Chapter I
Malicious Software in Mobile Devices

Thomas M. Chen
Southern Methodist University, USA

Cyrus Peikari
Airscanner Mobile Security Corporation, USA

ABSTRACT

This chapter examines the scope of malicious software (malware) threats to mobile devices. The stakes for the wireless industry are high. While malware is rampant among 1 billion PCs, approximately twice as many mobile users currently enjoy a malware-free experience. However, since the appearance of the Cabir worm in 2004, malware for mobile devices has evolved relatively quickly, targeted mostly at the popular Symbian smartphone platform. Significant highlights in malware evolution are pointed out that suggest that mobile devices are attracting more sophisticated malware attacks. Fortunately, a range of host-based and network-based defenses have been developed from decades of experience with PC malware. Activities are underway to improve protection of mobile devices before the malware problem becomes catastrophic, but developers are limited by the capabilities of handheld devices.

INTRODUCTION

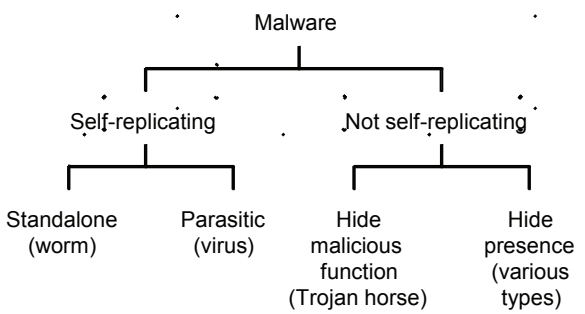
Most people are aware that malicious software (malware) is an ongoing widespread problem with Internet-connected PCs. Statistics about the prevalence of malware, as well as personal anecdotes from affected PC users, are easy to find. PC malware can be traced back to at least the Brain virus in 1986 and the Robert Morris Jr. worm in 1988. Many variants of malware have evolved over 20 years. The October 2006 WildList (www.wildlist.org) contained 780 viruses and worms found to be spreading "in the wild" (on real users' PCs), but this list is known to comprise a small subset of the total number of existing viruses. The prevalence of malware was evident in a 2006 CSI/FBI survey where 65% of the organizations reported being hit by malware, the single most common type of attack.

A taxonomy to introduce definitions of malware is shown in Figure 1, but classification is sometimes difficult because a piece of malware often combines multiple characteristics. Viruses and worms are characterized by the capability to self-replicate,

but they differ in their methods (Nazario, 2004; Szor, 2005). A virus is a piece of software code (set of instructions but not a complete program) attached to a normal program or file. The virus depends on the execution of the host program. At some point in the execution, the virus code hijacks control of the program execution to make copies of itself and attach these copies to more programs or files. In contrast, a worm is a standalone automated program that seeks vulnerable computers through a network and copies itself to compromised victims.

Non-replicating malware typically hide their presence on a computer or at least hide their malicious function. Malware that hides a malicious function but not necessarily its presence is called a Trojan horse (Skoudis, 2004). Typically, Trojan horses pose as a legitimate program (such as a game or device driver) and generally rely on social engineering (deception) because they are not able to self-replicate. Trojan horses are used for various purposes, often theft of confidential data, destruction, backdoor for remote access, or installation of other malware. Besides Trojan horses, many types of non-replicating malware hide their presence in order to carry out a malicious function on a victim host without detection and removal by the user. Common examples include bots and spyware. Bots are covertly installed software that secretly listen for remote commands, usually sent through Internet relay chat (IRC) channels, and execute them on compromised computers. A group of compromised computers under remote control of a single "bot herder" constitute a bot net. Bot nets are often used for spam, data theft, and distributed denial of service attacks. Spyware collects personal user information from a victim computer and transmits the data across the network, often for advertising purposes but possibly for data theft. Spyware is often bundled with shareware or installed covertly through social engineering.

