10-2011

It's my iPad! Protecting Critical Data on Personal Mobile Devices in the Medical Setting

Michael R. Lehrfeld
East Tennessee State University, lehrfeld@etsu.edu

Rita M. Barrios
University of Detroit Mercy, barriorm@udmercy.edu

Chris Phillippe
East Tennessee State University, phillippec@etsu.edu

It's my iPad! Protecting Critical Data on Personal Mobile Devices in the Medical Setting

Michael R. Lehrfeld
PO Box 70711
East Tennessee State University
Johnson City TN 37614
lehrfeld@etsu.edu

Rita M. Barrios
University of Detroit Mercy
4001 W. McNichols Road
Detroit MI 48221
barriorm@udmercy.edu

Chris Phillippe
PO Box 70711
East Tennessee State University
Johnson City TN 37614
phillippec@etsu.edu

Abstract: The pervasiveness of mobile devices has forced many organizations to support connectivity of corporate and private devices. Corporate devices are highly configurable regarding authentication, encryption, and remote wiping. BlackBerry devices can be fully deployed and managed using a centralized Blackberry Enterprise Server, however when a user owned device connects to enterprise servers, data security becomes a concern. Introduce a litany of complex legislative rulings and laws concerning protected data across various business domains and now personal mobile devices become security risks. This paper will discuss current issues in securing personal mobile devices in the healthcare environment and present possible solutions.

INTRODUCTION

Mobile devices have been continually increasing their capability for many years. The ability to have a high degree of portability coupled with content creation capabilities and rapid email response are an attractive combination in the medical community. Unlike an institution issued laptop which has robust encryption, complex passwords, and remote administration functionality, mobile devices like Android tablets and iPhones are less mature in the data protection domain. Modern mobile devices include fully standard compliant web browsers which are capable of running applications such as JavaScript and Flash as well as the ability to use content rich email and text editors for document or presentation creation.

Mobile devices also have the additional capability to connect to a cell provider and function wirelessly on those networks. This new functionality provides for a real-time, push data to these devices. The mobile office is no longer limited to instantaneous text messages, but now instant email notification as well as complex collaboration capabilities. This instant connection allows for a more productive and robust workforce, but at the cost of data security.

The iPad can be seen in the hands of various professionals from doctors to executives in the current corporate environment. Often times, this occurs as a bottom up integration into the workplace by consumers and employees instead of the traditional top down corporate leadership driven distribution (Greyer & Felske, 2011). What this

means is that the individual is often seen using their personally owned devices to complete their daily corporate tasks. This in and of itself poses risks to the corporate data assets. For example, many corporations rely on Microsoft Exchange Server for e-mail services. Most mobile devices currently support Microsoft Exchange ActiveSync natively, thus enabling instantaneous push data from the Exchange server. This ability has the potential to transfer protected data to an unsecured device which leaves the organization vulnerable to a myriad of privacy and security laws. It should be noted that push technology creates a data security issue by its very nature. This being the fact that any person in control of a device where push functionality has been enabled can access the data received unless the proper precautions have been enabled on the device.

This paper will present an overview of the usage of mobility in the medical setting, the risks of having protected data on a personal device, security enablement of mobile devices, solutions that will enable the institution to move forward with personal device usage in the corporate setting, concluding with future works.

USAGE OF MOBILITY IN THE MEDICAL SETTING

The usage for mobile devices in the medical setting is vast. Healthcare professionals can stay connected with patient information in a real-time setting. As noted by Prgomet, Georgeiou & Westbrook (2009), mobility can be seen as a central feature of the healthcare delivery system by supporting clinical work, location multiplicity, communication, collaboration and movement between patients without the limitations in a traditional bedside system or desktop device. Mobility is a key driver for all these features. Traditional paper charts are highly mobile, however, accuracy, accessibility and simultaneous access by multiple users are not supported. With the mobile device, not only is mobility supported but also overcomes all of the limiting factors found with the paper based system (Prgomet, Georgeiou & Westbrook, 2009).

