Mobile Application as a Critical Infrastructure Cyberattack Surface

Olha Mykhaylova[1], Taras Fedynyshyn[1], Anastasiia Datsiuk[1], Bohdan Fihol[1],
and Hennadii Hulak[2,3]

[1] *Lviv Polytechnic National University, 12 Stepan Bandera str., Lviv, 79013, Ukraine*
[2] *Borys Grinchenko Kyiv University, 18/2 Bulvarno-Kudriavska str., Kyiv, 04053, Ukraine*
[3] *National Academy of the Security Service of Ukraine, 22 Mykhaila Maksymovycha str., Kyiv, 03022, Ukraine*

Abstract

Mobile applications are becoming increasingly crucial for critical infrastructure, ensuring effective management and reliable communication in today's world. Postal services play a key role in logistics and serving citizens, providing a connection between people, the transfer of goods, and even delivering payments to the socially vulnerable segments of the population in remote regions. Mobile apps are increasingly becoming an integral part of postal services, offering convenience, speed, and ease of use for users, as well as access to additional features, such as scanning package barcodes and receiving notifications about shipment statuses. This article is dedicated to the security assessment of a mobile application of one of Ukraine's postal operators, which undeniably constitutes an element of the state's critical infrastructure. The research aims to evaluate the security of this app, considering potential threats and vulnerabilities that might arise during its operation. The study includes an analysis of the recommendations from popular security standards—ISO/IEC 27001:2022 and NIST Special Publication 800-163, and the application of static and dynamic analysis techniques to verify the security requirements established by OWASP Mobile Application Security Verification Standard (MASVS). The primary tool selected for this research is MobSF (Mobile Security Framework)—an automated, all-in-one framework for penetration testing, malware analysis, and security assessment of mobile apps (Android/iOS). The attack and the exploitation scenario of the identified vulnerabilities were verified in real time in an emulated environment. This article presents the vulnerabilities discovered in the mobile application. Our findings indicate the absence of usage confirmation and improper authorization for critically important functions, allowing malicious actors to remotely access the user's personal information, including name, contacts, and address, by only knowing the user's system identifier. Further, we propose countermeasures to protect the infrastructure and prevent adversaries from conducting reconnaissance and launching remote attacks using compromised accounts. The authors urge considering the possibility of applying the DevSecOps methodology when developing critical infrastructure information system applications.

Keywords

Mobile application security, OWASP, MASVS, critical infrastructure, NIST, NIST SP 800-163, risk management, risk tolerance.

1. Introduction

In recent times, there's been a marked surge in the adoption and widespread use of mobile devices worldwide [1]. These devices, powered by specific operating systems, offer users the ability to download a plethora of applications, often termed "apps," from online

CPITS-2023-II: Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2023, Kyiv, Ukraine
EMAIL: mykhaylovaolga1@mail.com (O. Mykhaylova); fedynyshyn.taras@gmail.com (T. Fedynyshyn); anastasiia.datsiuk07@gmail.com (A. Datsiuk); fidel2002beta@gmail.com (B. Fihol); h.hulak@kubg.edu.ua (H. Hulak)
ORCID: 0000-0002-3086-3160 (O. Mykhaylova); 0009-0006-8233-8057 (T. Fedynyshyn; 0009-0003-6626-1211 (A. Datsiuk); 0009-0004-8306-7303 (B. Fihol); 0000-0001-9131-9233 (H. Hulak)

platforms like the Apple App Store and Google Play [2]. Mobile apps are an integral part of our daily life. We use them for communication, work, learning, entertainment, and shopping. In recent years, the use of mobile apps has significantly increased, and this trend is likely to continue in the future. Here are some of the main trends that contribute to the growth of mobile app usage: Increase in smartphone usage. Every year, more and more people are using smartphones. This makes mobile apps more accessible and popular. Improvements in the productivity and functionality of mobile apps.

