Smartphone Security Challenges

Yong Wang, Kevin Streff, and Sonell Raman, *Dakota State University*

Because of their unique characteristics, smartphones present challenges requiring new business models that offer countermeasures to help ensure their security.

Smartphones are quickly becoming the dominant device for accessing Internet resources. Sales of smartphones overtook PC sales in the global market in Q4 2010.[1] Shipments of smartphones surpassed those of feature phones in Western Europe in Q2 2011.[2] According to a May 2011 Nielsen survey, smartphones outsold feature phones in the US in this same period.[3] Compared to 5.9 billion worldwide mobile phone subscribers, smartphone usage (835 million) is still steadily increasing.[4] IDC predicts smartphone shipments will approach one billion in 2015.[5]

Smartphones offer many more functions than traditional mobile phones. In addition to a preinstalled mobile operating system, such as iOS, Android, or Windows Mobile, most smartphones also typically support carrier networks, Wi-Fi connectivity, and Bluetooth so that users can access the Internet to download and run various third-party applications. Most smartphones support Multimedia Message Service (MMS) and include embedded sensors such as GPS, gyroscopes, and accelerometers, as well as a high-resolution camera, a microphone, and a speaker.

Smartphones' increasing popularity raises many security concerns.[6-9] Their central data management makes them easy targets for hackers. Since the first mobile phone viruses emerged in 2004, smartphone users have reported significant malware attacks. In the last seven months of 2011, malware attacks on the Android platform increased 3,325 percent.[10] As the use of smartphones continues its rapid growth, subscribers must be assured that the services they offer are reliable, secure, and trustworthy.

SMARTPHONE THREATS AND ATTACKS

In a smartphone threat model, a malicious user publishes malware disguised as a normal application through an app store or website. Users will unintentionally download the malware to a smartphone, which carries a large amount of sensitive data. After infiltrating a smartphone, the malware attempts to control its resources, collect data, or redirect the smartphone to a premium account or malicious website.

This model divides a smartphone into three layers:

- The *application* layer includes all of the smartphone's apps, such as social networking software, email, text messaging, and synchronization software.
- The *communication* layer includes the carrier networks, Wi-Fi connectivity, Bluetooth network, Micro USB ports, and MicroSD slots. Malware can spread through any of these channels.
- The *resource* layer includes the flash memory, camera, microphone, and sensors within a smartphone. Because smartphones contain sensitive data, malware targets their resources to control them and manipulate data from them.

An attack forms a loop starting with the launch of the malware, moving through the smartphone's application, communication, and resource layers, on to premium accounts/malicious websites, and back to the malicious user. Figure 1 shows such an attack.

