GNITED MINDS
Journals

International Journal of Information Technology and Management

Vol. VIII, Issue No. XI, February-2015, ISSN 2249-4510

MOBILE DEVICE MANAGEMENT TO ENHANCE HIGHER EDUCATION SYSTEM

AN INTERNATIONALLY INDEXED PEER REVIEWED & REFEREED JOURNAL

www.ignited.in

International Journal of Information Technology and Management
Vol. VIII, Issue No. XI, February-2015, ISSN 2249-4510

Mobile Device Management to Enhance Higher Education System

Subhi Singh[1] Ritesh Rastogi[2] Prem Sagar Sharma[3]

[1]CSE Department of NIET Greater Noida affiliated by UPTU Lucknow, UP (INDIA), subhisingh0786@gmail.com

[2]MCA Department of NIET Greater Noida affiliated by UPTU Lucknow, UP (INDIA), riteshrastoginiet@gmail.com

[3]CSE Department of JPIET Meerut affiliated by UPTU Lucknow, UP (INDIA), premsagar1987@rediffmail.com

Abstract – given the adaptability of Mobile learning, there are certain threats can emerge with excessive use of technology in education. Mobile technology can bring revolutionary changes in the education system but at the same time it can be harmful if not used under control. So there is a need to fully control mobile devices so that they can be used in education system in a positive way and illegal/unauthorized usage can be blocked. This paper presents a comprehensive model for use of the concept of mobile device management (MDM) in mobile based education. It includes the policy design for MDM client, a mechanism for use of MDM server to control the devices and a method of implementation of this model in current scenario.

Keywords— MDM, Mobile Education, Education Model, Change in education system.

---------------------------♦-----------------------------

I. INTRODUCTION

The use of mobile devices on campus networks is exploding. The accelerating adoption of mobile devices in education, both institution-owned and personal, is forcing IT departments to rethink the way they manage end-user devices. Because mobile device are powerful, versatile and reasonably priced, many educators — especially in K-12 schools and districts — are eager to purchase those mobile products for use in the classroom. At the same time, more and more students and employees — especially in colleges and universities — are asking for the chance to run academic and personal applications on their personal mobile device, laptops and Smart phones. This paper outlines an approach that has been developed and tested to meet the unique needs of education. Conceived as an easy-to-use solution for education institutions, it is designed to be simple to implement and manage, and to address a variety of mobile devices.

Technology can be used in both constructive and destructive ways if not used under proper guidance and control. If the educationalists provide only education apps on mobile device then students can use the tablet for any purpose for example: If the teacher instructs the students to look for a particular video on YouTube then after opening YouTube it is not necessary that all the students will be watching the prescribed video and some of the students may start watching some other videos as admin will have no logs regarding the usage of mobile device by the students.

Having a mobile device without the proper security, device management and monitoring, and a positive user experience can put the enterprise at risk. Information can be monitored or leaked, devices and mobile infrastructure could enter into in an untrusted state, and users become frustrated with the use of their device in the classroom. If the institute fails in their BYOD plan they will be at a disadvantage for using technology in the process of education.

Mobile security risks as well as threats by agents pose an ever growing and complicated problem to the information security of a mobile enterprise. Having the device compromised by authorized or unauthorized users or resources on the device, man in the middle, or end points compromised will lead to information being monitored or leaked. Protecting the confidentiality, integrity and availability of the mobile device and infrastructure is at the core of mobile security. Mobile device management, monitoring, and user experience that can work across many platforms and be scalable also pose challenges. With BYOD users, privacy of the user's personal assets is a great concern.

By providing security through defence in depth there is a known understanding that any single solution may have vulnerabilities but by applying layers of security there are levels of redundancy to increase security. Specific layered security solutions from the moment the device is turned on until the device is powered off are discussed. Solutions are discussed for the supply chain and physical security of the device.

To solve this purpose we need to design an environment in which the mobile device distributed to students will be in complete control of the school admin. All the application running in this environment will be under the guidance of the admin and admin will have the power of uninstalling/limiting usage of applications and certain features of a mobile device.