App developers constantly work on enhancing the productivity and functionality of their products. This makes mobile apps more attractive to users. Growing demand for business mobile apps. Businesses are increasingly using mobile apps for interaction with clients, sales, and marketing. This also contributes to the growth of mobile app usage. Modern mobile applications are prevalent and readily installable on most mobile operating systems, such as iOS, Android, and the like. The fierce competition among app providers has led to the emergence of increasingly sophisticated and tailored applications, that address intricate challenges. Such applications significantly transform user habits by simplifying their daily tasks [3]. Critical infrastructure refers to a set of systems, facilities, and institutions that play an indispensable role in the life of society and national economic development [4, 5]. These facilities include energy networks, transportation systems, financial institutions, postal services [6], and communication infrastructure. One of the important daily services is postal, as it facilitates the transfer of information and goods between individuals and organizations. It is vital for business, government, and private individuals. Postal communication ensures a connection between people. Mail allows people to stay in touch with each other, regardless of their location. This is important for families, friends, and business. It enables the transfer of goods. Mail is used for delivering items such as letters, packages, and parcels. This is crucial for businesses, governments, and private individuals. It is relatively inexpensive. Mail is a relatively cheap way to transfer information and goods. This is important for people with limited budgets. Mail is an essential element of modern society. It allows individuals and organizations to stay connected and work efficiently. The postal system is a critical infrastructure in most countries around the world. It is vital for businesses, governments, and private individuals. In some countries, the postal service is a state monopoly. In these nations, the postal service is mandatory, and governments are obligated to provide it to their citizens. In other countries, the postal service is a private company. However, governments often regulate private postal operators to ensure that they provide quality services and are accessible to everyone. Here are some examples of countries where the postal system is a critical infrastructure:

- Ukraine: The postal system is a state monopoly in Ukraine. It is a mandatory service, and the government is committed to providing it to its citizens.
- USA: The postal system is a private company in the USA. However, the government regulates private postal operators to ensure that they provide quality services and are accessible to everyone [7].
- United Kingdom: The postal system is a state monopoly in the United Kingdom. It is a mandatory service, and the government is committed to providing it to its citizens [8].
- China: The postal system is a state monopoly in China. It is a mandatory service, and the government is committed to providing it to its citizens [9].

Disruptions in the postal service can have severe consequences for society. For instance, if the postal system becomes non-operational, businesses won’t be able to deliver goods and services, the government won’t function efficiently, and private individuals won’t be able to stay in touch with each other. In recent years, postal operators have been actively implementing mobile apps. The mobile app of a postal service offers several advantages over using a website or a post office branch. Here are some of them:

- Convenience. A mobile app can be used at any time and any place with internet access. This allows users to track shipments, order services, and get information about post offices without leaving their homes or workplaces.

- Speed. Mobile apps are typically faster than websites since they do not require the user to load web pages. This enables users to quickly access information and accomplish tasks.
- Ease of use. Mobile apps are usually more user-friendly than websites. They are designed with mobile device usage in mind, making them more intuitively understandable and easy to use.
- Access to additional features. Some mobile apps offer extra functions that aren't available on websites. For example, certain apps allow users to order products from online stores, scan shipment barcodes, and receive notifications about the status of shipments.

Specific examples of how postal service mobile apps can be beneficial include:

- Users can track shipments in real time. This allows them to know where their shipment is and when it will be delivered.
- Users can order services, such as branch pick-up or courier delivery. This saves them time and effort.
- Users can receive information about post offices, such as operating hours, location, and available services.