Published by the IEEE Computer Society

0018-9162/12/$31.00 © 2012 IEEE

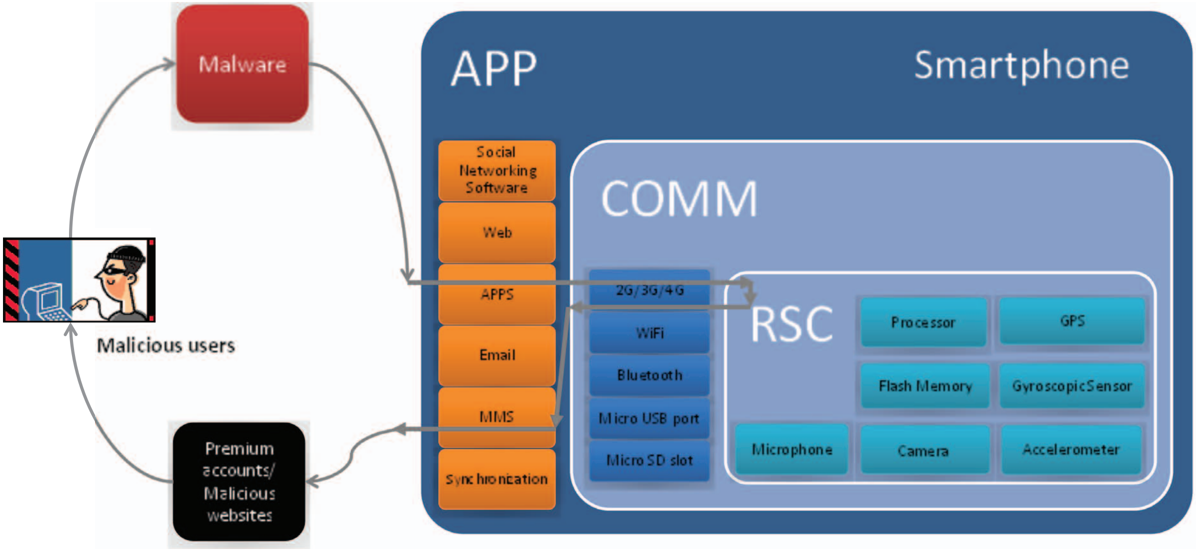

Figure 1. Smartphone threat model. In this attack, the smartphone user unwittingly downloads malware to a smartphone through social networking software via a carrier's network. The malware hijacks the smartphone's resources and sends Multimedia Message Service (MMS) messages to a premium account.

Affected services

Malware's impact can range from minor issues, such as degraded performance, spam messages, and slow operation, to more significant challenges, such as the user not being able to receive and make phone calls or incurring financial loss. The impact to any one smartphone user might be completely different from that experienced by other subscribers.

Jeopardized resources

Resources containing sensitive data are attractive to hackers. Once malware finds a way into the smartphone, it will try to gain privileges to access and control these resources.

For example, flash memory can be quickly reprogrammed with malware that cannot be removed until the user reprograms the flash memory. Some smartphones also include MicroSD memory cards. With a data cable or a card reader, a malicious user can easily disclose the memory card's content.

Sensors, such as GPS, gyroscopes, and accelerometers, also contain sensitive information. GPS, for example, can reveal a smartphone subscriber's location, which the subscriber might not want to disclose.

In addition, a user might not be aware that malware has turned the smartphone camera or microphone on. Malware with full control of a smartphone can thus transform it into a tapping device.

Moreover, data can be leaked when a user transfers data from a smartphone to a computer through a Wi-Fi or Bluetooth network.

Finally, smartphones depend on batteries to power on. Battery exhaustion attacks can dissipate battery power faster than normal, disabling a smartphone's functions.

Malware

Smartphone malware falls into three main categories: viruses, Trojans, and spyware.[10]

Viruses are typically disguised as a game, security patch, or other desirable application, which a user downloads to a smartphone. Viruses can also spread through Bluetooth. Two Bluetooth viruses have been reported in smartphones:

- Bluejacking sends unsolicited messages over Bluetooth to a Bluetooth-enabled device within a limited range (usually around 33 feet).
- Bluesnarfing accesses unauthorized information in a smartphone through a Bluetooth connection.

Most smartphone Trojans are related to activities such as recording calls, instant messaging, finding a location via GPS, or forwarding call logs and other vital data. Smart Message System Trojans comprise a large category of mobile malware that run in an application's background and send SMS messages to a premium rate account owned by an attacker. HippoSMS, for example, increases users' phone charges by sending SMS messages to premium mobile accounts and blocks service providers' messages alerting users of the additional charges.

Spyware collects information about users without their knowledge. According to a 2011 report, spyware was the dominant malware affecting Android phones, accounting for 63 percent of the samples identified.[10]

Carrier IQ software, which runs hidden in the background and does not require authorized consent to function, is usually preinstalled in a smartphone to collect usage data intended to help carriers improve service. Mobile operators, device manufacturers, and application vendors can use this information to deliver high-quality products and services. However, smartphone subscribers usually are not aware of what data is being collected or how it is processed and stored.

Threats and attacks

Smartphone threats and attacks include sniffing, spam, attacker spoofing, phishing, pharming, vishing, and data leakage.

The WebKit engine, which most mobile platforms use, has a vulnerability that lets attackers crash user applications and execute malicious code.

Sniffing captures and decodes packets as they pass over the airwaves. There are various ways to sniff or tap a smartphone. In 2010, Karsten Nohl showed that A5/1, the Global System for Mobile Communications (GSM) encryption function for call and SMS privacy, could be broken in seconds.[11] Thus, all GSM subscribers are at risk for sniffing attacks. Further, as eavesdropping software continues to be available, smartphone subscribers using 3G or 4G networks are also at risk.

