Data Security Analysis in EMM Systems

Olga Cherednichenko[1], Iryna Kyrychenko[2], Kostiantyn Nechvolod[2], Kirill Smelyakov[2] and Oleksandr Dolhanenko[2]

1 Univ Lyon, Univ_Lyon 2, UR ERIC – 5 avenue Mendès France, 69676 Bron Cedex, France
2 Kharkiv National University of Radio Electronics, 14 Nauky Ave., Kharkiv, 61166, Ukraine

Abstract

In the work the peculiarities of functioning and construction of Enterprise mobility management systems are investigated. An analysis of the one of the most popular Samsung KNOX systems has been conducted. A software implementation for the Android OS in Java programming language has been developed. The program enables the device camera to be turned off for all applications, even for the Camera system application. This implementation made it possible to disable the device's camera for all applications, including the system 'Camera' application. As a result, in practice, we can see how to configure policies.

Keywords

KNOX, MDM, EMM, ROOT OF TRUST, Viruses, Penetration, Mobile Devices, Android, Virtual Machine, Security, Container, Cryptology, Scheduling, Root Access, Permissions

1. Introduction

In the modern world, thanks to the development of mobile technologies, personal devices have deeply integrated into all spheres of human activity. Organizations now face the question of how to protect corporate information on mobile devices. Therefore, developers are tasked with making the processing and storage of information as secure as possible, and to allow the configuration of security policies on various mobile devices intended for corporate use. Using one's own device is a new trend among enterprises that is rapidly gaining popularity, aimed at increasing mobility and productivity of employees through their own smartphones. Threats and risks to enterprises are also growing rapidly. However, such threats can be mitigated by running software in a "protected container" on a personal device.

One such system is the KNOX platform, developed by Samsung. It provides a high level of protection for some of the most common devices for any organization. This platform is a software-hardware complex that provides hardware security measures, policy management, and compliance with regulatory requirements that go beyond the standard functions typical for the contemporary device market.

This work requires the analysis of existing systems, investigating the main threats to smartphones, and protection against them using Samsung Knox, a platform that is a real means to satisfy modern business needs.

In the modern world, almost every person has at least one "smart" device such as a smartphone, tablet, or laptop. We use them every day; they are always with us. A lion's share of the information we receive, we get through such devices. In most cases, smartphones store not all, but a very large amount of personal, and sometimes even confidential information. If this information belongs only to the owner of this device, then the responsibility for its preservation

COLINS-2024: 8th International Conference on Computational Linguistics and Intelligent Systems, April 12–14, 2024, Lviv, Ukraine

olga.cherednichenko@univ-lyon2.fr (O. Cherednichenko); iryna.kyrychenko@nure.ua (I. Kyrychenko); kostiantyn.nechvolod@nure.ua (K. Nechvolod); kyrylo.smelyakov@nure.ua (K. Smelyakov), oleksandr.dolhanenko@nure.ua (O. Dolhanenko)

0000-0002-9391-5220 (O. Cherednichenko); 0000-0002-7686-6439 (I. Kyrychenko); 0009-0000-5879-6644 (K. Nechvolod); 0000-0001-9938-5489 (K. Smelyakov), 0000-0002-3996-6940 (O. Dolhanenko)

rests solely on them, but if the device is also used for interaction with corporate information, then the issue of information security comes to the fore. Sometimes the possibility of using personal devices for work issues can be quite complicated, or even impossible, due to the established security policies in organizations. Therefore, at the beginning of the 21st century, a new IT policy was proposed, called Bring Your Own Device (BYOD), but this concept only reached its peak popularity in the 2010s with the support of companies such as Intel, Citrix Systems, and Unisys [1].

Let's take a closer look at the Enterprise Mobility Management systems and analyze existing systems.

2. The necessity for using MDM (EMM) systems

The first implementation of this policy was the Mobile Device Management (MDM) systems, which included a set of services and technologies that provided control and protection of mobile devices used by the organization and its employees. Mobile device management pursues two tasks: ensuring the security of corporate information on devices that are outside the network infrastructure, as well as controlling the state of the devices themselves.

Some of the most common problems that most companies encounter are:

- Loss or theft of a mobile device
- Attacks on devices that are already being utilized
- Viral attacks
- Phishing attacks
- Automatic downloading of unauthorized applications
- Attacks through unsafe networks

The impact of such threats can affect assets such as personal data, enterprise intellectual property, financial assets, device functionality, and the availability of devices and services.

The mere thought that access to confidential information could be outside the corporate network raises many doubts about the feasibility of using similar systems among IT security professionals. Therefore, first and foremost, before implementing a system, it is necessary to weigh all the advantages and risks for the business and then make further decisions.

Bringing your own device (BYOD) is a common concept in most enterprises. Using personal devices at work is a trend that affects most IT departments. Although BYOD helps enterprises reduce costs and may improve employee satisfaction, it can also be a security problem.

