Mobile Security: Finally a Serious Problem?

Neal Leavitt

The growing popularity of wireless technology may have finally attracted enough hackers to make the potential for serious security threats a reality.

In the world of computers and communications, the more widely a technology is used, the more likely it is to become the target of hackers.

Such is the case with mobile technology, particularly smartphones, which have exploded in popularity in recent years. According to market analysis firm ABI Research, 370 million smartphones were in use globally last year.

Many users download mobile applications with little regard to whether they're secure, providing a ready way for hackers to attack the devices.

In addition, said Gustavo de Los Reyes, executive director for AT&T Security R&D, "These phones are being used frequently for sensitive transactions like banking, mobile payments, and transmitting confidential business data, making them attractive targets if not protected."

"The payoffs—financial and personal information—could be huge," noted Purdue University computer science professor Richard P. Mislan.

Smartphones generally connect to the Internet, as well to PCs for software updates or media synchronization, providing convenient attack vectors.

Device makers and wireless-service providers have long focused on communications and other services, with security remaining an afterthought.

Referring to the two most popular smartphone platforms, Ed Moyle, senior analyst with market research firm Security Curve, said, "Security is now playing catch-up with the rapid adoption of Android and iPhone, both of which are hard for enterprises to manage."

Thus, after years of warnings about mobile security, there finally appears to be a reason to worry.

In fact, the number and types of mobile threats—including viruses, spyware, malicious downloadable applications, phishing, and spam—have spiked in recent months.

For instance, McAfee Labs' threat report for 2010's fourth quarter reported a 46 percent increase in malware targeting mobile phones over the same time period the previous year.

"We're seeing more than 55,000 new pieces of [mobile] malware on a daily basis," said Dave Marcus, McAfee Labs' director of security research and communications.

THREATS ON THE MOVE

Mobile devices increasingly face various types of threats, as Figure 1 shows.

Botnets

Attackers form a botnet by infecting multiple machines with malware that victims generally acquire via e-mail attachments or from compromised applications or websites. The malware gives hackers remote control of the "zombie" devices, which can then be instructed to perform harmful acts in concert.

"These command channels could also provide a way to update the malicious code so that it will communicate or act differently," said Juniper Networks research engineer Troy Vennon.

The easiest way for an attacker to benefit from a mobile zombie network is to send SMS or multimedia message service (MMS) communications to a premium phone account that charges victims fees per message, explained Vennon.

The scammers act as the premium-account owner's affiliates, receiving some of the money that their attacks generate, noted Bradley Antsis, vice

0018-9162/11/$26.00 © 2011 IEEE Published by the IEEE Computer Society

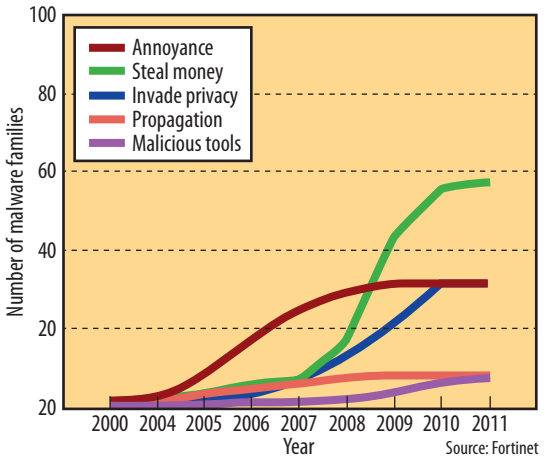

Figure 1. The number of threats to mobile devices, particularly those designed to steal money, has increased steadily during the past few years.

president of technical strategy for security vendor M86.

The Yxe malware family that hit China last year caused this problem.

Also in 2010, malware originating in Holland exploited a vulnerability in jailbroken smartphones—those that owners have modified to gain OS root access and remove manufacturers' usage limitations—to create a botnet. The network sent SMS messages to premium numbers.