Spam can be carried through email or MMS messages. These messages can include URLs that direct users to phishing or pharming websites. MMS spam can also start a denial-of-service (DoS) attack. According to industry analyst Richi Jennings, the number of spam text messages generated in the US increased 45 percent in 2011 to 4.5 billion messages.[12]

Another threat involves an attacker spoofing a caller ID and pretending to be a trusted party. Researchers have spoofed MMS messages that appear to come from 611, which carriers use to send alerts or update notifications.[13] Base stations can also be spoofed.

A phishing attack can masquerade as a trusted party to steal personal information, such as a username, password, or credit card account number. Many phishing attacks have occurred in social networking, email, and MMS messages. For example, a malicious application could include a “Share on Facebook” button that redirects users to a spoofed target application, which could request the user’s secret credentials and steal the data.

Pharming attackers can redirect Web traffic on a smartphone to a malicious or bogus website. By collecting the subscriber’s smartphone information, a pharming attack can lead to other attacks. For example, when a user browses a website on a smartphone, the HTTP header usually includes information about the smartphone’s operating system, browser, and version number. With this information, an attacker can learn the smartphone’s security vulnerabilities and start other directed attacks.

Vishing is short for “voice phishing.” In a vishing attack, malicious users try to gain access to a smartphone user’s financial and other private information. By spoofing a caller ID, the attacker might look like a trusted party and fool the smartphone user into releasing personal credentials.

Data leakage is the unauthorized transmission of personal information or corporate data. Malicious software can steal personal information such as a contact list, location information, or bank information and send this data to a remote website. A smartphone’s data leakage can put its owner at risk of identity theft. Business owners or classified users such as government and military personnel have even more concern about data leakage. ZitMo, a mobile version of Zeus, has been found in Symbian, BlackBerry, and Android devices. An attacker could use ZitMo to steal one-time passwords sent by banks to authenticate mobile transactions.

Web browsers are also vulnerable to smartphone attacks. The WebKit engine, which most mobile platforms use, has a vulnerability that lets attackers crash user applications and execute malicious code. CrowdStrike revealed that attackers could use the WebKit vulnerability to install a remote access tool to eavesdrop on smartphone conversations and monitor user locations. The vulnerability has been found in BlackBerry, iOS, and Android devices.

For various reasons, smartphones are also vulnerable to DoS attacks:

- Because they are based on radio communication technology, smartphones can incur an attack in which a jamming device is used to disrupt the communication between the smartphone and its base station.
- Flooding attacks can generate hundreds of text messages or incoming calls, thus disabling a smartphone.
- A battery exhaustion attack on a smartphone causes more battery discharge than is typically necessary.
- A malicious user could use a smartphone’s blocking features to start a DoS attack. If a malicious user keeps calling a smartphone from a blocked phone number, the subscriber cannot use any of the smartphone’s functions.

Many attacks operate in a stealth mode. Users might not notice these attacks for days or even months. In addition, a malicious user could plant malware in a smartphone but not use it until later.

MOBILE DEVICE FORENSICS

Mobile device forensics—which covers cell phones, smartphones, tablets, personal digital assistants, and GPS receivers—is a subspecialty of computer forensics, necessitated by the near-ubiquity of these devices in today's society. Because mobile devices are increasingly the instrument, target, or record keeper of criminal and other nefarious behaviors, they are of interest in criminal investigations, civil litigation, and intelligence collection. Some would argue that mobile devices contain more probative information per byte examined than traditional computers.

Because most smartphones now come with sophisticated applications, built-in cameras, lots of storage capacity, and high-speed network connectivity, a vast amount of computing power is readily available within the user's grasp. Indeed, smartphones are more properly thought of as portable Internet terminals than merely as phones.

Although mobile device forensics involves retrieving and examining data even if it might have been deleted, for both criminal and civil proceedings, the processes and tools are also used in applications outside the courtroom. Data that can be recovered from a mobile device includes call history, sent and received Short Message Service (SMS) and multimedia messages, contacts and phone numbers, emails, photos, videos, geolocation and GPS information, wireless network settings, Web browsing history, voicemail messages, social networking information, application histories and logs, and other data that might be retained within smartphone apps.

Numerous commercial and open source products are available for extracting and analyzing mobile device data, ranging from camera kits that take screenshots to products that can acquire a file system (logical) or the entire memory (physical) to software that parses databases and hardware to physically examine the device's chips. Figure A shows two of the most widely used products for logical and physical data extraction and analysis: the Cellebrite Universal Forensics Extraction Device (UFED) Ultimate (www.cellebrite.com) and the Micro Systemation XRY Complete/XACT (www.msab.com).