Figure 1. A taxonomy of malicious software



Since 2004, malware has been observed to spread among smartphones and other mobile devices through wireless networks. According to F-Secure, the number of malware known to target smartphones is approximately 100 (Hypponen, 2006). However, some believe that malware will inevitably grow into a serious problem (Dagon, Martin, & Starner, 2004). There have already been complex, blended malware threats on mobile devices. Within a few years, mobile viruses have grown in sophistication in a way reminiscent of 20 years of PC malware evolution. Unfortunately, mobile devices were not designed for security, and they have limited defenses against continually evolving attacks.

If the current trend continues, malware spreading through wireless networks could consume valuable radio resources and substantially degrade the experience of wireless subscribers. In the worst case, malware could become as commonplace in wireless networks as in the Internet with all its attendant risks of data loss, identity theft, and worse. The wireless market is growing quickly, but negative experiences with malware on mobile devices could discourage subscribers and inhibit market growth. The concern is serious because wireless services are currently bound to accounting and charging mechanisms; usage of wireless services, whether for legitimate purposes or malware, will result in subscriber charges. Thus, a victimized subscriber will not only suffer the experience of malware but may also get billed extra service charges. This usage-based charging arrangement contrasts with PCs which typically have flat charges for Internet communications.

This chapter examines historical examples of malware and the current environment for mobile devices. Potential infection vectors are explored. Finally, existing defenses are identified and described.

BACKGROUND

Mobile devices are attractive targets for several reasons (Hypponen, 2006). First, mobile devices have clearly progressed far in terms of hardware and communications. PDAs have grown from simple organizers to miniature computers with their own operating systems (such as Palm or Windows Pocket PC/Windows Mobile) that can download and install a variety of applications. Smartphones combine the communications capabilities of cell phones with PDA functions. According to Gartner, almost 1 billion cell phones will be sold in 2006. Currently, smartphones are a small fraction of the overall cell phone market. According to the *Computer Industry Almanac,* 69 million smartphones will be sold in 2006. However, their shipments are growing rapidly, and IDC predicts smartphones will become 15% of all mobile phones by 2009. Approximately 70% of all smartphones run the Symbian operating system, made by various manufacturers, according to Canalys. Symbian is jointly owned by Sony Ericsson, Nokia, Panasonic, Samsung, and Siemens AG. Symbian is prevalent in Europe and Southeast Asia but less common in North America, Japan, and South Korea. The Japanese and Korean markets have been dominated by Linux-based phones. The North American market has a diversity of cellular platforms.

Nearly all of the malware for smartphones has targeted the Symbian operating system. Descended from Psion Software's EPOC, it is structured similar to desktop operating systems. Traditional cell phones have proprietary embedded operating systems which generally accept only Java applications. In contrast, Symbian application programming interfaces (APIs) are publicly documented so that anyone can develop applications. Applications packaged in SIS file format can be installed at any time, which makes Symbian devices more attractive to both consumers and malware writers.

Mobile devices are attractive targets because they are well connected, often incorporating various means of wireless communications. They are typically capable of Internet access for Web browsing, e-mail, instant messaging, and applications similar to those on PCs. They may also communicate by cellular, IEEE 802.11 wireless LAN, short range Bluetooth, and short/multimedia messaging service (SMS/MMS).

Another reason for their appeal to malware writers is the size of the target population. There were more than 900 million PCs in use worldwide in 2005 and will climb past 1 billion PCs in 2007, according to the *Computer Industry Almanac.* In comparison, there were around 2 billion cellular subscribers in 2005. Such a large target population is attractive for malware writers who want to maximize their impact.

Malware is relatively unknown for mobile devices today. At this time, only a small number of families of malware have been seen for wireless devices, and malware is not a prominent threat in wireless networks. Because of the low threat risk, mobile devices have minimal security defenses. Another reason is the limited processing capacity of mobile devices. Whereas desktop PCs have fast processors and plug into virtually unlimited power, mobile devices have less computing power and limited battery power. Protection such as antivirus software and host-based intrusion detection would incur a relatively high cost in processing and energy consumption. In addition, mobile devices were never designed for security. For example, they lack an encrypting file system, Kerberos authentication, and so on. In short, they are missing all the components required to secure a modern, network-connected computing device.

