian's latest version, OSv9, works with Symbian Signed. In this industry-supported program, application developers sign their programs with a tamper-proof digital certificate to verify their identity.

Any Symbian Signed-compliant application will install on a Symbian phone without requiring warning boxes, noted company spokesperson Peter Bancroft. Users could refuse to accept unsigned applications.

"This digital certification will prevent applications from being tampered with, such as by including malware," Bancroft said.

Neal Leavitt *is president of Leavitt Communications, an international marketing communications company based in Fallbrook, California. He writes frequently on technology-related topics. Contact him at neal@leavcom*

Editor: Lee Garber, *Computer*, l.garber@computer.org