2.1. Main tasks and characteristics of EMM systems

The EMM system is focused on corporate governance, security, management, and control of mobile transactions. It covers all processes and policies on all mobile devices that are part of or key elements of business processes. The area of activity is mainly aimed at security, application integration and management, as well as the financial implications of such decisions.

For example, corporate policy should ensure that an application can be integrated and used on a mobile device, while necessary mechanisms for secure access must be provided. In addition, the organization must control and manage all processes related to the business and financial expenses associated with the use of such device solutions that may belong to either the organization or the employee.

Thus, the EMM system can be defined as a set of people, processes, and technologies focused on managing mobile devices, wireless networks, and other mobile computing services in a business context.

To achieve separation of personal and corporate information, certain methods have been developed:

1. Mobile Application Management (MAM)

Managing devices at the application level. For example, configuring their access to information (both from the business network and from other applications on the device).

2. Mobile Identity Management (MIM)

Functionality that limits the use of a mobile device. For example, assigning user roles.

3. Mobile Content Management (MCM)

Complete control at the corporate content level. May include restrictions on copying and pasting, access to business content repositories. Almost always a part of the EMM system.

4. Mobile Device Management (MDM)

A system that operates at the level of the mobile device and provides full access to all its capabilities.

Despite the fact that all methods of separating personal and business information have the same goal, namely the protection of corporate applications and information, the approaches can vary [2,3].

An additional space for storing corporate information is necessarily created on the device. A schematic representation of that secured container is shown in Fig. 1

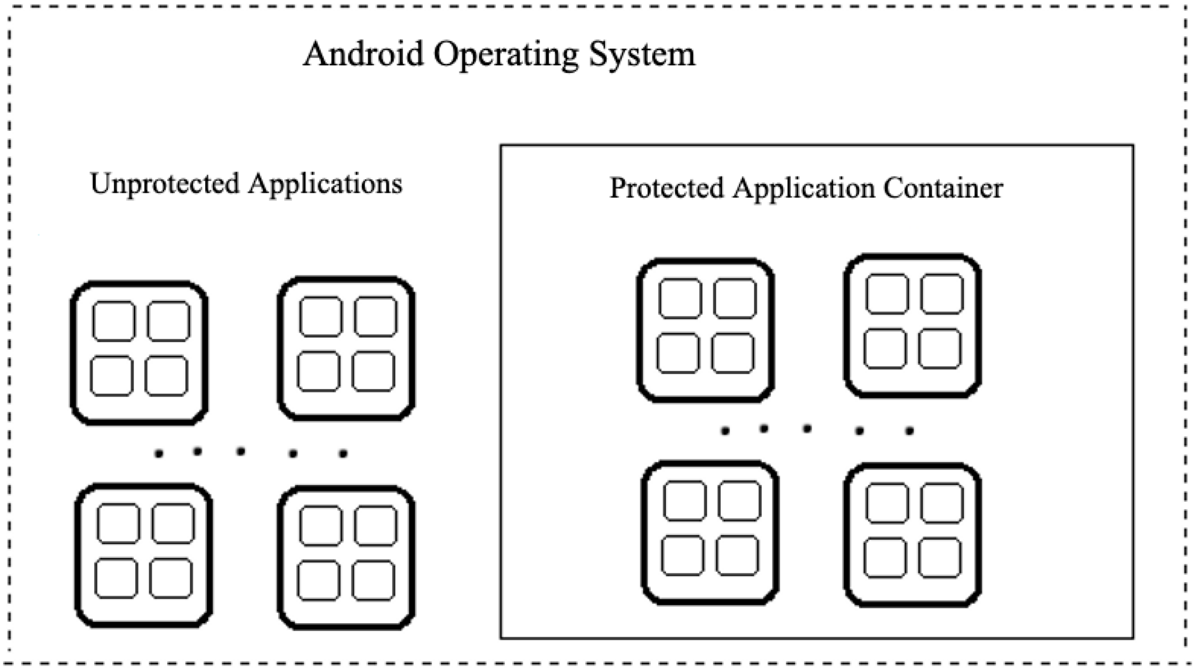


Figure 1: Data segregation

It allows for the provision of various security mechanisms such as:

1. Downloading content updates directly to a secure container
2. Restricting access to data within the container depending on the time or location of the device
3. Remotely deleting data in the container

This allows for the distribution of content on a user's personal device, which ensures security. The implementation of this function can vary and directly affects the level of protection from attacks.

2.2. Advantages and disadvantages of EMM systems

The advantages of EMM systems include the ability of an organization to control how employees use their devices within the work network.

It increases the efficiency of the organization's employee communications, improves the quality of corporate security provision because security administrators do not need to configure each device separately, and policies are set an masse on connected devices. Additionally, there is the possibility of delivering email, synchronizing calendars, and contacts on smartphones, tablets, and other personal devices. To achieve protection, channel protection is applied using a virtual private network and remote desktop services.

Among the disadvantages, first and foremost, is the cost of implementing such systems. Secondly, there is the fragmentation of devices and their software. In most cases, this, if not making it impossible, greatly complicates the management, configuration, and timely updating of software on all devices. For the normal functioning of the system as a whole, it is necessary to have qualified administrators on staff. Some employees may negatively perceive the tight control by the organization, which can lead to difficulties. The company's security policy may altogether prevent the use of personal devices, making the implementation of an EMM system impractical.