There is a risk that mobile users may have a false sense of security. Physically, mobile devices feel more personal because they are carried everywhere. Users have complete physical control of them, and hence they feel less accessible to intruders. This sense of security may lead users to trust the devices with more personal data, increasing the risk of loss and appeal to attackers. Also, the sense of security may lead users to neglect security precautions such as changing default security configurations.

Although mobile devices might be appealing targets, there are certain drawbacks to malware for mobile devices. First, mobile devices usually have intermittent connectivity to the network or other devices, in order to save power. This fact limits the ability of malware to spread quickly. Second,

if malware is intended to spread by Bluetooth, Bluetooth connections are short range. Moreover, Bluetooth devices can be turned off or put into hidden mode. Third, there is a diversity of mobile device platforms, in contrast to PCs that are dominated by Windows. Some have argued that the Windows monoculture in PCs has made PCs more vulnerable to malware. To reach a majority of mobile devices, malware writers must create separate pieces of malware code for different platforms (Leavitt, 2005).

EVOLUTION OF MALWARE

Malware has already appeared on mobile devices over the past few years (Peikari & Fogie, 2003). While the number is still small compared to the malware families known for PCs, an examination of prominent examples shows that malware is evolving steadily. The intention here is not to exhaustively list all examples of known malware but to highlight how malware has been developing.

Palm Pilots and Windows Pocket PCs were common before smartphones, and malware appeared first for the Palm operating system. Liberty Crack was a Trojan horse related to Liberty, a program emulating the Nintendo Game Boy on the Palm, reported in August 2000 (Foley & Dumigan, 2001). As a Trojan, it did not spread by self-replication but depended on being installed from a PC that had the "liberty_1_1_crack.prc" file. Once installed on a Palm, it appears on the display as an application, Crack. When executed, it deletes all applications from the Palm (www.f-secure.com/v-descs/lib_palm.shtml).

Discovered in September 2000, Phage was the first virus to target Palm PDAs (Peikari & Fogie, 2003). When executed, the virus infects all third-party applications by overwriting them (http://www.f-secure.com/v-descs/phage.shtml). When a program's icon is selected, the display turns gray and the selected program exits. The virus can spread directly to other Palms by infrared beaming or indirectly through PC synchronization.

Another Trojan horse discovered around the same time, Vapor is installed on a Palm as the application "vapor.prc" (www.f-secure.com/v-descs/vapor.shtml). When executed, it changes the file attributes of other applications, making them invisible (but not actually deleting them). It does not self-replicate.

In July 2004, Duts was a proof-of-concept virus, the first to target Windows Pocket PCs. It asks the user for permission to install. If installed, it attempts to infect all EXE files larger than 4096 bytes in the current directory.

Later in 2004, Brador was a backdoor for Pocket PCs (www.f-secure.com/v-descs/brador.shtml). It installs the file "svchost.exe" in the Startup directory so that it will automatically start during the device bootup. Then it will read the local host IP address and e-mail that to the author. After e-mailing its IP address, the backdoor opens a TCP port and starts listening for commands. The backdoor is capable of uploading and downloading files, executing arbitrary commands, and displaying messages to the PDA user.

The Cabir worm discovered in June 2004 was a milestone marking the trend away from PDAs and towards smartphones running the Symbian operating system. Cabir was a proof-of-concept worm, the first for Symbian, written by a member of a virus writing group 29A (www.f-secure.com/v-descs/cabir.shtml). The worm is carried in a file "caribe.sis" (Caribe is Spanish for the Caribbean). The SIS file contains autostart settings that will automatically execute the worm after the SIS file is installed. When the Cabir worm is activated, it will start looking for other (discoverable) Bluetooth devices within range. Upon finding another device, it will try to send the caribe.sis file. Reception and installation of the file requires user approval after a notification message is displayed. It does not cause any damage.

