International Journal of Research
Available at https://edupediapublications.org/journals

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 02 Issue 10
October 2015

Some Important Features of Mobile Device Management – An Integral Part of BYOD

Ms.Pragati Vaidya
Student
Symbiosis Centre for Information Technology,
Pune,India
pragati.vaidya@accosiactes.scit.edu

Mr.Parth Desai
Student
Symbiosis Centre for Information Technology,
Pune,India
parth.desai@accosiactes.scit.edu

Ms. MeghanaPande
Student
Symbiosis Centre for Information Technology,
Pune,India
meghana.pande@accosiactes.scit.edu

Mr. ShreyasAmte
Student
Symbiosis Centre for Information Technology, Pune,India
shreyas.amte@accosiactes.scit.edu

Dr. PritiPuri
Assistant Professor
Symbiosis Centre for Information Technology, Pune,India
priti@scit.edu

Abstract: *This paper initially gives an overview of Bring Your Own Device (BYOD), its advantages disadvantage, policies and some security steps. The paper attempts to provide a complete view of Mobile Device Management (MDM) software with its basic details. After that mobile application related issues have been discussed. The main highlight of the paper is on the vulnerabilities, risks due to those vulnerabilities, and impact and risk mitigation for MDM approach of BYOD. At the end of the paper, enterprise mobility management has been discussed and suggested it should consider four M's instead of three M's.*

Keywords: Mobile device management (MDM), Simple Certificate Enrolment Protocol (SCEP), Demilitarized Zone (DMZ), risk mitigation, vulnerabilities.

Introduction

In this section, first we will start with introduction of BYOD with its advantages and disadvantages. After that paper will also give BYOD policies overview and some points for BYOD security studied by literature.

In today's world, Bring your own Device (BYOD) is researchable area in the business. This enablesstaffs in the company to bring their own mobile gadgets to use thecompany assets for both work and their own use. In 2009[9], Intel acknowledged the significance of employees using their personal devices for using business assets [1].

Advantages of BYOD

- Employees are more comfortable and happy their personal devices for their office work.

- Modern and up to date devices will be in use.

- More comfort with their own device will lead more productivity

- Employee will responsibly maintain and handle the device which makes less pressure on IT staff and at the same time they can resolve other issues.

- By this concept, employees are more reachable after work hours to answer emails and complete other tasks if required.[10]

Disadvantages of BYOD

- Device cost comes to employee end of the day. If employee doesnot have such a device, he needs to buy that and the increased usage and daily carrying to the office will depreciate the device. Repairs or maintenance will also increase the cost.

- Different device with different operating systems and with different capabilities will increase the cost to company to provide services on those devices. On the other side, whenever company are buying devices for their workers they are buying in bulk with same configurations on lower cost.

- Companies pay a big amount for security structuresto protects their data from malicious attacks. Employees are not at the same wavelength of security concern as the company.Additionally, it is difficult to trust the home based devices with that level of security to handle crucial official confidential data.Both the parties (company and employee) are on the risk at the same time, if employee leaves the company, company data is on risk and at the same time, employee's personnel internet surfing is connected to organization's system[10]

BYOD Policies

Andrus [15] [14] has given ten steps for considering the mobile devices for bring your own devices purpose by organizations. According to his recommendation, for an organization to commit BYOD, first mobile enablement requirements should be found out. For this, assessment, proposal, creation or development and planning's last stage implementation is required.

The following are beautiful ten steps given by him as

1. Define mobile devices for your organization
2. Decide on the operating system versions which organization will permit.
3. White list of applications and those who are permitted
4. User Category who are going to use these devices
5. Decide network accesses pattern based on users category as who is using network, where network is used and when is used and what the purpose of using network.
6. Users training when they are buying their devices and before when they are going to use these devices on company network.
7. Make inventory for authorized users and unauthorized users and track them also
8. At the same time, make documentation for devices which are authorized and unauthorized.

