US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Cyber Threats to Mobile Phones

Paul Ruggiero and Jon Foote

Mobile Threats Are Increasing

Smartphones, or mobile phones with advanced capabilities like those of personal computers (PCs), are appearing in more people's pockets, purses, and briefcases. Smartphones' popularity and relatively lax security have made them attractive targets for attackers. According to a report published earlier this year, smartphones recently outsold PCs for the first time, and attackers have been exploiting this expanding market by using old techniques along with new ones.[1] One example is this year's Valentine's Day attack, in which attackers distributed a mobile picture-sharing application that secretly sent premium-rate text messages from the user's mobile phone. One study found that, from 2009 to 2010, the number of new vulnerabilities in mobile operating systems jumped 42 percent.[2] The number and sophistication of attacks on mobile phones is increasing, and countermeasures are slow to catch up.

Smartphones and personal digital assistants (PDAs) give users mobile access to email, the internet, GPS navigation, and many other applications. However, smartphone security has not kept pace with traditional computer security. Technical security measures, such as firewalls, antivirus, and encryption, are uncommon on mobile phones, and mobile phone operating systems are not updated as frequently as those on personal computers.[3] Mobile social networking applications sometimes lack the detailed privacy controls of their PC counterparts.

Unfortunately, many smartphone users do not recognize these security shortcomings. Many users fail to enable the security software that comes with their phones, and they believe that surfing the internet on their phones is as safe as or safer than surfing on their computers.[4]

Meanwhile, mobile phones are becoming more and more valuable as targets for attack. People are using smartphones for an increasing number of activities and often store sensitive data, such as email, calendars, contact information, and passwords, on the devices. Mobile applications for

---

[1] PandaLabs. "Quarterly Report PandaLabs (January-March 2011)." http://press.pandasecurity.com/wp-content/uploads/2011/04/PandaLabs-Report-Q1-2011.pdf

[2] Symantec. "Symantec Report Finds Cyber Threats Skyrocket in Volume and Sophistication." http://www.symantec.com/about/news/release/article.jsp?prid=20110404_03

[3] National Institute of Standards and Technology. "Guidelines on Cell Phone and PDA Security (SP 800-124)." http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf

[4] Trend Micro. "Smartphone Users: Not Smart Enough About Security." http://trendmicro.mediaroom.com/index.php?s=43&news_item=738&type=archived&year=2009

© 2011 Carnegie Mellon University. Produced for US-CERT, a government organization.

social networking keep a wealth of personal information. Recent innovations in mobile commerce have enabled users to conduct many transactions from their smartphone, such as purchasing goods and applications over wireless networks, redeeming coupons and tickets, banking, processing point-of-sale payments, and even paying at cash registers.

Typical Attacks Leverage Portability and Similarity to PCs

Mobile phones share many of the vulnerabilities of PCs. However, the attributes that make mobile phones easy to carry, use, and modify open them to a range of attacks.

- Perhaps most simply, the very portability of mobile phones and PDAs makes them easy to steal. The owner of a stolen phone could lose all the data stored on it, from personal identifiers to financial and corporate data. Worse, a sophisticated attacker with enough time can defeat most security features of mobile phones and gain access to any information they store.[5]
- Many seemingly legitimate software applications, or apps, are malicious.[6] Anyone can develop apps for some of the most popular mobile operating systems, and mobile service providers may offer third-party apps with little or no evaluation of their safety. Sources that are not affiliated with mobile service providers may also offer unregulated apps that access locked phone capabilities. Some users "root" or "jailbreak" their devices, bypassing operating system lockout features to install these apps.
- Even legitimate smartphone software can be exploited. Mobile phone software and network services have vulnerabilities, just like their PC counterparts do. For years, attackers have exploited mobile phone software to eavesdrop, crash phone software, or conduct other attacks.[7] A user may trigger such an attack through some explicit action, such as clicking a maliciously designed link that exploits a vulnerability in a web browser. A user may also be exposed to attack passively, however, simply by using a device that has a vulnerable application or network service running in the background.[8]
- Phishing attacks use electronic communications to trick users into installing malicious software or giving away sensitive information. Email phishing is a common attack on PCs, and it is just as dangerous on email-enabled mobile phones. Mobile phone users are also vulnerable to phishing voice calls ("vishing") and SMS/MMS messages ("smishing").[9] These attacks target feature phones (mobile phones without advanced data and wireless capabilities) as well as smartphones, and they sometimes try to trick users

