MAM Security Enhancement: Proposed Control Mechanism

Radhia Khellaf[1], Souheila Boudouda[1], Salima Hacini[1]
[1]*LIRE Laboratory, Abdelhamid Mehri- Constantine2, University Constantine, Algeria*

Abstract

With the advent of the mobile enterprise, the need for a dynamic and flexible security framework to balance risk and trust becomes urgent. This need has led to the rapid expansion and growth of enterprise security technologies for mobility. In this article, the two most used mobile ecosystem management tools (Mobile Device Management and Mobile Application Management) are analyzed from a security point of view. In addition, a protection mechanism which strengthens the security aspect of the Mobile Device Management application is proposed. It fixes the Mobile Device Management security vulnerabilities and reduces the impact of attacks. On the basis of the characteristics of proposed approach activities, a functional diagram is presented.

Keywords

Security; mobile security; mobile enterprise; Mobile Device Management; Mobile Application Management.

1. Introduction

The use and development of the mobile application is a new and rapidly growing sector. Mobile applications are executed on a small mobile device, easy to use and accessible from anywhere and any place. According to research works presented in[1][2], the advantages of a mobile workforce are obvious: First, remote workers will be more productive and happier. Second, they work an additional five hours per week adding more than 250 hours of work every year. Furthermore, Teleworkers continue to work when they are sick and do not come to the office to potentially infect their coworkers. Finally, companies can reduce their expenditures on real estate and office operations. The benefits of mobility in enterprise are therefore numerous. However, companies are also raising many security issues and challenges with mobility [3]. A huge challenge is therefore to protect the data from unauthorized access.

Consequently, it is a question of finding a security compromise between the use of different types of personal mobile devices and the control that the company must put in place on these devices. The main goal is to limit the security risks [4]. Therefore, in a heterogeneous environment imposed by mobility, it is very difficult, if not impossible, to build a single approach that adjusts to all security and surveillance requirements. It is also difficult to manage the administration of all mobile devices of an organism [5].This is the reason why a particular category of tools was born, namely: Mobile Device Management (MDM) [7], Mobile Application Management (MAM)[8], Enterprise Mobility Management (EMM), Mobile Content Management (MCM) and Unified Endpoint Management (UEM), Identity and Access Management (IAM)[5][6]. But the implementation of these solutions can generate certain problems to which the company must be very attentive.

RIF'20: The 9th Seminary of Computer Science Research at Feminine, March 7th, 2020, Constantine 2-Abdelhamid Mehri University, Algeria

EMAIL: radhia.khellaf@univ-constantine2.dz (R. Khellaf); souheila.boudouda@univ-constantine2.dz (S.Boudouda); salima.hacini@univ-constantine2.dz(S.Hacini)

In this paper, we have proposed a securing approach which can strengthen the MAM applications. The goal is to enable the company to take advantage of the business benefits of the mobile revolution, while protecting it, as well as its employees and customers, from potential risks. The main idea is to introduce a control mechanism at the MAM application level which makes a reaction requesting the intervention of administrators in the enterprise. It also applies a strategy for controlling access to resources and system services separately.

The remaining of this paper is organized as follows. Section 2 reviews the current state of the mobile enterprise and describes the risks associated with the most popular mobile device platforms and technologies. Then, it outlines the ways in which many of these risks can be mitigated. Section 3 and 4 specifies the main management tools used by mobile enterprise. Section 5 describes the proposed security mechanism which strengthens the security aspect of the applications. Section 6 includes a discussion of the direction of research taken by this work. Finally, some conclusions and research lines are presented.

2. Risks in mobile enterprise

A mobile enterprise is a company whose employees are nomads and who work on a collaborative information system. This system allows employees in real time to consult, verify, or record information in the database of the mobile enterprise (mobile ecosystem). [9](See Figure 1).

The emergence of the concept of mobile enterprise has been generated by a number of needs such as:

- Employees not required to be present in the same workplace
- Real-time access to up-to-date information (availability)
- Simple use
- Rapid deployment of information.

The mobile enterprise essentially consists of four parts [10]:
1. End user
2. Mobile device (hardware, operating system and applications)
3. Company (servers, applications and services, and data sources);
4. Network path (connects the mobile device to the enterprise via, for example, local WiFi or cellular communications, network operators, Internet, routers, etc.).