9. Control or manage the network access according to company's risk policies
10. Regular attention should be given to vulnerabilities assessments and solutions
According to me,

Blended threats present for mobile devices (Markelj & Bernik, 2012). This blended threat is the threat to both the parties (user and organization).If the user is not educated properly of basic security (for e.g. authentication should be on) and he is storing the critical information on the phone, company's data and personal data both will be at risk. Indirect threats, by nature are unpredictable so they are more dangerous. [14]

For BYOD security, six major points are given.

- Data Segregation:
- Users device registration
- Access to a mobile device remotely
- Encryption of data
- Strong Password policies
- Virtual Private network setup

Mobile Device Management (MDM)

This section of the paper will talk about introductory level Mobile device management, its features.

During the process of implementing a BYOD system in a company, an integral part is MDM, (Mobile Device Management).A MDM software helps in addressing many critical problems.

MDM is a security definition for mobile devices; and mobile operating systems are important depending parameter for MDM product's capabilities. With the different operating systems, MDM enterprise management capabilities vary for each and every platform. Additionally, no alteration on operating system platforms is possible by MDM products and by third party software.

MDM has three components-one is a mobile device agent, second is-anorganization's server administrator, and third is- an intermediaryplatform vendor's service [2].

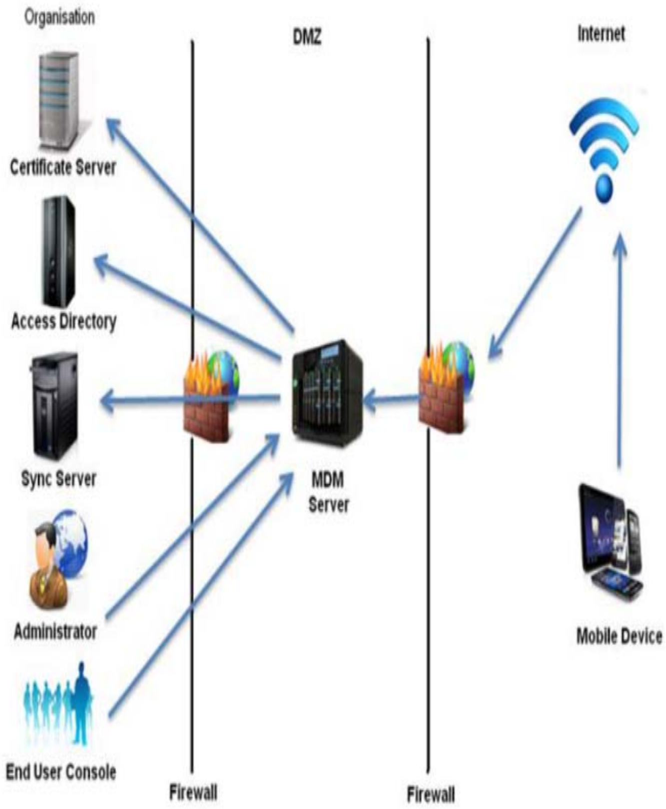


Figure 1: A MDM architecture.

First, that is, mobile agent can be secretedoperating system part itself, or provided by third party mobile app taken from online app stores which provides some additional rightsfor handling its activities. The other part, intermediate platform vendorupholdsa constantlink to the devices to enable organizationsoninstructionsand queries.

According to "Demilitarized Zone" (DMZ) concept, mobile device management servers have least access of internet and company's intranet.

MDM Features

- The platform's encryption services are in place and consistent with organization's security strategy, users can not make them disabled [2].
- Remotely wiping the device by administrator but this feature will be more effective if device is reachable through network during loss of device.[2].
- App Installation policies should be there and they should sync with enterprise's security policies.
- Organization's approved apps distribution helps to understand the application distribution infrastructure and its effect on network attack area.
- Operating system versions information reporting and app installation handled by administrator manually, automatically or integrated approach.
- MDM can detect malicious software, jail breaking or root tools to some extent but they may sometimes detect user's misbehaviour which can interfere with security policies.[2]
- MDM can easily complement VPN connection to mobile OS.
- White list for Wi Fi networks i important feature.
- Handling the PKI certificates is one more essential feature of MDM. Mostly MDM permits a company to take company's internal CA to the list. Check should be there to verify genuine CA lists.

