Mobile Device Security: Current Challenges and Future Forecast

An analysis on the security field and its challenges for the business world and individuals

Hugo J. Martinez
# Mobile Device Security: Current Challenges and Future Forecast

## Table of Contents

I. ABSTRACT ..................................................................................................................................................2

II. INTRODUCTION .......................................................................................................................................2

III. MOBILE DEVICE SECURITY CONCEPT .............................................................................................3

IV. CHALLENGES ...........................................................................................................................................5
   A. Current Status in Business ..................................................................................................................5
   B. Key Procedures and Existing Solutions ............................................................................................7
   C. Proper Authentication .........................................................................................................................8
   D. Key Features in Common Devices .....................................................................................................13
   E. Native Security ...................................................................................................................................14

V. FUTURE FORECAST ................................................................................................................................17
   A. Upcoming Technologies and Procedures .........................................................................................17

VI. CONCLUSION .........................................................................................................................................19

VII. REFERENCES ..........................................................................................................................................20
I. ABSTRACT

The industry of electronics and mobile devices has increased exponentially over the past couple decades. This has created a great demand for the devices and therefore great usage of them as well. While the public benefits from the capabilities of these devices it is also important to notice how these devices carry very important information and most users do not realize that it needs to be protected.

In order to provide proper protection for mobile devices, specific security measures for this type of devices is needed that meet the general information security requirements as well. Safeguards such as pins, passwords and locks work. However, several others that could even be more effective can also be implemented with the opportunity of the implementation of some futuristic development for these mobile security technologies as well.

II. INTRODUCTION

The world of mobile devices and gadgetry is one of significant importance in today’s world. The computing environment has moved from largely sized mainframes to hand sized devices that the public carries in the comfort of the pocket. These devices also have been showing the trait of increasingly developing capabilities. These exciting tools have made of technology a very important part of the everyday life for most people living in our age. There is an assortment of these devices among which we can find laptops, PDAs, tablets, and smartphones. All these provide an important way of making personal communications and business capabilities greater.

The usage of these devices varies greatly but one thing can be said and it is that they are necessary in our world today. However, because of the provided handiness and storage capacities of the devices, large amounts of valuable information end up being handled or stored by the
devices. In addition, even though these devices are useful they also come with added risks to the user. These gadgets are vulnerable to several threats to the user such as loss, damage, and theft as well as exposure to electronic attacks or hacking. Therefore, there is an increasingly great need for protection in order to keep these devices more useful than threatening.

The main reason why a careful look needs to be taken at mobile security is because of the nature of the devices that are used and their ability to access and store sensitive user information. Moreover, most of these devices also pose a different security challenge than a regular desktop computer. Devices that handle the personal messaging, personal and business e-mailing, personal banking, and even the location of the person at all times need to be protected without falter and this is why this security field in particular has become so important to our world.

III. MOBILE DEVICE SECURITY PRINCIPLE

Mobile device security deals with the protection of the systems and the information of mobile devices from unauthorized access, disclosure, use, disruption, recording, or destruction (§ 3542 Definitions, n.d.). The task of maintaining the devices and the information secure also comes with the added responsibility of maintaining the information confidential, integral, and available to the user. Confidentiality, integrity, and availability (CIA) compose the main requirements for mobile device security and considering the amount of information that these devices handle, this becomes a challenge (Furnell, 2009).

Confidentiality deals specifically with how to keep the information from being disclosed into unauthorized hands. An example of this would be how to keep the information of a credit card transaction done on a mobile device from being intercepted by a third party. A secure mobile system ensures the confidentiality of the information being transferred without hindering
the transaction itself. If this is not accomplished, a breach of confidentiality has come to pass.

The trait of confidentiality is one of the necessary factors in a secure system but is not sufficient for maintaining complete security on a system (§ 3542 Definitions).

Integrity is another one of the pillars of the security of a system. The function of the integrity factor is to ensure that the information is not modified without it being detected by the system. This ensures that all the information accessed by the authorized user is trustworthy and therefore useable. There are multiple ways in which integrity can be breached and most of them include a message or a certain piece of information being changed in transit or in the system itself. A secure system typically provides message integrity along with information confidentiality. However, these still do not make a completely desirable system (§ 3542 Definitions).

In order for any information to be of use to its users it has to provide available information when it is required. This is the principle of availability (§ 3542 Definitions). This entails that the systems in the device that save and process the information, the controls employed to keep it safe, and the channels for the transport of the information need to be working correctly. Moreover, when all three of the before mentioned factors are working conjointly and properly, it can be said that a system is secure.