To support the effectiveness of the mobile device in the healthcare environment several studies have been conducted between 2000 and 2006 (Prgomet, Georgeiou & Westbrook, 2009). Three studies in the usage of mobile devices in the emergency medicine environment. In these studies, ECGs were transmitted to a desktop computer located at the study site, where ER nurses wirelessly forwarded the images to the cardiologists' PDAs. (Adam et al, 2006; Clemmensen et al, 2005; Reponen et al, 2000). This resulted in a reduction of the median time by about 50% for the door-to-reperfusion time. Similarly, Clemmensen et al found that when the ECGs (electrocardiographs) were transmitted to the desktop and the cardiologist PDA simultaneously, there was a substantial reduction of 54 minutes in the door-to-treatment time (Clemmensen et al, 2005). In the study presented by Reponen et al, (2000), accuracy was measured by assessing the CT image quality. This study found that 86% of the radiology reports from the handheld device were identical to the traditional methods, while 3 of the cases had minor differences which were determined to be of no clinical consequence and 1 case resulted in an additional diagnoses via the handheld that hand not been documented by traditional methods (Reopen et al, 2000). There are many other studies that address areas of patient management, medication safety when prescribing via the mobile device, data management and accessibility as well as other areas where there is an overwhelming support for the usage of mobile device within the medical setting (Prgomet, Georgeiou & Westbrook, 2009).

Device Usage

Organizations are still trying to figure out the role of the mobile device within the healthcare organization. A pivotal concern in healthcare is how a mobile device can be integrated into the daily activities of the healthcare professional in a secure and supported fashion. With the usage of mobile devices, the healthcare organization must approach the solutions to this question in a different fashion than has traditionally been implemented when considering a technology addition. Many healthcare professionals are beginning to use their own devices to successfully conduct their daily tasks. While this does encourage the usage of mobile devices in the organizational setting and aids in the completion of various goals (Geyer & Felske, 2011), it poses security risks that the healthcare organization may not be ready to take on. When considering the usage of the personal device, the primary risks posed to the healthcare organization are non-supported user applications from external locations such as Apples App Store and the ability of the healthcare professional to download critical patient data to the personal device during the work. The latter is by far the most significant of the risks posed to the healthcare organization due to the potential exposure or loss of

critical patient data. An in depth look at the protected patient data on a personal mobile device that is used to support the healthcare professional is presented.

RISKS POSED TO PROTECTED PATIENT DATA

The protected patient data when used in the mobile setting that includes the usage of a healthcare professionals' personal device is at risk of exposure by a variety of situations. These include the cohabitation of the patient data along with the user personal data, the risk of data loss by leakage, exposure or breach, and the theft of the device. Additionally, risk is imposed on the healthcare organization when there is the sharing the personal device with unauthorized outsiders such as family members as well as others in medical setting who may not be authorized. Once of the most significant and what can be considered to be the most critical security risk comes with the removal of the patient data from the secured medical data store which may result in the risk of complete data exposure to unknown entities.

Cohabitation of Data

Cohabitation, also known as co-mingling, of data occurs when there is usage of a personal mobile device in the healthcare organization. As the healthcare professional moves throughout their day retrieving critical patient data, taking case notes when talking with the patients, prescribing medication as needed, responding to emails and performing subsequent information searches, the information is being stored on the mobile device alongside of whatever internet actions the healthcare provider has performed during their personal time. This could mean that personal financial information is store alongside the healthcare organizational information; Social networking sites may have access to various files that were stored on the mobile device while the healthcare provider was moving throughout their day; there may be comingling of critical emails along with the personal emails. When presented with this situation, it becomes nearly impossible to separate the personal data from the healthcare data and this data may be accessible by many personal applications that have been downloaded by the professional that are not secured. It has been noted on numerous occasions that encryption keys as well as passwords are stored in mobile device applications. While this unsecure method of authentication and authorization does facilitate the end user experience with the mobile device, exposure of the co-mingled data, both personal and professional, is a significant risk to the healthcare organization. As noted by Clarke and Maurushat (2007), the personal device can be considered virtually impossible to impose security regulations on when it comes to what the owner of the device chooses to enable on the device. Given the inability to secure personal mobile devices, co-mingling of data which includes various personal and professional applications opens the device up to vulnerabilities that expose the organization to undue risk (Clarke & Maurushat, 2007).

