Mobile Computing Device Threats, Vulnerabilities and Risk Factors Are Ubiquitous

feature

Mobile computing devices (i.e., laptops, tablets and smart phones) can cause serious harm to organizations and to device owners, their friends and families, because mobile devices are far less secure than desktops and laptops. The *Verizon 2015 Data Breach Investigations Report*[1] states that there are tens of millions of mobile devices. And, according to Statista,[2] there will be 4.77 billion mobile phone users in 2017 and 1.15 billion tablets in use in 2016.[3] As the number of mobile computing devices increases, so do mobile security concerns. There are already many existing and new threats related to mobile devices.

This article discusses the actors, threats, vulnerabilities and risk associated with mobile computing devices and highlights the pervasiveness of security and privacy problems and issues.

Actors

The actors (aka threat vectors) include the device itself, the applications (apps) on the device, compromised web sites, wireless data connections, other users and organizations, the organization to which the device user belongs, and the service providers.

Mobile Computing Device Threats

Newly purchased mobile devices can be configured insecurely. Devices can contain the original vulnerable operating system (OS) that has not been updated to eliminate known vulnerabilities. If a device does not require some type of access controls such as a personal identification number (PIN) or fingerprint, it is ripe for unauthorized use by anyone who has access to it. There are many types of malware that can provide people with malicious intent the ability to obtain sensitive data stored on a device. Protecting data can be more of a problem if one makes the mistake of loading sensitive organizational information on it. Users need to be aware that they are responsible for protecting the device, preventing physical tampering, setting security-specific features, and avoiding supply chains that provide compromised or unsecure mobile devices.

If a mobile device has an attachment to read credit cards, it, too, can be compromised by a technique known as skimming.[4] A smartphone can perform surveillance via its audio, camera and Global Positioning System (GPS) capabilities, as well as recording call logs, contact information and Short Message Service (SMS) messages. Mobile computer devices can cause financial problems because, if compromised, they can send premium SMS messages, steal transaction authentication numbers, allow extortion via ransomware and make expensive calls without the device owner's knowledge. A device can even be hijacked and turned into a distributed denial-of-service (DDoS) bot, making it harder for organizations to detect and prevent such DDoS attempts.

App-based threats include malware, spyware, vulnerable apps, compromised apps and data/information leakage due to poor programming practices. The types of app attacks include:

- Disabling or circumventing security settings
- Unlocking or modifying device features
- Apps that were obtained (free or purchased), but contained malicious code

Examples of malware capabilities include:

- Listening to actual phone calls as they happen
- Secretly reading SMS texts, capturing call logs and emails
- Listening to the phone surroundings (device is used as a remote bugging device)
- Viewing the phone's GPS location
- Forwarding all email correspondence to another inbox
- Remotely controlling all phone functions via SMS

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*,find the article and click on the Comments link to share your thoughts.

Larry G. Wlosinski, CISA, CISM, CRISC, CAP, CBCP, CCSP, CDP, CISSP, ITIL v3
Is a senior associate at the Veris Group LLC and has more than 16 years of experience in IT security. Wlosinski has been a speaker on a variety of IT security topics at US government and professional conferences and meetings, and has written numerous articles for professional magazines and newspapers.

Enjoying this article?

- Read ***Security Mobile Devices Using COBIT® 5 for Information Security.*** *www.isaca.org/securing-mobile-devices*
- **Learn more about, discuss and collaborate on mobile computing in the Knowledge Center.** *www.isaca.org/topic-mobile-computing*

- Accepting or rejecting communication based on predetermined lists
- Evading detection during operation

A compromised web site can be a danger to everyone's information. It can be the source of phishing scams, drive-by downloads of malware and browser exploits. Wi-Fi via free hotspots can provide criminals the means to obtain banking access and financial account information. These web sites can be used to obtain personal data about device owners, their families and friends, and the places they work. Vulnerabilities to avoid include keeping a Wi-Fi connection enabled at all times, not using or enabling a device firewall, browsing unencrypted web sites, failing to update security software, and not securing home Wi-Fi.

