Comparative analysis of enterprise mobility management systems in BYOD environment

Dragan Peraković
University of Zagreb
Faculty of Transport and Traffic Sciences
Zagreb, Croatia
dragan.perakovic@fpz.hr

Siniša Husnjak, Ivan Cvitić
University of Zagreb
Faculty of Transport and Traffic Sciences
Zagreb, Croatia
sinisa.husnjak@fpz.hr, s-icvitic@fpz.hr

Abstract—**Mobile terminal devices in a BYOD model are representing the vulnerability for organization's information infrastructure. Storage and processing of business data within the device, which is not under the control of the organization, can have negative consequences for its sensitive information, and control of such devices can compromise users' privacy. Therefore, the separation of business and personal data within the device is of great importance to organization's information security, but also for protection of users' privacy. This paper analyzes the enterprise mobility management systems with the aim of determining the most used approach to separate data and other security mechanisms used to protect sensitive information.**

Keywords- BYOD; data containerization; enterprise mobility management system; data separation

I. INTRODUCTION

The application of information and communication technologies has resulted in a revolution of the way business is conducted. Further advancement of technology and the rapid development of smart mobile devices provided to employees greater mobility and flexibility, and thus greater efficiency in performing everyday tasks. The rapid development of mobile devices has led to the emergence of BYOD model that has enabled the employees an opportunity of using private mobile devices for business purposes.

Although the BYOD as a model is more supported in organizations due to the mutual benefit for the organization and its employees, there is the problem of the sensitive information security. Through the device, which is not owned by the organization, are stored, processed and transmitted sensitive information and unauthorized access to this information could potentially have major negative consequences for the organization itself. It is logical that in such a scenario, the organization wants and needs to have some control over devices in order to reduce the risk of unauthorized access or manipulation of information. On the other hand, through control mechanisms, the organization may compromise privacy of the device owner, which is the legal and regulatory protected.

The resulting problem can be solved by separating private and business data in the device and thus reduce the risk of compromising user privacy and unauthorized access to sensitive information of the organization. Such solutions are often implemented within a comprehensive enterprise mobility management system (EMM).

This paper explores the existing approaches used in the development of data separation solutions. In the paper is also carried out comparative analysis of solutions that are developed by several manufacturers in order to determine the current state of the EMM market. The ultimate goal of the analysis is to determine the most popular approach to the separation of private and business data.

II. PROBLEM DEFINITION

Smart mobile terminal devices, with help of the rapid development and decline in market prices have become affordable to a large number of users. Characteristics of such devices almost can be measured with a conventional computers, personal and laptop. They differ from conventional mobile devices in many advanced functionalities, such as [1]:

- The ability for small distance connections (WLAN, Bluetooth, NFC, WiMAX, etc.),
- Constant Internet connectivity through a packet based technologies (GPRS, EDGE, UMTS, HSUPA, LTE, etc.),
- The ability to determine the location (GPS),
- The possibility of extending the basic functionality of the mobile operating system by installing additional third-party applications,
- Large memory capacity of data storage media.

Smart mobile terminal devices, therefore, are rapidly becoming widely used among users and not only for private but for business purpose also. A large number of organizations allow the use of private devices, of its employees and associates, for a business purposes, such as to conduct business calls, send and receive business e-mail and perform other business activities. Applied model is also called Bring Your Own Device (BYOD) [2].

Introducing BYOD model into organizational structure led to a redefinition of the way in which users perform their daily tasks, but also gave a clear insight into the way the organization manages its computer network, a mobile terminal devices, as well as human resources [2].