II. LITERATURE SURVEY

It has become apparent that as more and more educational institutions began use of Mobile devices for education the threat for using these solutions is increasing day by day. Recent surveys shows that M-learning has been a trend that most educational institutions around the globe are trying to implement. Institutions are trying that students should be able to use their personal mobile phones for learning purpose also. There has been a sudden increase in development of mobile applications on different mobile platforms. The use of mobile phones in education range from taking assessments to watching lectures, asking doubts to teachers etc.

With the increase in the usage of mobile phones in education there has been also several problems faced by institutions that arise due to this. This problem is no different from those faced by enterprise using BYOD solutions Thus the essential problem that corporate America, the U.S. government, an educational institution and in fact the world face today is the same. How can an institution allow BYOD in the educational place/workplace while keeping information secure? When mobile devices have access to privileged data security policy needs to follow the core information security principles of: Confidentiality, Integrity, and Availability (CIA) (Goodrich & Tamassia, 2011, p. 3)(4). According to Hayes and Kotwica (2013)(5) four in ten enterprise level organizations have had a security breach related to BYOD.

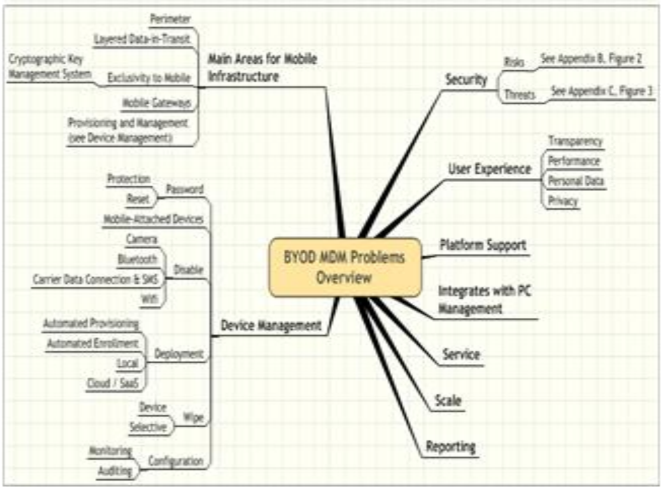

Figure-1: Problems facing BYOD device management

For any organization to have a successful and secure BYOD environment there are a number of challenges to overcome (see Figure 1). These challenges are discussed in more detail in the sections below.

MOBILE SECURITY RISKS

Some of the greatest security risks (see Figure 2), as adapted from National Security Agency (2013, p. 24)(6) include: Voice and Data-in-Transit (DIT) leaks or monitoring; Malware or Advanced Persistent Threat (APT) on mobile device or infrastructure; Unauthorized modification of user equipment or infrastructure; Data-at-Rest (DAR) unprotected on mobile device; Authentication controls lost or stolen; Phone number leaked opening up vishing and phishing; disposal of phones with sensitive information; Denial of services done via battery drain or other means; Social media applications being used outside the policy of an organization; Unpatched Operating System, Applications, or Firmware and unknown vulnerabilities in these; EMI; Eavesdropping techniques such as Magnetic field coupling or Near Fielding Communication (NFC).

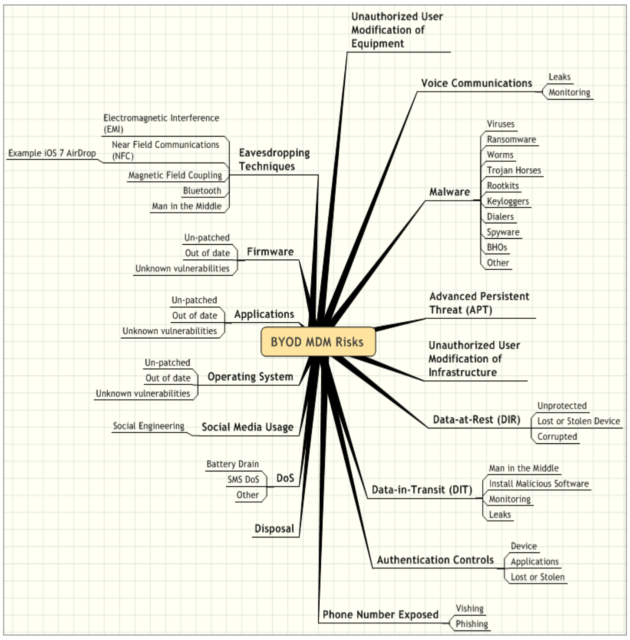

Figure-2: BYOD MDM risks

These risks evolve and change on an almost daily basis. For example it was recently discussed by Steele (2013)(7) where AirDrop on iOS7 can only be blocked when the phone is in supervisor mode which currently requires a physical connection to a MAC. This is a potential new vulnerability for many phones and MDM environments.