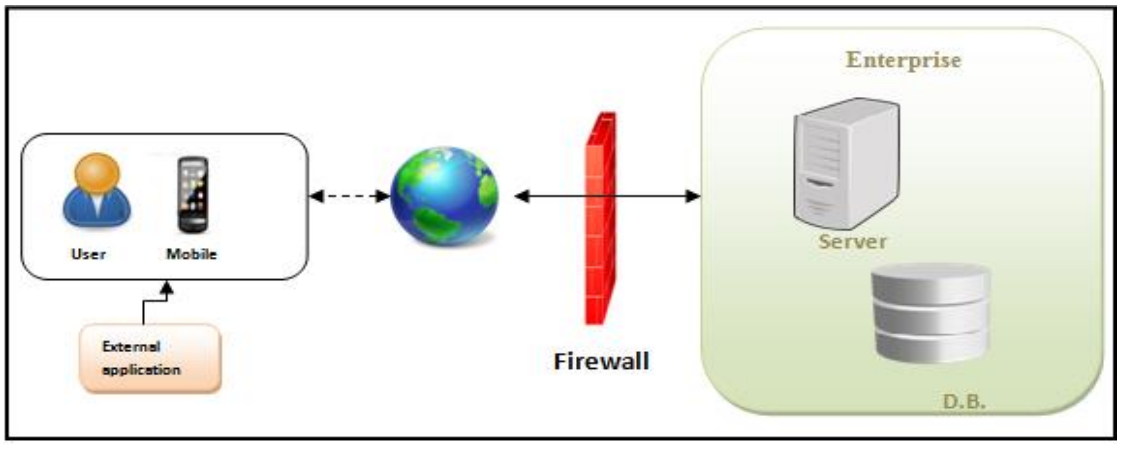

Figure 1: Architecture of a mobile ecosystem

To achieve sufficient security for the entire mobile enterprise, it is necessary to secure these four parts. Each part suffers from a specific set of vulnerabilities and therefore requires a security solution that meets its particular needs.

Mobility certainly has a positive influence on the turnover (gain and reduction of costs) of a company. However, it also brings a lot of disadvantages, particularly if it is not enough taken care of. Threats to the mobile ecosystem can indeed increase and affect the security of users and organizations.

Table 1 presents the risks and vulnerabilities that accompany the use of mobiles devices [2] [11][12].

Table 1: Risks and vulnerabilities related to mobiles enterprises

Device and material	• Unauthorized access; • Lack of security configuration; • Obsolete legacy devices; • The loss or theft of personal media containing personal data. According to Winn Schwartau, 25% of mobile owners lose their Smartphone at least once. This implies that professional data may be lost and / or be accessible by anyone who has this device; • Risks of intrusion into the enterprise system (Virus, malware, spy, etc.).
Networks and communications	• Data leaks in the cloud; • Misconfigured SSL / TSL; • Vulnerable services on an unsecured network; • Lack of encryption of transferred data.
Application	• Bad authorization and authentication; • Attacks on mobile / PC and insecure applications; • Lack of security configuration; • Unsecured password recovery; • No application or password lock; • Collecting unnecessary personal data and sharing on the network.

3. Managing an Enterprise Mobile Environment

Several solutions have been created to protect a mobile enterprise against these threats, including mobile application management (MAM), mobile device management (MDM), enterprise mobility management (EMM), mobile content management (MCM), Unified Endpoint Management (UEM), and Mobile Identity Management IAM.

As an architect, you are responsible for determining which approach is best for the environment you manage. Which approach (MDM, MAM, EMM, UEM, IAM, or MCM) is right for your environment? Let's go through each one [17] [5] [18]:

3.1. Mobile Device Management (MDM)

Monitors, manages, and secures mobile devices that are deployed across different cellular carriers. The process installs an application on the device to give access to and control of the device.

3.2. Mobile Application Management (MAM)

Provides control at the application level that would enable administrators to manage and secure app data [19]. 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.

3.3. Enterprise Mobility Management (EMM)

EMM is a global approach for devices and platforms that centralize the management, configuration, and security of all mobile devices managed by an enterprise.
EMM goes beyond traditional device management to include the management and configuration of enterprise applications and content. Thus, a complete EMM strategy also aims to help employees be more productive by providing them with the tools they need to do their work on mobile.