Data communications via a personal or company network can also be a nonsecure means of communications. The communication problems include video, audio and data that can be collected over the air by an insecure network. There are many types of network exploits including Wi-Fi sniffing, manipulation of data in transit, data exposure through radio frequency (RF) emission, connection to an untrusted service, signal jamming and flooding, and monitoring a GPS/geolocation. All of these threats need to be avoided.

User-based threats include: social engineering, inadvertently (or intentionally) releasing classified information, theft and/or misuse of device and app services, and malicious insiders who steal devices for their own purposes or for someone else.

Social engineering can be accomplished by:

- **Phishing**—Masquerading as a trustworthy entity
- **Vishing**—Tricking a victim into calling a phone number and revealing sensitive information
- **Smishing**—Tricking someone via messaging into downloading malware onto their mobile device
- **Exploiting Social Media Accounts**—Using shortened malicious web site names (to describe one example)

Your own organization's network infrastructure can be a threat. Used maliciously, a wireless network can pose threats such as:

- Providing a means for unauthorized access
- Permitting or promoting the installation of malware
- Permitting the loss of data integrity of the system and associated databases
- Spreading compromised apps
- Acting as the source of insecure coding
- Permitting eavesdropping, data interception, voice/data collection, drive-by downloads, location tracking (via GPS) and behavior tracking

An Internet service provider (ISP) can also be a threat to individuals and organizations. The ISP gathers and stores device location; device ownership information; application usage behavior; email routing/forwarding information; information about purchased music, movies, TV shows, apps and books; and sensitive internal reports. All of this information can be stored in the cloud for years.

Other information that can be kept in the cloud for a long time includes: photos and videos; personal contact information, calendar events, reminders and notes; device settings; application data; Adobe PDFs; books added to an order list; call history; home screen and application organization; text and email messages; ringtones; home system security settings (HomeKit[5] data); personal health information (HealthKit[6] data); and voicemail.

Vulnerabilities

Mobile computing device vulnerabilities exist in the device itself, the wireless connection, a user's personal practices, the organization's infrastructure and wireless peripherals (e.g., printers, keyboard,

mouse), which contain software, an OS and a data storage device.

If not secured by encryption, wireless networks often pass sensitive information in the clear that can do harm to individuals and/or organizations. Unintentionally released sensitive data can not only affect the organization's reputation and the lives of those affected, but can also be the cause of legal action. Wireless communications can carry and install malware on any computing device configured to receive it. This malware can cause data corruption, data leakage, and the unavailability of services and functionality. Personal privacy can also be affected if the audio (e.g., Bluetooth) and video/picture communication (e.g., device camera) are intercepted and used with malicious intent. The wireless protection provided by an organization will work only if a user is in the organization's network perimeter where the security controls are in place.

Unencrypted organization, customer and employee information stored on the computing device can inadvertently be made available to others if someone intercepts it while in transit or if the device is stolen (and no access controls are in place). It is not difficult to intercept wireless communications traffic because there are free tools available on the Internet to help hackers do this.

In this age of wireless technology, many roles (e.g., doctors, medical support staff, retail and wholesale inventory personnel, registration support staff) depend on mobile computing devices to efficiently capture and transmit data. The users of these devices rely on them for their productivity and livelihood. In many cases, the information is sensitive to the organization and, if it is employee- or customer-related, it can be personal and privacy-related (i.e., personally identifiable information [PII]).

If one's organization does not have a wireless encryption program (i.e., virtual private network [VPN]) in place, then mobile devices may interact with personal devices' email and obtain sensitive correspondence. The lack of encrypted communication can allow malware to access the network and propagate Trojans and viruses throughout the organization. More serious is the fact that it can allow intrusion into the enterprise, which can then compromise the entire organization. Remember that a VPN connection requires authentication—a critical protective control—to permit network access.

"If not secured by encryption, wireless networks often pass sensitive information in the clear that can do harm to individuals and/or organizations."