Last year, another mobile botnet targeted European customers of a Dutch online bank. The malware used in the attack included command logic that gave the hacker remote control of victims' smartphones.

With PCs, hackers often use zombies within botnets to launch denial-of-service attacks. Thus far, though, there have been no major mobile DoS incidents.

Malicious applications

In some cases, hackers have uploaded malicious programs or games to third-party smartphone-application marketplaces—such as those for Apple's iPhone and Google's Android devices—or have otherwise made them available on the Internet.

"These malicious apps are usually free and get on a phone because users voluntarily install them," said Pierluigi Stella, chief technology officer for Internet security vendor Network Box USA.

Once on a handset, the programs steal personal information such as account passwords and logins and send it back to the hacker. They also open backdoor communication channels, install additional applications, and cause other problems.

Most mobile application marketplaces don't require that code in applications be cryptographically signed by the developer before it can be uploaded, noted Kurt Stammberger, vice president of market development for security vendor Mocana.

"Until this becomes common," he said, "malicious apps will proliferate quickly on mobile platforms."

Social networking

As smartphone use has grown, so has mobile social networking.

Malicious links on social networks can effectively spread malware. Participants tend to trust such networks and are thus willing to click on links that are on "friends'" social networking sites, even though—unknown to the victim—a hacker may have placed them there, said M86's Antsis.

Clicking on a link could download a malicious application on a victim's computer, said Network Box USA's Stella. This could let a hacker place Trojans, spyware, and backdoors on the machine and even conduct identity or information theft, he added.

Some schemes use a sensational headline or promise information on a current hot topic to grab readers' attention and encourage them to click on a malicious link.

Spyware

Hackers can use spyware available online to hijack a phone, allowing them to hear calls, see text messages and e-mails, and even track a user's location through GPS updates.

Most commercial mobile spyware applications send an update of captured communications or location data to a website where the spy logs in to view the data, noted Juniper Networks' Vennon. In some cases, SMS communications inform the spy that the system has obtained new data.

The software can even create a hidden access point inside a mobile phone that lets a hacker turn on the device without it ringing, in essence converting it into a microphone, said Purdue University's Mislan. The spy could then hear nearby conversations.

While some malware writers sell or give away mobile spyware, there are also online vendors—such as ClubMZ, FlexiSPY, and Retina-X Studios—that sell the software commercially.

These companies say their products are only for legal uses and can be helpful in finding a stolen mobile device or in monitoring the activities of children, as well as employees using company phones.

Mobile phone spyware is illegal in the US but is sold by websites hosted elsewhere, noted Simon Heron, principal with Network Box's UK office.

Bluetooth

Bluetooth enables direct communication, including the sharing of content, between mobile devices.

Wireless devices can broadcast their presence and allow unsolicited connections and even the transmission of executables if users don't configure their Bluetooth operations appropriately.

On rare occasions, mobile malware—such as the Cabir worm—has used Bluetooth to propagate.

Wi-Fi

Hackers can intercept communications between smartphones and Wi-Fi hotspots.

The fundamental vulnerability is hotspot architecture with no encryption to protect transmitted data.

"If a user connects to [such] a hotspot for the first time, the end-to-end connection between the user's device and the hotspot provider is not secured, so the [hacker] can intercept and control the user's traffic," said Carnegie Mellon University computer science professor Patrick Tague. In this scenario, the hacker gets between the user and the hotspot provider and hijacks the session via a man-in-the-middle attack.

A hacker can also set up a peer-to-peer network that mimics a Wi-Fi hotspot offering a high-quality connection, which entices users to connect. The hacker then intercepts victims' transmissions without their knowledge.

Phishing

Phishing poses the same risk on smartphones as it does on desktop platforms.

In fact, many users trust their mobile device more than their computers and thus are more vulnerable to phishing.