Loss of Data

Data leakage and breach laws are a relatively new phenomenon, which require companies, in specific instances, to inform the public when personal or private information has been leaked from their authorized channels. Adding to the complexity of securing protected data, data breach laws have been applied in a sectored approach, each data breach law being applied to specific government and business types. This makes compliance with the law very convoluted (Stevens, 2010; 2006).

Recently data breach laws have moved forward through congress like H.R. 2221, the Data Accountability and Trust Act (DATA). If enacted, this law will require all businesses to notify the FTC if any covered personally data was leaked to unauthorized parties. This bill passed the United States House of Representatives on December 8, 2009 but was not voted on in the senate before the bill was cleared from the docket. This bill or a similar one is likely to re-emerge in the coming years as and will probably be passed (Congressional Budget Office, 2009).

Data leakage and breach law suits are also the subject of extraordinarily high fines. In 2007, TJX, a retail conglomerate owning TJ.Maxx, Marshalls, Winners, HomeGoods, T.K.Maxx, A.J.Wright, and HomeSense were sued for a data breach. TJX was ordered to pay an estimated 256 million dollars for their security failures (Hole &

Netland, 2010). The issue of data leakage and its broad application coupled with high fines for failure to protect data is concerning considering the growth in personal device connectivity. Consider a scenario wherein a private individual, in the employ of a company, connects to the employer's network with a personal electronic device. This is done ostensibly, in order to handle electronic communication more efficiently. This device now contains one or more email attachments which have personal information about the employer's customers. Given that the device has now been exposed to unknown entities, the healthcare organization must now consider the following: In the case of a lost or stolen mobile device, what are the required actions that healthcare organizations take? At what point would the critical data be considered to be breached, and how can the critical data be tracked and recovered across multiple private devices? If the device is being routinely backed up to a server, such as with the Blackberry system, which exists in the cloud, has the critical data been breached? When considering healthcare, data breach laws must be strictly adhered to in order to avoid costly legal battles and the loss of patient-trust in not only the medical facility but also the medical staff. The following sections discuss security implementation techniques to help mitigate the risk of securing private mobile devices connected to the medical facility's infrastructure.

Theft and Misplacement of the Mobile Device

Without the protection of the physical building protecting the mobile device, device theft has an increased risk of probability of occurring given the smaller nature of the device (Ghosh & Swaminatha, 2001). The devices are fairly easy to pick up, conceal and transport in a covert fashion. Often times, when this occurs, the data can be lost forever and is exposed to exploitation by the entity in position of the device. When considering patient information, this leaves the medical facility exposed to repercussion imposed by the various acts and laws in place to protect the patient, as noted above. As Ghosh & Swaminatha note (2001), the lost or misplaced internet enabled mobile device, includes an added risk of allowing the exploiter to access corporate systems including email as well as file systems.

As is commonly understood, the personal mobile device is often shared amongst family members as well as the acquaintances of the owner of the device. In addition, sharing of the personal device that is used in the organizational setting also occurs between professionals regardless of whether that individual has been authorized and authenticated to the information they are given access to. This situation should be considered when the personal mobile device is used in the organizational setting when understanding the security of the personal mobile device. Because the device may contain private critical information, and access to the device may be given in an unsecured manner, the individual in possession may not be authorized to the information the mobile device houses. This creates a condition that can be equated with "theft" or "misplacement" of the mobile device.

The Insider Threat

The insider threat is far more prevalent in the setting where the personal mobile device is allowed to be used as part of the corporate technology stack. This is because the professional using their personal device is afforded the ability to download pertinent patient data to the device and there is no mechanism for its removal before the professional leaves the medical facility. What makes this threat even more covert is that the professional is unaware they are putting the organization at risk simply by leaving the facility with the patient data on their personal devices. As is commonly known, the insider threat poses the greatest risk for organizations (Fonesca, Vieira, & Mederia, 2006). In 2006 the FBI reported in their survey, 52% of the respondents had reported an unauthorized use of information by internal professionals, while 10% of those reporting were unsure if the critical data had been exposed (Fonesca et al, 2008). Given this and the fact that the healthcare professional may not realize the risk they pose by storing and transporting critical data assets the risk of the insider threat grows exponentially.

