Strong Security Posture for the Mobile Data Age at Universities in the U.S.

By: Stephen Allen

East Carolina University

Abstract

This paper will present the current security strategies for securing mobile data at U.S. Universities. In today's high tech world each worker has a mobile device that can also connect to the organization's WiFi and provide a possible breach. My paper will present ways to help prevent these security issues by a combination of training users and adding security measures like encryption and lock and erase software for mobile devices. There are many proactive actions companies can take to stop this type of breech and I plan to elaborate on those areas. I will also list current hardware and software products that I think will help assist in those security threat areas. I plan to also include current and future types of protection to deter and stop advance persistent threats. Since the topic can be so large I will try to narrow my scope to that of a university as a healthcare or banking organization would have an even more in depth approach.

There are many ways to help prevent mobile device security issues by using a combination of training users and adding software or hardware like Mobile Device Management. Some features of the mobile security suites include security measures such as data encryption, lock features and data erase software for mobile devices. In today's workplace most employees have a smart phone, tablet, or laptop that can be connected to their organization's Wi-Fi and have access to sensitive employee and student data. There are many proactive actions Universities can take to stop mobile technology breeches and I plan to elaborate on those areas. I review a mobile device management platform Mass360 by IBM. Since the topic can be so large I will try to narrow my scope to that of a university as a healthcare or banking organization would have an even more in depth and large scale approach.

Mobiles devices can include but are not limited to Smart Phones, Tablets, and Laptops. The issue that arises is these devices can contain work sensitive data and it is our job as Information Security specialist to protect and provide a secure solution to managing this data. Mobile Data is any data used on a non-permanent device and it can be easily transmitted unsecurely outside of a monitored system for a business. With some current products and mobile security polices we can now prevent these data leaks and provide a strong security posture for our mobile devices connected to our work network.

East Carolina University for bring your own device uses a combination of security polices and mobile device management. During the business day you can be connected by Wi-Fi with you tablet in a meeting, your laptop at your desk, and checking sports news on your personal phone. All these actions are transmitting data from mobile devices and University's need to make sure these devices are secure when they come back on campus. This data can contain email info, logins, or more important students Banner information. In case of theft, the hard drives are encrypted using AES also known as Rijndael which was established by the U.S. National Institute of Standards and Technology (NIST) in 2001. (Wikipedia) In order to get access to a server as admin you would need to RDP and know the admin login. First you need to access our VPN with your INTRA login, than are prompted for two-factor authentication. Using your phone and the mobile application Defender we then login with a temporary one time key code using Two-Factor authentication. Once in you can access our Key Pass program using the master password you have memorized which is rotated every 90 days. Once in you can select the admin login and RDP to a server in the network. The static IP address is bound to our laptop and only that IP can also access the box which is grouped by teams.

Another security issue is securing the mobile data traffic that is bombarding your network. Mobile Ad hoc Networks (MANET) routing protocols, we require a network-level or link layer security. Since without appropriate security provisions, the MANETs is subjected to attacks like network traffic, replay transmissions, manipulate packet headers and redirect routing messages. In order to address these needs, a policy based network management system that provides the capability to express network requirements is required. While this is out of the scope of this paper for the University looking into a policy based network management system may help secure the mobile traffic. (*Kartheesn, Srivatsa)

Current security strategies for securing mobile data includes using software like Mass360 which is a mobile device management suite, having up to date antivirus, complex passcodes, swipe codes, encryption, and remote wipe features enabled. All University employees should have a free or paid Antivirus program for all 3 major phones operating systems. IOS, Android, and Windows all have free and paid for antivirus for mobile devices which help detect and remove malware and the help desk will assist with installing. Most cell phone carriers themselves like US Cellular also have an anti-virus suite that they will support for a small fee each month. The ability to remotely wipe an employee's personal phone may seem extreme but because interoffice emails these days which can contain sensitive information it may have to be done due to lose, theft or a system breech. This may only be used in instances where the stolen device is being held at ransom for the data it contains or has access to. This feature would not be used to erase or wipe an employee personal data from a personal mobile device for any other non-business related reason.

