Mobile Security & Its Threats

Anita Goyal[1]
Jaswinder Kaur[2]

Abstract

In today's time it's hard to imagine a day without a mobile device. We are using our mobile devices as our transactions of money and much more. By increase in usage of mobile devices for money related stuff the risk of getting spam is increased. So the Security is needed not just any type of security but the best, cause the money involved in transactions which we done in today's time can be in Billions. So the risk is always high. Like we use Wi-Fi for our transactions some time we thought that our Wi-Fi is secure but if we didn't use any security for our Wi-Fi how can we so secure about our system that it is safe or not or there is no malware or virus in it or may be someone is already watching while you doing the transactions. The reality is we don't if we are not using any Security for our mobile devices how can we so secure that our money is save or our system is not hacked in by some Chinese group or some other Hackers. The thing is we need Mobile Security and we need it now.

Keywords: Mobile Security, Intrusion Detection, Trusted Mobile

Introduction

Today, smart phones and other mobile devices are playing an increasingly central role in how people are entertained, communicate, network, work, bank, and shop. Advancements within the mobile market—whether in performance, storage, applications, or capabilities—have been occurring at a dizzying pace. However, there is a fundamental area in which broad advancements have not been realized on mobile devices, particularly when compared to the personal computer, and that area is security. While mature security software such as antivirus is ubiquitous on laptops and desktops, the vast majority of mobile devices today remain completely devoid of security protection. Not surprisingly, today's mobile devices and the corporate assets they may connect to are vulnerable. The following sections outline the threats currently plaguing mobile devices. Many different types of security circumstances and actions can be set up and employed from its tiers. Security circumstances can range from temporary misplacement of a mobile device at home to malicious theft in a hostile region. Security actions can range from ringing a simple alarm to automatically erasing, overwriting, and re-erasing drives. People and organizations are more likely to provide their computer systems and devices with advanced security systems after they've been infected, lost, or stolen, than before.

Security Tools

The principal categories of computer security are **data confidentiality, integrity**, and **availability** (also known as "CIA"). The most common tools for each of those categories, plus the authentication category, are described here.

Confidentiality

Data confidentiality refers to limiting data access to specifically authorized people, or to preventing access to data by unauthorized people. It is what is typically thought of as data security, and it incorporates tools that provide confidentiality and prevent unauthorized people from reading sensitive information, such as personal data, credit card and payment information, corporate data, and passwords. Theft of confidential data can cause long-term damage to individuals and organizations that is difficult to resolve. Today, one of the most common and most serious threats to confidential data is identity theft. In 2007, 8.1 million identity thefts were reported in the U.S., costing Americans $45 billion. In 2006, there were 8.4 million identify thefts in the U.S., costing $51 billion5. While not all identity thefts are related to mobile devices, a substantial number are. The top ten information leaks from mobile devices, occurring May 2006 to January 2007, resulted in well over 50 million identity theft victims, with a potential cost of over $49 billion6. American identity theft has dropped slightly each year as more security measures are put to action. But as these numbers clearly show, much more is needed. The continuing development and implementation of security tools is imperative. Many types of security tools are implemented to protect data confidentiality. The most common one is also the oldest: the user name and password. As most of us know, its success depends on creating complicated passwords and changing them frequently. Most of us also know that difficult-to-guess passwords are also difficult to remember. Writing them down is counter-productive, and changing them frequently makes them more difficult to conjure and recall. And if a mobile device is logged onto a network or account when the device is lost or stolen, even the most complicated user name and password are useless until the login session expires. Lastly, even successful passwords operate on the theory of “security through obscurity,” which has been proven time and again to be weak7 because any password can be broken using the hacking technology that exists today. For these reasons and more, using passwords alone is an inadequate way to secure confidentiality.

Integrity

Data integrity refers to protecting the consistency and accuracy of the data and the content of software, ensuring that neither is modified without authorization. Integrity doesn’t mean that the information cannot be accessed; it only means that it is protected from being modified. So, tools that protect data confidentiality do not necessarily protect integrity. Nothing may happen if your data is seen by unauthorized people. But if your data is altered by anyone, regardless of whether the person is authorized or unauthorized, the problems that may ensue are vast.

For instance, some of the most valuable data integrity tools are those designed specifically to protect and audit a device’s configuration files. Classic examples of loss of configuration file integrity are the all too common man-in-the-middle attacks that have taken place in cybercafés and on secure Web sites, such as banking and payment sites. In one form of these attacks, a user accesses a Web site not knowing that an intruder has intercepted his site request and replaced it with a proxy. From there, the intruder can record every keystroke the user enters, including passwords and personal information. This type of attack is caused by making changes to the network connection configuration file on the user’s device. Protecting the integrity of the configuration files prevents the device from being taken over by man-in-the-middle attacks.

Antivirus programs and firewalls are probably the most common tools for protecting data integrity, as they protect from damage caused by viruses, Trojans, worms, and other types of malware and intrusion. A less common but valuable tool in protecting integrity is the reporting of device use to a network-based security manager. These tools work by recording the phone calls placed or received on a mobile phone, the Web sites visited, and any e-mails and text messages sent or received, then reporting that information to a central site. They protect integrity by providing information about whether or not tampering occurred and, if it did, where it originated and what happened.