Along with the different factors that affect mobile device security there is also different types of controls for it. Logical or technical controls are those that employ software to inspect and control the access to the information and the systems for the devices. Among the examples of these we can list: passwords, access control lists, data encryption, network intrusion detection systems, and host and network based firewalls.
In order for a mobile device to be completely secure there needs to be physical controls for it as well. These controls are different than the physical controls for the computing assets in a company since the mobile devices are carried on the person most of the time. Therefore, the physical security of the device will rely mainly on the owner and considering that over 80% of new critical data for companies is stored on mobile devices; this makes the technical controls even more important than before (Allen, 2005).

IV. CHALLENGES

A. Current Status in Business

Not everybody who owns and uses a mobile device realizes the potential threats associated to it and sometimes neither does the business world. On research conducted by Pointsec in 2005 it was found that 56% of professionals in the IT field use their mobile devices to store corporate information. However, only 22% of those were employing encryption and password protection on them (Pointsec News Release, 2006).

One of the main problems with the usage of mobile devices is that the public concentrates on their features and how we can use them to our advantage but pays no attention to how to protect the information being put into these devices. When one contemplates the information that gets put into a mobile device, it can be surprising to realize the mix of personal data and business related information that often remains in the devices for longer than it should. All of this is caused by the mobile device’s ability to keep this information readily at hand in case it is needed. This only ensures a greater risk for the user and the company for which the user works (Furnell, 2009).
Since devices are of such importance to companies and individuals because of the information they hold, it is understandable that one needs to be concerned for their security. In the findings of a survey of over two thousand IT professionals published by Quocirca in 2006, it was revealed that the thing that concerned the users the most was their data being accessed by unauthorized people through loss or theft and data loss because of damage. This is particularly interesting because not many of the surveyed professionals were concerned about other types of breaching such as malicious attacks or viruses, but only the physical aspect of the security for the devices (Airport Insecurity, 2008).

Each week around twelve thousand laptops are misplaced by passengers at only 106 airports of the United States (Airport Insecurity, 2008). Moreover, a survey of 300 London taxi drivers showed that over sixty two thousand mobile devices (including laptops) were left in the back of their cars in a period of only six months (Credant, 2008). What can be understood from this is that due to the size and ease of transportation of these devices losses can happen at any point. However, the factor that should concern companies is not the loss of the device itself but the misplacement and possible unauthorized access of the information contained within. In addition, even if the device is returned, this does not mean that the information has been kept safe. If a proper access control has not been implemented on the device, the information may have been accessed, deleted, or changed. Any of these breaches may have stronger and more dangerous consequences than the loss of the device itself. Therefore, stronger measures than just extra cautiousness are necessary to keep the device and the information safe.
B. Key Procedures and Existing Solutions

There are several basic measures that a company or single owner of a mobile device can take in order to increase the protection of the devices. One of these measures is to make the device identifiable in case of loss. This can be done in a significant amount of devices in order to display the information of the user. Another measure that can be implemented is to take note of the IMEI (International Mobile Equipment Identity) of the mobile device. This makes it easier for network carriers to identify the device and possibly shut it down or locate it. Finally, the user or company could consider an insurance policy for the device; this will at least take care of replacing the cost for the device while not helping with the information part. Although these measures can help increase security for the device and its information, they are not enough to ensure it so technical safeguards are necessary as well (Fuller, 2009)

When malicious attacks and unauthorized accesses are considered for mobile devices one must think about the primary source of these attacks: internet connection. Most of the mobile devices (including laptops) that users carry around connect to the internet by a Wi-Fi connection. One of the main concerns for this type of connection is that users normally do not make careful choices as to what network they connect to as long as it is free. Most users do not stop to think that the information that they are getting through that network (email, text messages, and transactions) can be possibly seen and handled by the owners of that network.

One of the main things that users should do when connecting to these public networks is to make sure they are not stealing the service and to actually know where it is coming from. Most of the Wi-Fi enabled devices have mechanisms in them that allow the users to know if the network is encrypted or if it is just an ad-hoc connection by another computer. Typically, open
public connections that appear too good to be true are so unless it is at a business providing the service. A very easy way to get personal information from users is to offer them free wireless access in public places like airports or ground transportation stations and therefore should be avoided by users (Fuller, 2009).