Some current mobile data security issues for information security managers are the multiple phone operating systems available on the market today, for example IOS, Android,

Blackberry, and Windows. It is tough to find a one size fits all solution with the multiple vendors and patching for these OS sometimes taking months to get to the carrier. Another major problem is employees having outdated personal phones having known security flaws and may have discontinued system updates which can expose a security risk because older models. One solution is to provide a work based smart phone and provide for each employee which can be costly or convince them to upgrade.

Hospitals, health insurance companies, and universities have all become a frequent target for hackers seeking massive databases of personal information. Profile data, Social Security numbers and health records sell on the black market (Pagliery*)*. Most are secured now by using encryption, enforcing a security posture, and providing Security awareness and training for employees and students alike. Most users connect to an Exchange Mail server with their phone and with Microsoft Exchange 2010 you can enforce the use of passcode with active sync turned on to protect email. A passcode has proven to be more secure than the basic swipe feature included on most phones due to the fact the residue can show your swipe. Some other security protocols include encryption for email, security features for email like complex passcodes, and adding two-factor token authentication.

There are ways to help prevent security issues by using secure awareness training, having up to date software and antivirus, and using a software program to enforce a security posture. Have the user connect to a Wi-Fi that is enforcing these polices is a big factor most universities have already put in place. We cannot control what are on user's phones or what they access outside of work but we can control a posture they need to meet in order to connect to the company network while preforming work tasks. As we search for solutions from an Information Security standpoint we see that the landscape has both Mobile Device Management (MDM)

applications and even Extensible Device Management (xDM). One such service is a "state-of-the-art management solution for mobile devices called Mobiliya Manage which ensures the security of sensitive corporate data, enforces compliance with corporate MDM policies and provides simple access to enterprise apps and services for employees." (*NewsRx LLC) While this solution is above the scope of a university this would be great management software for Hospitals, Fortune 500, or governments who need to adhere to script federal polices and guidelines.

In the Information Week article Jaquith says. "the real battle for mobile devices is not on security, but on privacy and the corporate equivalent of privacy, which is data leakage," (InformationWeek) This is very important and points out that no matter how secure your security team makes the devices that data leakage may occur. There are many ways a small or large organization that you can help protect your company's business intelligence and privacy. By providing security awareness training for your users before they are allowed to connect to the business with their mobile device which can be included at orientation. As we learned in our book you can use a combination of a free help line phone number for users to call, a weekly newsletter with mobile security tips, and a general up front culture of being aware of new threats and having open discussion about what can be done to mitigate advanced persistent threats. By working as a team and collaborating the IT security staff and employees can have a direct and personal experience with their mobile device and feel invested in being secure. During training I have learned that it helps to relate these security issues to personal stakes in the employee lives. Start by opening a discussion asking employee what would happen today if their Facebook or Bank account is hacked? Then explain steps they can take to prevent these kinds of issues and use that same information to start a discussion for the business and how it relates. They could

use features like Two-Factor authentication and Geo-Location to help add security measure to the login for both Facebook and business applications.

There are many vendor products out there for Mobile Data Management and Mass360 by IBM takes the spotlight. I will review this product as a security suite to provide total control and access to all your mobile devices connected to your network and give confidence back to the IT department and upper management. This software suite provide a comprehensive unified platform for securely managing all your mobile devices. Since mobile malware is the next big security threat it is important to get a secure grip on your devices now instead of once it because a major issue. In 2014 a Sophos Security Report stated "there are 2000 new Android malware samples discovered everyday alone." (Svajcer) Mass360 is a cloud based web solution that mobiles devices join if they want to access company data. You don't have to enforce your users to do anything even if they get on your Wi-Fi and browse the web. It is only when they connect to sensitive company data that they join the Mass360 network and security polices are enforced. These security policies can include but not limited to complex password enforcement, encryption, and a blacklist of apps. As the admin you can remotely scan a sense of health of your mobile security posture with one screen to view. Even detect and safety clean and remove the infected files remotely. The program has a GPS detect features to be able to view if devices are in locations of the United States where they shouldn't have it. There is also a feature that allows for the device to be turned off per user or per device remotely. The admin also has the ability to remote lock, reset passcode, wipe data, and reformat the phone. Accounts can be revoked until the admin turns it back on and recovers the mobile data; therefor the date still exists and is not lost. Admin is also able to create a container allowing secure document sharing

where users can create, add, and collaborate with other secure users remotely which links with into Microsoft SharePoint Exchange and other such document mangers.