EMM Combines MDM and MAM. This leads to increased complexity and costs

3.4. Unified Endpoint Management (UEM)

UEM provides enterprise management of endpoints, including mobile devices, printers, laptops, and desktops, IoT devices from a single management platform.
The disadvantage of this approach is that it is expensive with intense management.

3.5. Mobile Content Management (MCM)

(Sometimes called MIM for Mobile Information Management) supports and controls access to content from mobile devices. It uses either a secure container or content push (In both cases, device and app are secondary.); to ensure that only approved apps can access and share company data.

3.6. Identity and Access Management (IAM)

Which is the set of processes implemented by a company for managing the access authorization of its users (employees, partners or customers) to its information system or its applications. Thus, identity and access management is concerned with, for example, controlling how users acquire an identity, how to protect that identity, and the technologies that enable that protection.

4. Main management tools used by mobile enterprise

As mentioned above, a lot of mobile ecosystem management solutions for the mobile enterprise were introduced (MDM, MAM, EMM, MCM, UEM and IAM). The implementation of these solutions can produce certain problems to which the company must be very vigilant. In this section, we analyze in particular the two most used mobile ecosystem management tools (MDM and MAM).

4.1. Mobile Devices Management

The MDM is an application that manages the deployment, securing, monitoring, integration and administration of personal or professional mobile devices, such as smart phones or tablets that have access to critical data [10] [13]. MDM software provides asset inventory, live email, application and WiFi configuration, remote troubleshooting solutions, and remote lock and wipes features to secure devices and enterprise data. Thus, MDM can be considered as the foundation of a complete Enterprise Mobility Management (EMM) solution.

Its objective is to harmonize and secure the company's fleet by ensuring that all employees have up-to-date programs and that their devices are properly secured. The program also facilitates the spread of security patches or new software for all employees (Figure 2).

Figure 2 : Mobile Device Management software (MDM)

The MDM manages various sizes and types of fleets ranging from ten identical terminals, to thousands of terminals all different and using different operating systems.

The main security features of the MDM application are [14]:

- Deleting remote content;
- Remote blocking of the terminal;
- Limitation of roaming to restrict usage by geographic area;
- Limitation of physical capacities such as the USB port, card reader (micro) SD or other, etc;
- Deployment of configurations, certificates, security rules, etc;
- Encryption;
- Strong authentication including strong passwords, PIN code, biometrics, etc;
- Configuration of a firewall, proxy, VPN, etc;
- Anti-virus.

4.2. Mobile Application Management

The MAMtechnologies apply management and policy controls to individual applications rather than the entire device. MAM allows IT administrators to install, update, delete, audit and monitor enterprise applications on mobile devices [15][5].

MAM solutions generally offer a custom application store that allows to control and deliver internally developed and third-party applications (Figure 3).

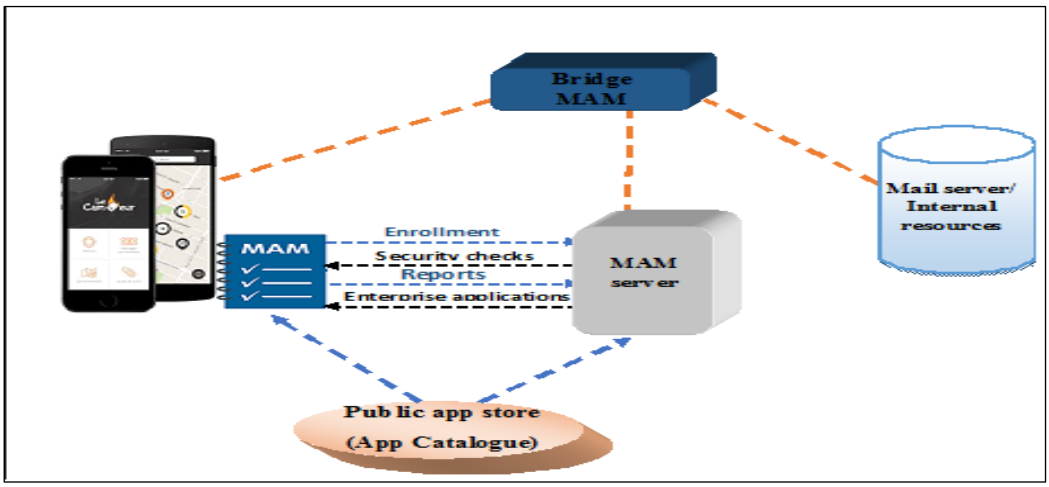

Figure 3: Conceptual architecture of MAM

MAM represents all the software and services responsible for supplying and controlling access to mobile applications. These applications are used in professional environments on smartphones and tablets provided by the enterprise.