Wi-Fi connectivity is not the only risk for mobile devices, most of the common devices also offer a type of connectivity named Bluetooth. There are several attacks that can happen to a device through the Bluetooth technology. These include: bluejacking, bluesnarfing, and bluebugging. Bluejacking is making use of the device’s Bluetooth to try to get the device owner to pair the device through an enticing or interesting message. If the device owner accepts, this might lead to the other two threats. Bluesnarfing is the use of the pairing of two devices to access such information as contacts, messages, calendar information, and e-mails. This compromises anything from the security of a company’s information to even the security of the device owner himself. Finally, Bluebugging is the most significant of all the threats because it is possible for the intruder to be in control of the device itself and access the information as well as manipulate certain aspects of the device such as calling, messaging and e-mailing. However, using the Bluetooth technology properly on mobile devices is not very difficult. Switching the Bluetooth on only when the user needs it, not leaving the device on discoverable mode, and not pairing the device with others of unknown origins are the main suggestions for keeping the device secure in this aspect (Legg, 2005)

C. Proper Authentication

Mobile devices often carry more personal and sensitive information than personal computers because of their nature and how much they get used. This makes it important for
owners to ensure that whoever is accessing the information is its rightful owner or an authorized user. In the before mentioned event of loss, theft, or misplacement of the device, there needs to be a proper system in place to ensure that only its rightful owner is accessing the information on it.

Establishing proper authentication makes for a good first measure of defense for the device. Without implementing authentication anyone who comes across the device would end up being able to browse its contents without any difficulty. Therefore, both individuals and organizations that give their employees devices would be in danger of an undesirable scenario.

Even though it seems pretty clear that these devices need protection, users mostly do not pay attention to it because they do not perceive it like that in part and because of the available methods to protect the device.

Something that most smartphone users in particular do not realize is the fact that they are carrying two things that require protection: their phones and their SIM (Subscriber Identity Module) cards. The device requires authentication at the device level because of all the information that might be contained within but it also requires security at the SIM level because of the risks associated with it. The authentication measures at the SIM level would protect the unauthorized usage of the account of the cellphone user. At this level, safeguarding only the device by authentication does not safeguard against the removal of the SIM card and the insertion into another mobile device. This might enable the intruder to perform calls, send and receive text messages, and use network services as an impostor and get crucial information.

In 2005 N.L. Clarke and S.M. Furnell conducted a research in order to determine the conduct of mobile device users. The research focused on the opinion and use of security
measures amongst mobile device users with special attention to the authentication feature. One of the main findings was the even though the devices were used extensively, as much as a third of the users did not implement any pin protection. About thirty percent of the users expressed the pin to be inconvenient and only a quarter of the surveyed were convinced that it actually protected their devices. Moreover, a significant part of the users that did implement the pin did not use properly since forty percent never changed the factory code which can be easily retrieved online. In addition, thirty six percent were using the same pin they used for other things which increased their risks to be attacked in several places and lastly twenty six percent were sharing their pins with someone else. This shows that the usage of pins, although recommended if nothing else is implemented is not widely and properly used by users because of the challenges it presents (Clarke, 2005).

Another one of the safest ways to ensure the protection of data being carried in a mobile device is encryption. This measure ensures that even if the device is lost and the data possibly accessed it cannot be read by the intruder. One of the advantages of this measure is that there are different levels of encryption for the different types of data for a device. Broadly speaking there are mainly three different types of information that can be held in a mobile device: that which can be held in plain text, information that can be held only if encrypted, and the information which should not be stored in a mobile device under any circumstance. Nevertheless, one of the drawbacks for this is that not all mobile devices accept a wide variety of encryption methods. One example of this is Figure 1. The device only allows for one type of encryption and it mandates that all the files in the card be encrypted instead of allowing per-file configuration (Furnell, 2009).
Encryption of the information in the device does not ensure the complete safety of the information. The user needs to also be aware of the kind of encryption being implemented and how reliable it is. It is recommended that users look to sources of widely known and used encryption methods such as the Advanced Encryption Standard (AES) which is widely recognized as a robust encryption system (“AES,” n.d.).

Another set of safety measures that might not be available to every device are the features of remote lock and remote wipe of the data. These features are available for the Blackberry, Android, Windows Phone, and iPhone users. This safety measure is used in case of theft or loss and is considered an emergency approach not an essential safeguard. On the other hand, when devices reach the end of the useful life for a user it is essential for the user to remove the data from the device with no chance for a latter recovery through any means.

Even though there have been several news reports and cases in which people are harmed because they did not remove their data entirely, organizations and users in general seem to be
unaware that deleting the data and formatting the devices is not enough for that data not to be recovered. Therefore, organizations need to become aware of the following measures: overwriting, degaussing, and destruction. These measures depend on the type of advice but prove effective in the mitigation of risks (Fullner, 2009).

