Information security management of enterprise mobile device

T A Omelchenko 1,2, A V Nikishova 1, M Yu Umntsyn 1, I A Omelchenko 1 and Yu P Umntsyn 1

1 Information Security Department, Volgograd State University, 100, prospect Universitetskii, Volgograd, 400062, Russia
2 omelchenko.tatiana@volsu.ru

Abstract. The development of the modern labour market involves increasing the level of mobility of personnel, so the current trend is the spread of mobile devices in the implementation of professional activities. This practice improves the efficiency of enterprise, but also has a negative impact on the security of information systems of enterprises. The growing requirements of employers have led to the growth of the functionality of mobile devices. However, this also causes an increase in the number of vulnerabilities in them, leading to an increase in the complexity of the security processes. The combination of the above problems determines the need to organize the process of information security management of enterprise mobile devices. The model of information security management of enterprise mobile devices is described in the article. It allows identifying vulnerabilities of operating system objects of enterprise mobile devices by modelling combinations of dangerous permissions more accurately.

1. Introduction

The development of the modern labour market involves increasing the level of personnel’s mobility, so more and more companies are seeking to move away from the traditional IT environment in the workplace to a more flexible and mobile strategy for the organization of the workplace [1].

According to a joint study conducted by Capita and Citrix in 2018, 71% of enterprises have already implemented or are considering implementing the Bring Your Own Device (BYOD) approach. Of those enterprises that use the BYOD paradigm, 92% of respondents believe that it has increased employee productivity, while 87% of respondents admitted that security risks have increased, 89% reported an increase in the load on IT support and 88% refer to the problems in IT management. Modern mobile devices perform functions similar to personal computers [2]. They perform such functions as - remote administration, VPN support, high-speed Internet, browsers with flash-and java-script, mail and notes synchronization, file sharing. All this is very convenient, but such a number of functions of mobile devices leads to an increase in the diversity of current threats [3, 4]. This in turn leads to an increase in the number of security tools used, and complicates the information security system. Therefore, it is advisable to organize the process of information security management of enterprise mobile devices.

An example of successful application of mobile devices are BlackBerry devices. The smartphone supports centralized management through the server, encryption, and the ability to remotely destroy data on the device. However, it is not very popular, and in the Russia it virtually absent.

However there are a lot of devices using Windows Mobile, Android, iOS, which are much weaker protected. The main security problems are related to the fact that the variety of operating systems for mobile devices is very large, as well as the number of versions in one family, also developers do not pay enough attention to the security of previously released versions [5].
The most common operating system is Android [6], so an important task is to ensure the security of the Android operating system.

Employee mobile devices are typically used in locations not controlled by the company, and even when used inside the office, they are moved from place to place, creating a risk of confidential data leakage [7]. Smartphones and tablets can be lost or stolen, and the data stored on them is at risk of being compromised [8, 9]. When creating policies and regulations for the use of mobile devices, it is necessary to consider that such devices can fall into the hands of attackers who will try to get sensitive data either directly from the device or using them for remote access to the resources of the organization.

One of the main features of Android is the openness of the system. This means open source access and the ability to install applications from unofficial sources. This is convenient for developers and manufacturers of Android devices. But this is also convenient for intruders as it makes it easier for them to find vulnerabilities that can be exploited. The openness of the system has also led to unofficial firmware that may contain additional vulnerabilities.

The architecture of Android is made in such a way that all applications run with limited rights. This means that they do not have access to the protected data of other applications. Therefore, one of the main security concerns of Android is the vulnerability of the system, allowing gaining root rights. It allows accessing any data of any application.

Another important feature of Android is the fragmentation of the platform [10]. Android updates are released quite often. So it is difficult for developers to cover all vulnerabilities and attackers take advantage of it. Due to the fragmentation of the platform, many users are exposed to already known attacks, because the vulnerabilities used for their implementation are closed only in the latest versions of Android.

Statistics show that the most common type of malware for mobile devices is RiskTool. Such programs are not malicious, user installs it himself. However, sometimes attackers insert dangerous functions hidden from the user into these applications. The research is focused on the search for such hidden functions. Based on search results, the functionality of applications must be limited.

To do this, it is necessary to organize the process of information security management of enterprise mobile device.