The main security functionalities of the MAM application are [6]:

- Distribution of applications (Enterprise App Store);
- Update applications;
- Monitoring application performance;
- User Authentication;
- Logging of incidents;
- User and group access control;
- Application version management;
- Management of the configuration of the applications;
- Push services (sends information to the user through a mobile application);
- Usage analysis;
- Event Management;
- Wrapping apps;

With MAM, employees can gather their personal and professional information in a smartphone capable of retaining independent operational identities. The idea is that users can install Facebook and other apps of personal interest in the personal partition, but that work-related apps and data are stored in the working partition.

Ina security model centered on the MAM application, an application establishes its own autonomous encrypted communication channel at the application level or in the closed environment where the application exists, without depending on the operating system or the device. This provides a tampon between personal space and corporate space. The separation of enterprise applications from personal space fulfills several key functions [16]:

• It preserves the user experience without modifying the device or controlling personal applications;

• It provides the necessary level of access control for enterprise applications with the ability to exceed current standards;

• It reduces the company's risk posture by eliminating the use of endpoints for data entry on the approved network.

4.3. Main differences between MDM and MAM

Each mentioned security method has its strengths and limitations in terms of protecting internal data reachable from mobile devices (Table2). A robust security analysis should include a security strategy, which should significantly reduce the security risks associated with BYOD. Table 2 presents the main differences between the two most used mobile ecosystem management tools: MDM and MAM.

The next section presents the proposed control mechanism. It strengthens the security of MAM and ensures a perpetual update in order to counter any new attack in a short time. In addition, it relies on detections from other applications which themselves benefit from continuous updates.

5. Proposed control mechanism

In this article, we propose to introduce a control mechanism at the MAM application level which autonomously applies a strategy for controlling access to resources and system services and generates a reaction requesting the intervention of administrators in the enterprise.

The basic idea of this approach is to provide MAM with the control faculty that will allow it to make decisions as to whether or not to authorize an application that requests access to a system service. This control is based on MAM's ability to intercept interactions between applications and a few system processes to retrieve detailed information on applications requests necessary for fine-grained access control

Table2: Main differences between MDM and MAM

Mobile Device Management (MDM)	Mobile Application Management (MAM)
• Management, security and control of the mobile device (MDM touches terminals).	• Management and security only of applications specially designed by the enterprise (MAM targets applications).
• Remote deletion of all content from the device in the event of theft or loss.	• Deletion only of professional data.
Focuses on security: • The application of defined password policies; • Encryption of data on the device; • Control of data sharing options at the device level, for example, wifi, camera, Bluetooth and 3G; • Blocking, remote erasure, location of the device, ...; • Control of mobile devices such as printers and scanners.	Focuses on making available: • Creation of a catalog of safe and approved applications to download to give users the opportunity to do more effective work on their devices; • Management of multi-user profiles for the same application; • Change the configuration of the application without the need to update the version.
• Managing and securing applications; • Prevention of data loss; • Distribution of application based on the configuration; • Management of a whitelist and a blacklist of the device, the user and the applications; • Inventory management of applications and peripherals.	

5.1. General architecture of the proposed control mechanism

The role of the proposed security mechanism is to quickly detect an attack to counter it as quickly as possible, to be able to react in real time to an intrusion attempt and to improve the security of the MAM by local processing (at the mobile level) alerts. The help of the company security administrator will only be required in the event of ambiguity (the control mechanism could not confirm or deny the attack).

We assume the existence, at the mobile device level, of other intrusion detection tools such as HIDS (Host Based Intrusion Detection System). The security information collected by these different tools will be used by the proposed security mechanism to improve detection.

The proposed mechanism uses three components present on the mobile (Figure 4):

• A collector component;
• An analyzer component;
• An executor component.