MOBILE SECURITY THREATS

Dealing with agents that want to or can attack and harm an organization is another problem category. Some of the greatest security threats to mobile security (see Figure 3), as adapted from National Security Agency (2013, p. 24)(6) include: Attackers from rogue cellular systems; Modifications to devices hardware or software without authorization physically, remotely or in the supply chain; Attempted access to the data on the device, including RAM if was powered on, or infrastructure from a lost or stolen device; Masquerading as an authorized user to gain access to the infrastructure; Attackers attempting to disrupt service or gain access from devices or directly; Authorized users misuse of privileges; Authorized users attempting to use unauthorized applications or services; Infrastructure administration misuse of privileges; Malware masquerading in common applications installed from untrusted sources.

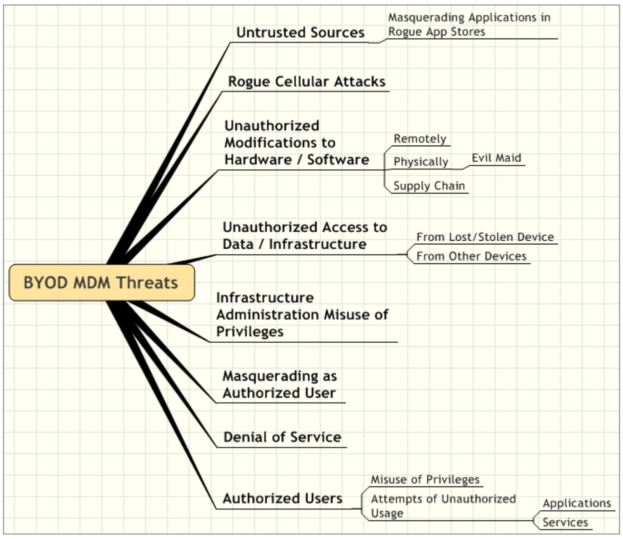
Untrusted Sources
Masquerading Applications in Rogue App Stores
Rogue Cellular Attacks
Unauthorized Modifications to Hardware / Software
Remotely
Physically
Evil Maid
Supply Chain
Unauthorized Access to Data / Infrastructure
From Lost/Stolen Device
From Other Devices
BYOD MDM Threats
Infrastructure Administration Misuse of Privileges
Masquerading as Authorized User
Denial of Service
Authorized Users
Misuse of Privileges
Attempts of Unauthorized Usage
Applications
Services

Figure-3: BYOD MDM threats enterprises and organizations face today

DEVICE MANAGEMENT

Another major problem area is management of the device. It is imperative that an organization have methods in place to handle the problems: Password protection and reset; Management of mobile attached devices such as printers; Ability to disable cameras, Bluetooth, Wi-Fi, SMS, and carrier data connections; Deployment, both local and Cloud or SaaS, with automated enrollment and provisioning; Wipe of entire device and selective; Configuration Monitoring and Auditing.

USER EXPERIENCE

With any solution the user experience is important to have large scale adoption. Privacy of users in a BYOD environment as Steele (November 8, 2013)(8) discussed what users expect when it comes to their privacy and the legal ramifications of companies if not handled properly. Users also expect their personal data to not be intruded upon and a level of transparency both in using their personal data and applications as well as privacy controls used. Performance and transparency to the user are important as well.

OTHER PROBLEM AREAS

There are a number of other problem areas besides the listed security risks and threats, device management and user experience. Other problem areas that need to be handled include: Reporting capabilities; Scalable architecture; Service; Integration with PC Management; Platform Support; Mobility Infrastructure; Cryptographic Key Management System (CKMS); Overall device performance.

The ability to secure, manage and monitor enterprise portions of a BYOD and allow users to have their personal area of the device is a problem. Information Security and BYOD is the challenge all enterprises, organizations and countries face. The solutions proposed in this paper look to merge these nearly polar opposite concepts.