2. Existing Approach

According to the requirements of normative legal documents of Russian Federation, it is recommended to use the family of standards GOST R ISO/IEC 27000 for the organization of the information security management process [12], defining the order of creation, implementation, operation, constant monitoring, analysis of maintenance and improvement of the information security management system.

The process approach for information security management system presented in the family of standards, is based on the operational principle accepted in the ISO management system standards [13, 14] and commonly known as the process “Plan – Do – Check – Act” [15].

This approach is universal, but is applicable mainly to traditional components of the enterprise information system, such as hosts, workstations, etc. [16]. To solve the problem of information security management of enterprise mobile devices, it is necessary to modify the process approach for information security management system, taking into account the peculiarities of the functioning of enterprise mobile devices.

The scheme of the modified process approach for information security management system of enterprise mobile devices is offered (figure 1).
3. Model of Information Security Management

According to the scheme the process of information security management of enterprise mobile devices $F_u$ can be described by a set of sequentially applied functions (1):

$$F_u = F_{or}(F_{ru}(F_{pr}(O, F_{km}(R))))$$

Function to build a conceptual model of dangerous combinations of permissions of the enterprise mobile devices’ operating system of $F_{km}$ is described as following:

$$F_{km} = F_{km}(R) = R \cup C = K$$

where $C$ – set of permissions’ combinations; $R = R_s \cup R_o = \{r_1, ..., r_N\}$ – set of signature $R_s$ and dangerous $R_o$ permissions of enterprise mobile device’s operating system; $C = \{c_1, ..., c_y\}$ – set of permissions’ combinations; $c_i = (r_i, ..., r_L)$ – i’th permissions’ combination; $K$ – conceptual model of dangerous combinations of permissions of enterprise mobile devices’ operating systems.

The function of permissions’ receiving of set of objects of enterprise mobile devices’ operating systems $F_{pr}$ is described as (3):

$$F_{pr} = F_{pr}(K,O) = M, M \subset R$$

where $O = \{o_1, ..., o_k\}$ – set of objects of enterprise mobile devices’ operating systems, $M = \{M^1, ..., M^k\}$ – set of files “AndroidManifest.xml” of objects of enterprise mobile devices’ operating systems; herewith $M^i = \{r_1^i, ..., r_L^i\}$, where $i = 1 ... k$, $k$ – number of objects of enterprise mobile devices’ operating systems.

The function of recognition of vulnerabilities of objects of enterprise mobile devices’ operating systems $F_{ru}$ is described as (4):

$$F_{ru} = F_{ru}(M) = OU, OU \subset O$$

where $OU = \{ou_1, ..., ou_z\}$ – set of dangerous objects of enterprise mobile devices’ operating systems, such that the condition is satisfied for its elements (5):

$$o_j \in OU \mid \exists c_i \lor r_k \in K \land \epsilon \in M^j$$

The function of restriction of permissions of subset of vulnerable objects of enterprise mobile devices’ operating systems $F_{or}$ is described as (6):

$$F_{or} = F_{or}(OU) = D$$

where $D = \{d_1, ..., d_z\}$ – set of levels of danger of objects of enterprise mobile devices’ operating systems.

**Figure 1.** Scheme of the modified process approach.
Level of danger of object of enterprise mobile devices’ operating systems $d_i$ can take one of the following values (7):

$$
\begin{align*}
    d_i &= 0, \text{object is secure,} \\
    &= 2, 0 < d_i < 40, \text{low level of danger,} \\
    &= 3, 40 \leq d_i \leq 140, \text{medium level of danger,} \\
    &= 4, d_i \geq 140, \text{high level of danger}
\end{align*}
$$

Level of danger of object of enterprise mobile devices’ operating systems $d_i$ is calculated by the formula (8):

$$
    d_i = \sum_{r_j \in M^i} d_{r_j} + \sum_{c_l \in M^i} d_{c_l}
$$

where $d_{r_j}$ – level of danger of j’th permission, $d_{r_j} \in \{1,2,3,4,5\}$.

Level of danger of j’th permission $d_{r_j}$ can take one of the following values (9):

$$
    d_{r_j} = \begin{cases}
        1, \text{very low potential damage,} \\
        2, \text{low potential damage,} \\
        3, \text{medium potential damage,} \\
        4, \text{high potential damage,} \\
        5, \text{very high potential damage}
    \end{cases}
$$

Level of danger of l’th permissions’ combination $d_{c_l}$ is calculated by the formula (10):

$$
    d_{c_l} = x_l \sum_{r_j \in c_l} d_{r_j}
$$

where $x_l$ – danger coefficient of l’th combination of permissions of object of enterprise mobile devices’ operating systems. It is estimated by experts.