Application of BYOD model provides concrete benefits for employees, but also for the organization, such as increased employee satisfaction, increased productivity and financial savings [3]. However, due to the high mobility, small size and

connectivity options through several available technologies, mobile terminal devices are more vulnerable to security threats, listed below, then other client terminal devices (such as PCs and laptops), [4] [5]:

- Theft or loss of a mobile terminal device,
- Attacks on devices intended for recycling,
- Attacks through malicious content (viruses, worms, spyware, adware and Trojan horses)
- Monitoring data implemented sensors attacks (GPS, accelerometer, microphone, camera)
- Phishing attacks,
- Exploiting vulnerabilities in web browsers,
- Automatic downloads of applications,
- The attacks through spoofed network information,
- Exploitation of network oversights,
- Social engineering.

The impact of these threats can be reflected as a negative consequence on the asset covered by threats [4]:

- Private data,
- Organization's intellectual property,
- Financial assets,
- The availability and functionality of devices and services,
- Personal and political reputation.

As each segment of information and communication structures, mobile terminal devices also must support the three main objectives of security, confidentiality, availability and integrity. These goals can be achieved by combined application of security mechanisms, embedded within mobile devices as well as implementation of the additional security controls at different levels of information and communication structures [5].

The number of total malicious content variations for the Android operating system (OS) in year 2013 was decreased by 14% compared to the year 2012, as shown in figure 1 a) [6].

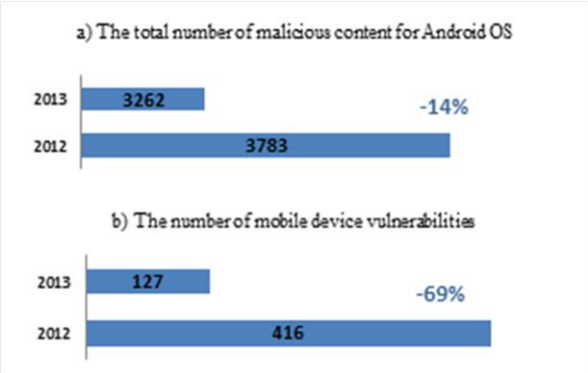

Figure 1. A) DECREASE OF TOTAL NUMBER OF MALICIOUS CONTENT FOR ANDROID OS; B) DECREASE OF THE NUMBER OF MOBILE DEVICE VULNERABILITIES [6]

Also, as shown in figure 1 b), the number of vulnerabilities for mobile devices was decreased by 69% [6].

Despite the trends of decline, the number of vulnerabilities and threats is still extremely high and must not be ignored.

Within a BYOD environment private and business data is stored and processed within the same device, which is owned by the user, and these devices often have access to the network and sensitive data of the organization [7]. Such a merging of private and business purpose of the device increases the likelihood of malicious activity and compromised sensitive information of the organization. It is therefore of great interest to the organization, which supports BYOD model, that with the application of safeguards reduce the security risk to a lower level, as far as possible. At the same time, the organization should not affect or have the insight and control over personal data and applications on user devices in order to avoid invasion of privacy or breach of law and regulatory provisions.

III. METHODS USED IN DEVELOPING SOLUTIONS FOR DATA SEPARATION

As previously mentioned in chapter 2 of this paper, the problem for the organization, but also for users in the BYOD model represents the processing, use and storage of private and business data within the same device without any security restrictions among them. This means that unauthorized access to the user device also means access to all of the data that the user owns on the device, residential and business. The problem for users is, for an example, management and device configuration by the organization where the organization can have an insight to, not only business but also in the private information of employees or the owner of the device. Therefore, a good data separation strategy is crucial for the security of the data, but also to preserve the privacy of users within BYOD environment.

For the purpose of private and business data separation within the device certain methods were developed. Those methods are covered by a single term, mobile content management system (MCM). Mobile content management system is almost always part of a larger, organization's mobility management system (EMM). This system, along with MCM, combines several methods that cover aspects of the management and security of organizations mobile devices, data and applications, such as [8]:

- Mobile Email Management (MEM),
- Mobile Device Management (MDM),
- Mobile Application Management (MAM),
- Mobile Information Management (MIM).