This allows them to easily find the nearest branch and obtain the necessary information. Overall, mobile apps for postal services offer several advantages over using a website or a post office branch. They are convenient, fast, easy to use, and offer access to additional features. Together with the conveniences that mobile apps bring, challenges arise in the realm of cybersecurity [10]. Vulnerabilities in the mobile apps of postal operators can have serious consequences for both users and the operators themselves. For users, the consequences may include Personal Data Theft: Vulnerabilities can be exploited to steal users' personal information, such as names, addresses, credit card numbers, and other confidential details. This data can be used for fraud, identity theft, and other crimes [11]. Shipment Information Theft: Vulnerabilities can be exploited to steal shipment information, such as tracking numbers, sender's address, and recipient's address. This information can be used for stealing or redirecting shipments. Malware: Vulnerabilities can be exploited to download malicious software onto a user's device. These programs can be used to steal data, breach privacy, or even destroy the device. For postal operators, the consequences may include Loss of Customer Trust: If users learn about vulnerabilities in the postal operator's mobile apps, they may lose confidence in the operator and decide to refrain from using their services [12]. Decreased Sales: If users are not confident in the security of a postal operator's mobile apps, they may be less inclined to use these apps for sending or receiving parcels. Fines: In some instances, postal operators might face fines due to the presence of vulnerabilities in their mobile apps. Thus, security and protection measures become crucial in today's world [13]. This article is dedicated to the investigation of the security of a mobile application of one of Ukraine's postal operators, which undoubtedly is an element of the nation's critical infrastructure. The study aims to analyze the security of this application in light of potential threats and vulnerabilities that may arise during its operation. The research includes an analysis of the most up-to-date security standards—ISO/IEC 27001:2022 and NIST Special Publication 800-163 in the context of mobile applications, as well as a review of the security requirements set by OWASP Mobile Application Security Verification Standard (MASVS). We are focused on identifying design flaws in the interaction of various components, as this requires a deeper understanding of the ecosystem and advanced threat modeling. We use reverse engineering techniques and code analysis to gain insight into the functionalities embedded in the mobile postal application, as well as the security measures implemented by these applications. Accordingly, based on static analysis, we conduct dynamic functionality analysis to test the interaction of these apps with other components. Additionally, we analyze the traffic between the mobile application and the server side to understand their interactions. We also studied the exchanged information by breaking SSL using Man-In-The-Middle (MITM) monitoring to reveal encrypted interactions. As the primary research tool, the MobSF (Mobile Security Framework) application was chosen—it is an automated, all-in-one framework for penetration testing, malicious software analysis, and security evaluation of mobile applications (Android/iOS/Windows), capable of performing both static and dynamic analysis. The static and dynamic analysis of the application revealed vulnerabilities in the application and helped develop recommendations for their subsequent correction. The vulnerabilities found in the mobile application are presented in the article. The main one is a critical vulnerability in the application architecture that allows one to obtain confidential data about any system user by knowing only their identifier. Future research directions can be a detailed security study of the server side of the application and the development of recommendations to fix the discovered vulnerabilities.

The remainder of this paper is organized as follows. In Section 2, we present ISO/IEC 27001:2022 and NIST Special Publication 800-163 security frameworks controls and features related to mobile applications. In Section 3, we discuss the OWASP Mobile Application Security Testing Standard. In Section 4, we discuss our findings in terms of identified interactions and vulnerabilities, along with attack feasibility. In Section 6, we discuss research results and a mitigation framework along with security measures that will help defend against vulnerabilities found.

2. Critical Infrastructure

Critical infrastructure refers to a set of systems, facilities, and institutions that play an irreplaceable role in the life of society and national economic development. These entities encompass energy networks, transport systems, financial institutions, and communication infrastructure. As the modern world's reliance on these systems continually grows, ensuring their cybersecurity becomes a priority for governments and organizations worldwide. In the era of information technology and communication development, mobile applications have become an integral part of critical infrastructure. Along with the convenience brought by using mobile apps, an additional attack surface emerges for the information systems of critical infrastructure. Improperly configured or inadequately protected mobile applications can become the target of targeted cyberattacks, leading to significant disruptions in services and the leakage of confidential information.