Cabir was not only one of the first malware for Symbian, but it was also one of the first to use Bluetooth (Gostev, 2006). Malware is more commonly spread by e-mail. The choice of Bluetooth meant that Cabir would spread slowly in the wild. An infected smartphone would have to discover another smartphone within Bluetooth range and the target's user would have to willingly accept the transmission of the worm file while the devices are

within range of each other.

In August 2004, the first Trojan horse for smartphones was discovered. It appeared to be a cracked version of a Symbian game Mosquitos. The Trojan made infected phones send SMS text messages to phone numbers resulting in charges to the phones' owners.

In November 2004, the Trojan horse—Skuller—was found to infect Symbian Series 60 smartphones (www.f-secure.com/v-descs/skulls.shtml). The Trojan is a file named "Extended theme.SIS," a theme manager for Nokia 7610 smartphones. If executed, it disables all applications on the phone and replaces their icons with a skull and crossbones. The phone can be used to make calls and answer calls. However, all system applications such as SMS, MMS, Web browsing, and camera do not work.

In December 2004, Skuller and Cabir were merged to form Metal Gear, a Trojan horse that masquerades as the game of the same name. Metal Gear uses Skulls to deactivate a device's antivirus. This was the first malware to attack antivirus on Symbian smartphones. The malware also drops a file "SEXXXY.SIS," an installer that adds code to disable the handset menu button. It then uses Cabir to send itself to other devices.

Locknut was a Trojan horse discovered in February 2005 that pretended to be a patch for Symbian Series 60 phones. When installed, it drops a program that will crash a critical system service component, preventing any application from launching.

In March 2005, ComWar or CommWarrior was the first worm to spread by MMS among Symbian Series 60 smartphones. Like Cabir, it was also capable of spreading by Bluetooth. Infected phones will search for discoverable Bluetooth devices within range; if found, the infected phone will try to send the worm in a randomly named SIS file. But Bluetooth is limited to devices within 10 meters or so. MMS messages can be sent to anywhere in the world. The worm tries to spread by MMS messaging to other phone owners found in the victim's address book. MMS has the unfortunate side effect of incurring charges for the phone owner.

Drever was a Trojan horse that attacked antivirus software on Symbian smartphones. It drops non-functional copies of the bootloaders used by Simworks Antivirus and Kaspersky Symbian Antivirus, preventing these programs from loading automatically during the phone bootup.

In April 2005, the Mabir worm was similar to Cabir in its ability to spread by Bluetooth. It had the additional capability to spread by MMS messaging. It listens for any arriving MMS or SMS message and will respond with a copy of itself in a file named "info.sis."

Found in September 2005, the Cardtrap Trojan horse targeted Symbian 60 smartphones and was one of the first examples of smartphone malware capable of infecting a PC (www.f-secure.com/v-descs/cardtrap_a.shtml). When it is installed on the smartphone, it disables several applications by overwriting their main executable files. More interestingly, it also installs two Windows worms, Padobot.Z and Rays, to the phone's memory card. An autorun file is copied with the Padobot.Z worm, so that if the memory card is inserted into a PC, the autorun file will attempt to execute the Padobot worm. The Rays worm is a file named "system.exe" which has the same icon as the system folder in the memory card. The evident intention was to trick a user reading the contents of the card on a PC into executing the Rays worm.

Crossover was a proof-of-concept Trojan horse found in February 2006. It was reportedly the first malware capable of spreading from a PC to a Windows Mobile Pocket PC by means of ActiveSync. On the PC, the Trojan checks the version of the host operating system. If it is not Windows CE or Windows Mobile, the virus makes a copy of itself on the PC and adds a registry entry to execute the virus during PC rebooting. A new virus copy is made with a random file name at each reboot. When executed, the Trojan waits for an ActiveSync connection, when it copies itself to the handheld, documents on the handheld will be deleted.