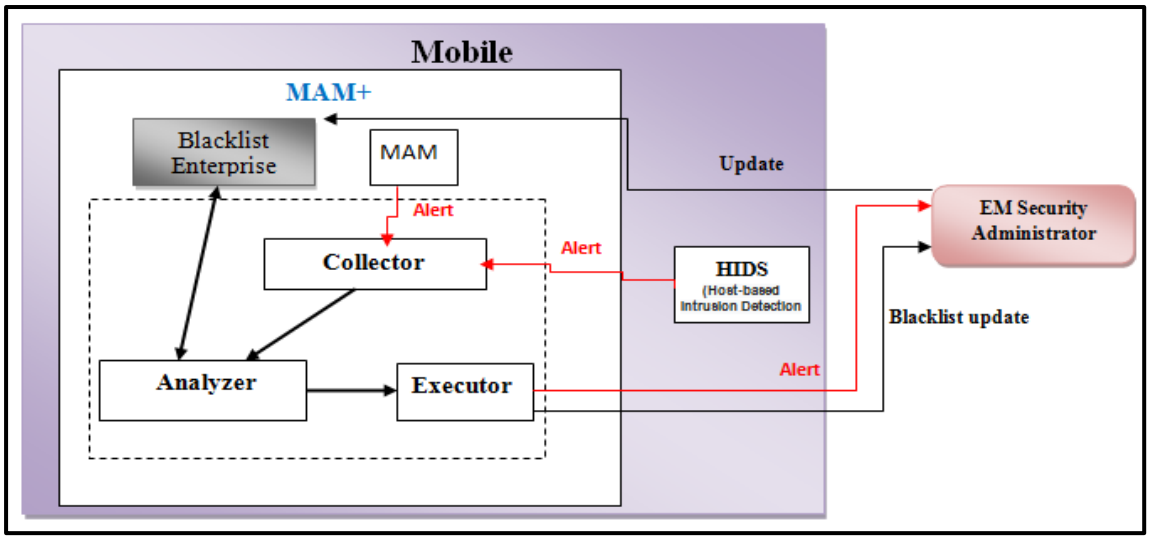

Figure 4: General architecture of the proposed control mechanism

5.1.1. Collector component

The collector component intercepts alerts from other existing control applications at the mobile level, such as the intrusion detection system, as well as suspicious activities detected by the MAM application itself and transfers them to the analyzer component (Figure 5).

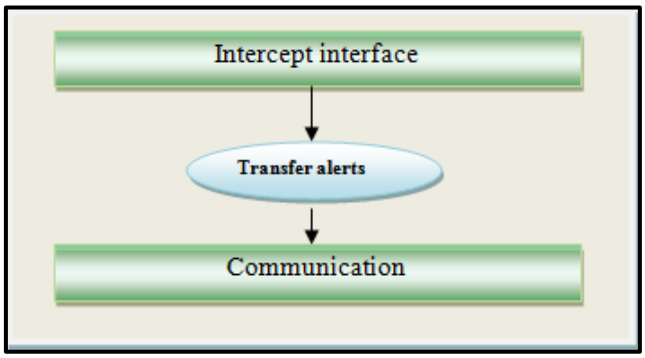

Figure 5: Internal architecture of the collector component

5.1.2. Analyzer component

The analyzer component analyzes the various alerts received from the collector component (each analyzer component has a blacklist (constantly updated by the mobile company).

If the component confirms the presence of an attack, it sends a notification to the executing component which will take the appropriate measures.

If the analyzer component suspects an attack, it requests the executing component to send a warning alert to ask the intervention of the security administration of the mobile enterprise in order to analyze this alert in turn (Figure 6). If the attack is confirmed, the operation to update the black lists present on the mobiles is launched.

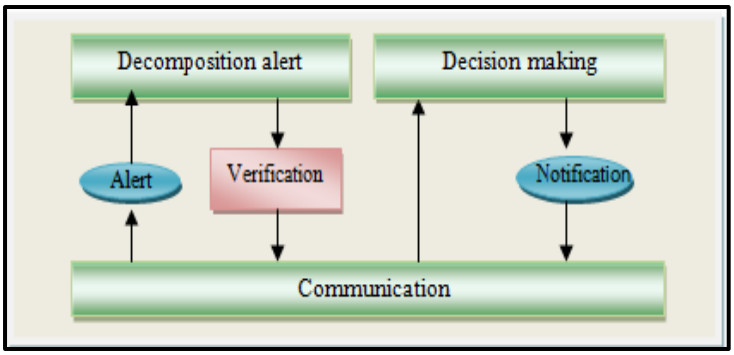

Figure 6: Internal architecture of the analyzer component

5.1.3. Component executor

The role of the component executor is to execute the tasks according to the notification of the analyzer component. These tasks may include restoring corrupted files, prohibiting network connection, etc. (Figure 7).