Mobile Device Application Security

Based on literature [16], this section is exploring application related issues and security for mobile devices.

Mobile device security not only includes security of device (hardware) but also installation, storing and using the data and the applications. Mobile Applications are now a day opening the door for security risks.

According to literature [16], Application assessment should be there by first planning the app, testing the app then approve or reject the app. Some Vulnerability they tried to mitigate is

- Permissions or access given wrongly
- Internally or externally exposed communication as application collect the data and generate new information sometimes Bluetooth, GPS are open exposed for attacks.
- Sometime app is collecting unintentional information - Application conspiracy
- Software related traditional flaws as java related vulnerability

Some app related policies are suggested by them for the organizations as

- Environment in which app should/should not be used and permission for using the app.
- Establish the app security requirements and securing the data which is used by app.

- Listing the critical assets which are there on mobile devices.
- Listing existing security controls, risk tolerance and MDM solutions for mitigating the app flaws.
- Finding organization's privacy and security policies as well as security and functionality of wireless system
- Test level and attacks type for which organization has concern

MDM Vulnerabilities, Risk and Mitigations

In this section, we are trying to give overview of vulnerabilities and risks related to MDM and their mitigation solutions.

o Log in tokens without encryption

In any two step authentication in addition to password one time password are generated which are known as log in tokens, if a log in token for MDM is generated without encryption then it can be easily accessed by anyone if a person physical access of the laptop. This may lead to possible attack.

Another vulnerability of MDM can be of tokens with never ending expiry limit. Hence, a possible solution for his can be log in tokens provided by MDM should in the encrypted format and also it should have an expiry limit so that future access of the token does not hamper the security.

o Passwords with improper Hashing function [3]

One of the vendors who provide MDM technology is Mobile iron. The MDM software provide by this vendor outlines some vulnerabilities of MDM. One of them is when passwords are generated, it is done using fixed set of few keys. This is a vulnerability of this software. Other part of this vulnerability is that the encrypted password using hash function is without salt and does not have much iteration which is responsible from the security perspective.

It uses only 5 keys for encrypting all the passwords. These keys have fixed initialization values.For password encryption, randomly choose one key out of these keys. At the time of verification each and every key will be tried one by one. For other passwords, same method will be used. [11]

To solve this problem one should add some salt in the hash function and at the same time number of iteration should be more in order to avoid the above stated risk.

- During simple certificate enrolment protocol,when public key cryptography standard certificate is required for authorization,it does not verify and identify the person who are requesting.Even the request content are also not verified.
  In-person submission or registration checks person's identity and certificate content, this practice is followed for ioS devices via iPhone configuration utility. Real time SCEP requests screening is recommended for checking the content and request validation.

- The Buffer overflow vulnerability in can be done by attacker to create denial of service attack ,so that availability of company information will be affected to authorized persons or to gain access to all mobile devices and hamper them.

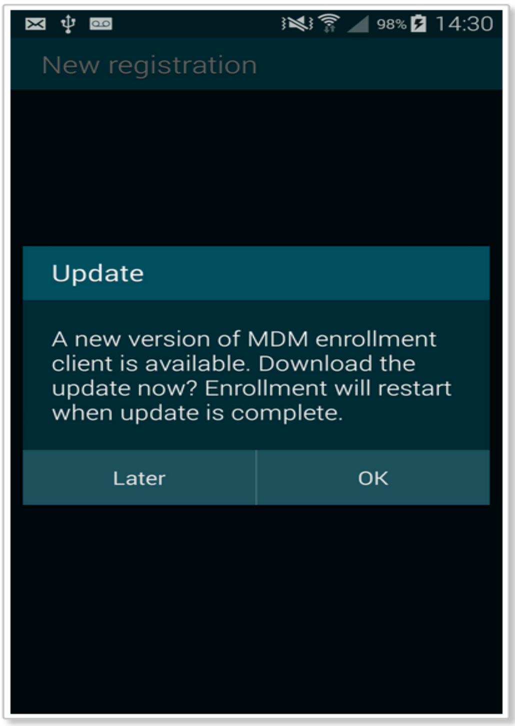
o MDM without Secure Containers [4]