In August 2006, the Mobler worm for Windows PCs was discovered (www.f-secure.com/v-descs/mobler.shtml). It is not a real threat but is suggestive of how future malware might evolve. When a PC is infected, the worm copies itself to different folders

on local hard drives and writable media (such as a memory card). Among its various actions, the worm creates a SIS archiver program "makesis.exe" and a copy of itself named "system.exe" in the Windows system folder. It also creates a Symbian installation package named "Black_Symbian.SIS." It is believed to be capable of spreading from a PC to smartphone, another example of cross-platform malware.

At the current time, it is unknown whether Crossover and Mobler signal the start of a new trend towards cross-platform malware that spread equally well among PCs and mobile devices. The combined potential target population would be nearly 3 billion. The trend is not obvious yet but Crossover and Mobler suggest that cross-platform malware could become possible in the near future.

INFECTION VECTORS

Infection vectors for PC malware have changed over the years as PC technology evolved. Viruses initially spread by floppy disks. After floppy disks disappeared and Internet connectivity became ubiquitous, worms spread by mass e-mailing. Similarly, infection vectors used by malware for mobile devices have changed over the past few years.

Synchronization: Palm and Windows PDAs were popular before smartphones. PDAs install software by synchronization with PCs (Foley & Dumigan, 2001). For example, Palm applications are packaged as Palm resource (PRC) files installed from PCs. As seen earlier, Palm malware usually relied on social engineering to get installed. This is a slow infection vector for malware to spread between PDAs because it requires synchronization with a PC and then contact with another PC that synchronizes with another PDA. Much faster infection vectors became possible when PDAs and then smartphones started to feature communications directly between mobile devices without having to go through PCs.

E-mail and Web: Internet access from mobile devices allows users away from their desktops to use the most common Internet applications, e-mail and the World Wide Web. Most mobile devices can send and receive e-mail with attachments. In addition, many can access the Web through a microbrowser designed to render Web content on the small displays of mobile devices. Current microbrowsers are similar in features to regular Web browsers, capable of HTML, WML, CSS, Ajax, and plug-ins. Although e-mail and the Web are common vectors for PC malware, they have not been used as vectors to infect mobile devices thus far.

SMS/MMS messaging: Commonly called text messaging, SMS is available on most mobile phones and Pocket PCs. It is most popular in Europe, Asia (excluding Japan), Australia, and New Zealand, but has not been as popular in the U.S. as other types of messaging. Text messaging is often used to interact with automated systems, for example to order products or services or participate in contests. Short messages are limited to 140 bytes of data, but longer content can be segmented and sent in multiple messages. The receiving phone is responsible for reassembling the complete message. Short messages can also be used to send binary content such as ringtones or logos. While SMS is largely limited to text, MMS is a more advanced messaging service allowing transmission of multimedia objects—video, images, audio, and rich text. The ComWar worm was the first to spread by MMS (among Symbian Series 60 smartphones). MMS has the potential to spread quickly. ComWar increased its chances by targeting other phone owners found in the victim's address book. By appearing to come from an acquaintance, an incoming message is more likely to be accepted by a recipient. MMS will likely continue to be an infection vector in the future.

Bluetooth: Bluetooth is a short-range radio communication protocol that allows Bluetooth-enabled devices (which could be mobile or stationary) within 10-100 meters to discover and talk with each other. Up to eight devices can communicate with each other in a piconet, where one device works in the role of "master" and the others in the role of "slaves." The master takes turns to communicate with each slave by round robin. The roles of master and slaves can be changed at any time.

Each Bluetooth device has a unique and per-

manent 48-bit address as well as a user-chosen Bluetooth name. Any device can search for other nearby devices, and devices configured to respond will give their name, class, list of services, and technical details (e.g., manufacturer, device features). If a device inquires directly at a device's address, it will always respond with the requested information.