The use of these systems cannot protect the device from loss or theft, but they allow to minimize the risks that are possible in these cases. One of the main features is remote control, erasing all data. It is even possible to block access to the work area if the attacker knows the access password. Regarding studies of disposed devices, encryption of all important data must be used in the system. Device rights settings mechanisms are used to protect against the installation of dangerous software. For example, administrators can block the installation of any programs, except for programs from the official application store, which is managed by the organization. In addition, some systems constantly monitor the state of the system and detect any intrusion, which ensures the quality and reliability of the system as a whole. When it comes to security when exchanging information online, the main tool is a VPN. Individual systems may also use authentication when accessing the corporate network, and of course encryption of all traffic is used. It is possible to create a separate VPN channel for each application, which also creates additional security if public or unreliable networks are used [4,5]. This also creates additional benefits for the server, because it does not need to constantly maintain a channel for all applications.

2.3. Comparison of the most popular EMM systems

There are quite a lot of EMM systems on the market today.

The AirWatch by VMware system products are in demand in such industries as energy, retail trade, transportation and others. AirWatch by VMware is supported by all current operating systems, such as Android, IOS, Windows, MacOS. It can be used to configure devices with Android Enterprise or Samsung Knox and consists of four subsystems:

- Mobile device management, which provides the possibility of quick initialization of devices for corporate use, application of security policy and protection of corporate data provided access from mobile systems
- Mobile Application Management, which provides the ability to manage and install or remove individual applications at the level of employees, personal or workstations of the enterprise
- Mobile Email Management, which ensures the security of corporate mail
- Mobile Content Management, which provides the possibility of protected access to work data

MobileIron Platform is a product of the MobileIron company, which is the fastest growing in the world [6]. It combines a classic set of security tools and EMM functionality, such as MDM, MAM, MCM. It also supports many popular operating systems, which allows you to quickly implement this system into the existing business infrastructure. Technologically, it consists of two servers: MobileIron VSP and MobileIron Sentry. The former is responsible for system management, device accounting, and spreading security policies to each device. The other controls the connection of devices, keeps records of all connection attempts, controls access to the mail server. Both servers can be installed as a virtual machine or as a separate distribution [7].

The MaaS360Cloud platform from IBM allows you to manage operating systems - Android, IOS, Windows and MacOS [8]. Allows you to manage documents, distribute applications. There is the possibility of protection against various virus attacks and device compromise, such as loss or theft. Provides the creation of a VPN channel to protect Internet connections. Also compatible with technology such as Android Enterprise and Samsung KNOX. Another advantage of this product is its integration with another product of the company by IBM Watson artificial intelligence.

Samsung KNOX for Enterprise is a development of the Samsung company, which is available only on the devices of this manufacturer. This can be attributed to the main disadvantage of this system, however, it provides features that are not available in other software products. The main advantages of this system are deep integration with hardware and device software, ensuring guaranteed protection of corporate data, the presence of separate VPN channels for each application in a so-called secure container, a separate secure environment for business applications, corporate information, etc. The presence of control over the state of the device, the possibility of full data management by administrators on a separate device. One of the features that sets this system apart from others is the ability to register the device in the system, configure all security policies on it, install the necessary software even before opening the factory packaging and starting the device for the first time, which greatly facilitates and speeds up the implementation of this product [9].

3. Android security

Android is a reliable operating system that is installed on a very large number of devices, from mobile phones to head units in cars. It is based on fundamentals such as separation of system processes, trusted OS architecture, and it uses a powerful threat analyzer that uses machine learning and cloud computing to identify threats using Google's extensive knowledge base [10].

Many enterprises will soon expand the number of mobile devices that will be used in the corporate sphere using modern approaches and concepts such as MDM or BYOD.

But despite the fact that the mobility of enterprises is increasing, data security remains the main obstacle to the implementation of new technologies for the use of mobile devices.

Currently, some of the most common threats to mobile devices are:

1. Use to access the global network through unprotected Wi-Fi access points, in which a MITM (man-in-the-middle) attack is possible
2. The possibility of theft or loss of the device, which will allow the attacker to gain full physical access to the device
3. Malicious software that can be installed unintentionally by the user and which will quietly collect all the information the attacker needs and even make photo, video and audio recordings of everything that happens around the device

However, the last threat is the least likely due to the very principle of building the Android system, where each application is executed separately from the others and it is impossible to access the data of another application without obtaining root rights.

