Mobile Device Security: Current Challenges and Existing Solutions

Hugo J. Martinez
Western Michigan University

Follow this and additional works at: https://scholarworks.wmich.edu/honors_theses

Part of the Technology and Innovation Commons

Recommended Citation
https://scholarworks.wmich.edu/honors_theses/2176

This Honors Thesis-Open Access is brought to you for free and open access by the Lee Honors College at ScholarWorks at WMU. It has been accepted for inclusion in Honors Theses by an authorized administrator of ScholarWorks at WMU. For more information, please contact wmu-scholarworks@wmich.edu.
Hugo J. Martinez, having been admitted to the Carl and Winifred Lee Honors College in the spring of 2011, successfully completed the Lee Honors College Thesis on April 18, 2012.

The title of the thesis is:

*Mobile Device Security: Current Challenges and Existing Solutions*

Dr. Nicholas Andreadis, Lee Honors College

Dr. Richard Gershon, Communication

Mr. Kevin Abbott, Office of Information Technology
Hugo J. Martinez, having been admitted to the Carl and Winifred Lee Honors College in the spring of 2011, successfully completed the Lee Honors College Thesis on April 18, 2012.

The title of the thesis is:

*Mobile Device Security: Current Challenges and Existing Solutions*

Dr. Nicholas Andreadis, Lee Honors College

Dr. Richard Gershon, Communication

Mr. Kevin Abbott, Office of Information Technology
Mobile Device Security: Current Challenges, Existing Solutions, and Future Forecast

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

Hugo J. Martinez
## Table of Contents

ABSTRACT ................................................................................................................. 2

I. INTRODUCTION ................................................................................................... 3

II. MOBILE DEVICE SECURITY PRINCIPLE ............................................................. 6

III. CHALLENGES .................................................................................................... 8

   A. Current Status in Business .................................................................................. 8

IV. KEY PROCEDURES AND EXISTING SOLUTIONS .............................................. 11

   A. Proper Authentication, Encryption, and Other Security Measures ..................... 13

   B. Market Leaders and Device-Specific Security ..................................................... 18

V. FUTURE FORECAST ............................................................................................. 23

   A. Upcoming Technologies and Procedures ........................................................... 23

VI. CONCLUSION .................................................................................................... 25

REFERENCES ........................................................................................................... 27
ABSTRACT

The mobile device industry has increased exponentially over the past couple decades. This has created a great demand for the devices along with great dependence on their capabilities. There is an assortment of mobile devices among which can be found laptops, tablets, smartphones, and personal music players. All these provide a way of making personal productivity and business capabilities greater. While businesses and the public benefit from the capabilities of these devices, not everyone notices how valuable the information that they handle is. Today’s mobile devices handle information such as contacts, banking details, GPS location, and personal and corporate e-mail to mention a few. Because of the reliance on mobile devices for everything from personal web browsing to banking information, their security is crucial to the owners.

In order to provide proper protection for mobile devices, specific security measures are needed that meet the general security requirements of confidentiality, integrity, and availability. Safeguards such as passwords and locks work but they are not the only nor in some cases the best ways to protect the information inside. With the advancement of the capabilities and convenience these devices provide, we will see more reliance on these devices and therefore a greater and increasing need to protect them. Moreover, there will also be thorough advancements in the means used to protect the devices in the future.
Mobile devices are any computing equipment with the capability for advanced information processing, internet browsing, and mobility. Mobile devices are of significant importance in today’s world. Current technology has made it possible to perform tasks with handheld devices that could only be done with large computers just a handful of years ago. The capabilities of mobile devices have increased dramatically in a short period of time, adding to the productivity of both personal usage and business processes. These exciting tools have made technology a very important part of the everyday life for most people living in the United States.

Figure 1. Mobile Device Usage. Source (Digital Buzz)

Figure one gives a chilling detail about how important mobile devices are becoming in regards to internet usage. It shows an increase in mobile device internet browsing of about 300 percent from 2007 to 2012 and it projects a surpassing quantity of browsing in comparison to
desktop usage for the year 2015. This is of special importance for companies and the public in
general because of the amount of browsing over unprotected networks with devices that are not
necessarily secure. Many of these devices contain important company data along with personal
information, if a breach of security occurs companies and individuals can end up losing a great
deal of important information. Figure 2 describes an important detail about smartphones. Out of
the world’s 4 billion mobile phones 1.08 billion are smartphones. This means that there are more
than a billion devices that on average are constantly handling GPS location, text messages, call
logs and even banking information. This makes it worthy to consider how to safeguard the
devices and what is contained within.