Mobile device forensics requires a process and tools that can extract information from at least six different mobile operating systems (OSs), including iOS, Android, and Windows Mobile, and thousands of models of phones, tablets, and GPS devices.

Even if an examiner can physically acquire the device's memory, examination of that binary dump might still require good, old-fashioned analysis with hex editors, standard computer forensics tools, and regular expressions. As an example, Android phones have considerable fragmentation and variation in OS versions, which makes locating common data across OSs and devices difficult. Even Apple's iPhone returns different data depending on the OS version and whether the phone is jail-broken (freed from the limitations imposed on it by Apple).

Many feature phones and dumb phones in the marketplace store contacts and SMS data on the SIM card, while they usually store images or videos locally on the device. Tablets typically perform the same as handsets with regard to returned forensic data. Despite the availability of many tools, this is not push-button forensics.

Because of the incredible amount of personal and business information stored on mobile devices—or that can be inferred from information on them—security and privacy challenges abound. In addition to placing user information on the phone, the OS also stores information unbeknownst to the user. For example, in April 2011, Apple received considerable media attention when it became known that the iPhone had been recording a detailed history of user geographical locations in an unprotected file; with a simple extraction, a forensic examiner could create a geotagged map of all of the places that iPhone (and presumably its user) visited. The key lesson: sensitive data should always be encrypted in smartphones.

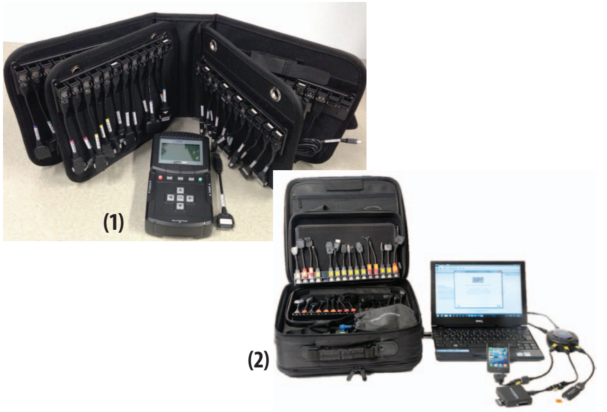

Figure A. Products for use in data extraction and analysis: (1) Cellebrite UFED and (2) Micro Systemation XRY Complete/XACT.

SECURITY CHALLENGES AND IMPACT

As the "Mobile Device Forensics" sidebar describes, the near ubiquity of devices such as smartphones in today's society necessitates the development of this subspecialty of computer forensics. Many techniques used to secure desktop and laptop computers such as antivirus and anti-malware software can be used for smartphone security. However, smartphones have some unique characteristics that make security extremely challenging.

Consumer products

The wide range of smartphone subscribers is matched by the variety of smartphone uses: communication, information, social networking, gaming, entertainment, business enterprise, and so on. Smartphones are consumer products, and different groups of people have different preferences, thus their needs for smartphone security also differ.

No single security tool is appropriate for all subscribers. Smartphone security tools should be configurable to meet the needs of different groups. For example, a business user is typically more concerned about smartphone security than a gamer and thus is willing to spend more to ensure device security.

Finally, most people do not expect to keep their smartphones for a long time. Instead, they expect them to be damaged or lost and to eventually need replacement. Thus, to merit the investment in its purchase, a security solution must be transferrable to a replacement device or it can be purchased in a replacement device at low cost.

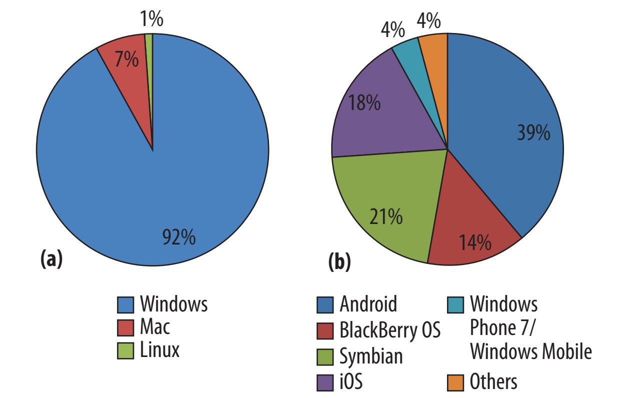

Figure 2. Comparison of desktop operating systems and smartphone operating systems market share.

