Mobile Device Management (MDM) Technologies, Issues and Challenges

Muhammad Mudassar Yamin
Norwegian University of Science and Technology
Gjovik, Norway
muhammad.m.yamin@ntnu.no

Basel Katt
Norwegian University of Science and Technology
Gjovik, Norway
basel.katt@ntnu.no

ABSTRACT

In the present research paper, the current status of the technology, issues and challenges of Mobile Device Management is reviewed in view of how these technologies can be used to enhance security and access control mechanism. The present methods as well as the new ones under development are discussed in this paper. Some of the current limitations and problem areas are also discussed. The paper will address Mobile Device Management technologies, issues and challenges related to it in detail.

KEYWORDS

Mobile Device Management, Security

ACM Reference Format:
Muhammad Mudassar Yamin and Basel Katt. 2019. Mobile Device Management (MDM) Technologies, Issues and Challenges. In *Proceedings of 3rd International Conference on Cryptography, Security and Privacy (ICCSP 2019) (ICCSP 2019).* ACM, New York, NY, USA, Article 4, 5 pages. DOI: https://doi.org/10.1145/10.1145/3309074.3309103

1 INTRODUCTION

MDM (Mobile Device Management) is the type of security software, which is used by the enterprise IT and information security departments to monitor mobile devices.The main functions of the MDM system are as follows [5]:

- Self-service device enrollment and management with end-user MDM console
- Managing both employee and corporate owned devices
- Supporting for multiple operating systems / platforms
- Supporting independent or integrative enterprise identity systems for device ownership
- Policy-driven device management for security, data, and device features
- Over-the-air deploy policies
- Compliance monitoring for reporting, alerting, and device provisioning
- Role-based access control
- Remote securely lock/wipe
- Tracking locations of enrolled devices
- Getting reports and analytic

We in this article focused on security issues and challenges present in mobile device management technologies with particular focus on:

- Enabling protocols for mobile device management technologies
- Infrastructure for mobile device management technologies
- Network access control for mobile device management technologies
- Centralized log management in mobile device management technologies
- Limitation and problems in mobile device management technologies

The major contribution of this article is to first present a brief state of the technology of MDM technologies and then identify major limitation and problems in MDM technologies for future research. The rest of the article is organized as follows. First, we share the related work related to MDM technologies. Second, we share our methodology to identify the issues and challenges in MDM technologies. After that we present the enabling protocols, infrastructure details, network access control and centralized log management technologies currently present in MDM technology domain. Continuing that we present the identified limitation, problems there solutions and conclusion of the research activity.

2 RELATED WORK

Pierer et al. at 2016 [18] commented about the market share of MDM technologies and the device types that are being used in MDM technologies for small and medium enterprises. The paper threw light on mobile platform support for multiple device types like Android supporting platforms ranging from smart displays to smart wearable technologies. The researchers identified the following MDM features which comprise of MDM device categorization, mobile asset management, mobile application management, mobile content management and mobile security management. Afterward, the researchers identified problem areas related to aforementioned features. Later, the researcher evaluated MDM technologies justification of usage in small and medium areas depending upon the technological limitation which the researchers identified. The researchers concluded that the market value and demand of enterprise users for MDM technologies is on raise, however they are doubtful about how MDM technologies will affect enterprise security and employees privacy.

Harris et al. at 2014 [1] made a research on the security challenges produced by MDM technologies. He stated that big organizations

ICCSP 2019, January 19-21, Kuala Lumpur, Malaysia

ACM ISBN ACM ISBN 978-1-4503-6618-2/19/01...$15.00.
DOI: https://doi.org/10.1145/10.1145/3309074.3309103

have a lot of resources to spend on the security of MDM technologies on work place and are able to afford complex MDM security solution. However, small and medium sized enterprises don't have such resources to spend on the security of MDM technologies. After analyzing this problem, the researchers suggested a set of minimum requirements for enhancing the MDM technologies, security. Their recommendations consist of device recommendation, user orientated recommendations and management oriented recommendations. The device oriented recommendations indicates that how a particular device should be allowed to operate within the organization and under what circumstances the operation should be conducted. The user oriented recommendations include the type of application the user is allowed to use and the type of device security feature that should be present on the device to be allowed in the environment of the enterprise. The management oriented recommendations focus on training of employees in using mobile technologies and developing policies for MDM infrastructure.