SECURITY OF PERSONAL MOBILE DEVICES

As previously discussed, the burden of safeguarding the protected data falls on the institution. With traditional PC's network connectivity, many robust solutions exist to ensure proper authentication and encryption capabilities are in place (Duffany, 2007). As technology moves to a more mobile platform, these traditional methodologies may not

always be the optimal solution. Layer into the problem that mobile devices are commonly purchased by individuals and not the institution, as is common with traditional computing platforms, things become more complex. This section will examine the current protection methods available to mobile platforms that can be employed to satisfy Information Assurance concerns.

Authentication

The ability to successfully determine the user accessing the institution's resources has previously been discussed in the literature. Multi-factor authentication using trust based models (Thomas, Menzel, & Meinel, 2008), training users to implement complex passwords and administrative enforcement (Shay et al., 2010), or implementing a two-factor authentication model using third party tools (RSA, 2011) are all traditional techniques for securing data and access to institutional resources. The question that will need to be addressed is will these methods transfer to the mobile domain while ensuring the same level of authentication that is required by mandate or law.

Controlling access to the mobile devices is seen as the first line of defense when securing protected data. To accomplish this, passwords are the most common method (note: smart cards and other two factor authentication techniques that are employed on laptops are presently not supported on the current generation of mobile devices). Another difficult problem is the differentiation between privately purchased and corporate provided devices. Most consumers do not password protect their phones or tablets and institutions should insist on this if protected data resides on the device.

Exchange Server 2010 can be used to push mobile device policies to any user who chooses to use ActiveSync. ActiveSync is the Microsoft technology that enables the communication between any device and the Exchange Server. Currently Apple's iOS, Google's Android, RIM's BlackBerry OS, and Microsoft's Windows Phone 7 all support the ActiveSync protocol. It is important to note that there are minor differences between the implementation of some of the setting in ActiveSync and the various Operating Systems. For example, Apple's iOS has a minimum password or 4 digits while Android devices ignore this setting and configure a default password length of 4. Table 1 contains some of the authentication related settings in ActiveSync and Figure 1 depicts the relationship between the Exchange Server running ActiveSync and the mobile device:

ActiveSync Setting	**Description**
AllowSimplePassword	Enable use of simple passwords - i.e. abcd or 1234
PasswordRequired	Mandates the use of a password for the device
IdleTimeoutFrequencyValue	Time allowed to enter password
MinPasswordLength	Sets default password length - i.e. 7 characters

Table 1: Mobile device settings in ActiveSync pertaining to authentication.

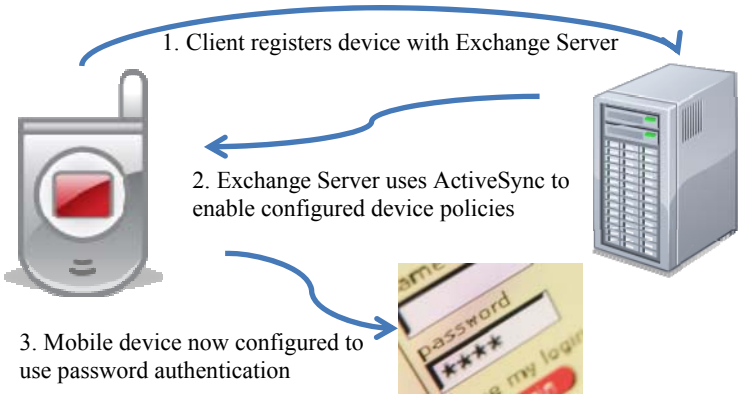

Figure 1: Relationship between mobile device and an Exchange Server.

Across all devices, a ***device wipe threshold*** can be configured that will automatically wipe the device if the password is entered incorrectly. The purpose of this setting is to limit the amount of brute force or manual password attempts someone could use to gain unauthorized access.