The purpose of secure containers to separatecorporate and personal data on the mobile.By this secure container idea, unauthorized persons should not able to access organization's business critical data Hence if secure containers are not present in an MDM software then it may create a vulnerability.

This vulnerability can be avoided by data encryption on the phone and with the help of security parameters. A secure container executes a wipe remotelyfor an ex-employee's corporateinformation; it's not touching the other mobile data at the same time.

o Malicious application susceptibility

By this vulnerability, attacker may install an malicious application on mobile device management client side android smart phone, and for this he can use random update mechanism



A new version of MDM enrollment client is available. Download the update now? Enrollment will restart when update is complete.

Figure 3: Screenshot of malicious update

When user says ok for update, malicious app is installed. An email/browsing chrome malicious page can be origin for this vulnerability.One more place for triggering this flaw is if hacker is doing man in the middle attack as injecting code of JavaScript inside HTML page.

Prevention can be possible by matching the name Android application package with the universal mobile device management package name. So, Android application package will the update of MDM application itself and same signing certificate will be there.

o App Installation

Other vulnerability is stopping the installation of app in between which is not possible.So context related access control is one solution to give the stop permissions to app installation at runtime. But again the flaw in this solution is that it's not checking if that app installation is carrying any trozen horse/virus with that app.For this flaw,it should followed by a virus scanner.The other concern is how much time it is going to consume to finish all this process.[5][7][8]

Enterprise Mobility Management (EMM)

This second last section is trying to give overview of Enterprise mobility management (EMM).

Enterprise mobility management (EMM) is transformed from Mobile device management tools. It includes not only app but also data security and many other things.[13]

EMM is an all-inclusive method for employee to access their personal mobile devices in a secured fashion. In addition to addressing security concerns, it gives employees to do their workrelated jobs on mobile itself. [12]EMM is a mixture of mobile application management (MAM), mobile information management (MIM) and mobile device management (MDM). The purpose of MDM is locking down mobile devices, which applications can be accessed by which user is controlled by MAM and at the same time, permitted applications that can use companydata and its transmission, is allowed by MIM.

Mobile Application Management (MAM)

Mobile Information Management (MIM)

Sensitive data are stored with controlled third party environment.In today's scenario, company preferring the local storage with the same protection and monitoring strategies.

The big task is managing overhead for all three areas.

One more feature which we think should come in this umbrella is MSM.

Mobile Security Management (MSM)

MSM provides monitoring of threats related to mobile devices dynamically. It also gives end to end strategy for mobile security to the clients by learning and handling new threats. [6].

According to our observation, EMM should be four M's approach rather than three M's. In three M's, we are discussing is mobile device management (MDM), Mobile Information Management (MIM) and Mobile Application Management (MAM), we should also consider Mobile security management. This MSM feature will provide security to the devices dynamically and also update latest vulnerabilities to the client.

Enterprise mobility management (EMM)
Four M's Approach

It offers safe containers for storing sensitive data at one location on the device and provides proper separation with personal data. It is protected by password, and policies can also be implemented for that container.

Conclusion

In this paper, we outline MDM vulnerabilities and recommended solutions for the same.

This is moreover a review paper. After going through literature on BYOD, advantages, disadvantages, some policies and security steps are also studied. After that, mobile application related issues have been discussed.