Garba et al. at 2015 [10] studied the security and privacy challenges in BYOD (Bring Your Own Device) environments. Firstly, the researchers gave an introduction about BYOD technologies and the benefits that the technology offers to enterprises, like accessibility, convenience and flexibility, employee satisfaction, cost savings, increased productivity and innovation. After that the researchers illustrated the security and privacy challenges of BYOD environment scenarios. The researchers stated that managing and securing mobile devices with different operating systems is a challenge itself and there is always a danger of theft that puts enterprise data at risk. Moreover, the management of employee personal devices in enterprise network will not only put extra stress on present security infrastructures, like firewalls, IDS, IPS etc, but this would also affect the privacy of the employee working in the organization. The researchers proposed methods to tackle the above mentioned problems. These approaches include network centric approach in which multiple solutions are offered by security vendors which are highlighted to manage network security in BYOD environments. A MDM approach is the one that puts emphasis on mobile device management using a software platform for enterprise security policies on BYOD scenario environment, the researcher also suggested phone centric approach in which MDM capabilities are already associated with the devices. And lastly, there is the virtualization approach in which mobile device are used only to access backed virtualized systems on which enterprise security policies are applied to ensure security.

Tse et al. at 2016 [21] researched about mobility management for enterprises in BYOD environment. They distributed the BYOD security scenario in the mobile device management, mobile application management and in mobile content management. The major mobile device management features are profile management, monitor and track mobile devices, access control, remotely wipe data, remotely lock device, detect malware and data encryption. The major application management features are application distribution, application installation, application catalog, application blacklisting/whitelisting, and application reports. The major mobile content management features are control access for corporate documents, secure content storage, synchronize content, encrypted content container, real time analysis, and reporting. After observing the major features in the enterprises, they compared multiple mobile device management tools like MAAS360 and Airwatch to check which of the major identified features they support and what features can be added in existing solutions to improve enterprise security in BYOD environment.

3 METHODOLOGY

In order to understand the literature review of the present research paper, a keyword-based research is employed. The researcher started with "Mobile Device Management" with "Security". The researcher investigated the following keywords in academic databases like Google scholar, IEEE and ACM to acquire the better understanding of the given terms [12]. The researchers also made themselves familiar with the related literature on the given topic. The researchers spotted a lot of related information but employed them in indexed research articles only. The researchers conducted a thorough research and collected good amount of relevant literature in an organized manner, but the repetition of literature gathering process is not good for other research articles [13].

4 ENABLING PROTOCOLS FOR MDM

In this section enabling protocols and technologies for mobile device management technologies are presented.

4.1 Open Mobile Alliance Device Management

The OMA (Open Mobile Alliance) DM (Device Management) group [4] is currently investigating upon a unified MDM protocol that has the ability support devices from different manufacture running different operating systems. Accordingly, the communication network of a MDM protocol can be seen in view of two variable aspects; a direct connectivity in which a group of similar devices can associate in a direct way with a single application, or a connection via a machine to machine gateway, this case is applicable for "Low-cost" devices that may not directly interact with an application because of their limited potential. OMA device management is a device management protocol specified by the Open Mobile Alliance *Device Management Working Group* and the *Data Synchronization Working Group*. OMA DM specification is formulated for the management of mobile devices such as mobile phones, PDAs, and tablet computers. This allows variations in the settings and parameters of the device. It also report errors from the device and query about status of the device. All of the above functions are supported by the OMA DM specification, and a device may optionally implement all or part of these features. Technically, the OMA DM protocol uses XML for data exchange, more specifically the sub-set defined by SyncML(Synchronization Markup Language). The device management happens by communication between a server and the client. Once the communication is established between the server and client, a sequence of messages might be exchanged to execute a given device management task.