[5] National Institute of Standards and Technology. "Guidelines on Cell Phone and PDA Security (SP 800-124)." http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf

[6] For example, two attacks in March and May 2011 made several Trojans, or seemingly legitimate apps bundled with malicious software, available in an official app store. The Trojans were downloaded tens of thousands of times before being removed from the store and users' phones.

[7] National Institute of Standards and Technology. "Guidelines on Cell Phone and PDA Security (SP 800-124)." http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf

[8] John Cox. "iPhone on Wi-Fi Vulnerable to Security Attack." http://www.macworld.co.uk/ipod-itunes/news/index.cfm?rss&newsid=27777

[9] US-CERT. "Technical Information Paper-TIP-10-105-01: Cyber Threats to Mobile Devices." http://www.us-cert.gov/reading_room/TIP10-105-01.pdf

into receiving fraudulent charges on their mobile phone bill. Phishers often increase their attacks after major current events, crafting their communications to look like news stories or solicitations for charitable donations. Spammers used this strategy after the March 2011 earthquake and tsunami in Japan.[10]

Consequences of a Mobile Attack Can Be Severe

Many users may consider mobile phone security to be less important than the security of their PCs, but the consequences of attacks on mobile phones can be just as severe. Malicious software can make a mobile phone a member of a network of devices that can be controlled by an attacker (a "botnet"). Malicious software can also send device information to attackers and perform other harmful commands. Mobile phones can also spread viruses to PCs that they are connected to.

Losing a mobile phone used to mean only the loss of contact information, call histories, text messages, and perhaps photos. However, in more recent years, losing a smartphone can also jeopardize financial information stored on the device in banking and payment apps, as well as usernames and passwords used to access apps and online services. If the phone is stolen, attackers could use this information to access the user's bank account or credit card account. An attacker could also steal, publicly reveal, or sell any personal information extracted from the device, including the user's information, information about contacts, and GPS locations. Even if the victim recovers the device, he or she may receive many spam emails and SMS/MMS messages and may become the target for future phishing attacks.

Some personal and business services add a layer of authentication by calling a user's mobile phone or sending an additional password via SMS before allowing the user to log onto the service's website. A stolen mobile phone gets an attacker one step closer to accessing the services as the user. If the device contains the owner's username and password for the service, the attacker would have everything necessary to access the service.

Take Steps to Protect Your Mobile Phone

Although mobile phones are taking on more capabilities formerly available only on PCs, technical security solutions for mobile phones are not as sophisticated or widespread as those for PCs. This means that the bulk of mobile phone security relies on the user making intelligent, cautious choices. Even the most careful users can still fall victim to attacks on their mobile phones. However, following best practices regarding mobile phone security can reduce the likelihood or consequences of an attack.

- **When choosing a mobile phone, consider its security features.** Ask the service provider if the device offers file encryption, the ability for the provider to find and wipe the device remotely, the ability to delete known malicious apps remotely, and authentication features such as device access passwords. If you back up your phone data to a PC, look for an option to encrypt the backup. If you plan to use the device for VPN

[10] Mathew Maniyara. "Phishers Have No Mercy for Japan." http://www.symantec.com/connect/blogs/phishers-have-no-mercy-japan

access, as some users do to access work networks, ask the provider if the device supports certificate-based authentication.