Platform-oriented

Smartphones have a preinstalled mobile operating system. Unlike desktop operating systems, which are dominated by Microsoft Windows, as Figure 2 shows, Android, iOS, BlackBerry, Symbian, and Windows Mobile share the mobile operating system market.[5]

Each mobile operating system provides different applications, features, and interfaces. The variety lets consumers personalize their devices; however, this presents a challenge to the hardware vendors and smartphone application developers who must support these various mobile operating systems. Further, multiple versions of each mobile operating system might exist, especially for the Android OS.

The differences between these operating systems dictate the security software, as the smartphones must also be platform-oriented. Because operating systems are vulnerable to different security breaches, security software must specifically address each type of breach. Mobile security software developers must therefore customize the software for each mobile platform to deal with multiple operating system and version issues.

Multiple-entrance open system

Smartphones are multiple-entrance open systems, and each entrance is a potential back door for malware access. Each smartphone communication channel is a potential path for malware disguised as an application.

Because smartphones offer multiple entrances, an attack loop can consist of many combinations, but an attack loop cannot be formed if malware is detected, prevented, and removed from the smartphone. Securing a smartphone requires using one of many possible approaches to break the attack loop. For example, resource control could break the attack loop by preventing the malware from gaining access to the smartphone's resources to manipulate its data.

Central data management

Some applications cache users' secret credentials in the smartphone's storage units. This sensitive data might include personal information such as home address, phone numbers, photos, and contact lists; correspondence such as email, text messages, and call logs; credit card information, user names, and passwords; files on flash memory or a memory card; geographic location; and corporate data.

Disclosing this data can end in data leakage resulting in invasion of the smartphone owner's privacy or leading to financial loss.

In addition to using encryption techniques to protect data, migrating data from smartphones to the cloud is another option for securing information and reducing the risk of data theft.

Limited battery life

A smartphone is a resource-constrained device that is powered by a battery with a limited life and that must be recharged when drained. Any security solution must consider this limitation as enhanced security cannot sacrifice battery life.

Vulnerability to theft and loss

Among all potential security issues, loss and theft are two primary concerns for smartphone users. According to a report by Lookout, nine million smartphones were lost in the US in 2011—that's one phone every 3.5 seconds.[14]

Losing control of a smartphone, even temporarily—say, by loaning it to someone—can have catastrophic consequences. With some simple setup, a malicious user can reprogram a smartphone's firmware and flash memory, physically clone the memory card, or install spyware.

Some simple techniques can help protect against smartphone theft and loss. For example, the user can add a password or enable auto-lock. Antitheft technology that remotely deletes sensitive data when a smartphone leaves a secure zone is also available through third-party applications.[15]

Embedded sensors

Smartphones often contain many embedded sensors. Although these sensors enrich a smartphone's functions, they also increase risk. For example, researchers found a way to use accelerometers to decipher computer keystrokes. With a 58,000-word dictionary, they achieved 80 percent accuracy.[16] Using this technique, it is easy to convert a smartphone into a tapping device. With more sensors planned for installation in smartphones, new threats and attacks might be explored and discovered.

However, smartphone owners are vulnerable to the abusive use of smartphone sensor data. For example, some smartphone applications disclose data to a third party. In addition, malware might be disguised as a normal application to request and receive access to GPS data. Finally, malware might jail break an iPhone or iPod Touch to allow the device to run code that is not authorized by Apple and thus gain control of its sensors.

Real-time resource monitoring can help reduce the risks of an attacker using a smartphone's embedded sensors. Further, smartphones could use real-time monitoring to detect and block illegal access of the embedded sensors.

Other concerns

As companies adopt smartphones for their businesses, the BYOD (bring your own device) concept is raising many security concerns for administrators and IT professionals.[17] Although this concept lets employees easily use their own devices to access corporate applications and resources, auditing and enforcing security policies on a personal device is difficult.[9]

The smartphone security challenges that enterprises face include users' failure to back up and encrypt critical data. Further, employees might be unaware that the company has security policies for using smartphones.

Inevitably, most smartphones will include both personal and business data. However, this raises concerns about the security of corporate data. One solution is to develop tools that can distinguish between the two types of data and enforce a higher security level on corporate data.