Encryption

PC's that have authentication protection are still vulnerable to physical theft and direct access to user data. A PC's hard drive can be removed and slaved to another machine and the data can be recovered. To combat this, data encryption is used (Snyder, 2006; Symantec, 2011). Mobile devices are no different than PCs, with the exception of mobile devices being easier to misplace, loose, or have stolen. As previously mentioned, many mobile devices are acquired outside of corporate purchasing channels that are being used to connect to company resources. This puts the institution at a crossroad. Does the institution have the ability to force users to encrypt their devices if the users decide to connect to institution resources? Each institution will need to develop an internal version of an acceptable use policy concerning this interaction. Outside of companies' policies, the ability to accomplish device encryption is available across 3 of the 4 major mobile operating systems. Table 2 outlines the type of device encryption by operating system (Android, 2011; Apple, 2011; BlackBerry, 2011; Microsoft_Technet, 2011).

OS	Encryption	Notes
Android	128/256 AES	Minimal support through ActiveSync - varies greatly by OEM (HTC, Motorola, etc). Use of 3rd party software recommended.
BlackBerry	256 AES	Full policy support through BlackBerry Enterprise Solution
iOS	256 AES	Full policy support through ActiveSync
Windows Phone 7	NA	Does not support device encryption

Table 2: Mobile device encryption properties by OS.

Password recovery on the 3 devices that support device encryption also varies. BlackBerry has the most robust solution that is tightly integrated with their BlackBerry Enterprise Server. Administrators have the ability to reset user passwords wireless as well as lockout and securely wipe lost devices. Figure 2 is the BlackBerry Web Desktop Manager that enables a user to control their device wirelessly. Note the "Secure a Lost Device" option.

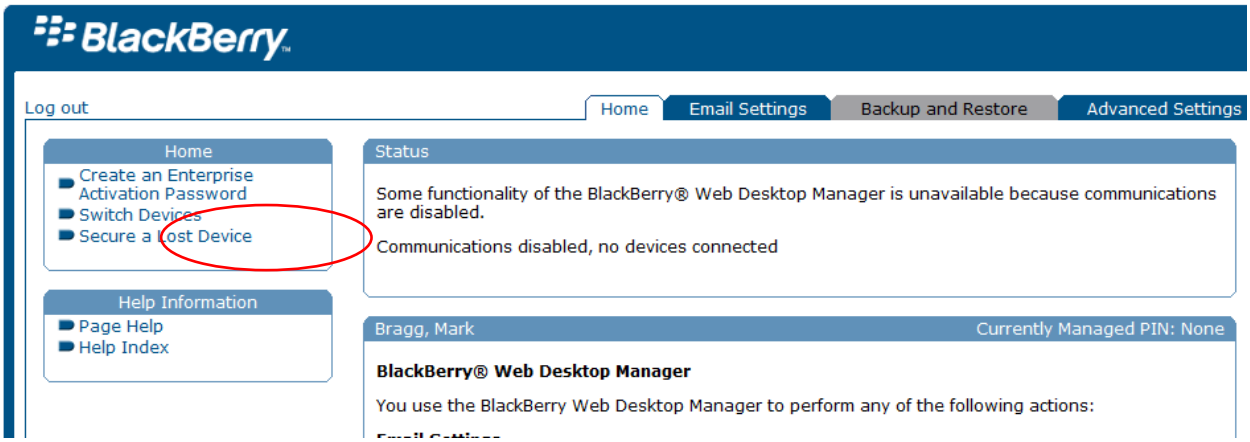

Figure 2. BlackBerry Web Desktop Manager.

Centralized enterprise password management and recovery is not a feature currently supported on either Apple's iOS or Google's Android Operating Systems. This missing enterprise feature may cause institutions problems when providing documentation of security processes for regulators or accrediting bodies. This results in password recovery being left in the hands of the users. All the Technology department can do with a recovered device from an ex-employee is wipe it to a factory state and re-provision it. Additional considerations for digital forensics when using device encryption also need to be considered. If a device is involved in an action that requires further investigation, encryption may cause recovery complications (Barrios & Lehrfeld, 2011).