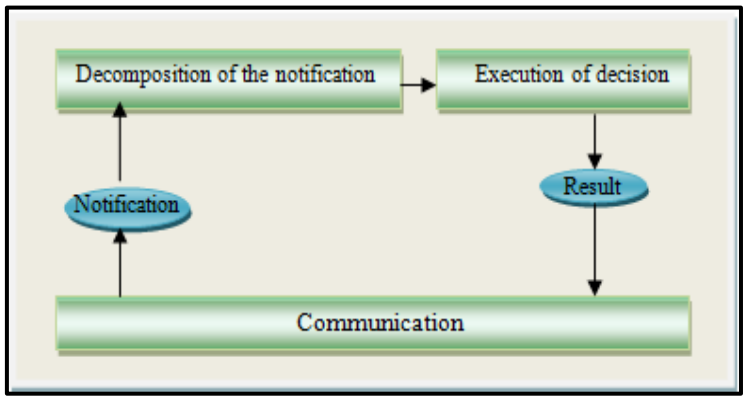

Figure 7: Internal architecture of the executor component

5.2. Blacklist:

When a new vulnerability is discovered, the security controls of the mobile enterprise determine which assets are vulnerable. Additionally, each component has local responsibilities to protect the mobile device from malware attacks, and then communicate the details of the attack to the mobile company's security department to build an up-to-date Black List Enterprise (BLE) and then distribute it to corporate resources to protect all other devices. In this way, the network defenses are constantly refined to protect each user and the entire computer system (Figure 8).

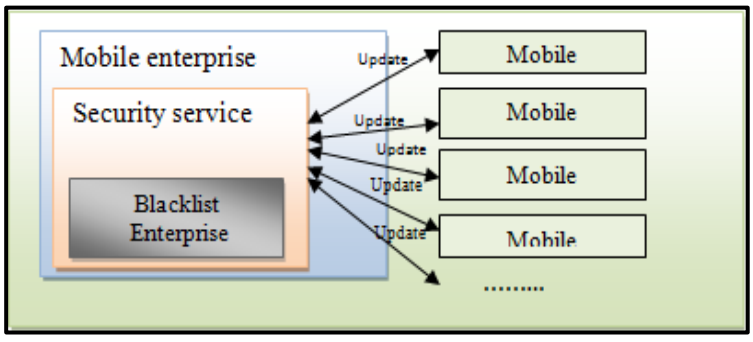

Figure 8: Creation, update and distribution of the enterprise blacklist

5.3. Functional diagram of the main security activities

Here we describe the main activities of our approach illustrated by a sequence diagram(Figure9) where the operations are:
Read_packets(): read packets;
Verify (BLE): check if the attack exists in the BLE;
Trait_alert(): process the alert based on the notification from the analyzer component;
Update_ BLE ( ): update the Blacklist enterprise.

And the events are:
Alert: send alert detected;
Request_ analysis: ask the analyzer component to analyze detected alerts;
Send_alert: send message about the detected attack;
Request_Update_BLE: ask the analyzer component to update the enterprise blacklist.