Another great feature that Mass360 takes advantage of is Android for Work which is an app that separates work apps and personal apps. This also allows the company to push custom or paid for apps that they have purchased to your mobile device. Also if the device is stolen or left at a specific location the admin has the option of wiping the data from the device. In an advanced feature they can locked the device and uninstall the Mass360 company login but keep the personal files intact. That way when the device is returned to the owner and brought back into the network they can redeploy the Mass360 login client and they can connect back to the business company data. This way as the information security manager you can control access even when a device is lost or stolen. The most interesting feature I could find was Geo Fencing which allows for policies based on Geo Location. (Mass 360) So you could add a policy to a personal bring your own device or BYOD and only allow users to access that specific app when they are in the geographic location of your business on personal mobile devices. Then when they exit the building and are at home the policy will not allow them to access the app. If this is a work provided mobile device and you want to use real time geo tracking the user interface provide a friendly graphical map and displays all your device. Along with using GPS in the paper Data Security in Mobile Device by Geo Locking the authors mention that they use a layer of encryption of the data is done using the location coordinates as key and round up. (*Prabu, Yadav) Along with a complex password this can add a level of security to your data but in the case of a University's data it would not need to be protected at this level.

At the same time you can turn up or down the level of monitoring and still continue to allow personal use of their device without monitoring that level of information when they are at

home. You can also turn off features on the phone like camera, audio recording, or video at sensitive workplaces such as Universities. Along with that feature you can even add a module for Data Protection Policy that will scan outgoing text message for sensitive information like SSN, or Banner ID's. Again it might not even be an intentional hack, it could be as simple as an employee forwarding a text from a college that had sensitive information at the bottom that they didn't see.

Along with Mobile Device Management Software you can also use hardware to secure you mobile data. Adding a VPN is common place among organizations but as Michael Cooney points out that while having VPN or encrypted communications is a great idea, letting your mobile devices connect to that virtual private network might not be a good idea. (Cooney) If the device is infected than it now has access to your network via VPN. One solution is to use Mass360 and require that a security posture check is enforce and once all the requirements are met then the device can connect to the network.

Another hardware solution to provide when securing mobile devices is Two-factor authentication. "Two-factor refers to an authentication system in which users are required to authenticate using at least two different "factors" something you know, something you have, or something you are before being granted access." (Cooney) By providing your employee with a Token app they can enter a password along with the token key on their mobile device to access specific services. When we VPN from offsite from our mobile device we have to enter our Intra password and then the token that is created on our mobile phone.

Polices and laws are currently still being created for mobile data and the security issues surrounding bring your own device. NIST Special Publication (SP) 800-124, Guidelines on Cell Phone and PDA Security provides general insights into securing these devices provide guidance

about the threats and technology risks associated with mobile devices to include potential methods for mitigation. (Dawson)

The above options of providing employees with mobile devices preloaded with secure software and the BYOD option with an installed application both have pros and cons. It ultimately comes down to how the company wants to be able to handle possible breeches in their system and the ability to monitor their users. It can be a very company specific choice but there are great secure options for both.

So you can see the importance of Information Security Management when is come to managing mobile devices. At the fore front, a combination of security training, weekly news blast, free fun training seminars on site will help spread security awareness to employees of all ages. It will be very difficult and spend an extreme amount of manpower if you take a re-active approach to security mobile devices. As presented in another paper there are several issues facing the acquisition of data from a mobile device after the fact. "The key issues of mobile forensics data acquisition as opposed to the traditional computer forensics on hard disk includes but not limited to battery life of mobile devices, platform used to access data stored and the synchronization of data across multiple devices." (Sawmadal)

Some other good ideas for the Information Security Management team is to constantly continue talking about the issues in the news and reviewing currently polices. Working with other universities and policy makers for Mobile Data Security will help show you what has worked at other Universities and their failures.