2.1. Defining Critical Infrastructure

Critical infrastructure refers to an asset or system that is essential for maintaining vital economic and social functions: healthcare, food, security, transportation, energy, information systems, financial services, and so on. Damage to critical infrastructure, its destruction due to natural disasters, terrorism, criminal activity, or malicious behavior by individuals can have a significant negative impact on Ukraine's security and the well-being of its citizens. Caring for the cybersecurity of critical infrastructure entails ensuring the continuity of operations and services provided to citizens [14]. Even a minor service disruption can have a significant impact on a company that falls victim to an attack, and consequently, affects a large number of people. The nature of cyberattacks has evolved. Gone are the days when the primary goal of cybercriminals was economic gain; now, the objectives of cyberattacks have changed as well. Modern cybercriminals search for vulnerabilities in critical infrastructure systems to obtain essential and sometimes classified information, take control of operations or an entire enterprise or government department, and as a result, paralyze or even cease its activities altogether. Thus, security and protection measures have become crucial in today's world. The safety of critical infrastructure objects is becoming arguably the most critical aspect in the context of a war that has been ongoing for nearly two years. Every day, energy companies, chemical industries, the financial system, and other critical infrastructure areas become targets for the enemy. Successful execution of attacks can pose a threat to the lives and health of citizens, inflict devastating financial losses on the state, and so forth.

In the context of current Ukrainian legislation, critical infrastructure refers to a combination of facilities, systems, tools, and resources that support the vital activities of society and the state, specifically:

- Energy

- Chemical
- Food
- Transport
- Financial and banking
- Information technology and telecommunications
- Municipal services: water, heating, and gas supply
- Healthcare, and so on.

The Law of Ukraine "On Critical Infrastructure" dated November 16, 2021, defines the legal and organizational principles for the protection of Ukraine's critical infrastructure. The law sets out the procedure for classifying facilities as critical infrastructure, the powers of entities in the field of critical infrastructure protection, as well as the legal and organizational principles for responding to threats and cases of disruption to the functioning of critical infrastructure. The protection of Ukraine's critical infrastructure is funded by the state budget, funds from critical infrastructure entities, and other sources not prohibited by law.

2.2. Why is Critical Infrastructure Important?

Critical infrastructure often encompasses industrial control systems, including the Supervisory Control and Data Acquisition (SCADA) systems, which are used to automate industrial processes in a country's critical infrastructure sectors. Attacks against industrial control systems raise serious concerns. They have the potential to create widespread compromises in vital systems such as transportation, delivery of various energy resources to enterprises and citizens, water distribution, and wastewater collection, among others. The interconnections and interdependencies between infrastructure systems and sectors mean that if one or several functions are temporarily or entirely disrupted, there can be an immediate negative impact on multiple sectors or the entire system as a whole. Not only are adversaries increasingly targeting critical infrastructure and operational technologies, but they are also investing more in enhancing their capabilities to compromise these organizations.

Industrial control systems have undergone radical changes and improvements over the past decades. What was once a combination of isolated, proprietary systems based on serial protocols is now highly interconnected systems that use internet protocol and commercial solutions for operational optimization and cost reduction. While there have been many business benefits from this integration of information technologies and operational technologies, modernization has also increased the risk of cyber threats, affecting the availability of processes and the well-being of staff, citizens, the economy, and the environment. This factor, combined with a growing threat landscape and regulatory scenarios, has increased the burden on organizations trying to secure their critical infrastructure. Some of these challenges include:

- Gaining detailed visibility into operational network traffic at the application and user level to verify proper or anomalous usage [15].
- Segmenting networks with adequate access control to limit external and internal attack vectors while adhering to stringent productivity standards, such as ISA 62443.
- Protecting disparate commercial systems off the shelf from known cyber threats and reducing downtimes due to cyber incidents or patching.
- Preventing advanced cyberattacks that use zero-day methods to disrupt production, compromise data integrity, or steal intellectual property.
- Managing disconnected, distributed network, and endpoint security products.
- Protecting unmanaged, unsecured IoT and connected devices.
- Complying with regulatory standards like NERC CIP, TSA Security Directives, and NIST CSF, and effectively providing information for auditing.
- Ensuring the operation and safety of remote external plant environments using security solutions compatible with a broad range of extreme conditions.