- **Configure the device to be more secure.** Many smartphones have a password feature that locks the device until the correct PIN or password is entered. Enable this feature, and choose a reasonably complex password. Enable encryption, remote wipe capabilities, and antivirus software if available.
- **Configure web accounts to use secure connections.** Accounts for certain websites can be configured to use secure, encrypted connections (look for "HTTPS" or "SSL" in account options pages). Enabling this feature deters attackers from eavesdropping on web sessions. Many popular mail and social networking sites include this option.
- **Do not follow links sent in suspicious email or text messages.** Such links may lead to malicious websites.
- **Limit exposure of your mobile phone number.** Think carefully before posting your mobile phone number to a public website. Attackers can use software to collect mobile phone numbers from the web and then use those numbers to target attacks.
- **Carefully consider what information you want stored on the device.** Remember that with enough time, sophistication, and access to the device, any attacker could obtain your stored information.
- **Be choosy when selecting and installing apps.** Do a little research on apps before installing them. Check what permissions the app requires. If the permissions seem beyond what the app should require, do not install the app; it could be a Trojan horse, carrying malicious code in an attractive package.
- **Maintain physical control of the device, especially in public or semi-public places.** The portability of mobile phones makes them easy to lose or steal.
- **Disable interfaces that are not currently in use, such as Bluetooth, infrared, or Wi-Fi.** Attackers can exploit vulnerabilities in software that use these interfaces.
- **Set Bluetooth-enabled devices to non-discoverable.** When in discoverable mode, your Bluetooth-enabled devices are visible to other nearby devices, which may alert an attacker or infected device to target you. When in non-discoverable mode, your Bluetooth-enabled devices are invisible to other unauthenticated devices.
- **Avoid joining unknown Wi-Fi networks and using public Wi-Fi hotspots.** Attackers can create phony Wi-Fi hotspots designed to attack mobile phones and may patrol public Wi-Fi networks for unsecured devices. Also, enable encryption on your home Wi-Fi network.[11]
- **Delete all information stored in a device prior to discarding it.** Check the website of the device's manufacturer for information about securely deleting data. Your mobile phone provider may also have useful information on securely wiping your device.

[11] See "US-CERT Cyber Security Tip ST05-003 – Securing Wireless Networks" at http://www.us-cert.gov/cas/tips/ST05-003.html.

- **Be careful when using social networking applications.** These apps may reveal more personal information than intended, and to unintended parties. Be especially careful when using services that track your location.
- **Do not "root" or "jailbreak" the device.** Third-party device firmware, which is sometimes used to get access to device features that are locked by default, can contain malicious code or unintentional security vulnerabilities. Altering the firmware could also prevent the device from receiving future operating system updates, which often contain valuable security updates and other feature upgrades.

Act Quickly if Your Mobile Phone or PDA Is Stolen

- **Report the loss to your organization and/or mobile service provider.** If your phone or PDA was issued by an organization or is used to access private data, notify your organization of the loss immediately. If your personal phone or PDA was lost, contact your mobile phone service provider as soon as possible to deter malicious use of your device and minimize fraudulent charges.
- **Report the loss or theft to local authorities.** Depending on the situation, it may be appropriate to notify relevant staff and/or local police.
- **Change account credentials.** If you used your phone or PDA to access any remote resources, such as corporate networks or social networking sites, revoke all credentials that were stored on the lost device. This may involve contacting your IT department to revoke issued certificates or logging into websites to change your password.
- **If necessary, wipe the phone.** Some mobile service providers offer remote wiping, which allows you or your provider to remotely delete all data on the phone.

Additional Resources

US-CERT Resources

- "Technical Information Paper: Cyber Threats to Mobile Devices" (http://www.us-cert.gov/reading_room/TIP10-105-01.pdf)
- "Protecting Portable Devices: Physical Security" (http://www.us-cert.gov/cas/tips/ST04-017.html)
- "Protecting Portable Devices: Data Security" (http://www.us-cert.gov/cas/tips/ST04-020.html)
- "Securing Wireless Networks" (http://www.us-cert.gov/cas/tips/ST05-003.html)
- "Cybersecurity for Electronic Devices" (http://www.us-cert.gov/cas/tips/ST05-017.html)
- "Defending Cell Phones and PDAs Against Attack" (http://www.us-cert.gov/cas/tips/ST06-007.html)

Other Resources

- "Mobile Device Security: Threats, Risks, and Actions to Take" (podcast, http://www.cert.org/podcast/show/20100831frederick.html)
- Internet Crime Schemes: Phishing/Spoofing (http://www.ic3.gov/crimeschemes.aspx#item-14)
- Internet Crime Schemes: Identity Theft (http://www.ic3.gov/crimeschemes.aspx#item-9)