III. PROPOSED WORK

We have proposed an environment where mobile device distributed to students will be in complete control of the school admin. All the application running in this environment will be under the guidance of the admin and admin will have the power of uninstalling/limiting usage of applications (see Figure 4). We propose a solution that

The technology to have a centralized BYOD mobile device management system that integrates with PC Management is a fast growing sector. There are many approaches various companies provide. The solutions provided in this paper don't look at any particular vendor or solution, rather looks to provide sets of controls to solve the overarching problem. That is to allow BYOD to work transparently, efficiently, and securely in an international, national, and/or enterprise environment without prohibitive costs.

To solve the myriad of problems and to continuously be vigilant to security, as well as the user experience, a proper life cycle solution needs to be developed. Souppaya & Scarfone (2013, p. 10)(9) stated there are five life cycle phases: Planning; Development; Implementation, Operations and Maintenance; Disposal. The guidelines proposed by Souppaya & Scarfone should be an overarching goal of the overall management of mobile security in an enterprise. Souppaya & Scarfone (2013, Appendix A)(9) discussed supporting NIST SP 800-53 security controls and publications for enterprise mobile devices and need to be part of any BYOD policy, procedures, and standards solution.

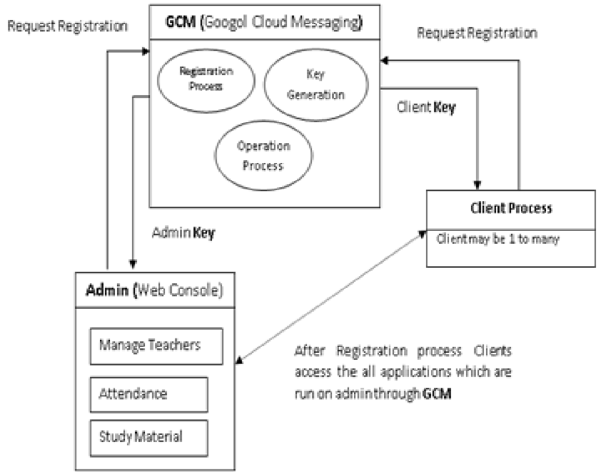

Figure -4: Proposed Architecture of Client Device Management System

Mobile device management software has a number of components that include the security ones discussed, but also monitoring, managing, and support for the devices. The key areas that need to be addressed include the following items.

a) Deployment options to include local, cloud etc.

b) Platform support for as many devices as possible will help a BYOD program succeed. Given many of the solutions proposed, this would require the commercial world to adopt their devices to support proper security controls that are lacking.

c) Besides the security solutions for applications and their data already presented, it is desirable to also have the ability to monitor application inventory and usage. A proper application auditing system should be part of the mobile device management solution.

d) Document and Content Management. If using data resident security solutions then the device needs to integrate with enterprise document and content management software.

e) Network Management to control data usage as to where, when, and if data can be uploaded or downloaded over cellular or Wi-Fi. Roaming cost control would also be part of the network management, as would device diagnostics, usage monitoring and block device access to email or other network access areas if any policy violations occur.

f) Service management monitoring and help desk support management.

g) PC management integration console standalone and 3rd party tools.

h) Reporting system with alerts, response actions to alerts, device and application level analytics. For example, excessive battery drain could be an alert with analytics to determine cause.

i) The ability to whitelist or blacklist applications.

j) The capabilities to remote device wipe or selectively wipe parts of the device.

k) The capabilities to remote lock and locate.

l) Able to manage VPN, APN, proxy and gateway settings.

m) The ability to disable Wi-Fi, carrier data connections, camera and Bluetooth.

n) Manage mobile attached devices such as scanner and printers if physical security allows.

o) Configuration monitoring and auditing.

p) Automated provisioning and enrollment.

A. COMPONENTS OF ENVIRONMENT:

The components required for building environment for education may be divided into two parts:

1. Hardware components

2. Software components

The details of these components are as below:

1. Hardware components

The components include parts that will be present with users of the environment. It includes of the below:

a) Mobile Device

These are the devices that will be owned by all the users and will assist there for their respective roles. The mobile device will be of any operating system (Android, IOS etc.) according to the choice of the users. There will be a minimum hardware requirement for all mobile devices for a better user experience. At least 1 GB RAM should be present with 1GHz processor and for saving of files 4 GB of internal storage should be present.

b) SIM/Wi-Fi Router

All the mobile device must be connected to internet (Network) so that they can be constantly monitored remotely so at the place of usage they can connected to a Wi-Fi connection with the help of Wi-Fi router whereas if there is a problem with Wi-Fi internet connection then we can insert SIM card in the mobile devices to access internet.

c) Server

There will be a cloud server that will store all the information gathered from mobile devices. Using this server the admin will be able to control the devices. Since the server is cloud based we need a Tablet/PC with internet connection for anytime/anywhere availability.