Overwriting is the process of reformatting the storage for the device in a low level which is then followed by multiple iterations of overwriting the complete disk with data that is random. This ensures that the original documents are very difficult to recover. On the other hand, the process of degaussing is only for data stored on hard drives and relies on the fact that they are based on magnetic media. Therefore, the disk gets demagnetized and becomes wiped. Finally, destruction is the most reliable process to prevent recovery of the data. Rendering the media inoperable does not ensure that it cannot be accessed; however, burning it almost to ashes does (“About Degaussing”, n.d.).

The choice on which of the approaches to use relies on the user or the organization and the necessity for each situation. Furthermore, some organizations have standards that they need to comply with related to this specific subject. It is important that organizations keep their staff trained in order to avoid mistakes in this area. In addition, it is also essential to recognize threats other than potential breaches and unauthorized access as a result. In this context it is normal for companies to back-up the data in the devices. It is important to back-up the data in case it is lost but still needed. The devices can either be synchronized automatically or manually.

Individuals and companies must protect the devices themselves as well as the systems the devices interact with. Security controls are required in both the host system and the mobile device so that neither become contaminated. There are a variety of techniques that can be used to
augment the control on mobile devices such as disabling auto-run features on memory sticks in order to avoid malware, activate anti-virus protection against removable media, and implement safeguards to regulate the ports (Fullner, 2009).

Even though all the previously discussed methods are effective when used properly, it must be stated that technology will never supply the complete solution for mobile device security. All of these measures have weaknesses that must be overcome in order to achieve full security for a mobile device. In addition, these measures only advice on what should be done. This does not mean that companies or individuals actually implement these measures.

In general it is understood that different measures will fit different companies and individuals depending on their security needs and their situation. In the case of a company, its information security management professionals should be aware of all these measures and make the most informed decision that suits their needs.

D. Key Features in Common Devices

Figure 2. Worldwide Smartphone Traffic (Source: gsmarena.com)
Figure 2 shows that at least fifty percent of the smartphone market is held by Apple in 2010 while at least a twenty-four percent is held by companies that use Google’s operating system. Therefore, the native features for these systems will be the focus for the next points.

The top companies in the industry of mobile device security are mainly the companies that produce the mobile devices themselves. Although, there are several applications that bring added bonus to the table for most smartphone platforms, companies such as Google and Apple which are the creators of Android OS and iOS respectively are the ones that bring most of these features to the table. These companies are not solely responsible for devices in the smartphone market but also for tablets, PDAs and media players that contribute to the majority of the market.

**E. Native Security**

All of the iPhone and android devices come with native ways of maintaining the devices secure by default. Among these we can find the iPhone passcode, Android’s pattern unlock, Find my iPhone, and Lookout Security.

![iPhone's Passcode Feature](source: intomobile.com)
Figure 3 shows the iPhone’s passcode mechanism. This mechanism designed by Apple gives the user two options. The first one is to set the before mentioned 4 digit pin number which allows the user to unlock the phone and access the information. The user also can choose if the device locks itself under the pin number immediately or after a determined period of time. The user can also decide if after a certain number of failed attempts to input the code, the device wipes itself of all the information or not. If the user does not feel comfortable allowing all of the information on the device to be secured by only a pin number then the alphanumerical feature can be activated on the passcode. This feature allows the user to use letters, caps, and characters along with a more extensive length for the passcode.

Figure 4. Android's Pattern Unlock (Source: askdavetaylor.com)
Android’s pattern unlock takes the simple passcode to another level. In this feature the user is able to design whichever pattern he/she wants of whichever length in order to unlock the phone. This makes it very complicated for anybody trying to decipher the pattern in case the device has been lost or stolen. Along with its logical strengths, there are also weaknesses for the pattern unlock such as smudges on the screen that would allow a person to trace back the unlock pattern.

Apple’s Find my iPhone feature is a nice feature that comes with both the iPad generations and the new iPhone and iPod touch generations. It is a free service that allows your device to be discovered if it is connected to the internet at any location. It then allows the owner to remotely lock or completely wipe the device as well as play a sound and send a message to the person who holds it through the service. It is accessible through other Apple devices or iTunes with the owner’s Apple ID.