4.2 Smart Message [19]

Smart Message is a protocol designed by Intel and Nokia. It can be used for updating software including ringtones that could be made "over the air", through the wireless connection. Smart Messaging is basically a special type of short messages, with its own prefixes and codes, that makes it possible for the phone to interpret the message

as, a "functional" message that should be treated as: a ringtone, a screen logo and in some cases even a business card or group graphics that can be used to identify who is calling. Smart Message delivery make use of ASCII format streams so smart messages can be passed via different transport protocols. Smart Messaging has been used by major GSM mobile phone suppliers for short messaging services and in messaging for personal digital assistant (PDA) devices, and wireless connection devices using radio frequency transmission bands such as Bluetooth.

4.3 Open Mobile Alliance Client Provisioning [2]

OMA Client Provisioning is a device management protocol specified by the Open Mobile Alliance (OMA) Device Management (DM) Working Group. The OMA CP protocol encompasses WAP (Wireless Application Protocol) with lesser user interaction, typically over-the-air or via SIM Card. OMA provided content messages are special SMS messages that consists of information used to configure certain settings of a mobile phone, such as settings for the browser (APN, proxy, bookmarks), MMS client, IM client, or SyncML client. These messages are sometimes called as OTA configuration messages, where OTA is an acronym for Over-The-Air.

4.4 Over-The-Air Programming [6]

Over-the-Air programming (OTA) refers to different methods of distributing new software, configuration settings, and updates of encryption keys to devices like cellphones, set-top boxes and secure voice communication equipment (encrypted 2-way radios). One significant characteristic of OTA is that one central location can send an update to all the users, who are unable to refuse, defeat, or alter that update, and that the update applies immediately to everyone on the channel. A user could "refuse" OTA but the "channel manager" could also "kick them off" from the channel automatically. In the background of the mobile content world, they consist of over-the-air service provisioning (OTASP), over-the-air provisioning (OTAP) or over-the-air parameter administration (OTAPA), or provisioning handsets with the important settings to access services such as WAP or MMS. As mobile phones gather new applications and become more advanced, OTA configuration has become more significant as new updates and services come on stream. OTA via SMS regulates the configuration data updates in SIM cards and handsets and enables the distribution of new software updates to mobile phones and provisioning handsets with the necessary settings with which to access services such as WAP or MMS. OTA messaging provides remote control of mobile phones for service and subscription activation, personalization and programming of a new service for mobile operators and for the third parties. Different standardization bodies have been formed to assist in the development, overseeing , and management of OTA. One of them is the Open Mobile Alliance (OMA).

5 INFRASTRUCTURE FOR MDM

Driven by the rising demands of Cloud and big data, the MDM of present times is very different, offering greater capabilities, hybrid deployment options, a variety of entry points, and more business user flexibility than ever before. This consists of supporting MDM implementations of modest scope, and supporting proof-of-concept, development and testing activities before placing a premise on MDM solution into production. The challenge of protecting the enterprise data on these devices are just as great as if the devices were within the enterprise. Mobile device vulnerabilities reflect poorly on carriers who sell these devices, so they are motivated to protect devices in a good manner. An important difference between mobile devices and desktop computing is the multitude of sensors in most mobile smart phone devices, which can be used for collecting personal and enterprise data in case of a security incident. Remote "Wipe" capability could be utilized if the device is lost or stolen. For Malware scanning and detection, device inventory and accounting, capabilities include the following: MDM software suites provide management of mobile devices and enterprise data stored on them. Strong authentication for Sysadmin via tokens separate them from the mobile devices they use for administration. If an enterprise allows systems administration from unmanaged mobile or BYOD devices, it should take into view the following limitations: Potential advantages of allowing system administrators to perform their duties from mobile devices do not outweigh the security risks. With the exception of mobile device management technologies, many enterprise tools are not applicable on individually owned computing devices [7]. MDM is also about managing the device features, but it is associated with Mobile Content Management (MCM) and Mobile Identity Management (MIM), Application management (MAM) it is called Enterprise Mobility Management (EMM). As EMM was particularly about managing the apps and content on mobile devices, it was not able to manage older devices such as Windows laptops/desktops and new MACS, so EMM evolved into UEM (Unified Endpoint Management) with additional functionality to manage both mobile and traditional devices such as desktops and laptops.