![What is the size of the mobile market?](image)

Figure 2. Smartphones and the Mobile Market (Source: Digital Buzz)

The primary feature of these devices is exactly what makes them so vulnerable:
connectivity. This connectivity includes both connection to the internet and direct connection to
other devices. Because taking away these features would make the device almost useless the only
option is to protect its connectivity. Along with electronic attacks and hacking these devices are also vulnerable to physical damage and loss.

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. The risk involved with these devices is based on the users’ reliance on them. Most of these devices also pose a different security challenge than a regular desktop computer in regards to the information being handled, for example, constant GPS location. 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 and this is why this security field in particular has become so important to our world.

Figure 3. Information Input to Mobile Devices (Source: Digital Buzz)
II. MOBILE DEVICE SECURITY PRINCIPLE

Mobile device security deals with the protection of the system and the information stored on mobile devices. Its aim is to guard the devices from unauthorized access, disclosure, use, disruption, recording, or destruction (§ 3542 Definitions, n.d.). The task of maintaining the device’s security also comes with the added responsibility of keeping 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 keeping the information on a device from being disclosed into unauthorized hands. An example of this would be protecting 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 occurred and this can potentially end up in losses of financial or personal importance for the owner. 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 mobile system. The function of the integrity factor is to ensure that the information is not modified without the modification being detected by the system. This ensures that all 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. This can result in catastrophic damage. For example, if a user decides to
purchase an item over an unsecured network and the purchase is intercepted and the information is changed, the payment could be rerouted or the user’s banking information can be compromise. A secure system typically provides message integrity along with information confidentiality. However, ensuring that the information is not tampered with does not make a system secure. (§ 3542 Definitions).

In order for any system to be of use to its users it has to provide available information when it is required. This is the principle of availability, which means 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 for the information to be accessed (§ 3542 Definitions). Moreover, when the information of a system is confidential, integral, and available, it can be said that a system is secure.

Along with the different factors that affect mobile device security, there are 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. Examples include: 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 it also needs to be physically secured by the user. Physically securing mobile devices is significantly different than physically securing stationary devices. Making sure that stationary devices are held on a table by physical chains is easy. However, maintaining the security of a device that is designed to be in constant movement is more difficult. 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).
III. CHALLENGES

A. Current Status in Business

The major problem with mobile device security is lack of awareness about the risks related to usage of the technology. Not everybody who owns and uses a mobile device realizes the potential threats associated with it and this even includes IT professionals. Figure 4 shows research conducted by Pointsec in 2005 where it was found that 56% of professionals in the IT field use their mobile devices to store corporate information. (Pointsec News Release, 2006).

Figure 4 also shows that out of the 56% of the only 22% were using passcode and encryption of their information. This shows how one of the main problems with the usage of mobile devices is that the public, including IT professionals, concentrate on their features and how we can use them to our advantage but pays less 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).

In the findings of a survey of over two thousand IT professionals published by Quocirca in 2006, it was revealed that what 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).

In relation to physical security and the current status in business, 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.

![Figure 5. Mobile Device Security Statistics (Source: Kensington)](image-url)
Figures 5 and 6 show statistics about the importance of keeping devices safe and protected and what it means to businesses and the public. However, as it is seen in figure 6 the factor that should concern companies the most is not the loss of the device itself but the misplacement and possible unauthorized access of the information contained within. This can mean losses of anywhere between $3.3 million dollars in 2005 and $7.2 million dollars in 2010. The increasing amount of costly data loss clearly shows the increasing reliance on mobility of data storage for business purposes. 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 simple cautiousness are necessary to keep the device and the information safe.
IV. 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. Some devices have the capability to lock the screen after a certain amount of time and then display the “in case of loss” information of the owner. Another measure that can be implemented is to take note of the IMEI (International Mobile Equipment Identity) of the mobile device. This number is a unique number that each phone or network connected device possesses that can help in retrieving it or de-activating it. Finally, the user or company could consider an insurance policy for the device, of which there are two primary types. In the case of smartphones or network connected tablets, the owner can purchase insurance from the network carrier and the equipment itself would be replaced but not the data. There is also the option of insuring the phone and the cost of the data through insurance companies. 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 avenue of these attacks: the device’s internet’s 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 sending and receiving through that network (email, text messages, and transactions) can be possibly seen and handled by the owners of that network.
Two essential 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 to be free without the owner having any interest to gain are false. 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. It does not necessarily have to be a hacker that wants to steal the user’s identity or credit card. It can also be a company that would like to acquire people’s browsing habits or collect more information about them so that they can sell them something later on (Fuller, 2009).