Although all the methods of separation of private and business data have the same goal, protecting organization's applications and data, approaches to defined problem vary considerably. There are several approaches for the development of data separation methods [9]:

- Virtualization
  - Mobile virtual desktop infrastructure (mobile VDI),
  - Mobile operating system virtualization (mobile OS virtualization).
- Containerization
  - Application-specific containers,
  - Application neutral containers,
  - Integrated containers.

A. Virtualization

Virtualization is a method of software and / or hardware environment emulation which runs on top of other software. This simulated environment is called a virtual machine [10]. The virtual machine is logically equivalent to a physical machine, and the reason for the wide application of virtualization is the ability to run multiple virtual machines on a single physical.

Figure 2 shows the generalized view of virtual machine work principles. Virtualization layer allows simultaneous execution of multiple instances of operating systems on one computer dynamically sharing available hardware resources (CPU, RAM, HDD, I / O devices) [11].

1) Mobile access to virtual desktop

Mobile VDI refers to the infrastructure that provides access to a virtual desktop through a variety of mobile devices. Generally, it supports two basic client architectures [12]:

- Client-based mobile VDI - mobile VDI client application is installed on the mobile terminal device and it is used to create a session between the device and the computer infrastructure within the organization. Created session allows the mobile terminal device access to organization's applications and data through virtualized interfaces.
- Mobile VDI based on web browser - this, alternative, architecture uses a web browser with support for HTML 5, to access the web-based mobile VDI client. Using this architecture eliminates the need for installation of client applications on the device.

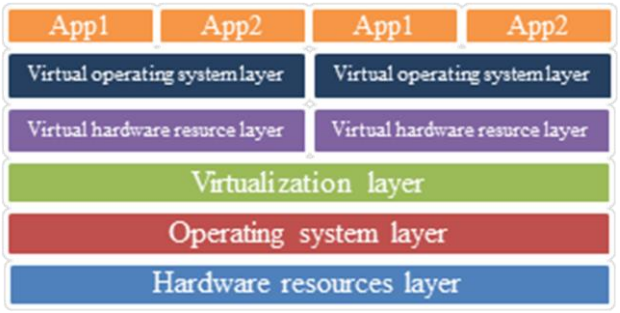

Figure 2. GENERALIZED VIEW OF VIRTUAL MACHINE WORK PRINCIPLES

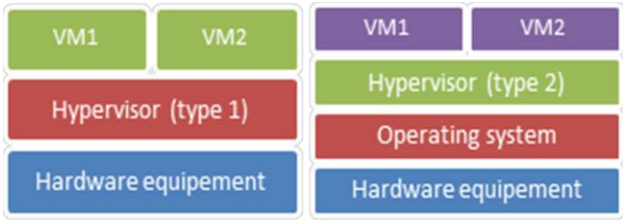

Figure 1. Comparison of virtualization architecture: a) Hypervisor type 1; b) Hypervisor type 2

Regardless of the architecture, mobile VDI provides the user with only a snapshot of the desktop, which means that all data and applications are retained within the organization's infrastructure, [12] [13].

The disadvantage of the described approach lies in the fact that today mobile terminal device does not have the physical input units (mouse and keyboard), but rely on the application of virtual alternatives. Without classical input units it is difficult and sometimes impossible to use certain applications through solutions based on mobile VDI access. Also, due to the small dimensions of the device, users cannot always see the entire virtual desktop; for example, drop down menus of certain applications will not be visible. Therefore, it is necessary to test applications before they become available to users [12].

2) Mobile operating system virtualization

Due to the limited hardware capabilities of mobile terminal devices, implementation of mobile operating system virtualization solutions is the hardest viable method of separating private and business data. There have developed two types of virtualization hypervisor [14].

Type 1 hypervisor is hardware based and implemented into device that creates a new instance of an existing operating system. Both instances of the operating system are running on two separate processor regions [14].