Additionally, said Juniper Networks' Vennon, the lack of maturity in phishing filters and reputation-based services in mobile browsers, combined with the immediacy and portability of telephone communications, makes the platform attractive for phishers.

Mobile phishing is particularly tempting because wireless communications enable phishing not only via e-mail, as is the case with PCs, but also via SMS and MMS, noted AT&T's de Los Reyes.

Social media phishing is becoming a major issue as social networking sites contain an increasing amount of personal information that phishers can use to make their attacks more effective, said Paul Henry, security and forensics analyst for market research firm Lumension Security.

The number and types of mobile threats—including viruses, spyware, malicious downloadable applications, phishing, and spam—have increased in recent years.

TRADITIONAL SECURITY APPROACHES

Mobile communications can use the same types of security—including antivirus and firewall products—as fixed communications. Vendors include Fortinet, F-Secure, Juniper Networks, Kaspersky Lab, Lookout Inc., Mocana, NetQin, Trend Micro, and Trusteer.

Most of these products work much like their PC counterparts. For example, mobile antivirus products scan files and compare them against a database of known mobile malware code signatures. Noted Mocana's Stammberger, this approach is compute-intensive and "eats batteries for lunch."

Mobile security software is also more likely to use the cloud to offload some of the processing typically associated with PC-based products, said Chris Perret, CEO of security vendor Nukona.

There are only a few mobile encryption software products, including SecurStar's Phonecrypt and Credant Technologies' Mobile Guardian for Handhelds. They're scarce primarily because they're challenging and expensive to develop.

"Restricted [OS] kernel access means you can't put the cryptographic processes sufficiently low down in the stack, close to the silicon. Processor limitations, memory constraints, and battery-life issues make some of these apps as slow as molasses," explained Stammberger.

OTHER MEASURES

Security vendor MobileIron recently launched a storefront so that businesses can deliver mobile applications directly to employees without posting them publicly. This lets businesses enforce security policies about which users and devices can access specific corporate applications.

This summer, trials will start for the AT&T Smart Mobile Computing platform, which will include features such as mobile security, mobile device management, a virtual private gateway, encryption, policy controls, a virtual desktop, and cloud computing capabilities. Customers will also be able to apply their own security policies to this platform.

The AT&T Security Research Center recently opened in New York City. Employees have expertise in a broad range of areas, including security, cellular systems, networking, and data mining.

Under a distribution and marketing agreement signed last year, Verizon Wireless will promote Lookout Inc.'s mobile security products to customers.

Handset and chip makers are also addressing mobile threats. For example, Mocana's Stammberger said his

company is working with Freescale Semiconductor, IBM, Intel, LG, Motorola, and Nokia to "better leverage and improve their on-chip crypto-acceleration hardware."

Mocana also sells Acceleration Harness, a technology for connecting OS-based security software with on-chip hardware acceleration.

As the mobile ecosystem evolves and hackers probe for vulnerabilities, devices will face a growing number of the types of attacks traditionally launched against desktop systems, said Trusteer chief technology officer Amit Klein.

"We need to implement mobile security solutions now to protect against these new threats," he added.

"The greater visibility of these attacks will place an increasing importance on mobile device makers having enterprise-grade security features and configuration options in place. It will become necessary for security to be considered in all phases of application development to ensure that resiliency against attacks is built into mobile devices from the start," said Adrian Stone, director of security response for BlackBerry vendor Research in Motion.

"Our dependence on an always-on, connected, mobile device environment is going to be profound in critical contexts that we can't imagine today," said Stammberger. "We have to be able to trust these devices, but we can't now. There's still a lot of work that needs to be done to get to the point where that trust is warranted."

Neal Leavitt is president of Leavitt Communications (www.leavcom.com), a Fallbrook, California-based international marketing communications company with affiliate offices in Brazil, China, France, India, and the UK. He writes frequently on technology topics and can be reached at neal@leavcom.com.

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

Selected CS articles and columns are available for free at http://ComputingNow.computer.org.