ENSURING SECURITY ON MOBILE DEVICES

Securing mobile devices using passwords, encryption, ActiveSync, and BlackBerry Enterprise Server aid Technology departments in their task to ensure an institutions data is protected. An all too common problem with the security of mobile devices is their high degree of portability combined with a high loss/thief rate, which in the United Kingdom accounts for half of all street crime and saw a 50% increase in New South Wales (NSW, 2001; Unit, 2011). This loss rate would make remote administration of these devices very important in an enterprise setting. This section will further discuss the capabilities of ActiveSync and BlackBerry Enterprise Server support of remote wipe, the emerging field of contextual aware security settings, and a brief discussion of third party solutions.

Remote Wipe

As demonstrated in the BlackBerry Web Desktop Manager in Figure 2 and Outlook Web Access in Figure 3, both solutions enable end users to remote wipe their devices. According to Microsoft, the remote wipe feature will remove any Microsoft Exchange Server data from the device should the device be lost or need to be re-provisioned (Microsoft_Technet, 2011b). Similar functionality exists with enterprise BlackBerry tools. Windows Phone 7 currently has no support for remote wipe. Windows Phone 7 is currently being marketed to consumers who, presumably, do not have the need for remote wipe capabilities (Microsoft_Technet, 2011a).

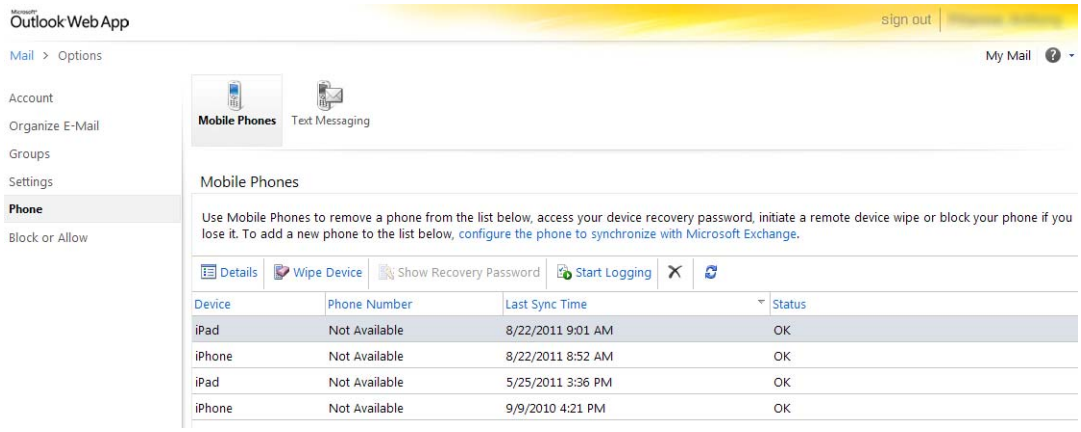

Figure 3: Outlook Web Access interface for remote administration.

Remote wiping varies by OS. Within Apple's iOS, a remote wipe command does not overwrite existing data. Instead it deletes the encryption keys that are used to decrypt the data thus effectively rendering the data inaccessible. With all remote wipe implementations, the device that is being wiped must connect to the remote server to receive the remote wipe command. Should an assailant disable communications on a device using either 'Airplane Mode' or a faraday bag the remote wipe command is never received and the potential for data loss increases. To combat this, as previously discussed in the previous section, a device wipe threshold can implemented in a device's policy to diminish the success of a brute force password attack. For example, BlackBerry devices default settings allow for 10 password attempts before they trigger a wipe of the device. This functionality further bolsters the security of mobile devices should an incident occur.

Contextual Aware Security

Contextual aware security is not a new concept, rather a concept that is being applied to the ever increasing domain of mobile devices. The premise of context security is the ability of a device to use available information to "characterize the state of an entity" (Wrona & Gomez, 2005). In the mobile device setting, this would include GPS location information, sensed wireless access points currently within range, or resources and applications that are currently being utilized. Previously mentioned was the difficulty that institutions are facing with respect to ownership of mobile devices. Contextual aware security policies have the potential to address some of these concerns. Take the following scenario as an example of the potential uses for contextual aware policies. A user purchases a mobile device and connects to the institutions Exchange Server via ActiveSync. A contextual aware policy is pushed to the device. The policy dictates that a complex password always be used and after 10 incorrect attempts the device is wiped. When the GPS unit discovers that the device is on company property, the policy automatically disables the use of the camera and voice recorder applications. If the device should ever be connected to an unsecured or unknown wireless access point, the policy will establish an encrypted VPN connection to protect transmitted data. All of the enhanced security measures would be enacted without the user having to interact with the device.