To effectively protect modern SCADA networks and critical infrastructure, a modernized approach to security is needed. To learn how it helps ICS and SCADA system operators worldwide safeguard their brands and operational environments, download the Security Reference Blueprint for industrial control systems.

2.3. The Postal Service as an Important Part of Ukraine's Critical Infrastructure

The postal service is a crucial part of the transport sector of Ukraine's critical infrastructure. It facilitates the transmission of information, goods, and services vital to the economy, society, and the state. The primary functions of the postal service in Ukraine are:

- Executing state functions, namely the delivery of correspondence, essential documentation, and government services. A disruption in postal operations in this context could lead to the cessation of vital state services to citizens (such as pension or social assistance delivery) and could also disrupt the functioning of the judicial system (since the postal service delivers court decisions and summonses).
- Supporting businesses. Every day, hundreds of thousands of goods, documents, product samples, financial papers, and more are sent by mail. If the postal service's operations were to be halted or disrupted, it would substantially impact the business and financial sectors of the country.
- Connecting people. In this context, the postal service ensures the transportation of various cargoes, letters, and cards between individuals and legal entities, such as between a bank and a consumer, etc.

Measures to protect the postal service in Ukraine since the onset of the full-scale invasion by the Russian Federation. Since the beginning of the full-scale invasion by Russia, the role of the postal service has become even more crucial. In 2023, the Ukrainian Post was classified as part of Ukraine's critical infrastructure. This means it is subject to specific legislation that provides for additional protective measures.

To protect the postal service in Ukraine, a set of measures in domains different is implemented. Physical security enhancement:

- Improved security for postal branches (installation of motion detectors, glass break detectors, and panic buttons in case of attempted robbery or threats to the lives of employees).
- Implementing protective measures for technical equipment within the enterprise.
- Conducting appropriate briefings for employees.

Information security assurance:

- Application of modern information protection technologies.
- Conducting external audits of the enterprise's information security.
- Enhancing the qualifications of employees in the field of information security (organizing and conducting training in cybersecurity literacy and online behavior).

Resilience to cyber attacks:

- Implementing cyber-attack protection systems (installing high-quality software to guard against cyber-attacks).
- Conducting regular training sessions for employees to counteract cyber-attacks.
- Engaging external cybersecurity service providers to ensure additional round-the-clock protection against cyber-attacks.
- Collaborating with governmental authorities in the field of cybersecurity.

During wartime, the operation of the postal service has several distinct features, namely:

- An increase in transportation volumes.
- A reduction in delivery times.
- Changes in delivery routes.
- Inability to deliver to certain regions (temporarily occupied territories not under state control).

These peculiarities are related to military actions, infrastructure destruction, and movement restrictions.

The operation of the postal service is vitally important for Ukraine during wartime. It helps ensure citizens have access to state services, supports businesses, and helps people maintain communication with one another. In addition to its primary functions, the postal service also carries out several additional tasks in times of war.

Specifically, it helps to:

- Deliver humanitarian aid to Ukrainians living in temporarily occupied territories, as well as assistance to internally displaced persons who were forced to leave their homes.
- Deliver weapons, clothing, food, and other essential items from volunteers to servicemen and women.
- Convey messages from soldiers to their families.
- Collect information about infrastructure damage.

The postal service is an essential element of the Ukrainian economy and society. It supports the country's vital functions during wartime. Once the war is over, Ukraine's postal service will need time to recover. It will require investments in new technologies and equipment, as well as staff training. However, thanks to the experience gained during the war, the Ukrainian postal system stands a good chance of not only recovering but also becoming an even more effective tool in the transport sector of the country's critical infrastructure.

2.4. The Importance of Cyber Defense for Critical Infrastructure During Wartime

Cyber defense of critical infrastructure (and in particular, the postal service) is one of the priorities in today's world, especially in the context of warfare, as it is vital for ensuring the stability and security of society. Critical infrastructure refers to a system of assets, systems, networks, processes, and services that are vital for the functioning of society. Disruption of critical infrastructure can lead to severe consequences, such as economic losses, loss of life, and destabilization of society.