Type 2 hypervisor is located on top of the operating system for which it is not have to be implemented during the manufacturing process, but it can be installed later. He is considered less secure then the hypervisor type 1 because of the possibility of compromising the operating system and the creating a path to achieve the attack on the virtual machine [15]. The difference between the above mentioned hypervisors architecture is shown in figure 3.

Virtualization allows the creation of business unit instances of the OS in a virtual environment and its management without affecting the private user OS instance. As a user's business OS always located on a virtual machine the data transmission is disabled as well as communications of applications between the private and business instance of the OS.

Usability problems may be related to the performance of the two instances of an operating system executing concurrently on a single device. Also, this method requires switching from private to business mode which can be impractical for the user [16].

B. Containerization

Containerization provides administrators the ability to create secure containers on the device within which are all organization's applications and data. While applying this method, data can be shared exclusively between applications

that are within the safe container. This method allows the implementation of the organization's security policy over predetermined safe containers without affecting the functionality and data of the private portion of the device, [17] [18].

Containerization allows the implementation of various security mechanisms, such as [19]:

- Pushing content updates directly to secure container,
- Access restriction based on the time and location of the mobile device,
- Encryption of contents stored in secure container using the 256-bit SSL encryption,
- Removing the stored contents immediately after leaving the application.

1) Application specific containers

Application specific containers require special application development because of the need to adapt the application programming interface (API) to protect data. They are also known as bolt-on Software Development Kit (SDK) containers. Because of the need to adapt the source code applications, this kind of standardized containers causes changes in the appearance of the user interface, which often leads to customer dissatisfaction [9].

2) Application neutral containers

Application neutral containers used a process called application wrapping for providing security mechanisms that are not part of the source code of the application. It is possible to impact on them remotely, through management applications. Applications wrapping can be implemented in a very short period of time because the application neutral containers do not require changes to the original application code. This data separation approach, in terms of usability, provides users with original application layout and consistency in ways of using private and business space [9].

3) Integrated containers

Due to the deep integration into the operating system, an approach based on an integrated container provides a high level of safety, significantly reducing the vulnerabilities associated with the performances of safe containers that are not integrated into the operating system. A holistic approach when designing integrated container allows optimization of security and business productivity by taking advantage of opportunities grouping of tools and applications designed for this purpose [9].

IV. COMPARATIVE ANALYSIS OD DEVELOPED SOLUTIONS

A comparative analysis was performed in order to define the most effective approach in developing solutions for private and business data separation with the aim of providing a clear insight into the future direction of development. The analysis covered solutions of manufacturers that are located in different market positions (leaders, challengers, visionaries and niche players) [20]:

- IBM MaaS360
- SAP Mobile Secure
- BlackBerry Enterprise Service 10
- Symantec Mobile Management Suite

All of listed manufacturers have developed EMM solutions and with the analysis will be compared only those functionalities that affects the separation of private and business data and applications, such as:

- Operating systems support,
- Mobile device management functionalities,
- Mobile applications and content management functionalities,
- Additional security mechanisms.

A. Operating system support

The purpose of introducing BYOD model, in addition to the advantages brought to the organization is enabling users to use private devices to increase their satisfaction and productivity in the workplace. As users often use different devices that run different operating systems, support for multiple operating systems is extremely important.

B. Mobile device management functionalities

Mobile device management functionalities play an important role in protecting organization's data. Some of the most important in terms of safety are:

- Selective, remote data wipe from the device - where it is possible to delete only the organization data without affecting the user data,
- Password protection of device,
- Ability to remotely lock the device,
- Multiuser support on a single device - automatic configuration of devices based on the currently logged user.

C. Mobile application and content management functionalities

In an organizational environment, applications are the key for delivery of content to users. Because of that, mobile applications and content management functionalities are very important segment of each EMM solutions. A quality approach to applications management is of great importance for the isolation of the business from private environment, which includes the separation of private and business data generated by the application itself or exchanged between.