5.1 Mobile Content Management

A Mobile Content Management system (MCMs) is a type of Content Management System (CMS) which has the ability of storing and delivering content and services to mobile devices, such as mobile phones, smart phones, and PDAs [11]. Mobile content management systems may be hidden systems, or may exist as features, modules or add-ons of larger content management systems capable of multi-channel content delivery. Mobile content delivery has unique, specific constraints including widely variable device capacities, small screen size, limited wireless bandwidth, small storage capacity, and comparatively weak device processors.

5.2 Mobile Identity Management

Mobile identity is a development of online authentication and digital signatures, where the SIM card of a mobile phone works as an identity tool. Mobile identity enables legally binding authentication and transaction signing for online banking, payment confirmation, corporate services, and consuming online content [16]. The certificates of users are maintained on the telecom operator's SIM card and in order to use them, the user has to enter a personal, secret PIN code. While using mobile identity, no separate card reader is needed, as the phone itself already performs both functions. In contrast to other approaches, the mobile phone in association with a mobile

signature-enabled SIM card aims to offer the same security and ease of use as compared to smart cards in existing digital identity management systems.

5.3 Mobile Application Management

Mobile Application Management (MAM) provides control at the application level that would enable administrators to manage and secure app data [14]. MAM differs from mobile device management (MDM) as MAM focuses on controlling the entire device and requires that users enroll their device and install a service agent. MAM provides administrations capabilities to enterprise system administrators to remotely manage mobile applications on mobile devices in BYOD scenario. The administration abilities include control the provisioning, updating and removal of mobile applications via an enterprise app store, monitor application performance and usage, and remotely wipe data from managed applications.

5.4 Enterprise Mobility Management

Enterprise Mobility Management (EMM) is the arrangement for individuals, procedures and innovation concentrated on overseeing mobile phones, remote systems, and other versatile figuring administrations in a business setting. With the progression of time, an immense number of employees have beginning to bring cell phone and tablet registering gadgets and have looked for help for utilizing these gadgets in the work environment, EMM has turned out to be essential [8]. The objective of EMM is to decide whether the accessible portable IT is to be incorporated with work procedures and goals and how to help employees when they are utilizing these gadgets in the working environment. As mobiles phones are easily lost or stolen, information contained in those gadgets is entirely defenseless.

5.5 Network Access Control

The best form of cyber security comes in the layers, making it difficult or frustrating for an intruder to fight through each line of defense to break into the network and gain access to data. One of the front-line defenses should be network access control and its ability to restrict network access to devices and users that are authorized and authenticated [17]. The emphasis of NAC(Network Access Control) is on the access control - who or what has authorized permission to access the network. The NAC network looks for the connection requests, which are then authenticated against a designated identity and access management system. While this concept is fairly straightforward, deploying network access control is more challenging. It allows the administrator to define multiple access policies that assist users and devices connecting to the network based on specific situations such as user profile, device type or user location. If the device fails in any of these compliance checks, it will likely be denied access to the network until appropriate updates are made. Although these goals and use cases can be used across any industry, there can be specific advantages for deploying network access control solutions for specific situations, as in heavily regulated industries such as healthcare and financial services. Permitting the users to connect to the network with their own devices has the potential to pose danger, as it is difficult for IT departments to control. NAC control can also determine how many devices a user can connect to the network or what type of devices would be allowed. A sensitive research project may have permission to set up a security camera system with network access so it can be monitored remotely giving permissions that may not be offered to other individuals or departments.

NAC restricts access for devices that did not comply with company policy or had become infected with malware. If devices ever left the network and became infected, or if devices were used improperly and were in danger of being compromised, NAC could restrict access to these internal servers and thus prevent infected or otherwise non-compliant endpoints from connecting to corporate data. Traditional NAC solutions were formulated when PCs were dominant access device and applications were hosted in the main data center. Even if employees do not use their personal devices for official business purposes, they may expect to be able to connect their personal devices to the network and to sensitive cloud resources anyway [15]. They will likely to expect access to the network on their devices. To monitor devices and protect corporate data stored on endpoints, the endpoint monitoring, endpoint detection and response, and mobile device management solutions may be necessary.