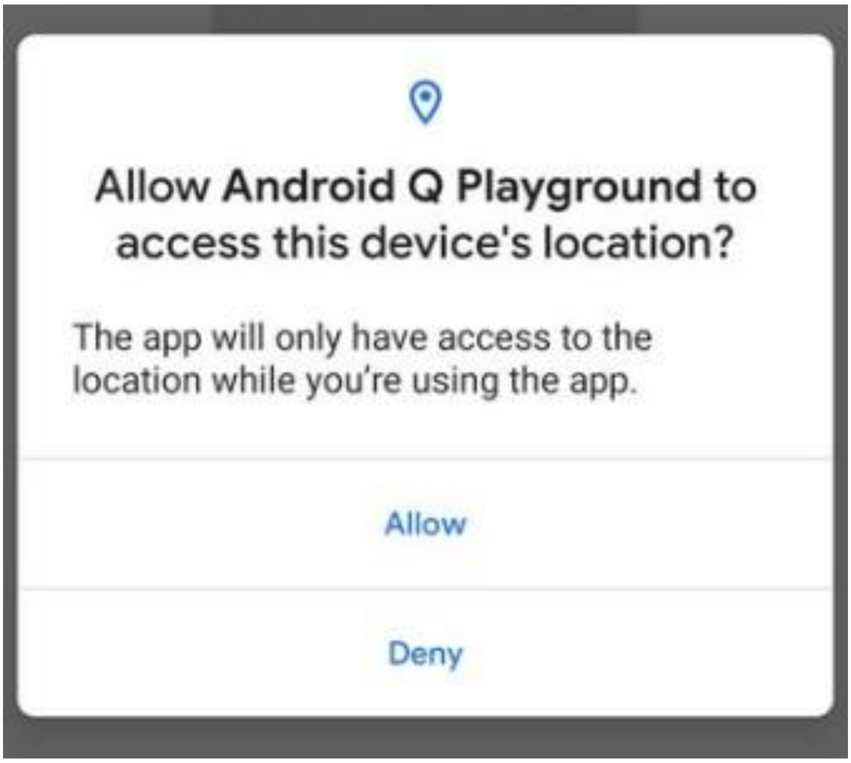
The developers of the Android operating system included security at the stage of its design. This is well reflected in the two-tier security model used by Android applications. Android, at its core, relies on one of the security features provided by the Linux kernel, namely running each application as a separate process with its own set of data structures and preventing other processes from interfering with its execution [11].

At the application level, to obtain system permissions, Android uses smaller permissions to allow interaction with system resources or other applications. Almost every permission requires explicit user confirmation. By default, no application is allowed to perform any operations that may adversely affect other applications, user data, or the system. Examples of such operations include sending SMS messages, retrieving contact information, and accessing the Internet. Playing music files or viewing images are not subject to such operations, and thus the application does not need to explicitly request permission to do so. Application-level permissions provide a means to access restricted content and APIs.

Each Android application (or component thereof) runs in a separate Dalvik or ART virtual environment. A virtual machine (VM) is a sandbox. However, it should not be assumed that it is this sandbox that provides security. The virtual machine is optimized for efficient operation on devices with a small amount of memory. Android's permission checks are not done inside the virtual machine, but rather inside the Linux kernel code and are applied at runtime.

Access to Linux's low-level facilities is provided through user ID and privilege groups, other additional, less system-sensitive security features are obtained through Manifest permissions.

Linux kernel sandboxes separate applications and prevent them from accessing other applications' data or user information or performing operations such as accessing the Internet, making phone calls, or receiving SMS messages. If an application needs to perform the above operations (such as accessing the Internet), retrieve user information (such as contacts), or communicate with other applications (such as communicating with an email application), it must specifically request these permissions. These permissions are declared in the configuration file (Manifest.xml) [12]. When an app is installed, Android prompts the user to either allow or deny permissions (see Figure 2).



Allow Android Q Playground to access this device's location?

The app will only have access to the location while you're using the app.

Figure 2: Permission dialog box

The user cannot select certain permissions – i.e. allow access to the Internet and deny access to SMS. The app asks for a set of permissions, and users either approve or deny them all. When the user has approved these permissions, Android (via the Linux kernel) will grant access to the requested operations or allow interaction with various applications / components. It should be noted that since Android 6.0, the ability for the user to adjust permissions even after he has confirmed them has been introduced [13].

The presence of system security functions certainly improves the overall ability of the system to counter threats, but basic methods and sets of rules are not enough to confirm the level of security required for the corporate segment. The rest of the article discusses methods for improving these characteristics.

3.1. Additional security measures

As number of devises which have various versions of running android os is very big, it is necessary to create some cloud based services to improve current security level. The count of android versions is described in Table 1.

Table 1
Fragmentation of OS Android

Version	Name	API	Prevalence
2.3.3-2.3.7	Gingerbread	10	0.3%
4.0.3-4.0.4	Ice Cream Sandwich	15	0.3%
4.1.x	Jelly Bean	16	1.2%
4.2.x		17	1.5%
4.3		18	0.5%
4.4	KitKat	19	6.9%
5.0	Lollipop	21	3.0%
5.1		22	11.5%
6.0	Marshmallow	23	16.9%
7.0	Nougat	24	11.4%
7.1		25	7.8%
8.0	Oreo	26	12.9%
8.1		27	15.4%
9	Pie	28	10.4%

Although devices running the Android operating system have strong security foundations, a number of cloud services support Android devices to further enhance and ensure the overall security of the platform. Google Mobile Services (GMS) is a suite of applications licensed to Google by third-party software manufacturers and Android partners that allows you to easily control the pre-installation of applications such as Gmail, Hangouts, Maps, Photos, YouTube, Google Play Store, and other core Google applications. Less obvious to Android users are the basic security features that come with GMS. Any GMS-licensed device also has device-based software scanning and cloud-based security tools, namely a core set of services and features called Google Play Protect. These range from on-device scanning for potentially dangerous apps (PHAs) and app exploits, to Find My Device (formerly Android Device Manager) to locate lost or stolen devices and detect rooting.