Educating smartphone users can improve their security awareness. A company should enforce its security policies and regularly audit employee smartphones to ensure their security.

DESIRED SECURITY FEATURES

Confidentiality, integrity, and authentication are three of the most desirable security features in a smartphone.

Most smartphones support synchronization between the device and a computer. This function makes it possible for another user to access the smartphone file system. Thus, to keep data confidential, users should employ encryption techniques and avoid storing sensitive information in plaintext on a smartphone.

Integrity applies to both data and the system. App stores should verify software integration to avoid malicious modification. Further, smartphones should provide mechanisms to protect system integrity. They should also block unauthorized data access requests.

A smartphone authentication service could protect smartphone users against malware attacks that spoof caller IDs and MMS. Because femtocells help improve both coverage and capacity, authentication becomes important to validate a carrier's identity.

Separation of sensitive from nonsensitive data

A smartphone should separate sensitive from nonsensitive data and give users the flexibility to assign data as sensitive. Although sensitive data might be an easy target for hackers, having a clear target to protect instead of taking extra computational and battery power to protect the entire flash drive or memory card is advantageous. In addition, simple security techniques, such as encryption and steganography, can protect sensitive data.

Isolating sensitive data is also good for business. Smartphone users can identify corporate data as being sensitive and assign a higher security level to it.

Encryption

In addition to encrypting sensitive data stored in smartphones, users should encrypt their memory cards. Without a proper decryption key, the smartphone should not disclose the memory card's contents. However, public-key cryptography, such as RSA, usually requires additional computational power and should be used with caution to avoid draining the battery.

> **To keep data confidential, users should employ encryption techniques and avoid storing sensitive information in plaintext on a smartphone.**

Migrating data from smartphones to the cloud is another way to protect sensitive data. Cloud-based intrusion-detection techniques could help detect misbehavior and protect sensitive data.[18] This option would involve a cost for the cloud service. Migrating smartphone data to the cloud also involves background data and thus increases data usage.

Many enterprises have started to explore security solutions for smartphones. Currently, smartphone subscribers are solely responsible for installing applications and ensuring that they are secure. However, security requires collaboration among mobile users, service providers, and industry partners. New business models for smartphone security are therefore highly desired.

Smartphone security is challenging and complicated. However, there are some easy ways to improve smartphone security:

- Increase security awareness. Like a desktop PC or a laptop, a smartphone can be hacked, infected, or phished. Smartphone users should be aware of potential threats and attacks when installing software[19] or authorizing it to access flash memory or smartphone sensors.

- Apply password and auto-lock after a period of time. Most smartphones support these protective features.
- Do not store irreplaceable data in a smartphone. Smartphones can easily be lost or stolen.
- Backup smartphone data regularly. Sync your smartphone with a computer and always keep a backup of your data.
- Turn off Bluetooth when you are not using it. Viruses can spread through Bluetooth to your smartphone.
- Do not use unsecure Wi-Fi hotspots to connect to the Internet. Packet sniffer software such as Wireshark can disclose useful information from smartphone data traffic.
- Use a reliable and trusted security tool to secure your smartphone.
- Ask the smartphone vendor or service provider about antitheft technology such as "erase data" or "default smartphone" remotely.

Some subtle signs might indicate that a smartphone is under attack. For example, the phone's battery is warm even when the device has not been used; the phone lights up at unexpected times, including when it is not in use; or the phone unexpectedly beeps or clicks during phone conversations. If any of these occur, have a security professional check the smartphone. C