In May 2006, F-Secure and Secure Networks conducted a survey of discoverable Bluetooth devices in a variety of places in Italy. They found on average 29 to 154 Bluetooth devices per hour in discoverable mode in the different places. In discoverable mode, the devices are potentially open to attacks. About 24% were found to have visible OBEX push service. This service is normally used for transfer of electronic business cards or similar information, but is known to be vulnerable to a BlueSnarf attack. This attack allows connections to a cellular phone and access to the phone book and agenda without authorization. Another vulnerability is BlueBug, discovered in March 2004, allowing access to the ASCII Terminal (AT) commands of a cell phone. These set of commands are common for configuration and control of telecommunications devices, and give high-level control over call control and SMS messaging. In effect, these can allow an attacker to use the phone services without the victim's knowledge. This includes incoming and outgoing phone calls and SMS messages.

The Cabir worm was the first to use Bluetooth as a vector. Bluetooth is expected to be a slow infection vector. An infected smartphone would have to discover another smartphone within a 10-meter range, and the target's user would have to willingly accept the transmission of the worm file while the devices are within range of each other. Moreover, although phones are usually shipped with Bluetooth in discoverable mode, it is simple to change devices to invisible mode. This simple precaution would make it much more difficult for malware.

MALWARE DEFENSES

Practical security depends on multiple layers of protection instead of a single (hopefully perfect) defense (Skoudis, 2004). Fortunately, various defenses against malware have been developed from decades of experience with PC malware. A taxonomy of malware defenses is shown in Figure 2. Defenses can be first categorized as preventive or reactive (defensive). Preventive techniques help avoid malware infections through identification and remediation of vulnerabilities, strengthening security policies, patching operating systems and applications, updating antivirus signatures, and even educating users about best practices (in this case, for example, turning off Bluetooth except when needed, rejecting installation of unknown software, and blocking SMS/MMS messages from untrusted parties). At this time, simple preventive techniques are likely to be very effective because there are relatively few threats that really spread in the wild. In particular, education to raise user awareness would be effective against social engineering, one of the main infection vectors used by malware for mobile devices so far.

Host-Based Defenses

Even with the best practices to avoid infections, reactive defenses are still needed to protect mobile devices from actual malware threats. Reactive defenses can operate in hosts (mobile devices) or within the network. Host-based defenses make sense because protection will be close to the targets. However, host-based processes (e.g., antivirus programs) consume processing and power resources that are more critical on mobile devices than desktop PCs. Also, the approach is difficult to scale to large populations if software must be installed, managed, and maintained on every mobile device. Network-based defenses are more scalable in the sense that one router or firewall may protect a group of hosts. Another reason for network-based defenses is the possibility that the network might be able to block malware before it actually reaches a targeted device, which is not possible with host-based defenses. Host-based defenses take effect after contact with the host. In practice, host-based and network-based defenses are both used in combination to realize their complementary benefits.

The most obvious host-based defense is antivirus software (Szor, 2005). Antivirus does automatic analysis of files, communicated messages, and system activities. All commercial antivirus programs depend mainly on malware signatures which are sets of unique characteristics associated with each known piece of malware. The main advantage of signature-based detection is its accuracy in malware identification. If a signature is matched, then the malware is identified exactly and perhaps sufficiently for disinfection. Unfortunately, signature-based detection has two drawbacks. First, antivirus signatures must be regularly updated. Second, there will always be the possibility that new malware could escape detection if it does not have a matching signature. For that case, antivirus programs often include heuristic anomaly detection which detects unusual behavior or activities. Anomaly detection does not usually identify malware exactly, only the suspicion of the presence of malware and the need for further investigation. For that reason, signatures will continue to be the preferred antivirus method for the foreseeable future.