Android’s Lookout is a similar application to Find my iPhone from Apple in the mobile OS by Google. This application offers everything Find my iPhone offers but also adds anti-virus protection to the phone. Since most of the applications on the Android market are free they could include malicious software so the Lookout application scans every app being installed to the phone. Moreover, the Lookout application can also provide users with automatic back-up and device scans without the need for the user to initiate those. These are some of the examples for the native and external applications that can easily be obtained and implemented into a mobile device for its security. In almost every chance, these features are free of charge to the user.
V. FUTURE FORECAST

A. Upcoming Technologies and Procedures

When current security measures are brought up it is inevitable to start thinking about what the future is going to bring to this field because of technological advancements. There are already available options that could easily set the stage for the future advancements in mobile device security. These technologies go beyond simple passwords, pins and patterns. The technology is available for things such as biometric implementation of security systems in mobile devices. Moreover, since mobile phones are the ones carrying so much of the crucial data nowadays, this would make them more secure allowing companies and individuals to exploit their whole potential and processing power.

Fingerprint readers are one of the most newly added security features to devices such as laptops and flash drives. This technology is slowly making its way to mobile devices as well. Marking a new era in which passcodes and pins will take a backseat to something that is uniquely identifiable to a single user. Technology such as fingerprint readers will be very useful to users that contain highly classified or private information within their devices. This technology provides a much more significant level of authentication because it is tied biometrically to the legitimate owner (Clarke, 2008).
Over the course of the next few years and technology develops further, there is a high chance that the industry will start seeing more of the safeguards shown in figure 5 becoming commonplace among modern devices. It is possible that devices with built-in microphones and cameras will start coming out with facial and voice recognition for different tasks during the operation of the phone. In addition, most of the mobile devices that are in place today have the basic qualities to accomplish these tasks, however, the software and possibly the power to carry out the tasks is lacking. These technologies have already been implemented in labs at places such as the University of Plymouth to mention one and it is only a matter of time until they are actually available to the market in a capitalized form by the mainstream telecommunications and electronics companies (Clarke, 2008).

The implementation of such measures would give the users an advantage in which the way they interact with their mobile devices would be more like a personal assistant in the case of Siri with the iPhone than just a regular portable device. The possibilities for the exploitation of
this kind of technology could signify the difference between the mobile computing of today and that of the future.

VI. CONCLUSION

In today’s technology driven world, mobile electronics have marked our culture and set the pace for technological development. These devices have reshaped the way our society thinks in terms of information speed, instant gratification, mobility, and operability of a device. The newly founded market of smartphones and tablets is shaping our approach to mobile computing step by step. However, lost in the fast paced development and the technological development is that most of the users of this technology who are pouring their life information into them are not concerned or aware of the risks of doing so.

Most people and unfortunately organizations that decide to take advantage of the ease of use and features that mobile technologies offer often do not stop to consider the security threats to their information and the necessary steps to ensure its security. Therefore, information security management professionals and individuals who own mobile devices should be aware of the several types of safeguards that exist and make a balanced decision on which of the measures to implement for every specific situation. Whether it be simple passwords, simple or complicated encryption, or device wiping mechanisms, people and organizations need to be aware that a certain security measure needs to be implemented for every situation.

Lastly, the mobile device industry is looking forward and awaiting for the next changes that the industry will bring about such as biometric implementation for the security of the mobile devices. This is proving to be an interesting topic for both those who are interested in futuristic electronics and the information security field. The future will be marked by technology that not
only does what we want it to do but technology that recognized what it should do by itself and
does it and the field of mobile device and its security field is bringing the industry a step closer
to that.

VII. REFERENCES

§ 3542 Definitions. (n.d.) Legal Information Institute. Law.cornell.edu available:


About Degaussing (n.d.) Periphman.com Retrieved from


Airport Insecurity: The Case of Missing & Lost Laptops. Ponemon Institute 2008. Executive

Summary, U.S. Research, 30 June 2008


Evaluation’, Deliverable 4, Flexible and Non-Intrusive User Authentication for Mobile


‘Companies see risk of removable media but still turn a blind eye’, Pointsec News Release, 8

Credant Technologies (September, 2008). ‘Credant Technologies: Almost 60,000 mobile phones have been left in London taxis in the last six months’, Global Security Mag, Available: www.globalsecuritymag.com/Credant-Technologies-Almost-60-000,20080916,5003.


Figures Sources

Figure 1. Steve Furnell, Mobile Security: A pocket guide

Figure 2. Smartphone Traffic Worldwide, gsmarena.com

Figure 3. Android Pattern Unlock, intomobile.com

Figure 4. iPhone Passcode, askdavetaylor.com

Figure 5. Steve Furnell, Mobile Security: A pocket guide.