2. Software components

Below are the software components that are needed for creation of environment:

a) Admin Application

This will be the application that will be installed on the mobile devices as an administrator of the devices so that the commands/policies applied from the server can be applied on the devices. This application will depend on the OS and permission for installation will give accordingly. For example: In android we need declared permission for this application in manifest file so that when application will be installed on the device it will have all the permission s to apply on the device as per the need of the admin.

Using this application device will be registered on the server and maintained accordingly.

b) Applications/Application store

We need an application store from where all the registered users will be able to download applications to install on the devices. All the registered users will be able to download applications and use them for required purpose. The application store can be cloud based or they can be kept on local server accordingly to need of the institution.

IV. POLICY DESIGN

MDM policies need to be designed for this environment for the use of admin so that the usage can be controlled by the admin as per the need. One thing that needs to be taken care is that policy should be designed and implemented so that user experience may not be compromised.

These policies will be available to admin and will be applied on the devices with the help of admin application installed on the devices. The application will receive the policy from the server and apply it on the devices.

B. POLICIES

Policies will be distributed accordingly to functionalities and policy API will be written under MDM them. Below are the set of policies that will be required:

a) Application policies

These will be the set of policies that will be applicable on the applications installed on the devices. There will be a set of API that will control and manage the installation and usage of all the applications installed on the devices at a given point of time. These policies will ensure that the user is using the device as per directed by the admin and no unauthorized application is installed on the device.

Below are the major requirements for application policies:

1) Admin should be able remotely install any application on the device.

2) Admin should be able to retrieve list of applications installed on device at any point of time.

3) Admin should be able to block any applications usage at any point of time.

4) Admin should be able to block installation of any/all applications.

5) Admin should be able to retrieve the history of usage of any application.

Admin should be notified when a particular application (selected by admin) will be launched.

b) Password policies

These set of policies will help the admin to apply password related restrictions on the devices so that all the registered devices will be secure.

These policies will instruct the users to set the password as directed by admin so that devices will be secure enough.

Below are the requirements for password policies:

1. Admin should be able to set password quality for example: minimum length of password, minimum number of numbers/characters/special characters in password etc.

2. Admin should be able to reset device password.

c) Browser policies

These will be the policies that will be applied on the Internet Browser so that admin can control the Internet Browsing of the devices. For example: The admin doesn't want the users to watch YouTube on the devices then he can block it in two ways:

1. Either blocks youtube.com on the browser.

2. Or block java script so that no video browsing websites may be opened.

d) Connectivity policies

These policies will empower the admin to control the connections on the devices. The connection includes Wi-Fi, Bluetooth, and NFC etc. The admin will be able to block/unblock these connections and also control the connection to a particular device/Wi-Fi. For example: Admin doesn't want the devices to exchange files at a point of time then he will block the Bluetooth (Wi-Fi if Wi-Fi-direct is available) connections and later unblock them. Hence all the device connections will be under control of the admin.

These will be the basic type of policies that needs to be applied on the devices to assist the admin to control all the devices.

Apart from this the admin should also be given power to send certain messages to the devices at any point of time and also tracking the position of the devices.

V. THINGS TO BE TAKEN CARE

There are certain things that need to be taken care for the implementation of this model:

1) There must be a mechanism designed in applications / environment for loss of internet connectivity.

2) Applications data must be stored in a directory whose access will be restricted for data protection.

3) Policies must be applied so that user experience may not be affected.