If $d_i = 3 \cup 4$ then the function of information security management of enterprise mobile devices $F_u$ is performed (11):

$$
    F_u = F_u(M^i) = \tilde{M}^i
$$

where $\tilde{M}^i$ – modified file AndroidManifest.xml of the of object of enterprise mobile devices’ operating systems, that satisfies the condition (12):

$$
    \tilde{M}^i \not\exists c_l \land r_k \in K \land \in \tilde{M}^i
$$

In the case of $d_i = 4$ it is advisable not just to limit the functionality of the object of enterprise mobile devices’ operating systems, but to perform the procedure for its removal.

The collection and analysis of information about the permissions of enterprise mobile devices’ operating systems is carried out on the basis of the order of functioning of the permissions’ system for applications.

In order to use the features of the Android operating system’s and enterprise mobile device’s functions, perform certain actions and receive information, application must request permission. Even if attacker hides a dangerous feature in an application from user, application must still ask the operating system for permission to use the feature. This means that it is possible to learn the full dangerous potential of an application by learning what permissions it requests.

In most cases, an object requires a set of dangerous permissions to implement malicious actions [17]. Therefore, the analysis of individual permissions should be supplemented by the analysis of their combinations.

After analyzing combinations of permissions, a conceptual model of dangerous combinations of permissions of enterprise mobile device’s operating system was compiled, which is a weighted oriented graph (figure 2).

Dangerous combinations of enterprise mobile device’s operating system have a numerical level of danger. The total level of danger is determined by the sum of all levels of danger of permissions and their combinations that the object requests.

The identified combinations, in addition to the list of dangerous permissions, are used to identify vulnerabilities of objects of enterprise mobile devices’ operating systems.
To study the proposed model of information security management, software tool is developed. Its architecture is shown in the figure 3.

![Figure 3. Architecture of software tool of information security management.](image)

The user interface is designed in graphical form. It organizes the user’s interaction with the tool. The user interface is used to enter data and output the result of software tool’s functioning.

Module of conceptual model of dangerous combinations of permissions of enterprise mobile devices’ operating systems building. It uses data stored in the database of dangerous permissions and their combinations.
combinations and builds model of chains of dangerous permissions of objects of enterprise mobile devices’ operating systems.

Module of permissions of set of objects of enterprise mobile devices’ operating systems receiving. It works with loadable into the system apk-files of objects of enterprise mobile devices’ operating systems, finds files AndroidManifest.xml in them, reads information from these files, passes it to module of vulnerabilities of objects of enterprise mobile devices’ operating systems detection.

Module of vulnerabilities of objects of enterprise mobile devices’ operating systems detection. It retrieves content of file AndroidManifest.xml, analyzes it to determine whether studied object has dangerous permissions that make up the chain of dangerous combinations in accordance with data of constructed model of chains of dangerous permissions of objects of enterprise mobile devices’ operating systems and passes the results of the analysis to module of permissions of vulnerable objects of enterprise mobile devices’ operating systems restriction.

Module of permissions of vulnerable objects of enterprise mobile devices’ operating systems restriction. It gives recommendation about the need to limit functionality of vulnerable objects of enterprise mobile devices’ operating systems based on obtained data about danger of objects. If recommendations are taken, it makes changes to AndroidManifest.xml and transfers the changes to the Apk-file of objects of enterprise mobile devices’ operating systems.

Apk-file of object of enterprise mobile device’s operating system contains AndroidManifest.xml that stores information about permissions requested by the object.

Database of dangerous permissions and their combinations contains a list of dangerous, signature permissions, their combinations and weighted estimates to determine level of danger of permissions’ combinations.

4. Experiments
Experiments are carried out for four modelled objects (table 1).

| Experiment | Modelled object      | Expected result                                                                 |
|------------|----------------------|--------------------------------------------------------------------------------|
| 1          | com.exp.exptest1     | No object is considered dangerous                                              |
| 2          | com.exp.exptest2     | Modelled object is assigned low level of danger                                |
| 3          | com.exp.exptest3     | Modelled object is assigned medium level of danger. A decision is made on the need to limit permissions of object |
| 4          | com.exp.exptest4     | Modelled object is assigned high level of danger. A decision is made to remove the vulnerable object |

Experiment for the 3’rd object is given as an example. Object com.exp.exptest3 is modelled and software is launched (figure 4).