Currently there are applications that take a subset of contextual aware information and provide information for users. For example, on iOS devices, a shopping application can query the location services of the device and provide the user with prices for a particular item at stores that are geographically close. Similarly, a movie application can display the current movie times for all local theaters.

CONCLUSIONS

The ability to safeguard the data that an institution maintains maybe legally mandated, needed for accreditation, or just a policy of sound business practices necessitating the securing of mobile devices. The straightforward implementation that has been traditionally implemented on corporate purchased equipment can no long be assumed

when many of the connected devices are owned by employees. The extent that an institution can force security policies onto private devices relies heavily on the established acceptable use policy and the invasiveness of the settings. The largest perceived security setting for the end user is the logon password. Policies may require authentication every time the device goes into a sleep state. The result is now a user is prompted for a password every time the device is used. Encryption, by itself, is not invasive to the end user but highly sought after to meet legal and policy regulations. Potential issues can come from a user incorrectly entering their password and reaching the device wipe threshold and erasing their device. Alternatively, based upon the OS and device, the ability to perform a remote wipe of a stolen device is very important.

There are still many limitations in securing mobile devices. ActiveSync is not implemented in a standardized way across all mobile Operating Systems. Password recovery is another area where mobile devices lag behind their desktop counterparts. However, there are third party solutions that purport to work as a stopgap where ActiveSync leaves off. For example, Good Technology (Good, 2011) offers a solution that enhances the remote administration capabilities of mobile devices and allows for password recovery and application deployment.

Future work will include the development of a more robust contextual aware security policy that will remove the end user from concerning themselves with different security settings based upon various contextual situations. Also, the implementation of ActiveSync across the different mobile devices needs to be rigorously examined for policy implementation inconsistencies and a methodology in which to deploy the policies.

REFERENCS

Adams G.L., Campbel P.T., Adams J.M., et al,. (2006). *Effectivenss of prehospital wireless transmission of electrocardiograms to a cardiologist via hand-held devices for patients with acute myocardial infaction (from the timely intervention in myocardial emergency, notheast experience (TIME-NE).* American Journal Cardiol, 98(9); 1160-4

Android. (2011). Android Encryption Implementation. Retrieved August 20, 2011, from http://source.android.com/tech/encryption/android_crypto_implementation.html

Apple. (2011). Exchange ActiveSync and iOS 4 Devices. Retrieved August 20, 2011, from http://developer.apple.com/library/ios/#featuredarticles/FA_Exchange_ActiveSync_and_iOS4_Devices/Introduction/Introduction.html

Barrios, R., & Lehrfeld, M. (2011, May 25 - 27). *Forensicating iOS Mobile Devices.* Paper presented at the 2011 ADFSL Conference on Digital Forensics, Security and Law, Richmond VA.

BlackBerry. (2011). Stored Data Security. Retrieved August 20, 2011, from http://us.blackberry.com/ataglance/security/features.jsp#tab_tab_stored_data

Clarke, R. & Maurushat, A., (2007). *Passing the buck: Who will bear the financial transaction losses from consumer device insecurity.* Journal of Law, Information and Science, 18(1), 8-56.

Clemmensen P., Sejersten M., Sillesen M., et al,. (2005). *Diversion of ST-elevated myocardial infarction patients for primary angioplasty based on wireless prehospital 12-lead elctrocardiolographic transmaission directly to the cardiologist's handheld computer. A progress report.* Journal of Electrocardiol, 38(4), 194-8.

Congressional Budget Office. (2009, Dec 7). *HR 2221: Data accountability and trust act*. Retrieved August 23, 2011 from http://www.cbo.gov/ftpdocs/108xx/doc10855/hr2221.pdf.

Duffany, J. L. (2007). *Optimal resource allocation for securing an enterprise information infrastructure*. Paper presented at the Proceedings of the 4th international IFIP/ACM Latin American conference on Networking.