Cyberattacks are deliberate actions aimed at disrupting the operation of information systems. Cyberattacks can be carried out to steal information, spread disinformation, disable systems, or cause harm. In the context of war, cyberattacks are one of the tools used in hybrid warfare. Russia actively employs cyberattacks as a means to destabilize Ukraine and its economy. The postal service is an essential element of critical infrastructure. It ensures the delivery of mail, cargo, and documents, and also serves as an important communication channel. Disruption of the postal service can lead to severe issues for the population, businesses, and government agencies. In the realities of war, the postal service becomes even more crucial. It's one of the few channels that allow maintaining communication between people in different regions of the country. Disruption of the postal service can lead to the isolation of certain regions and complicate the provision of humanitarian aid.

Ukraine has already taken steps to strengthen the cybersecurity of its critical infrastructure. Specifically, the National Cybersecurity Center was established, which is responsible for ensuring the cybersecurity of government bodies and critical infrastructure. Additionally, legislation has been adopted that strengthens the responsibility for cyberattacks. However, to ensure effective cybersecurity, it is essential to continue implementing appropriate measures and cooperate with international partners. This will protect critical infrastructure from cyberattacks and ensure the normal functioning of society, even in times of war. Additional arguments in favor of strengthening the cybersecurity of critical infrastructure, including the postal service are:

1. Cyberattacks can be highly destructive. They can lead to significant financial losses, disruption of essential systems, and even human casualties.
2. Cyberattacks can be challenging to deflect. Hackers continually develop new cyberattack methods, which can be tough to detect and halt.
3. It's challenging to prevent cyberattacks entirely. It's impossible to fully protect any system from cyberattacks.

In conclusion, strengthening the cybersecurity of critical infrastructure is a vital task for any country, whether at war or peace. It allows society to be protected from the severe consequences of cyberattacks and ensures its stable and safe functioning.

3. Analyses of ISO/IEC 27001: 2022 and NIST Special

Publication 800-163 in the Context of Mobile Applications

Overseeing information security within an organization can be a challenging endeavor. This complexity stems from its encompassing nature, covering everything from physical and network security to human resource safeguards and supplier management. For newcomers or those with limited experience in the field, there's a risk of overlooking key facets due to a dearth of hands-on experience. This is where security frameworks become invaluable, offering structured guidance in formulating and implementing security strategies. With such a framework, processes and procedures are more straightforward to establish, ensuring the organization can assess, monitor, and address cybersecurity risks while implementing the right controls to safeguard critical data. However, selecting the perfect framework tailored to an organization's specific needs presents another layer of challenge. This decision must consider unique business-related factors, such as organizational context, operational domain, and relevant laws and contractual commitments. Broader factors, like the framework's maturity, scope, and popularity, also play a role. While numerous information security frameworks exist, NIST SP 800-53 and ISO/IEC 27001:2022 stand out as popular choices among security professionals globally [10]. These frameworks are favored for their comprehensive security controls, spanning vital security aspects, and their adaptability across diverse organizational types. Yet, each has its unique attributes, which may make one more fitting for certain organizations than the other. This article aims to provide a concise overview of these two predominant security frameworks, delving into their main features, and contrasting their controls.

3.1. Security of Mobile Devices within the ISO/IEC 27001 Framework

Considerations for an Information Security Policy. According to ISO/IEC 27001, the purpose of the information security policy is to establish management's direction and commitment to information security. The Information Security Policy serves as a guiding and strategic document, detailing the goals and strategies for safeguarding information. Given the particular vulnerabilities and significance of mobile device security, it demands explicit attention and incorporation within the Information Security Policy. This policy should encompass elements such as the vision for information security, objectives, strategies, scope, organizational structure, roles, assets, and more. Notably, policies specific to mobile devices must be clear, comprehensive, and efficient, while specific procedures and detailed processes should be kept separate from the policy itself.