Application Vulnerabilities

Other vulnerable components of the mobile computing device environment are the apps loaded on it. Each application can contain a vulnerability that is susceptible to exploitation. The apps on the mobile device can have a variety of vulnerabilities including:

- Incorrect permission settings that allow access to controlled functionality such as the camera or GPS
- Exposed internal communications protocols that pass messages internally within the device to itself or to other applications
- Potentially dangerous functionality that accesses the resources or the user's personal information via internal program data calls or hard-coded instructions
- Application collusion, where two or more applications pass information to each other to increase the capabilities of one or both applications
- Obfuscation, where functionality or processing capabilities are hidden or obscured from the user

- Excessive power consumption of applications running continuously in the background, which drain the battery, thereby reducing system availability
- Traditional software vulnerabilities such as insufficient editing of data entered, Structured Query Language (SQL) query exploitation and poor programming practices
- Privacy weaknesses in configuration settings that allow access to the application's sensitive information (e.g., contacts, calendar information, user tasks, personal reminders, photographs, Bluetooth access)

Risk

The most common risk factors that apply to using mobile devices are: computer viruses, worms or other personal computing device-specific malware; theft of sensitive data; exposure of critical information through wireless sniffers; wireless intruders capturing emails, email addresses and attached data (if the security safeguards are insufficient); loss, theft or damage of the device; use of the device as a proxy to establish a virtual connection from an attacker to an internal network; data loss/leakage due to the small size and portability; fraud enabled by remote access or copying mass amounts of sensitive data; spam causing disruption and driving up service costs if targeted toward mobile devices; and malformed SMS messages causing devices to crash.

Conclusion

Each day, mobile device attack vectors are continuously undergoing dynamic changes, and it is difficult to represent a complete set of the threats and vulnerabilities. With the development of mobile computing devices that can be carried in a pocket or a duffle bag comes the responsibility to protect those devices and the data within them. Being aware is only the first step in the fight to protect the data.

References

Lookout, "What Is a Mobile Device Threat?," *https://www.lookout.com/resources/know-your-mobile/what-is-a-mobile-threat*

Mobile App Security Guide, infographic, *http://autosend.io/mobile-app-security-guide/*

Wysopal, C.; "Mobile App Top 10 List," Veracode, 13 December 2010, *www.veracode.com/blog/2010/12/mobile-app-top-10-list*

European Union Agency for Network and Information Security, "Top 10 Smartphone Risks," *https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/top-ten-risks?_ga=1.234877470.1254580284.1439215552*

Quirolgico, S.; J. Voas; T. Karygiannis; C. Michael; K. Scarfone; *Vetting the Security of Mobile Applications*, Special Publication 800-163, National Institute of Standards and Technology (NIST) USA, 2015, *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-163.pdf*

Althuser, J.; "7 Ways Hackers Can Use Wi-Fi Against You," *CSO*, 9 November 2015, *www.csoonline.com/article/3003220/mobile-security/7-ways-hackers-can-use-wi-fi-against-you.html*

Apperian, "Mobile App Security," *https://www.apperian.com/mobile-application-management/mobile-app-security/*

ISACA, *Securing Mobile Devices*, USA, 2010, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Securing-Mobile-Devices-Using-COBIT-5-for-Information-Security.aspx*

Milligan, P. M.; D. Hutcheson; "Business Risks and Security Assessment for Mobile Devices," *ISACA® Journal*, vol. 1, 2008

Absolute, US Mobile Device Security Survey Report 2015, *https://www.absolute.com/en/resources/whitepapers/mobile-device-security-survey-report-us*

Endnotes

1 Verizon, *2015 Data Breach Investigations Report*, 15 April 2015, *www.verizonenterprise.com/DBIR/2015/*
2 Statista, "Number of Mobile Phone Users Worldwide From 2013 to 2019 (in Billions)," 2016, *www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/*
3 Statista, "Number of Tablet Users Worldwide From 2013 to 2019 (in Billions)," 2016, *www.statista.com/statistics/377977/tablet-users-worldwide-forecast/*
4 Skimming is the capturing of credit card information using a card reader that records and stores the user's card information.
5 Apple, HomeKit, *www.apple.com/ios/homekit/?cid=wwa-us-kwm-features*
6 HealthKit, *https://www.healthkit.com/*