Fonseca, J., Vieira, M., & Maderia, H. (2006). *Monitoring database application behavior for intrusion detection.* In proceedings of 12th Pacfic Rim International Symposium on Dependable Computing (PRDC'06), 383-386.

Fonseca, J., Vieria, M., & Maderia, H. (2008). *Online detection of malicious data* access using DBMS auditing. In proceedings of the 2008 ACM Symposium on Applied Computing (Fortaleza, Ceara, Brazil, March 16-20, 2008). SAC'08. ACM. New York, NY, 1013-1020

Geyer, M., & Felske, F. (2011, July-Aug). *Consumer Toy or Corporate Tool: The iPad Enters the Workplace.*ACM Interactions.

Ghosh, Anup K. & Swaminatha, Tara M. (2001, February). *Software security and privacy risks in mobile e-commerce.* Communications of the ACM, 44(2), 51-57.

Good. (2011). Good Technology Home Page. Retrieved August 21, 2011, from http://www.good.com/

Hole, K., & Netland, L.H., (2010, May-June). *Towards security assessment of large-impact and rare events.*IEEE Security and Privacy, 8(3), 21-27.

Jones, J.F., Hook, S.A., Park, S.P, & Scott, L.M. (2011). *Privacy, Security and Interoperability of Mobile Health Applications.* Lecture Notes in Computer Science. 46-55.

Microsoft_Technet. (2011a). Exchange ActiveSync Considerations When Using Windows Phone 7 Clients. Retrieved August 20, 2011, from http://social.technet.microsoft.com/wiki/contents/articles/exchange-activesync-considerations-when-using-windows-phone-7-clients.aspx

Microsoft_Technet. (2011b). Perform a Remote Wipe on a Mobile Phone. Retrieved August 22, 2011, from http://technet.microsoft.com/en-us/library/aa998614.aspx

NSW. (2001). *The Problem of Mobile Phone Theft*. Retrieved from http://www.lawlink.nsw.gov.au/lawlink/bocsar/ll_bocsar.nsf/vwFiles/cjb56.pdf/$file/cjb56.pdf.

Prgomet, M., Georgiou, A., & Westbrook, J. (2009). *The impact of mobile handheld technology on hospital physians' work practices and patient care: A systematic review.* Journal of American Medical Information Association, 16, 792-801.

Reponen J., Ilkko, E., Jyrkinen L., et al. (2000). *Initial experience with wireless personal digital assistant as a teleradiology terminal for reporting emergency computerized tomography scans.* Journal of Telemed and Telecare, 6(1), 5-28.

RSA. (2011). RSA SecurID. Retrieved August 19, 2011, from http://www.rsa.com

Shay, R., Komanduri, S., Kelley, P. G., Leon, P. G., Mazurek, M. L., Bauer, L., et al. (2010). *Encountering stronger password requirements: user attitudes and behaviors*. Paper presented at the Proceedings of the Sixth Symposium on Usable Privacy and Security.

Snyder, R. (2006). *Some security alternatives for encrypting information on storage devices*. Paper presented at the Proceedings of the 3rd annual conference on Information security curriculum development.

Stevens, G. (2010). *Federal information security and data breach notification laws.* Retrieved August 23, 2011 from http://www.fas.org/sgp/crs/secrecy/RL34120.pdf.

Stevens, G. (2006). *CRS report for congress: Data security federal and state laws.* Retrieved August 23, 2011 from http://www.asisonline.org/newsroom/crisisResponse/CRS_report0807.pdf.

Symantec. (2011). PGP. Retrieved Sugust 19, 2011, from http://www.symantec.com/business/theme.jsp?themeid=pgp

Thomas, I., Menzel, M., & Meinel, C. (2008). *Using quantified trust levels to describe authentication requirements in federated identity management*. Paper presented at the Proceedings of the 2008 ACM workshop on Secure web services.

Unit, N. M. C. (2011). United Kingdom National Mobile Phone Crime Unit. Retrieved August 21, 2011, from http://www.met.police.uk/mobilephone/

Wrona, K., & Gomez, L. (2005). *Context-aware security and secure context-awareness in ubiquitous computing environments.* Paper presented at the XXI Autumn Meeting of Polish Information Processing Society.