The most important functionalities of mobile applications and content management are the following:

- Possibility of applications containerization,
- Support for application-specific containers,

- Disabling copying files between applications, Support for the application neutral containers, Mobile access to the desktop (mobile VDI),
- Disabling copying the contents of e-mail,
- Secure access to e-mail.

D. *Additional security mechanisms*

Additional security mechanisms are also in function of organization's applications and data protection during storage, processing or transmission and at the same time ensuring the privacy of user data. Some of the most important are, for example:

- Detection of malicious content,
- Secure data storage containers,
- Firewall functions.

V. RESULTS OF COMPARATIVE ANALYSIS

Results of comparative analysis of EMM solutions, in which emphasis is placed on essential functionalities used in private and business data separation, are shown in table 1.

Based on the analysis results, it is concluded that all manufacturers of the developed solutions (regardless of their position on the market) are oriented toward neutral application containerization approach for the separation of private and organization data. The only manufacturer providing virtualized access (mobile VDI) is Symantec. However, this functionality is available exclusively through integration of third-party solutions within the existing system.

In addition to the application neutral containers IBM and Blackberry support application specific containers. This approach is not used often because of the cost of application development and complexity of such implementation and impact to the original layout of the user interface.

From the results it is evident that all developed solutions support the most common mobile operating systems, in addition to the BlackBerry Enterprise Service 10, which does not offer support for mobile operating systems based on Windows platform.

Unlike IBM and SAP solutions, Blackberry and Symantec have multi-user support, which has greater importance for smart mobile devices, which are owned by the organization and used by multiple users (e.g. tablet devices).

From additional security mechanisms aspect, IBM does not provide firewall functionality and BlackBerry does not provide firewall and possibility of malicious content detection.

TABLE I. COMPARATIVE ANALYSIS OF EMM SOLUTIONS

Functionalities	EMM solutions	IBM MaaS360	SAP Mobile Secure	BlackBerry Enterprise Service 10	Symantec Mobile Management Suit
mOS support	Apple iOS	✓	✓	✓	✓
	Android	✓	✓	✓	✓
	BlackBerry	✓	✓	✓	✓
	Windows Mobile	✓	✓	✗	✓
	Windows Phone 7	✓	✓	✗	✓
	Windows Phone 8	✓	✓	✗	✓
Mobile device management functions	Selective device wipe	✓	✓	✓	✓
	Device password protection	✓	✓	✓	✓
	Device remote lock	✓	✓	✓	✓
	Multiuser support	✓	✓	✗	✗
Application and content management functions	Application containerization	✓ through MaaS360 Secure Productivity module	✓ through SAP Mobile App Protection module	✓	✓
	Application specific containers	✓	✗	✓ (only for BlackBerry devices)	✗
	Application neutral containers	✓	✓	✓	✓
	Mobile VDI	✗	✗	✗	✓ (with integration of third-party solutions)
	Disabling files c/p between applications	✓	✓	✓	✓
	Disabling copying the contents of e-mail	✓	✓ (with integration of third-party app)	✓	✓
	Secure access to e-mail	✓	✓	✓	✓
Additional security mechanisms	Secure containers for data storage	✓	✓	✓	✓
	Malicious content detection	✓	✓	✗	✓
	Firewall functions	✗	✓	✗	✓ (only for windows mobile)

VI. CONCLUSION

Smart mobile terminal devices, with the rapid advancement of technology, are becoming an integral part of every organization. With the advent of BYOD model and its integration into the organizational structure there are seem to appear multiple problems while trying to protect such devices. The main goal of any organization is to protect business data and private information infrastructure, but at the same time they are legal and regulatory obliged to respect the privacy of the owner of the device, that is employees.

In order to adequately and in a safe way separate private and business data on the user device, it is not enough to develop a solution that will be based solely on one approach to the data separation. With solutions for data separation is necessary, in parallel, to apply a range of additional functionality and security mechanisms.