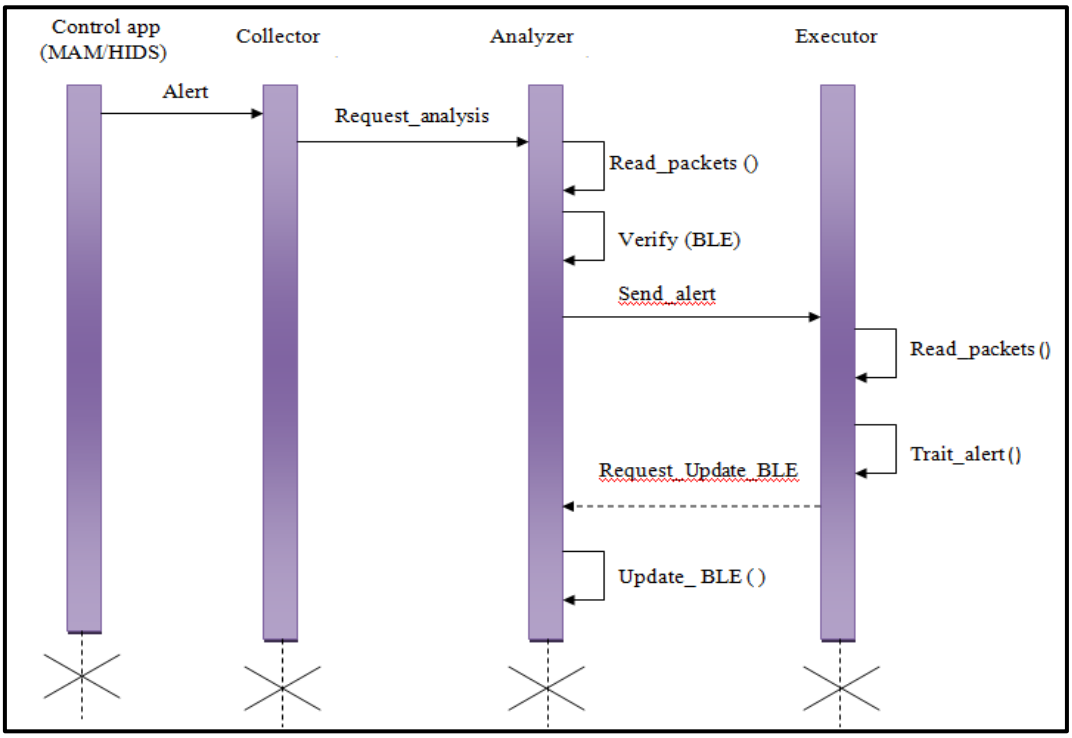

Figure 9: Sequence diagram

6. Discussion

The mobile enterprise presents many IT security challenges as the threat environment is constantly changing. Even if we keep the current threats and vulnerabilities, we must remain aware of emerging technologies and potential vulnerabilities that result. Business IT staff will need to pay attention to the threatening surface of mobile platforms and help users understand how to defend their devices. It's about thinking in specific terms: who needs access to the enterprise's applications and services and how to integrate it into the activation of single sign-on? Which users in which roles should be allowed to use mobile devices to access the network and which applications should be allowed to access? What should and shouldn't these users be allowed to do? What types of devices and operating system versions should be allowed? How will managers measure the activities of mobile businesses to

measure their success? Does a security policy have to duplicate the location and the type of device of the user? To get a head start on the mobile enterprise, those responsible for intelligent enterprise management, IT and security will need to answer all these questions.

Unfortunately, existing security controls suffer from certain limitations and do not meet the requirements of mobile companies. But after studying the two most used applications "MDM and MAM", we noticed that the only weak point of MAM compared to MDM concerns only the security aspect, which leads us to believe that it would be wise to provide MAM with specific security features adapted to a given company and to each of the users of its information system.

Therefore, we have proposed the MAM+ approach which is a mobile-level component that seamlessly enriches and strengthens any MAM application with new analytics and security capabilities which are not present in the original applications source code. The proposed approach permits to ensure that we will always stay abreast of all the threats that are happening and this is done using BLE database that it is always updated. It allows the company to take advantage of the benefits of the mobile revolution, while protecting all users from possible risks.

Our proposed approach offers several advantages:

• It significantly simplifies the task of controlling access to corporate data at the mobile level;
• It reduces network traffic (the majority of checks are at the local level);
• It improves the detection rate;
• It makes it possible to benefit from the advantages of existing applications while avoiding its disadvantages.

7. Conclusion

Mobile enterprises need a tailor-made strategy to guarantee security, but unfortunately the current range of security tools is not designed to meet the security requirements of mobile enterprises. The dilemma of the mobile enterprise mobility strategy described above is serious. However, these new technologies and new security concerns create an opportunity for future research in several areas. How aware are mobile businesses of the new threats? What are the costs and implications for companies of investing in new technological security solutions, such as MDM or MAM? What other security solutions could be more effective at lower cost? What IT capabilities should mobile enterprise acquire to stay in the mobility sector?

In this article, we have proposed a control mechanism which strengthens the security aspect of the MAM application. The objective of this solution is to apply a dynamic control capable of quickly detecting and countering the various threats which are constantly increasing (responding in real time to an intrusion attempt).It decreases the network traffic and progresses the detection rate.

Our work opens the way to several research perspectives because we envisage improving our approach by integrating other measures for detection of a wider range of attacks with an improvement in development costs, speed and performance.