5.6 Centralized Log Management

Log management deals with what you need to log, how you log it, and how long those logs stick around. It also regulates the generation, transmission, storage, indexing, and disposal of the enterprise's log data. The centralization of log data in a log management solution is an old standard. A log management solution should improve enterprise ability to monitor all events across the enterprise at once, improving enterprise IT security teams' security detection efficiency and increasing activity awareness [20]. What exactly enterprise will need to log and for how long is different for every enterprise. Log management is simply collecting and processing event information from across the enterprise. Log management might be the right solution for a smaller enterprise that can review all the logs for security events. The mobile device management software is often combined with additional security services and tools to create the complete mobile device and Enterprise Mobility Management system.

In short, many enterprises have used traditional log management solutions. Traditional log management's job is to collect data, and therefore it generally can't make the differentiation between data that results from everyday business activities and data that are red flags for malicious activity [3]. In a similar manner, when log management solutions collect data, it does not coordinate that data in a sensible manner in the centralized "Bucket." Therefore the collected logs will require a specific search language to make sense of them and allow your team to find ongoing attacks or breaches. Log management can make finding serious threats in your data logs like finding a needle in a haystack.

In the field of computer security, SIEM (Security Information and Event Management) software products and services combine security information management and security event management. Vendors sell SIEM as software, as appliances or as managed services; these products are also used to log security data and produce reports for compliance purposes. The segment of security management

that deals with real time monitoring, correlation of events, notifications and console views is known as security event management. The second area provides long-term storage as well as analysis, manipulation and reporting of log data and security records of the type collected by SIEM software, and is known as security information management. The potential of such activities lie in gathering, analyzing and presenting information from network and security devices. Log management collects data from many sources, including network, security, servers, databases and applications, providing the ability to illustrate monitored data to help avoid missing crucial events. Correlation is typically a function of the Security Event Management portion of a full SIEM solution [9]. Visualization with a SIEM using security events and log failures can help in pattern detection.

6 LIMITATIONS AND PROBLEMS

Research challenges which are identified during the the review of state of the technology of MDM are given below:

- User identity management for devices with multiple users. Often in enterprise environment a single device is used by multiple user. New methods are required to seamlessly mange their identity without requiring extensive login processes.
- Logs collected from mobile devices contains personally identifiable information which cause employee privacy related problems. There is a need to develop homomorphic encryption methods to to hide personally identifiable information from the mobile device management solution logs.
- MDM solution collects allot of behavioral data which can be use full in certain use cases however there is need to preprocess that data to transform it in a manner that the behavior information of employees remain secure. Behavioral data transformation techniques are need to be developed and it aslo require to verify there scientific utility after transformation
- The technical mechanisms that are implemented in data-management policies as user data is collected, stored, processed, and shared need be GPPR compliant as currently most of the MDM solution are not developed considering GDPR requirements.

7 CONCLUSION

In this paper the researchers have presented a brief sate of the technology discussion on current mobile device management technologies. Firstly, the researchers have briefly introduced the topic and defined it by quoting relevant references. The researchers have then stated opinion of other researchers about the given topic and have presented some research questions to be investigated. Later, the methodology employed for conducting the survey report is discussed. Later the researcher have discussed about some protocols of Mobile device management technologies including Mobile application management and mobile identity management. Later, they have thrown light on network access and bring you own device scenarios in reference to MDM. They wound up the discussion with the mobile log management. MDM technologies that are prevalent in different scenarios are discussed in detail in the present paper. The researchers have posed a solid framework for the report by presenting some important research questions and facilitated the report with related literature review. They have presented the current status of security in BYOD scenario in enterprises and shared the key enabling technologies to ensure enterprise security. They have also identified the current challenges, problems and limitation in mobile device management technologies with respect to security and shared probable solutions. In future, the researchers plan to extend the work with more comprehensive sate of the art review.

REFERENCES

[1] Mark A. Harris and Karen P. Patten. 2014. Mobile device security considerations for small-and medium-sized enterprise business mobility. *Information Management & Computer Security* 22, 1 (2014), 97–114.