Wi-Fi connectivity is not the only risk for mobile devices. Most of these devices offer a type of connectivity named Bluetooth, which allows a device to connect wirelessly to other electronic devices such as wireless headsets for music, calling or both, speakers, computers, car systems, etc. 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 the most significant of all the threats allow the intruder take 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 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).

A. **Proper Authentication, Encryption, and Other Security Measures**

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 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 often ignore threats of this nature because they do not perceive it as something crucial.

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. Smartphones require authentication at the device level because of the information that might be contained within, but it also requires security at the SIM level because of the risks associated with the information that is contained in the SIM. The authentication measures at the SIM level would protect the unauthorized usage of the account of the cellphone user. Stealing the SIM card of a phone would enable somebody to pose as the owner, send texts, access call logs,
and contact information. At this level, safeguarding the contents in the device only by authentication does not safeguard against the removal of the SIM card and the insertion into another mobile device.

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 many as 33 percent of the users did not implement any pin number protection. The pin protection mechanism enables a user to set a sequence of normally 4 numbers in order to unlock a device. About thirty percent of the users in the study expressed that the pin mechanism was inconvenient and only a quarter of the surveyed were convinced that it actually protected their devices. Moreover, a significant number of the users that did implement the pin protection did not use it 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 number they used for other things which increased their risks to be attacked in several places. Lastly, twenty six percent were sharing their pins with another person. This shows that the usage of pins, although recommended 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, which is a mechanism to converting data or information into difficult to decipher codes. This measure ensures that even if the device is lost and the data possibly accessed it cannot be read by the intruder. Broadly speaking, data for mobile devices can be classified in 3 ways: that which can be stored in plain text, information that can be stored only if encrypted, and the information that 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 encryption. One example of this is Figure 7. The device allows for encryption which is an advantage for the owner. However, not many mobile devices have this feature (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.).

Figure 7. Windows Mobile 6 Encryption Feature (Source: Steve Furnell, Mobile Security: A pocket guide)

Another set of safety measures available on some devices are remote lock and remote wipe of the data, which allow the user to lock down the phone or delete all of the information contained within from a remote location. 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. 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.

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 using a method which does not allow for recovery through any means. 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. The process of degaussing, which involves demagnetizing the storage media, is only for data stored on hard drives and relies on the fact that they are based on magnetic media. Finally, destruction is the most reliable process to prevent recovery of the data. The goal of the process of destruction is to render the media inaccessible and inoperable. This can be done through compression or burning of the storage device (“About Degaussing”, n.d.).

The choice as to which of the approaches to use relies on the user or the organization and the necessity for each situation. Some organizations have standards that they need to comply with related to this specific field. It is important that organizations keep their staff trained in order to avoid mistakes in the disposal of media. It is also essential to recognize threats other than potential breaches and unauthorized access such as loss of data because of violated procedures. 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. Most devices can either be synchronized automatically or manually.
Individuals and companies must protect the devices themselves as well as the networks the devices interact with. Security controls are required in both the host networks 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 there might never be a single 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. This does not mean that companies or individuals actually implement these measures to their full capacity. 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. For a company to successfully implement mobile device technology into its day-to-day operations, one of the most widely recommended policies is mobile device management, which is a set of policies that ensure the security, monitoring, management and support of mobile devices deployed across mobile operators. This ensures that the company will have control over the device even if the devices being used are of personal nature and not necessarily owned by the company. If mobile device management is in place, companies have control over the type of safeguards such as lock screen and the remote wiping of the phone and this gives the company a wide advantage over the possible loss of data in the future.
B. Market Leaders and Device-Specific Security

In order to undertake a study of device specific security it is important to understand which are the major players in the market of mobile devices. The mobile device market has gone through significantly rough changes with ex major competitors now holding small percentages of the market, such as, Motorola. Figure 8 shows that fifty percent of the smartphone market was held by Apple in 2010 while a twenty four percent was held by companies that use Android. Because of their popularity, the native security features for both of these mobile operating 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 security bonus for most smartphone platforms, companies such as Google and Apple 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.

![Smartphone Traffic - Worldwide](image)

Figure 8. Worldwide Smartphone Traffic (Source: gsmarena.com)
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. Figure 10 shows the iPhone’s passcode mechanism. This mechanism designed by Apple gives the user two options. The first one is to set a 4-digit pin number which allows the user to unlock the phone and access its information. The user also can choose if the device locks itself immediately after pushing the lock button 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. If the user does not feel comfortable allowing all of the information on the device to be secured by only a pin number, then both operating systems offer an alphanumerical feature that 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 10. 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 a pattern he/she of any length, in order to unlock the phone. This makes it very difficult 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 in some situations.