Then paper flows with basics of MDM and its features. MDM vulnerabilities, related risks and its mitigation have been discussed. At last, Enterprise Mobility management has been described which has three parts as MIM, MDM and MAM. On our observation based, we also suggested that EMM should not consist of three M's ,it should consist of four M's.

One more proposed approach is-there should be some enterprise certified application(provided by enterprise only) which will daily scan employee's mobile for finding the vulnerabilities or any viruses on employee's phone. This application should also generate report of vulnerabilities and risk matrix. Risk matrix should able to generate impact rating (high, medium and low) for those vulnerabilities.

Reference

[1] “Bring your own device (byod): security risks and mitigating strategies” by “Prashant Kumar Gajar”,”Arnab Ghosh” and “Shashikant Rai” in “Journal of Global Research in Computer Science” Volume 4, No. 4, April 2013.

[2] “Mobile Device Management: A Risk Discussion for IT Decision Makers” from the Information Assurance Mission at NSA, DSN: 244-6632.

[3] “The Security of MDM systems Hack in Paris” by Sebastien Andrivet, 2013.

[4] “Practical Attacks against Mobile Device Management (MDM)” by Daniel Brodie, inLacoon Mobile Security ltd.

[5] “Threats and Vulnerabilities of BYOD and Android” by Sandip Yadav, UdyanGanguly, Saurav Suman, Dr.PritiPuri in “International Journal of Research (IJR)” p- ISSN: 2348-795X Volume 2, Issue 8, Aug. 2015. https://edupediapublications.org/journals/index.php/ijr/article/view/2692/2581

[6] Mobile security management http://www.webopedia.com/TERM/M/mobile-security-management.html

[7] M. Conti, B. Crispo, E. Fernandes, and Y. Zhauniarovich, “CRePE: A System for Enforcing Fine-Grained Context-Related Policies on Android,” IEEE Trans.

[8] Pritam R. Tarle, Comparative Study of Smart Phone Security Techniques,International Journal of Emerging Technology and Advanced Engineering, Volume 5, Issue 2, February 2015

[9] Bring your own device http://en.wikipedia.org/wiki/Bring_your_own_device#cite_no te-6 (as accessed on 1st February 2013)

[10] The Advantages and Disadvantages of BYOD http://www.businesszone.co.uk/community-voice/blogs/scott-drayton/the-advantages-and-disadvantages-of-byod

[11] The Security of MDM systems Hack In Paris 2013 Sebastien Andrivet http://www.advtools.com/Cms_Data/Contents/advtools/Media/Downloads/MDM-Hack-In-Paris-2013-public-version.pdf

[12] Enterprise mobility management (EMM) definition http://searchmobilecomputing.techtarget.com/definition/enterprise-mobility-management-EMM

[13] MDM features and functions compared http://www.cio.com/article/2895024/mobile-device-management/mdm-features-and-functions-compared.html

[14] Factors for Consideration when Developing a Bring Your Own Device (BYOD) Strategy in Higher Education http://wp.vcu.edu/assistivetechnolgy/wpcontent/uploads/sites/1864/2013/09/Emery2012.pdf

[15] Mansfield-Devine, S. (2012). Interview: BYOD and the enterprise network. Computer Fraud & Security, 2012(4), 14-17. doi:10.1016/S1361-3723(12)70031-3

[16] Assessing the Security of MobileApplications (Part 1) – Planning by Ricky M. & Monique L. Magalhaes [Published on *25 March 2015* / Last Updated on *25 March 2015*]

http://www.windowsecurity.com/articles-tutorials/Mobile_Device_Security/assessing-security-mobile-applications-part1.html

Profile **:** Dr. Priti Puri

Dr. Priti Puri is a Doctorate in Computer Science from Kurukshetra University and has an MTech degree in Computer Science from Kurukshetra University. She has over 8 years of experience including academics, research and as a Patent Analyst for Microsoft. She has published and presented many research papers at various refereed/indexed International journals and Conferences.