References

1. IDC, "Mobile Phone Market Grows 17.9% in Fourth Quarter, According to IDC," press release, 28 Jan. 2011; www.idc.com/about/viewpressrelease.jsp?containerId=prUS22679411.
2. IDC, "Smartphones Outstrip Feature Phones for First Time in Western Europe as Android Sees Strong Growth in 2Q11, Says IDC," press release, 9 Sept. 2011; www.idc.com/getdoc.jsp?containerId=prUK23024911.
3. Nielsen, "In US, Smartphones Now Majority of New Cellphone Purchases," blog, 30 June 2011; http://blog.nielsen.com/nielsenwire/online_mobile/in-us-smartphones-now-majority-of-new-cellphone-purchases.
4. ITU, "Key Global Telecom Indicators for the World Telecommunication Service Sector," Nov. 2011; www.itu.int/ITU-D/ict/statistics/at_glance/KeyTelecom.html.
5. IDC, "Worldwide Smartphone Market Expected to Grow 55% in 2011 and Approach Shipments of One Billion in 2015," June 2011; www.idc.com/getdoc.jsp?containerID=prUS22871611.
6. N. Leavitt, "Mobile Security: Finally a Serious Problem?", *Computer*, June 2011, pp. 11-14.
7. W. Jeon et al., "A Practical Analysis of Smartphone Security," *Proc. Int'l Conf. Human Interface and the Management of Information—Part I*, Springer-Verlag, 2011, pp. 311-320.
8. N. Husted, H. Saïdi, and A. Gehani, "Smartphone Security Limitations: Conflicting Traditions," *Proc. 2011 Workshop on Governance of Technology, Information, and Policies*, ACM, 2011, pp. 5-12.
9. McAfee, *Mobility and Security: Dazzling Opportunities, Profound Challenges*, tech. report, May 2011; www.mcafee.com/us/resources/reports/rp-cylab-mobile-security.pdf.
10. Juniper Networks, *2011 Mobile Threats Report*, tech. report, Feb. 2012; www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2011-mobile-threats-report.pdf.
11. K. Nohl, "Attacking Phone Privacy," *BlackHat Lecture Notes*, July 2010; http://media.blackhat.com/bh-us-10/whitepapers/Nohl/BlackHat-USA-2010-Nohl-Attacking.Phone.Privacy-wp.pdf.
12. O. Kharif, "Mobile Spam Texts Hit 4.5 Billion Raising Consumer Ire," *Bloomberg Businessweek*, 30 April 2012; www.businessweek.com/news/2012-04-30/mobile-spam-texts-hit-4-dot-5-billion-raising-consumer-ire.
13. Z. Lackey and L. Miras, "Attacking SMS," BlackHat, 2009.
14. BusinessWire, "Lookout Projects Lost and Stolen Phones Could Cost U.S.Consumers over $30 Billion in 2012," 22 Mar. 2012; www.businesswire.com/news/home/20120322005325/enLookout-Projects-Lost-Stolen-Phones-Cost-U.S.
15. "Virginia Tech Cybersecurity Breakthrough Keeps Sensitive Data Confined in Physical Space, Engineering Team Says," *Virginia Tech News*, 17 Oct. 2011; www.vtnews.vt.edu/articles/2011/10/101711-outreach-cybersecurephones.html.
16. P. Marquardt et al., "(sp)iphone: Decoding Vibrations from Nearby Keyboards Using Mobile Phone Accelerometers," *Proc. 18th ACM Conf. Computer and Communications Security* (CCCS 11), ACM, 2011, pp. 551-562.
17. J. Burt, "BYOD Trend Pressures Corporate Networks," *eWeek*, Sept. 2011, pp. 30-31.
18. A. Houmansadr, S. Zonouz, and R. Berthier, "A Cloud-Based Intrusion Detection and Response System for Mobile Phones," *Proc. Dependable Systems and Networks Workshops* (DSN-W 11), IEEE, 2011, pp. 31-32.
19. D. Barrera and P. Van Oorschot, "Secure Software Installation on Smartphones," *IEEE Security and Privacy*, May 2011, pp. 42-48.

***Yong Wang** is an assistant professor in the National Center for the Protection of the Financial Infrastructure at Dakota State University. His research interests include wireless networks, optical networks, smartphones, and related security and privacy issues. Wang received a PhD in computer science from University of Nebraska-Lincoln. He is a member of IEEE and the IEEE Communications Society. Contact him at yong.wang@dsu.edu.*

***Kevin Streff** is the director of the National Center for the Protection of the Financial Infrastructure and founder of Secure Banking Solutions, a security consulting firm focused on improving security in community banks. His research interests include banking assurance and security risk management. Streff received a PhD in electronic business from Capella University. Contact him at kevin.streff@dsu.edu.*

***Sonell Raman** is a second-year graduate student at Dakota State University majoring in database management. His research interests focus on smartphone security with respect to mobile applications. Raman received a BS in computer science and engineering from Jawaharlal Nehru Technological University, Hyderabad, India. Contact him at sraman17633@pluto.dsu.edu.*