Availability

Data availability refers to how accessible the device and its data and resources are. Availability is important because having inaccessible data and resources is nearly the same as having no data or resources at all. Tools that protect data availability provide protection to the device's hardware and functionality. This includes protection from hardware loss, technical function, and damage. Damage can range from something as simple as accidentally dropping a laptop on a hard floor or leaving a cell phone outside during a rainstorm to something as insidious as intentionally destroying or erasing a mobile phone, laptop, or PDA.

Design, Configuration, Circumstances and Actions

The tiered system has a user-friendly graphical user interface (GUI) that makes it easy for users to define and configure the actions and circumstances they want and need. It can be set up to invoke a variety of security actions under a wide range of circumstances. Programmable actions can range from ringing an alarm to deleting, overwriting, and re-deleting drives, with many levels in between. Circumstances may range from temporarily misplacing the device at home to malicious theft in a hostile country. Examples of tiered circumstances and actions are listed in the table below.

Type of Security	Security Description
Availability	Activate a ringer to help the owner find the device.

Availability	Automatically send a text message to the device with instructions to call a number or send an email or text message.
Availability	Activate GPS tracking, base station triangulation, or other tracking mechanism.
Availability	Automatically place a call from a security manager and play a recorded message to the device.
Authentication and Confidentiality	Activate password-only and digital signature user access.
Availability	Force outgoing calls to a service number.
Availability and Confidentiality	Deactivate functions, such as phone call placement, data viewing, email sending, or Internet browsing.
Integrity	Record and report device use to a security manager, such as calls placed, calls received, Web sites visited, emails sent or received, text messages sent or received.
Confidentiality	Partition sensitive data from non-sensitive data and move it to secure storage.
Confidentiality	Encrypt sensitive data.
Confidentiality	Delete sensitive data.
Confidentiality	Overwrite deleted data in

	corresponding clusters.
Confidentiality	Re-delete clusters of data a set number of times to be sure that no data can be recovered.

The security levels, triggering events, and actions are defined and configured by an authorized user. The triggers that can be used and the actions that can be taken depend on the device and the operations that are available on it. Examples of triggering events include:

Entering a user name and password.

Calling the device from a telephone.

Sending an email to the device.

Sending a text message to the device.

Invoking actions when acknowledgment is not received from the user or the device.

Activating security on a specific date or at a certain time of day.

Activating security upon receipt of sensitive data.

THE FUTURE OF MOBILE SECURITY

Most systems today depend on static passwords to authenticate the user's identity. However, such passwords come with major management of security concerns that have been known to be exploited by hackers. Users have a tendency to to use easy-to-guess passwords, use the same password in numerous accounts, write the passwords or store them on their machines, etc. When users do this, hackers have the option of using many techniques to steal passwords such as shoulder surfing, snooping, sniffing, guessing, just to mention a few. Several 'proper' strategies for using passwords have been suggested. Some of the proposed strategies are very difficult to use and others might not meet the company's security concerns. One of the ways that mobile devices security can be improved is through two-step authentication system. It consists of a server connected to a GSM enabled service provider and a mobile phone client equipped with SMS receiving functionality. This system involves an implementation where corporate server web application authorize customer with username / password, then connect with a service provider who will generate token and send token to customer via SMS returning transaction ID, asking customer to enter token, then match entered token against transaction id obtained from service provider. Two step verification methods by CS networks (M) Secure authentication provides an additional level of security to web application, registration system, or login procedure. On top of the username with password, user is required to validate a one-time only code that CS Networks two-step authentication will send via SMS text message. CS Network Two Way Authentication is designed for everyone who needs to protect themselves from unauthorized access by stealing password, social engineering and similar techniques of gaining access without proper permissions. It significantly decreases the chances of having the personal information of your customers taken by someone else. The key reason why it is difficult for hackers is because not only do they need to get your password and your username, but must also gain access of your mobile phone as well.

References

1. A. Tversky and D. Kahneman, “The Framing of Decisions and the Psychology of Choice,” *Science*, vol. 211, no. 4481, 1981, pp. 453-458.

2. A. Bose and K. G. Shin, “Proactive Security for Mobile Messaging Networks,” *Proc. 5th ACM Workshop on Wireless Security*, ACM, 2006, pp. 95-104.

3. B. Prince, “The Security Threat in Your Pocket,” *eWeek*, 7 March 2008; http://www.eweek.com/c/a/Security/The-Security-Threat-in-Your-Pocket.

4. B. J. Halpert, “Authentication Interface Evaluation and Design for Mobile Devices,” *Proc. 2nd Ann. Conf. on Information Security Curriculum Development*, ACM, 2005, pp. 112-117.

5. E. Mitchell, “Old-school ID Thievery;” *The Philadelphia Enquirer*, 25 May 2008.

6. A. Dolya, “Mobile Device Security 2007;” *InfoWatch*, 23 May 2007; http://www.infowatch.com/threats?chapter=162971949&id=207784708.

7. H. Berghel, “Faith-based Security,” *Communications of the ACM*, vol. 51, no. 4, 2008, pp. 13-17.

8. D. Pogue, “State of the Art; Making Sure A Laptop Won’t Stray,” *New York Times*, 14 March 2002.

9. Y. Ijiri, M. Sakuragi, and S. Lao, “Security Management for Mobile Devices by Face Recognition,” *Proc. 7th Int’l Conf. on Mobile Data Management*, IEEE Computer Society, 2006, pp. 49.