The software tool showed the presence of a vulnerable object of enterprise mobile device’s operating system with medium level of danger.

It was decided to limit the functionality of vulnerable object enterprise mobile device’s operating system.

Repeated analysis of enterprise mobile device’s operating system shows decrease in level of danger of object com.exp.exptest3 (figure 5).
5. Conclusion
The analysis of experimental results shows that the result of enterprise mobile device’s management the number of vulnerable objects of enterprise mobile device’s operating system decreased. This leads to total level of danger of objects of enterprise mobile device’s operating system reduction.

Further research in this direction is associated with the expansion of the list of operating systems of enterprise mobile devices, for which information security management of enterprise mobile devices is carried out, as well as the expansion of the list of managed objects of operating systems of enterprise mobile devices.
Acknowledgment
The reported study was funded by the Council for grants of Russian Federation President, according to the research project No. MK-6404.2018.9.

References
[1] Harris M, Patten K 2014 Mobile device security considerations for small- and medium-sized enterprise business mobility Information Management & Computer Security (vol. 22) chapter 1 pp 97-114
[2] Eslahi M, Naseri M, Hashim H, Tahir N, Saad E 2014 BYOD: Current state and security challenges IEEE Symposium on Computer Applications and Industrial Electronics (ISCAIE) pp 189-192
[3] La Polla M, Martinelli F, Sgandurra D 2013 A survey on security for mobile devices IEEE Communications Surveys and Tutorials (vol. 15) chapter 1 pp 446-471
[4] Armando A, Merlo A and Verderame L 2014 Security considerations related to the use of mobile devices in the operation of critical infrastructures International Journal of Critical Infrastructure Protection 7 (4) 247
[5] Samawi V 2015 Security in mobile computing Mobile Computing and Wireless Networks: Concepts, Methodologies, Tools, and Applications ed. IGI Global (Jordan: Amman Arab University) pp 1925-1939
[6] Omelchenko T, Sadovnikova N, Nikishova A, Parygin D, Umnitsyn M, Kostyukov A 2018 Protection Software for Mobile Operating Systems Proceedings of the 2018 International Conference on System Modeling and Advancement in Research Trends (SMART) ed. IEEE pp 54-59
[7] Kleiner C, Disterer G 2015 Ensuring Mobile Device Security and Compliance at the Workplace Procedia Computer Science (vol. 64) pp 274-281
[8] Thompson N, McGill T J, Wang X 2017 “Security begins at home”: Determinants of home computer and mobile device security behavior Computers & Security (vol. 70) pp 376-391
[9] Pasquinucci A 2009 Mobile Devices: The security challenges of mobile devices Computer Fraud & Security Volume Issue 3 pp 16-18
[10] Robinson G, Weir G 2015 Understanding android security Communications in Computer and Information Science pp 189-199
[11] Fratantonio Y, Qian C, Chung S, Lee W 2017 Cloak and Dagger: From Two Permissions to Complete Control of the UI Feedback Loop In Proceedings - IEEE Symposium on Security and Privacy pp. 1041–1057
[12] Siponen M, Willison R 2009 Information security management standards: Problems and solutions Information & Management (vol. 46) Issue 5 pp 267-270
[13] Bongiovanni I 2019 The least secure places in the universe? A systematic literature review on information security management in higher education Computers & Security (vol. 86) pp 350-357
[14] Soomro Z A, Shah M H, Javed A 2016 Information security management needs more holistic approach: A literature review International Journal of Information Management (vol. 36) Issue 2 pp 215-225
[15] GOST R ISO/IEC 27001-2006 2008 Information technology. Security techniques. Information security management systems Requirements (Moscow: Standartinform)
[16] Omelchenko T, Umnitsyn M, Nikishova A, Sadovnikova N 2017 Model of enterprise’s information security management Advances in Computer Science Research (ACSR) (vol. 72) pp 183–187
[17] Jamil Q, Shah M 2017 Analysis of machine learning solutions to detect malware in android 6th International Conference on Innovative Computing Technology, INTECH 2016 pp 226-232