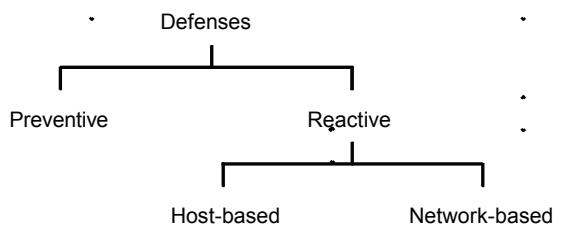
Several antivirus products are available for smartphones and PDAs. In October 2005, Nokia and Symantec arranged for Nokia to offer the option of preloading Symbian Series 60 smartphones with Symantec Mobile Security Antivirus. Other commercial antivirus packages can be installed on Symbian or Windows Mobile smartphones and PDAs.

In recognition that nearly all smartphone malware has targeted Symbian devices, a great amount of attention has focused on the vulnerabilities of that operating system. It might be argued that the system has a low level of application security. For example, Symbian allows any system application to be rewritten without requiring user consent. Also, after an application is installed, it has total control over all functions. In short, applications are totally trusted.

Although Windows CE has not been as popular a target, it has similar vulnerabilities. There are no restrictions on applications; once launched, an application has full access to any system function including sending/receiving files, phone functions, multimedia functions, and so forth. Moreover, Windows CE is an open platform and application development is relatively easy.

Symbian OS version 9 added the feature of code signing. Currently all software must be manually installed. The installation process warns the user if an application has not been signed. Digital signing makes software traceable to the developer and verifies that an application has not been changed since it left the developer. Developers can apply to have their software signed via the Symbian Signed program (www.symbiansigned.com). Developers also have the option of self-signing their programs. Any signed application will install on a Symbian OS phone without showing a security warning. An unsigned application can be installed with user consent, but the operating system will prevent it from doing potentially damaging things by denying access to key system functions and data storage of other applications.

Figure 2. A taxonomy of malware defenses



Network-Based Defenses

Network-based defenses depend on network operators monitoring, analyzing, and filtering the traffic going through their networks. Security equipment include firewalls, intrusion detection systems, routers with access control lists (ACLs), and antivirus running in e-mail servers and SMS/MMS messaging service centers. Traffic analysis is typically done by signature-based detection, similar in concept to signature-based antivirus, augmented with heuristic anomaly based detection.

Traffic filtering is done by configuring firewall and ACL policies.

An example is Sprint's Mobile Security service announced in September 2006. This is a set of managed security services for mobile devices from handhelds to laptops. The service includes protection against malware attacks. The service can scan mobile devices and remove detected malware automatically without requiring user action.

In the longer term, mobile device security may be driven by one or more vendor groups working to improve the security of wireless systems. For instance, the Trusted Computing Group (TCG) (www.trustedcomputinggroup.org) is an organization of more than 100 component manufacturers, software developers, networking companies, and service providers formed in 2003. One subgroup is working on a set of specifications for mobile phone security (TCG, 2006a). Their approach is to develop a Mobile Trusted Module (MTM) specification for hardware to support features similar to those of the Trusted Platform Module (TPM) chip used in computers but with additional functions specifically for mobile devices. The TPM is a tamper-proof chip embedded at the PC board level, serving as the "root of trust" for all system activities. The MTM specification will integrate security into smartphones' core operations instead of adding as applications.

Another subgroup is working on specifications for Trusted Network Connect (TCG, 2006b). All hosts including mobile devices run TNC client software, which collects information about that host's current state of security such as antivirus signature updates, software patching level, results of last security scan, firewall configuration, and any other active security processes. The security state information is sent to a TNC server to check against policies set by network administrators. The server makes a decision to grant or deny access to the network. This ensures that hosts are properly configured and protected before connecting to the network. It is important to verify that hosts are not vulnerable to threats from the network and do not pose a threat to other hosts. Otherwise, they will be effectively quarantined from the network until their security state is remedied. Remedies can include software patching, updating antivirus, or any other changes to bring the host into compliance with security policies.