8. References

[1]D.Bailey, The difficulty of securing your mobile workforce, Computer Fraud & Security journal, Volume 14, Num 9, September 2014, pp. 19-20. doi: 10.1016/S1361-3723(14)70532-9

[2] L. Feng, Mobile Security and Privacy. In: Xuemin (Sherman) Shen, XiaodongLin, KuanZhang; Encyclopedia of Wireless Networks. Springer, Cham. (2020 Edition), August 2020.
doi: 10.1007/978-3-319-78262-1_292

[3] K. Miller, J. Voas, and G. Hurlburt, BYOD: Security and Privacy Considerations, IT Professional, Volume 14, Num. 5, 2012, pp. 53–55.

[4] Y. Wang; J. Wei; K. Vangury, Bring your own device security issues and challenges, IEEE 11th Consumer Communications and Networking Conference (CCNC), 2014, pp. 80-85, doi: 10.1109/CCNC.2014.6866552.

[5] D. Jyoti, J. A. Hutcherson, Salesforce Architect's Handbook, chapter8 , January 20, 2021, pp. 257-292. doi: 10.1007/978-1-4842-6631-1_8

[6] D. Carroll, M. Rose, V.Sritapan, CIO Council and Department of Homeland Security Mobile Security Reference Architecture v1.0, May 23, 2013.

[7] K. Glowinski, C. Gossmann,D. Strümpf, Analysis of a cloud-based mobile device management solution on android phones: technological and organizational aspects. SN Applied Sciences 2 num 42. (Springer Nature journal Switzerland AG), 2020.
doi: 10.1007/s42452-019-1819-z

[8] M. Pistoia, O. Tripp, Integrating Security, Analytics and Application Management into the Mobile Development Lifecycle, Proceedings of the 2nd International Workshop on Mobile Development Lifecycle, October 2014, Pages 17–18doi: 10.1145/2688412.2688419

[9] O.Mungkasa,B.JarakJauh..Remote Working (Telecommuting): Concept, Application and Learning), Bappenas Working Papers, volume 3 Num.1,March 2020 pp.1-32. doi:10.47266/bwp.v3i1.52

[10] K.Nesma, Secure Mobile Application Management Framework, Master thesis, The University of Regina (Canada), April 2018.

[11] C. Montealegre , Rubia Njuguna, Muhammad Imran Malik, Peter Hannay, Ian Noel McAteer ; Security vulnerabilities in android applications; In proceedings of the 16th Australian Information Security Management Conference; 2018, pp. 14-28. Doi: 10.25958/5c5274d466691

[12] A. Harris, M. and P. Patten, K., Mobile device security considerations for small- and medium-sized enterprise business mobility, Information Management & Computer Security, Volume 22 Num. 1, 2014, pp. 97-114. doi: 10.1108/IMCS-03-2013-0019

[13] D. Hayes, F. Cappa, N. A.LeKhac.An effective approach to mobile device management: Security and privacy issues associated with mobile applications. International Journal of Digital Business Volume 1, Num1, September 30, 2020. doi:10.1016/ 2666-9544

[14] N. Devillard. MOBILE security and MDM, MISC: Multisystem & Internet, Security, Cookbook, Num 66, March 2013.

[15] M. Eslahi, V. M. Naseri, H. Hashim, N. Tahir, E. H. M. Saad "BYOD: Current state and security challenges" In Computer Applications and Industrial Electronics (ISCAIE), IEEE Symposium, IEEE, April 2014, pp. 189-192.

[16] A.Brunnert, S.Eicker, P. M. Schuler, MANAGING SECURE SYSTEM ARCHITECTURES FOR MOBILE ENTERPRISE APPLICATIONS, IADIS International Conference Applied Computing, September 2011, pp.131-138.

[17] M. Yamin, Basel Katt, Mobile Device Management (MDM) Technologies, Issues and Challenges, ICCSP '19: Proceedings of the 3rd International Conference on Cryptography, Security and Privacy, January 2019, pp 143–147. doi:10.1145/10.1145/3309074.3309103

[18] M. Migliardi, A. Merlo and Sh. Al-Haj Baddar, Adaptive Mobile Computing, book Chapter 10 - Exploring Mobile Data Security with Energy Awareness, 2017, pp. 203-215 doi: 10.1016/B978-0-12-804603-6.00010-3

[19] R. Koneru, P. Dasari, P. Deshpande, and al., Mobile application management systems and methods thereof. US Patent 9,405,723, August, 2016.