The creation of an information security policy should adhere to a process: defining the scope of the information security policy, risk assessment and analysis, and review, endorsement, and execution of the information security policy. When crafting this policy, state-of-the-art security technology for mobile devices is foundational. It's imperative to gather and keep abreast of all relevant technologies, ensuring timely updates [11].

Structuring Information Security. Information security will be overseen by the organization's management. They will endorse security policies, delegate security responsibilities, and oversee the integration of security measures throughout the entity. Information assets and technology related to mobile devices should be identified and promptly updated.

Human Resources Security. Given the constant use of mobile devices by individuals, securing human resources is vital. Every member of an organization needs to recognize their duties and be aware of practices that mitigate the risk of theft, fraud, or misuse related to mobile devices. Responsibilities should be structured in tiers. The uppermost tier typically oversees and reviews the organization's information security practices. The intermediate tier handles day-to-day information security activities, while the base tier consists of mobile device users who operate according to established policies and are overseen by the higher tiers.

Physical and Environmental Security. Despite the borderless nature of mobile devices, it's imperative to consider physical and environmental security to deter unauthorized access, harm, theft, breaches, and disturbances to mobile data and facilities.

Sites containing mobile devices will be fortified with suitable security measures and access controls, ensuring protection against unauthorized access and potential harm. Only those with the requisite permissions will be granted access to these secure areas. Security measures will also extend to equipment located off-site. Before disposal, all devices with storage capabilities will undergo checks to ensure sensitive information and licensed software has been either removed or securely overwritten, aligning with statewide policies.

Communications and Operations Management. Mobile devices experience a higher volume of communications and operations compared to other devices. As such, specific responsibilities and protocols for managing these devices should be set in line with the information security policy. It's crucial to identify and mitigate viruses and malicious code to safeguard the software and data on these devices. Exchanging sensitive information with external entities should adhere to a well-defined exchange policy. Moreover, mobile devices holding sensitive information must be shielded from unauthorized access and potential misuse.

Access Control. In organizations that utilize mobile devices, access control encompasses two facets: first, accessing organizational information systems via mobile devices, and second, mobile devices accessing external information resources. Both dimensions of mobile device access control should be governed by business needs and security imperatives. Structured protocols must be in place for these devices to manage access privileges to both internal and external information infrastructures, ensuring the prevention of unauthorized entries.

3.2. NIST SP 800-163: App Security Requirements

NIST SP 800-163 defines [16] a mobile app vetting process and provides guidance on planning and implementing an app vetting process, developing security requirements for mobile apps, identifying appropriate tools for testing mobile apps, and determining if a mobile app is acceptable for deployment on an organization's mobile devices. An overview of techniques commonly used by software assurance professionals is provided, including methods of testing for discrete software vulnerabilities and misconfigurations related to mobile app software.

General Requirements. General app security requirements outline the software features and behaviors that an app should or shouldn't exhibit to maintain its security. Termed "general" because they can be adapted across various mobile applications, these requirements can be fine-tuned to align with an organization's security expectations and risk appetite. These overarching app security criteria can be sourced from various standards, best practices, and resources, including those provided by entities like NIAP, OWASP, MITRE, and NIST.

1. National Information Assurance Partnership (NIAP)—The NIAP Protection Profiles (PPs) provide a comprehensive set of security requirements for IT products intended for use in national security systems and other federal applications, guiding their certification based on the ISO/IEC 15408 standards. While many mobile apps may not need this certification, their security analysis remains beneficial; thus, for these apps, the NIAP suggests following guidelines laid out in the Protection Profile for Application Software, which is categorized into Functional and Assurance Requirements.
2. OWASP Mobile Risks, Controls, and App Testing Guidance—The Open Web Application Security Project (OWASP) offers resources on mobile app testing and security, including the Mobile Application Security Verification Standard (MASVS), which outlines baseline security requirements for mobile apps and categorizes them into three verification levels. These levels further encompass various control categories like Architecture, Cryptography, and Resilience, tailored to the desired verification level. Additionally, the OWASP Mobile Security Testing Guide provides a comprehensive guide on how to technically verify the MASVS requirements.
3. MITRE App Evaluation Criteria—In 2016, MITRE Corporation analyzed the efficacy of mobile app security vetting solutions to aid enterprises in