Google Play Protect includes a set of APIs that interact and process information between applications on devices, using built-in device protection features and cloud security services. In 2017, Google Play Protect automatically disabled PHA from approximately 1 million devices. Google reviews all apps before publishing them on the Google Play Store. In addition to browsing apps submitted to Google Play, its cloud systems search for apps from publicly available sources. Google Play Protect also reviews apps it finds outside of Google Play for PHA. According to Google, Google Play Protect prevented Android users from installing PHAs outside of Google Play approximately 1.6 billion times in 2017. Google Play Protect covers all the security features that have kept Android users' devices safe for years. For example, Google Play Protect's Verify Apps service scans apps for PHAs before users install them, regardless of their origin.

The Verify Apps service runs a periodic device-wide scan that inspects apps before installation and performs regular scans of all installed apps. If a PHA is found, a notification prompts the user to remove it. In cases where a PHA does not provide any potential benefits to users, Google Play Protect can remove the PHA from affected devices and block future installations [15].

AutoScan is another service that scans Android devices daily for PHAs and other signs of tampering. (The service last year scanned nearly 800 million devices a day, including Android smartphones, tablets, and TVs.)

AutoScan works alongside Verify Apps as part of Google's multi-layered scanning approach to Android software and security. If AutoScan detects a PHA or other risk indicators on the device, it may trigger an additional local application scan to further investigate the issue. Although the cloud-based device/cloud security architecture provides robust protection, it largely operates out of sight of end users.

Google Play Protect was introduced in May 2017 to unlock this functionality and help users understand the "health" of their devices. Google Play Protect provides Android users with proactive notifications about when a device is being scanned, the security status of each app viewed or downloaded from the Google Play Store, and the overall health of apps on the device.

The rapid spread of software updates is a challenge in an ecosystem as diverse as Android. Google distributes critical security updates through GMS, a service that operates regardless of carrier or Android software version. This can make it easier to ship new software as soon as new threats are discovered [16].

Ensuring the security of the system as a whole is ensured by the use of hardware and software tools and by checking the status of the device from the moment it is turned on to the moment it is turned off.

Hardware Security - A trusted environment separates security-critical code from the rest of the operating system. This strategic separation ensures that only trusted processes, which are isolated and protected from attacks and exploits, can perform important operations such as data encryption and decryption. Trusted environments perform integrity checks before executing any software. These checks detect malicious attempts to change the trusted environment and software running on the device.

Hardware support - a trusted environment is supported by hardware if hardware protection isolates the environment from the rest of the running system. This isolation ensures that vulnerabilities in the underlying operating system do not directly affect the security of the trusted environment. The environment also links the integrity checks of the software running in the trusted environment to the cryptographic signatures stored in the device hardware. Hardware-backed integrity checks prevent an attacker from exploiting software vulnerabilities to bypass protections and download unapproved software into a trusted environment.

The KNOX platform uses a hardware-based trusted environment, and specific components depend on the device's hardware. For example, ARM processors provide a Trusted Execution Environment (TEE) that uses components such as TrustZone, ARM Hypervisor Mode, and Embedded Secure Elements. KNOX features that use a trusted environment include Real-time Kernel Protection (RKP), Trusted Boot, Device Health Attestation, Certificate Management, Sensitive Data Protection (SDP), and Network Analytics platform (NPA).

Application isolation is used to prevent rogue applications from intentionally or accidentally accessing unauthorized data. The Knox platform provides several forms of app isolation to create a secure space, an app container on Samsung devices. Each variant is based on the same kernel isolation technology called Security Enhancements for Android (SE for Android.) SE for Android is an integration of SELinux and Android, extended to cover Android components and design paradigms.

Android Enterprise on Samsung devices provides application isolation with work profiles that provide basic isolation of corporate applications from personal applications. When using Android Enterprise on Samsung devices, Knox provides features such as Real-Time Kernel Protection (RKP), secure enterprise applications, and hardware-level certificate and key storage, making Android Enterprise even better on Samsung devices.[17] A schematic representation of the system is shown in the Figure 4.