There is no way to prevent every cyber security breech but we can find ways to mitigate through security training awareness and software with hardware combinations. We have to straddle a spiked fence to provide upper management with the confidence that the data is secure

and that the users can maintain their privacy. By using granular access, security polices, and enforcing a strong security posture we can feel confident that your mobile data and devices are secure anywhere your employees may travel.

As IT security specialist it is our job to stop attacks and data leakage against the mobile data on the network. This is a tremendous task but rest assured that with proper polices and software or hardware enforcing these policies you are taking the right steps to protecting your network. There will be zero day exploits, software, and OS level vulnerabilities in the future and there is no way to stop that. What we can do is keep up to date and relevant within the security community and assist our peers in securing their network. One way ECU communicates is within our UNC schools to keep up to date about what software or hardware is working in IT. Though phone calls or workshops we share information about security and other IT solutions that specifically help the University. I encourage you to seek out other business partners in the same field and build a trust with IT to collaborate and share information and have a strong security posture for the mobile data age at Universities in the U.S

WORKS CITED

1. * NewsRx LLC Mobiliya Launches Innovative Mobile Data Security Solution Journal of Engineering Journal: (Atlanta, Ga.) ISSN: 1945-8711 Date: 1/12/2014

(http://jw3mh2cm6n.search.serialssolutions.com/?ctx_ver=Z39.88-2004&ctx_enc=info%3Aofi%2Fenc%3AUTF-8&rfr_id=info:sid/summon.serialssolutions.com&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.genre=article&rft.atitle=Mobiliya+Launches+Innovative+Mobile+Data+Security+Solution&rft.jtitle=Journal+of+Engineering&rft.date=2014-11-12&rft.issn=1945-8711&rft.eissn=1945-872X&rft.spage=836&rft.externalDocID=Journal_of_Engineering_2014_11_12_836_Computers_Software_Mobiliya_Launches_Innovative_Mobile_Data_Security_Solution&paramdict=en-US)

2. * Kumar, M Prabu. and K Praneesh Kumar Yadav Data Security in Mobile Devices by GEO Locking International Journal of Network Security and Its Applications ISSN: 0974-9330 Date: 10/01/2009 Volume: 1 Issue: 3

3. * Kartheesn, L; Srivatsa, S K A Policy Based Scheme for Combined Data Security in Mobile Ad hoc Networks . Journal of Computer Science 8.8 (2012): 1397-1406. http://search.proquest.com.jproxy.lib.ecu.edu/docview/1323982175/abstract

4. Aaron ND Sawmadal Mobile Forensics – Issues facing the acquisition of data (https://www.linkedin.com/pulse/mobile-forensics-issues-facing-acquistion-data-aaron-nd-sawmadal) Mar 23, 2015

5. Michael Cooney 10 common mobile security problems to attack, Network World (http://www.pcworld.com/article/2010278/10-common-mobile-security-problems-to-attack.html) Sep 21, 2012

6. Maurice Dawson Legal Issues: Security and Privacy with Mobile Devices http://www.academia.edu/13231237/Legal_Issues_Security_and_Privacy_with_Mobile_Devices

7. *Wikipedia*, *The Free Encyclopedia*. Advanced Encryption Standard. (2015, July 22). In Retrieved 03:03, July 23, 2015, from https://en.wikipedia.org/w/index.php?title=Advanced_Encryption_Standard&oldid=672604609

8. Mass360 (http://www.maas360.com/news/press-releases/2014-2/)

9. *Jose Pagliery* UCLA Health hacked; 4.5 million victims affected July 17, 2015 (http://www.ktvz.com/news/money/ucla-health-hacked-45-million-victims/34223796)

10. Vanja Svajcer Sophos Security Report Sophos Mobile Security Threat Report Launched at Mobile World Congress, 2014, Principal Researcher, SophosLabs (https://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-mobile-security-threat-report.pdf?la=en)

11. Information Week - 5 Mobile Security Issues To Watch http://www.informationweek.com/mobile/5-mobile-security-issues-to-watch/d/d-id/1100382