As a result of the aforementioned market demand, many manufacturers have developed solutions through which it is possible to manage the organization's mobile environment. Such solutions are grouping different functionalities which are applicable for the management and protection of devices that are associated with the organization.

In order to determine the most appropriate approach for the separation of private and business data a comparative analysis of EMM solutions, from different manufacturers that are at different positions in the market, was conducted. The functionalities that affect the separation of private and business data in the BYOD model were analyzed.

Based on the results of the comparative analysis it is possible to conclude that the most appropriate approach for separation of data is through the application of neutral container. The reason is uncomplicated process of application containerization that requires no modification of source code and does not change the appearance of the applications user interface.

The results of comparative analysis may serve as the basis for selection of optimal EMM solutions by organizations depending on their needs for managing BYOD environment.

REFERENCES

[1] ISACA: Securing mobile devices using COBIT 5 for information security, ISACA, Rolling Meadows, USA, 2012

[2] Bradley, J., Loucks, J., James, M.: Horizons BYOD : A global perspective harnessing employee-led innovation, Cisco Systems Inc., San Jose, USA, 2012, pp. 1–21

[3] Slottow, T.: Action learning project : Bring your own device (BYOD), Business Finance Leadership Academy, 2012

[4] Peraković, D., Husnjak, S., Remenar, V.: Research of security threats in the use of modern terminal devices, 23td International DAAAM Symposium, vol. 23, 2012, pp. 545–548

[5] Murugiah, S., Scarfone, K.: Guidelines for managing and securing mobile devices in the enterprise (Draft), NIST, National Institute of Standards and Technology, USA, 2013

[6] Symantec Corporation: Internet security threat report 2014, vol. 19, Symantec Corporation, 2014

[7] Weldon, K.: How to protect business information and empower your employees at the same time, vol. 33, Current Analysis Inc., 2012, pp. 1–11

[8] TechTarget: Enterprise mobility management : choosing the right approach and considering costs, Techtarget, USA, 2014

[9] BlackBerry: Finding the right mobile device containerization solution, BlackBerry, 2014

[10] Scarfone, K., Souppaya, Hoffman, P.: Guide to security for full virtualization technologies, NIST, National Institute of Standards and Technology, USA, 2011

[11] VMware Inc.: Understandingf full virtualization, paravirtualization, and hardware assist contents, VMware Inc., 2007

[12] CDW Government LLC: Virtual desktop infrastructure goes mobile (White paper), CDW Government LLC, 2013

[13] Cisco Systems Inc.: Cisco enterprise mobility solution: device freedom without compromising the it network, Cisco Systems Inc., San Jose, USA, 2014

[14] Dual-identity smartphones could bridge BYOD private, corporate divide - Computerworld, (2014, Jun 20) Online document, Available: http://www.computerworld.com/s/article/9233834/Dual_identity_smartphones_could_bridge_BYOD_private_corporate_divide?taxonomyId=227&pageNumber=4.

[15] Barr, K., Deasy, S., Newell, C.: The VMware Mobile Virtualization Platform : is that a hypervisor in your pocket ?, ACM SIGOPS Operating Systems Review, vol. 44, no. 4, ACM New York, USA, 2010, pp. 124–135

[16] Mobile virtualization: Hypervisors go small. (2014. Jun 23) Online Document. Available: http://mobilecomputingtrek.wordpress.com/2012/04/04/mobile-virtualization-hypervisors-go-small/.

[17] Kaspersky Lab: Security technologies for mobile and BYOD, Kaspersky Lab, 2013

[18] Prabhu, N., Rendell, J.: Smart containerization ™, CA Technologies, 2014

[19] Mobile device management technologies. (2014, Jun 23) Online Document. Available: http://ukblog.im-mobility.com/book/export/html/7.

[20] Terrence, C., Smith, R., Silva, C., Taylor, B., Girard, J., Basso, M.: Magic quadrant for enterprise mobility management suites market definition / description, 2014, pp. 1–12