ABSCHNITT IV.
TECHNISCHE WISSENSCHAFTEN

DOI 10.36074/24.01.2020.v1.14

INFORMATION SECURITY CONDITION ANALYSIS IN EMM SYSTEMS

ORCID ID: 0000-0001-6080-237X **Andrii Vlasov**
PhD in Technical Sciences,
Leading Researcher of Air Force Science Center
Kharkiv National University of the Air Force
UKRAINE

The rapid development of mobile management systems shows that this is a very promising area in the information business industry. The wide variety of companies that provide such services contributes to the better development of technologies for securing corporate information both on the device itself and during remote access to the corporate network. The current stage in the development of EMM (Enterprise Mobility Management) systems is to focus their capabilities on corporate management, security, management and control of mobile payments [1].

The scope of EMM systems covers all security processes and policies, especially mobile devices, and is an integral part of today's corporate business processes. These systems should be viewed as a set of people, processes, and technologies focused on managing mobile devices, wireless networks, and other mobile computing services in the context of doing business.

The components of the EMM (in terms of analyzing the capabilities of information security mechanisms and identifying possible threats) include [2, 3]:

- Mobile Application Management (MAM). Functionality that determines the settings for accessing devices to information (both from the business network and from other applications on the device);
- Mobile Identity Management (MIM). Functionality limiting the use of a mobile device. For example, assigning user roles;
- Mobile Content Management (MCM). Functionality that provides complete control at the level of corporate content (first of all limiting copy and paste, access to business content repositories);
- Mobile Device Management (MDM). Mobile-level functionality that provides full access to all of its features.

Today, there are quite a few EMM systems on the market, the main ones being:

- AirWatch by VMware;
- MobileIron Platform;
- MaaS360Cloud;
- Samsung KNOX for Enterprise.

Four major subsystems are implemented in AirWatch to ensure information security [4]:

- Mobile device management - for quick initialization of devices for corporate

use. Corporate data security and protection policies are enforced when accessed from mobile systems, with the ability to remotely lock and erase device data;

- Mobile Application Management for managing and installing / removing individual applications at the level of employees, personal or workstations of the enterprise;
- Mobile Email Management for corporate mail security;
- Mobile Content Management for implementing secure access to work data.

The MobileIron Platform is a product of MobileIron that integrates a classic suite of security features and EMM functionality such as MDM, MAM, MCM and supports many popular operating systems [5]. Technologically it consists of two servers: MobileIron VSP and MobileIron Sentry. The former is responsible for managing the system, keeping records of the devices, and extending security policies to each device. Another controls the connection of devices, keeps track of all attempts to connect, controls access to the mail server. Both servers can be installed as a virtual machine or as a separate distribution.

IBM's MaaS360Cloud platform [6] allows you to manage operating systems - Android, iOS, Windows and MacOS, documents and distribute other applications. The possibility of protection against various virus attacks and compromising of the device, creation of VPN channel for protection of Internet connections is realized. This platform is compatible with Android Enterprise and Samsung KNOX and allows you to integrate with another IBM product (Watson Artificial Intelligence).

Samsung KNOX for Enterprise [7] is a development of Samsung and is introduced only on devices of this company. The main advantages are deep integration with hardware and device software. This system provides guaranteed protection of corporate data, availability of separate VPN channels for certain applications in a secure container, implementation of a separate secure environment for business applications, corporate information, etc. The possibility of complete data management on a separate device is introduced with control over its current state. One of the features that sets this system apart from others is the ability to register a device on the system, configure all security policies on it, and install the necessary software before the device is first started.

One of the most common problems in companies that use EMM systems are: loss or theft of a mobile device; attacks on already disposed devices; viral attacks; phishing attacks; Automatically download unauthorized applications attacks through dangerous networks and more. These threats primarily affect personal data, business intellectual property, financial assets, serviceability and availability of devices and services.

The main ways to address these threats to information security in EMM systems are to:

- more space is created on the devices to store corporate information (usually temporary). This allows for various kinds of attacks on distributed content (primarily on a user's personal device), which does not provide the necessary level of security and provides an opportunity to influence information security;
- in the case of loss or theft of devices, the data on these devices are vulnerable, thus increasing the risk of unauthorized access to corporate applications and / or corporate data, interfering with the processes of authentication and authentication of users, hacking passwords, ciphers, remote control technologies, the ability to delete / data correction (primarily from this device);

- for the proper functioning of the system requires timely updating of the software on all devices, which allows the attacker to influence most of the devices and the security policy of the corporation (in case of interference with the system software update and introduction of "virus" content);

- the compulsory use between the mobile device and the data encryption organization (VPN tunnel or HTTPS);

- security policy in an organization may make it impossible to use personal devices (especially of different types, different manufacturers, with different operating systems), which can lead to the organization in question recognizing the inappropriate implementation of the EMM system.

Conclusions. Thus, the growth of the mobile device market is making it more widely used in the corporate segment for workflow optimization and cost savings, but using the new Bring Your Own Device (BYOD) IT policy requires a constant search for new and evolving information security technologies and methods in a timely manner identify possible threats to its security.

References:

1. Madden J., Madden B (2014). *Enterprise Mobility Management: Everything you need to know about MDM, MAM, and BYOD*. – San Francisco, CAlifornia.
2. Saravana Balaji B, Karthikeyan N.K., & Raj Kumar R.S. (2018). Fuzzy service conceptual ontology system for cloud service recommendation. *Computers & Electrical Engineering, Vol. 69, pp. 435–446.*
3. Android Enterprise Solutions Directory. Retrieved from: https://androidenterprisepartners.withgoogle.com/emm/ EMMs/.
4. VMWare AirWatch. Retrieved from: https://www.air-watch.com/
5. MobileIron. Retrieved from: https://www.mobileiron.com/.
6. IBM MaaS360 with Watson. Retrieved from: https://www.ibm.com/security/mobile/maas360.
7. Samsung. WhitePaper: Knox Platform for Enterprise, 2018.

DOI 10.36074/24.01.2020.v1.15

TECHNOLOGICAL PROCESSES OPTIMIZATION

Dmytro Levkin
PhD, Senior Lecturer, department of higher mathematics
Kharkiv Petro Vasylenko National Technical University of Agriculture

UKRAINE

The report addresses the optimization of multilayer microbiological systems containing local discrete sources of thermal loading. The aim of the work is to develop mathematical models, numerical methods, algorithms and specialized modeling devices to improve the quality of the biotechnological process of laser segmentation of multilayer microbiological material according to the criterion of viability of parts of the material.

To achieve this goal it is necessary to solve the following tasks.