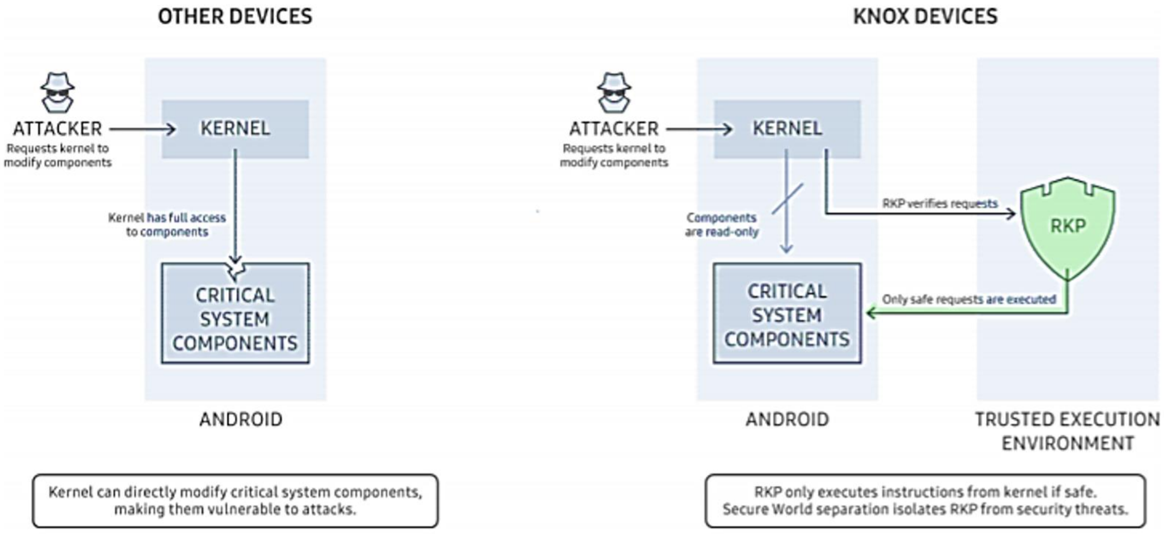

OTHER DEVICES
KNOX DEVICES
ATTACKER
Requests kernel to modify components
KERNEL
Kernel has full access to components
CRITICAL SYSTEM COMPONENTS
ANDROID
Kernel can directly modify critical system components, making them vulnerable to attacks.
ATTACKER
Requests kernel to modify components
KERNEL
Components are read-only
RKP verifies requests
RKP
Only safe requests are executed
CRITICAL SYSTEM COMPONENTS
ANDROID
TRUSTED EXECUTION ENVIRONMENT
RKP only executes instructions from kernel if safe. Secure World separation isolates RKP from security threats.

Figure 4: Comparison with a system without real-time protection

Knox Workspace is based on Android Enterprise, providing additional security and management improvements. In particular, Knox Workspace benefits from hardware-enabled integrity checks. These checks detect any tampering with the device or its protections and block the workspace.

Knox also supports Sensitive Data Protection (SDP), encrypting data while the device is running and decrypting only after the device user authenticates to unlock the Knox workspace. In addition, Knox Workspace provides more device management, such as enforcing two-factor authentication for Knox Workspace, using enterprise Active Directory credentials for authentication, and managed import and export of enterprise data to Knox Workspace.

The SE Management Service for Android (SEAMS) allows you to isolate a single app or a small set of trusted apps to lock down apps in a single container. Application containers built with SEAMS provide the same benefits as Knox Workspace. However, unlike the first two options, SEAMS containers do not have a dedicated graphical interface. Applications in the SEAMS container appears with other applications on the device but are marked with a shield icon to show that they are isolated and protected from applications that do not use the shared container. The user can create as many SEAMS containers as he wants on the fly.

4. Experiment

During the execution of the work, a software implementation was developed to block the possibility of using the device's camera in any application. To develop this program, it is necessary to obtain a key in the developer console, which should be used to obtain settings and policies for the device on which this software is run. A camera was chosen as an example because only a small number of permissions are available for free, and the camera is one of the most suitable for demonstrating the functionality of the Knox system. The program is implemented in the Java and XML programming languages using Android SDK and Knox SDK. Android Studio 3.5 is used for compiling and assembling the installation .apk file. To run the application, a Samsung device with an Android operating system version no lower than 8.0 and Samsung Knox services version no lower than 3.3 is required, without kernel or system modifications and without root rights.