4) The security of OS the mobile device is using should be taken in account

VI. CONCLUSIONS

We can conclude that we can design an environment which will be very beneficial for use of mobile devices in education. This will control the illegal and improper use of devices by the students. This will empower the admin to analyse the usage pattern of the devices by the students and take strategic decisions. Admin will also be able to analyse the data of the devices and properly guide them to the path. Also there will be no installation of illegal apps and admin will be able to apply security measures from one point. This design will also help the admin and students for usage of licensed apps. Without a well-defined BYOD policy enterprises and organizations at the local, national and international level will be left vulnerable, as well as mobile device users being left with a feeling of mistrust. Commercial products do very well at management and operations and do provide entire suites of security solutions. The challenge is to mash up the best possible solutions to all the problems discussed in this paper and to have the forethought to integrate new solutions as other problems, vulnerabilities and exploitations are encountered. If commercial mobile device vendors and 3rd party service providers do not find a way to work closely together to integrate solutions to the security problems of BYOD then entire nations will be unprepared for an ever growing and constantly evolving cyber threat.

REFERENCES

Casey, K. (2012, November 19). 6 Risks your BYOD policy must address. InformationWeek. Retrieved October 5, 2013, from http://www.informationweek.com/smb/mobile/6-risks-your-byod-policy-must-address/240142320.

Campbell, S. (2013, January 22). Study: BYOD brings employee productivity gains. CRN. Retrieved October 4, 2013, from http://www.crn.com/news/mobility/240146736/study-byod-brings-employee-productivity-gains.htm.

Hoover, J. (2012, February 03). National Security Agency plans smartphone adoption. InformationWeek. Retrieved October 4, 2013, from http://www.informationweek.com/government/mobile/national-security-agency-plans-smartphon/232600238.

Goodrich, M.T. & Tamassia R. (2011). Introduction to computer security. Reading, MA: Addison-Wesley.

Hayes, Bob; Kotwica, Kathleen (2013). Bring your own device (BYOD) to work : Trend report. Retrieved November 6, 2013, from http://www.eblib.com

National Security Agency (July 29, 2013). Mobility capability package. Retrieved October 21, 2013, from http://www.nsa.gov/ia/_files/Mobility_Capability_Pkg_Vers_2_2.pdf

Steele, Colin (2013). Blocking airdrop with iOS 7 MDM requires supervised mode. Retrieved November 9, 2013, from http://searchconsumerization.techtarget.com/news/2240207123/Blocking-AirDrop-with-iOS-7-MDM-requires-supervised-mode

Steele, Colin (November 8, 2013). BYOD trend in full effect despite privacy, legal concerns. Retrieved November 15, 2013, from http://searchconsumerization.techtarget.com/news/2240208754/BYOD-trend-in-full-effect-despite-privacy-legal-concerns

Souppaya, Murugiah; Scarfone, Karen (June 2013). Guidelines for managing the security of mobile devices in the enterprise (NIST special publication 800-124 revision 1). Retrieved November 4, 2013, from National Institute of Standards and Technology web site http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf

Conklin, WM. Arthur; White, Gregory. Principles of computer security comptia security+ and beyond (exam SY0-301), 3rd Edition. New York: McGraw-Hill.

Rhee, K., Won, D., Jang, S. W., Chae, S., & Park, S. (2013). Threat modeling of a mobile device management system for secure smart work. Electronic Commerce Research, 1-14.

Samsung Electronics Co. (2013). An Overview of Samsung KNOX™ [White paper]. Retrieved October 26, 2013, from http://www.samsung.com/global/business/business-images/resource/white-paper/2013/05/Samsung_KNOX_whitepaper_April2013_v1.1-0.pdf

Shabtai, A., Fledel, Y., Kanonov, U., Elovici, Y., Dolev, S., & Glezer, C. (2010). Google android: A comprehensive security assessment. Security & Privacy, IEEE, 8(2), 35-44.

Keromytis, A. D. (2012). A comprehensive survey of voice over IP security research. Communications Surveys & Tutorials, IEEE, 14(2), 514-537.

Traynor, P., Enck, W., Mcdaniel, P., & La Porta, T. (2008). Exploiting open functionality in SMS-capable cellular networks. Journal of Computer Security, 16(6), 713-742.

Nicholson, A. J., Corner, M. D., & Noble, B. D. (2006). Mobile device security using transient authentication. Mobile Computing, IEEE Transactions on, 5(11), 1489-1502.

Syta, E., Kurkovsky, S., & Casano, B. (2010, January). RFID-Based Authentication Middleware for Mobile Devices. In System Sciences (HICSS), 2010 43rd Hawaii International Conference on (pp. 1-10). IEEE.