FUTURE TRENDS

It is easy to see that mobile phones are increasingly attractive as malware targets. The number of smartphones and their percentage of overall mobile devices is growing quickly. Smartphones will continue to increase in functionalities and complexity. Symbian has been the primary target, a trend that will continue as long as it is the predominant smartphone platform. If another platform arises, that will attract the attention of malware writers who want to make the biggest impact.

The review of malware evolution suggests a worrisome trend. Since the first worm, Cabir, only three years ago, malware has advanced steadily to more infection vectors, first Bluetooth and then MMS. Recently malware has shown signs of becoming cross-platform, moving easily between mobile devices and PCs.

Fortunately, mobile security has already drawn the activities of the TCG and other industry organizations. Unlike the malware situation with PCs, the telecommunications industry has decades of experience to apply to wireless networks, and there is time to fortify defenses before malware multiplies into a global epidemic.

CONCLUSION

Malware is a low risk threat for mobile devices today, but the situation is unlikely to stay that way for long. It is evident from this review that mobile phones are starting to attract the attention of malware writers, a trend that will only get worse. At this point, most defenses are common sense practices. The wireless industry realizes that the stakes are high. Two billion mobile users currently enjoy a malware-free experience, but negative experiences with new malware could have a disastrous effect. Fortunately, a range of host-based and network-based defenses have been developed

from experience with PC malware. Activities are underway in the industry to improve protection of mobile devices before the malware problem becomes catastrophic.

REFERENCES

Dagon, D., Martin, T., & Starner, T. (2004). Mobile phones as computing devices: The viruses are coming! *IEEE Pervasive Computing, 3*(4), 11-15.

Foley, S., & Dumigan, R. (2001). Are handheld viruses a significant threat? *Communications of the ACM, 44*(1), 105-107.

Gostev, A. (2006). *Mobile malware evolution: An overview.* Retrieved from http://www.viruslist.com/en/analysis?pubid=200119916

Hypponen, M. (2006). Malware goes mobile. *Scientific American, 295*(5), 70-77.

Leavitt, N. (2005). Mobile phones: The next frontier for hackers? *Computer, 38*(4), 20-23.

Nazario, J. (2004). *Defense and detection strategies against Internet worms.* Norwood, MA: Artech House.

Peikari, C., & Fogie, S. (2003). *Maximum wireless security.* Indianapolis, IN: Sams Publishing.

Skoudis, E. (2004). *Malware: Fighting malicious code.* Upper Saddle River, NJ: Prentice Hall.

Szor, P. (2005). *The art of computer virus research and defense.* Reading, MA: Addison-Wesley.

Trusted Computing Group (TCG). (2006a). *Mobile trusted module specification.* Retrieved from https://www.trustedcomputinggroup.org/specs/mobilephone/

Trusted Computing Group (TCG). (2006b). *TCG trusted network connect TNC architecture for interoperability.* Retrieved from https://www.trustedcomputinggroup.org/groups/network/

KEY TERMS

Antivirus Software: Antivirus software is designed to detect and remove computer viruses and worms and prevent their reoccurrence.

Exploit Software: Exploit software is written to attack and take advantage of a specific vulnerability.

Malware Software: Malware software is any type of software with malicious function, including for example, viruses, worms, Trojan horses, and spyware.

Smartphone: Smartphones are devices with the combined functions of cell phones and PDAs, typically running an operating system such as Symbian OS.

Social Engineering: Social engineering is an attack method taking advantage of human nature.

Trojan Horse: A Trojan horse is any software program containing a covert malicious function.

Virus: A virus is a piece of a software program that attaches to a normal program or file and depends on execution of the host program to self-replicate and infect more programs or files.

Vulnerability: Vulnerability is a security flaw in operating systems or applications that could be exploited to attack the host.

Worm: A worm is a stand-alone malicious program that is capable of automated self-replication.