[2] Miller T Abel. 2014. Means for provisioning and managing mobile device configuration over a near-field communication link. US Patent 8,718,554.

[3] HL Akshaya, J Vidya, and K Veena. 2015. A Basic Introduction to DevOps Tools. *International Journal of Computer Science & Information Technologies* 6, 3 (2015), 05–06.

[4] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, and Moussa Ayyash. 2015. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials* 17, 4 (2015), 2347–2376.

[5] Ngoc Duong Bui, Alla Grigorievna Kravets, Tuan Anh Nguyen, et al. 2015. Tracking events in mobile device management system. In *Information, Intelligence, Systems and Applications (IISA), 2015 6th International Conference on*. IEEE, 1–6.

[6] Brian Kevin Daly. 2000. Method and apparatus for over-the-air programming of telecommunication services. US Patent 6,122,503.

[7] Scott E Donaldson, Stanley G Siegel, Chris K Williams, and Abdul Aslam. 2018. Enterprise Cybersecurity for Mobile and BYOD. In *Enterprise Cybersecurity Study Guide*. Springer, 249–274.

[8] Jill Dove. 2016. Evaluation of the suitability of the mobility common criteria protection profiles for enterprise mobility management. (2016).

[9] Joonas Forsberg. 2018. Implementation of Centralized Log Management Solution for Ensuring Privacy of Individuals as Required by EU Regulation. (2018).

[10] Abubakar Bello Garba, Jocelyn Armarego, David Murray, and William Kenworthy. 2015. Review of the information security and privacy challenges in Bring Your Own Device (BYOD) environments. *Journal of Information privacy and security* 11, 1 (2015), 38–54.

[11] Atiq Hashmi. 2013. Mobile Content Management System. US Patent App. 13/908,536.

[12] Jill Jesson, Lydia Matheson, and Fiona M Lacey. 2011. *Doing your literature review: Traditional and systematic techniques*. Sage.

[13] Barbara Kitchenham, Pearl Brereton, Zhi Li, David Budgen, and Andrew Burn. 2011. Repeatability of systematic literature reviews. In *Evaluation & Assessment in Software Engineering (EASE 2011), 15th Annual Conference on*. IET, 46–55.

[14] Raj Kumar Koneru, Pattabhi Rama Rao Dasari, Prajakt Deshpande, Vivek Iyer, Rajendra Komandur, Aravind Perumal, Sriram Ramanathan, Matthew Terry, Vamsi Krishna Vagvala, Sathyanarayana Vennapusala, et al. 2016. Mobile application management systems and methods thereof. US Patent 9,405,723.

[15] Steve Mansfield-Devine. 2012. Interview: BYOD and the enterprise network. *Computer fraud & security* 2012, 4 (2012), 14–17.

[16] Murali Krishna Medudula, Mahim Sagar, and Ravi Parkash Gandhi. 2016. Mobile Device: Applications, Over the Top Services, Identity Protection and BYOD Policy. In *Telecom Management in Emerging Economies*. Springer, 207–227.

[17] Yaser Mowafi, I Dhiah el Diehn, Ahmad Zmily, Tareq Al-Aqarbeh, Marat Abilov, and Viktor Dmitriyevr. 2015. Exploring a Context-based Network Access Control for Mobile Devices. *Procedia Computer Science* 62 (2015), 547–554.

[18] Markus Pierer. 2016. MDM evaluation for small and medium sized enterprises. In *Mobile Device Management*. Springer, 65–99.

[19] Herman Rao and Eric Lin. 2003. Instantaneous polling utilizing a message service mobile phone network. US Patent App. 10/137,033.

[20] Nader Shahata. 2018. Towards Academic Organizations Security. In *2018 3rd International Conference on Computer and Communication Systems (ICCCS)*. IEEE, 169–172.

[21] Daniel Tse, Lu Wang, and Yuxi Li. 2016. Mobility Management for Enterprises in BYOD Deployment. In *Trustcom/BigDataSE/IâĂŃ SPA, 2016 IEEE*. IEEE, 638–645.