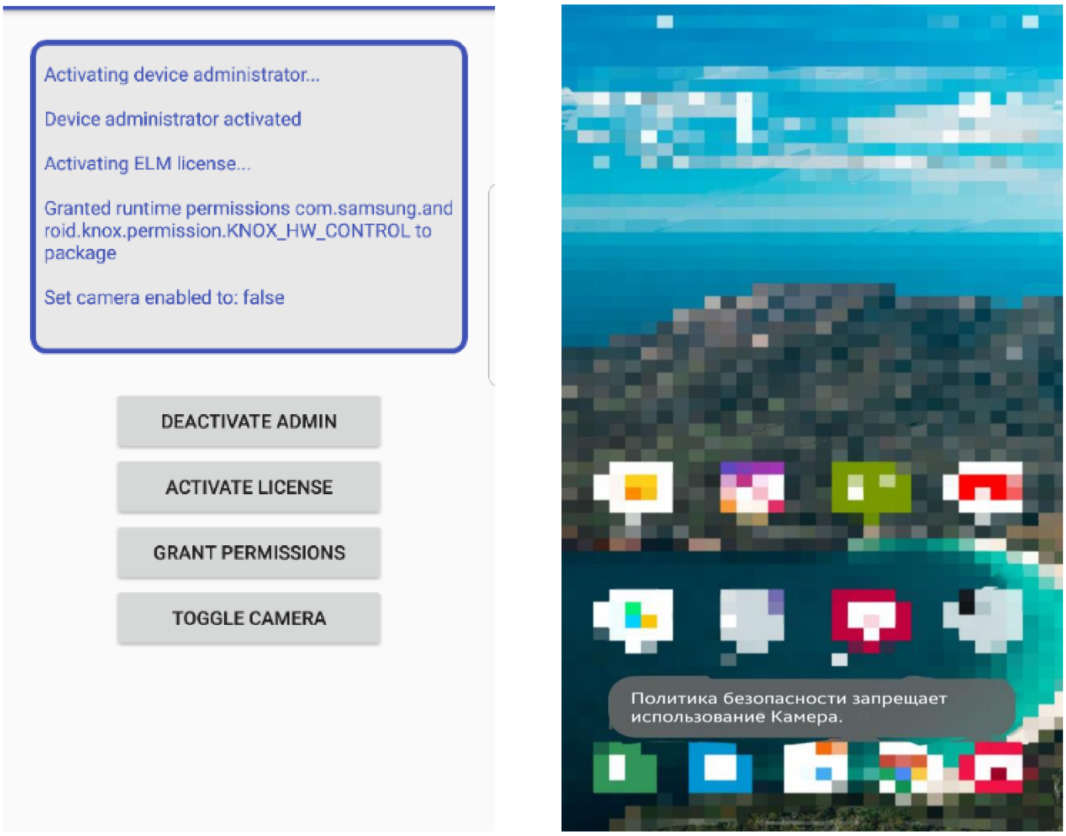
The program uses methods:

1. KnoxEnterprisLicenseManager.activateLicence(String key), where key – personal key of the developer. The method is used to activate the KNOX license.
2. KnoxEnterprisLicenseManager.deactivateLicence(String key)), where key – personal key of the developer. The method is used to deactivate the KNOX license.

3. ToggleCameraState() – method to change the camera enable status.
4. ToggleAdmin() – method for granting and revoking administrative rights for an application.
5. DevicePolicyManager.isAdminActive(ComponentName admin), where admin – the component to be checked. The method returns the status of the administrator rights for the application.
6. DevicePolicyManager.removeActiveAdmin(ComponentName admin), where admin – the component to be removed. The method removes administrator rights for the application.
7. ShowToast() – method for displaying messages.
8. EnterpriseDeviceManager.getInstance() – method that returns an instance of the class EnterpriseDeviceManager.
9. EnterpriseDeviceManager.getRestrictionPolicy() – method that returns an instance of the class RestrictionPolicy.
10. RestrictionPolicy.isCameraEnabled() – method that returns the enable state of the device's camera.
11. RestrictionPolicy.setCameraState(Boolean state), where state – the performance value of the device's camera.

Description of the logical structure:
1. The user is asked to grant permissions for the app to work
2. The user must activate the application as a device administrator
3. The user must request a license
4. The user can disable or enable the camera functionality

Examples of the result program are shown in Figure 3.



```
Activating device administrator...

Device administrator activated

Activating ELM license...

Granted runtime permissions com.samsung.android.knox.permission.KNOX_HW_CONTROL to package

Set camera enabled to: false
```

Политика безопасности запрещает использование Камера.

Figure 4: The App main screen and deny message of camera restriction

As a result of the development of software implementation, it was possible to obtain practical confirmation of the feasibility of establishing security policies and adjusting the device for working with EMM systems.

The main idea of the experiment is to demonstrate the possibility of blocking certain tools or policies or parts of the device in accordance with certain rules of the organization's security policy, provided that a personal device is used for corporate purposes. The use of this technology is quite relevant in modern realities. Moreover, this concept is suitable not only for making it possible to use personal devices at work, but also for allowing businesses to easily configure corporate mobile devices for use for their intended purposes. Examples are modern implementations of “mobile cash registers” when a cash register is not needed, but only a tablet with the appropriate software installed is enough. Or mobile devices for couriers\agronomists\forwarders, etc.

5. Conclusions

The increase in the market of mobile devices contributes to their more massive use in the corporate segment to optimize the work process and save money. The fairly rapid development of mobile device management systems shows that this is a promising direction in the IT and business industry. The wide variety of companies that provide such services contributes to the better development of technologies to ensure the protection of corporate information both on the devices themselves and during remote access to the corporate network. The analysis of the main concepts of the construction of the EMM system as a whole and the most popular representatives of the market of mobile device management systems showed that the choice of one of them depends on the activities of the organization, the operating system and the manufacturer of the devices used by employees in their professional activities. But each of the considered EMM systems provides a basic set of information security functions.