Apple’s Find my iPhone feature comes with both of the iPad generations and the new iPhone and iPod touch generations. It is a free service that allows your device to be located 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. This application offers everything Find my iPhone offers but also adds anti-virus protection. Most of
the applications on the Android market are free, and as a result they could include malicious software. The Lookout application scans every application being installed to the phone and it can also provide users with automatic back-up and device scan. 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 case, these features are free of charge to the user and the company.

Another very important subject in regards to mobile device security is that of application security. One of the strongest features of both iOS and Android OS phones is the versatility of installing different applications on them. However, this can prove to be another area where security implications need to be weighed. In order to decide which one is more appropriate for each situation we have to list the details of each operating system in regards to application security.

Figure 7. App Differences in iOS and Android OS
One of the major differences between the ways that the operating systems handle their application distribution is in the way that they handle which applications are stored in the AppStore/Marketplace. In the case of Apple, they review each application that is listed in their Appstore, whereas in the Android market applications are not reviewed. Moreover, in the case of Apple, all applications are given the same resources inside the phone. As shown in figure 11 in Android every application has access to different sections of the phone and the user knows when installing the application which resources those are. However, in iOS there is no way of telling which resources you are giving the application access to. This makes it so that apps have a further reach in the iOS system because the security of the system is more reliant on good gatekeeping when the applications are reviewed before being released in the AppStore, against potentially malicious apps. With the millions of applications that are constantly being developed for the iOS system it us up to the user to trust that every single application has been reviewed and thoroughly tested and install it. In the Android system each application lets the user know which resources it will be using to function and the user has more control over which applications to install. Because of the nature of some of these applications, they can include malware that users are not aware of. The main issue with this method is that it puts the burden of security on sometimes very inexperienced users.
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. Biometric security is based on the user’s unique physical traits such as fingerprints, voice input, and eye retina. Moreover, since mobile phones are the ones carrying so much of the crucial data, this would make them more secure allowing companies and individuals to exploit their whole potential and processing power with reduced fear of misusage.

Fingerprint readers are one of the most commonly added security features to devices such as laptops. This technology is slowly making its way to other 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. Technologies such as fingerprint readers are very useful to users that store 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 as this type of biometric technology develops further, there is a high chance that the industry will start seeing more of the safeguards shown in figure 12 becoming commonplace among modern devices. It is possible that devices with built-in microphones and cameras will include 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 processing power to carry out the tasks is lacking. These technologies have already been implemented in labs at places such as the University of Plymouth 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 voice recognition would allow users to interact with their mobile devices more like a personal assistant such as in the case of Siri with the iPhone. Siri uses voice as a biometric input in order to pull together the phone’s many resources (GPS location, maps, search engine, texting, calling, music player) to provide the needs of the users. Given the slow
moving of other biometric features the possibilities for the exploitation of this kind of technology for security purposes could signify the difference between the mobile computing of today and that of the future.

VI. CONCLUSION

In recent years the world of mobile electronics has 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 markets 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 the fact that most of the users of this technology are not concerned or aware of the risks of doing so. These risks involve loss, modification, or unauthorized access of GPS location, corporate information, contact information, and banking information.

Most people and some organizations that use these devices 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 threats that they face and the types of safeguards that exist and make a balanced decision on which of the measures to implement for every specific situation. Whether it is simple passwords, simple or complicated encryption, or device wiping mechanisms and mobile device management, 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 waiting 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 also recognizes what it should do by itself and does it. Since relying on human capabilities for the protection of data will be a risky option in the future due to increase in usage, technology like Siri that implements automatic actions to help the user would be a significant addition to mobile device security. The advancements in technology that are currently being seen are bringing the industry one step closer to that reality.
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,


Figures Sources

Figure 1. Mobile Device Usage. Source (Digital Buzz)

Figure 2. Smartphones and the Mobile Market (Source: Digital Buzz)

Figure 3. Information Input to Mobile Devices (Source: Digital Buzz)

Figure 4. IT Professionals & Security (Source: Pointsec)

Figure 5. Mobile device Security Statistics (Source: Kensington)

Figure 6. Cost of Lost Laptop (Source: Kensington)

Figure 7. Windows Mobile 6 Encryption Feature (Source: Steve Furnell, Mobile Security: A pocket guide)

Figure 8. Worldwide Smartphone Traffic (Source: gsmarena.com)

Figure 9. iPhone's Passcode Feature (Source: intomobile.com)

Figure 10. Android's Pattern Unlock (Source: askdavetaylor.com)
Figure 11. App Differences in iOS and Android OS

Figure 12. Future Biometric Security Measures (Source: Mobile Security: A pocket guide)