The disadvantages of EMM systems in general are the complexity of managing many different devices under different operating systems, and the lack of standardization between manufacturers and distributors of EMM systems.

However, EMM platforms will provide IT and security administrators with the ability to securely run massive software development for mobile devices and seamless integration with essential business infrastructure and support. They do a lot of checking to ensure access to confidential data in case of evidence of system compromise.

Despite all these disadvantages, there is a need to develop systems for implementation of BYOD policy will use a specific software product designed specifically for use with certain devices, many of the disadvantages associated with device fragmentation will be eliminated.

Acknowledgements

The research study depicted in this paper is funded by the French National Research Agency (ANR), project ANR-19-CE23-0005 BI4people (Business intelligence for the people).

References

[1] Madden J., Madden B. Enterprise Mobility Management: Everything you need to know about MDM, MAM, and BYOD. – Jack Madden, 2013. 176 p.

[2] Saravana, Balaji B,, Karthikeyan, N.K. and Raj Kumar, R.S., (2018), “Fuzzy service conceptual ontology system for cloud service recommendation”, Computers & Electrical Engineering, Vol. 69, pp. 435–446.

[3] Saravana, Balaji B., Mohamed, Uvaze Ahamed, Eswaran C. and Kannan R., (2019), “Prediction-based Lossless Image Compression”, Lecture Notes in Computational Vision and Biomechanics (Springer), Vol. 30, No 1, pp.1749 – 17961,

[4] Sivaram, M., Batri, K., Amin Salih, Mohammed and Porkodi V. (2019), “Exploiting the Local Optima in Genetic Algorithm using Tabu Search”, Indian Journal of Science and Technology, Volume 12, Issue 1.

[5] Kuchuk G., Nechausov S., Kharchenko, V. Two-stage optimization of resource allocation for hybrid cloud data store. International Conference on Information and Digital Technologies. 2015. P. 266-271.

[6] Ruban, I. Redistribution of base stations load in mobile communication networks / I. Ruban, H. Kuchuk, A. Kovalenko // Innovative technologies and scientific solutions for industries. – 2017. – No 1 (1) – P. 75-81.

[7] Sivaram, M., Yuvaraj, D., Amin Salih, Mohammed, Porkodi, V. and Manikandan V. (2018), “The Real Problem Through a Selection Making an Algorithm that Minimizes the Computational Complexity”, International Journal of Engineering and Advanced Technology, Vol. 8, iss. 2, 2018, pp. 95-100.

[8] Sivaram, M., Porkodi, V., Mohammed, A.S., Manikandan V. Detection of Accurate Facial Detection Using Hybrid Deep Convolutional Recurrent Neural Network. ICTACT Journal on Soft Computing. 2019. Vol. 09, Issue 02. pp. 1844-1850.

[9] Mohammed, A. S. Optimal Forecast Model for Erbil Traffic Road Data. ZANCO Journal of Pure and Applied Sciences. 2017. Vol. 29, No 5. P. 137–145. DOI: https://doi.org/10.21271/ZJPAS.29.5.15

[10] Kravets A. G., Bui N. D., Al-Ashval M. Mobile security solution for enterprise network //Joint Conference on KnowledgeBased Software Engineering. – Springer, Cham, 2014. – С. 371-382.

[11] Peraković D., Husnjak S., Cvitić I. Comparative analysis of enterprise mobility management systems in BYOD environment //The 2nd Reseach Conference In Technical Disciplines, RCITD. – 2014. – С. 82-85.

[12] Redman P., Girard J., Wallin L. O. Magic quadrant for mobile device management software //Gartner G00211101. – 2011.

[13] Ortbach K., Brockmann T., Stieglitz S. Drivers for the adoption of mobile device management in organizations. – 2014. 21.

[14] K. Smelyakov, A. Chupryna, D. Sandrkin and M. Kolisnyk, &quot;Search by Image Engine for Big Data Warehouse,&quot; 2020 IEEE Open Conference of Electrical, Electronic and Information Sciences (eStream), Vilnius, Lithuania, 2020, pp. 1-4, doi: 10.1109/eStream50540.2020.9108782.

[15] Kyrychenko, I., Shyshlo, O., Shanidze, N. “Minimizing Security Risks and Improving System Reliability in Blockchain Applications: a Testing Method Analysis”, 2023 7th International Conference on Computational Linguistics and Intelligent Systems (COLINS-2023), 2023. – CEUR-WS, 2023, ISSN 16130073. - Volume 3403, PP. 423-433.

[16] Kyrychenko, I., Malikin, D., “Research of Methods for Practical Educational Tasks Generation Based on Various Difficulty Levels”, 2022 6th International Conference on Computational Linguistics and Intelligent Systems (COLINS-2022), 2022. – CEUR-WS 3171, 2022, ISSN 16130073. - Volume I: Main, PP. 1030 - 1042.

[17] Samsung. WhitePaper: Knox Platform for Enterprise, 2018.