automating parts of their vetting processes. The evaluation criteria were developed based on NIAP's Protection Profile for Application Software, additional app vetting capabilities, and common app vulnerabilities. MITRE released a technical report detailing their methodology, evaluation criteria, and results, which is accessible on their GitHub site.

4. NIST SP 800-53—NIST Special Publication 800-53 offers a comprehensive catalog of security and privacy controls tailored for federal information systems, ensuring protection from threats like cyber-attacks, natural disasters, and human errors. The document facilitates the selection of controls, and customization based on organizational needs, and provides baselines for varying impact levels, while also explaining how to develop specialized control overlays for specific missions or technologies. These controls tackle both the functionality and assurance aspects of security, ensuring that IT products and systems are constructed with reliable security principles, making them trustworthy.

Organization-Specific Requirements. Organization-specific security requirements outline the rules and guidelines an organization adheres to for maintaining its security stance, such as prohibiting the installation of social media apps or apps from certain vendors on company mobile devices. For crafting these specific requirements, it's beneficial to recognize non-vulnerability factors impacting mobile app security, which can be determined using criteria like those in Table 1.

Table 1
Organization-specific security criteria

Criterion	**Description**
Policies	The security, privacy, and acceptable use policies; social media guidelines; and regulations applicable to the organization.
Provenance	Identity of the developer, the developer's organization, the developer's reputation, consumer reviews, etc.
Data Sensitivity	The sensitivity of data collected, stored, or transmitted by the app.
App Criticality	The level of importance of the app relative to the organization's business.
Target Users	The app's intended set of users from the organization.
Target Hardware	The intended hardware platform on which the app will be deployed.
Target Operating Platform	The operating system, operating system version/Software Development Kit (SDK), and configuration on which the app will be deployed.
Target Environment	The intended operational environment of the app (e.g., general public use vs. sensitive military environment).
Digital Signature	Digital signatures are applied to the app binaries, libraries, or packages.
App Documentation	User Guide, Test Plans, Test Results, Service Level Agreement

The NIST Risk Management Framework (RMF) describes a process through which an organization establishes, maintains, and communicates a strategy to manage organizational risk in an information system. The RMF is a seven-step process consisting of the following steps:

- Step 0: Prepare—identify key individuals and their assigned roles within the organization, as well as the identification, organization, and prioritization of required resources.
- Step 1: Categorize—identify the security requirements associated with a system by classifying the system according to legislation, policies, directives, regulations, standards, and organizational mission/business/operational requirements.
- Step 2: Select—determine the baseline set of security controls that match the organization's risk tolerance.
- Step 3: Implement—implementing and documentation of selected controls.

- Step 4: Assess—examine the implementation of the security controls concerning the organization’s requirements.
- Step 5: Authorize—enabling the system to be used within the organization.
- Step 6: Monitor—ongoing and/or reoccurring reassessment of the selected security controls.

A key activity in Step 0 involves identifying an organization’s risk tolerance. Risk tolerance is the level of risk or degree of uncertainty, that is acceptable to an organization. A defined risk tolerance level identifies the degree to which an organization should be protected against confidentiality, integrity, or availability compromise.

4. OWASP Mobile Application Security Testing Standard

Emerging technologies invariably come with fresh security challenges, and mobile computing follows this trend. Mobile apps present unique security issues distinct from conventional desktop software. While contemporary mobile operating systems might be seen as more secure than their desktop counterparts, overlooking security in mobile app development can lead to vulnerabilities. Considerations include data storage, communication between apps, the correct use of cryptographic APIs, and ensuring secure network communications.

4.1. OWASP Mobile Application Security Verification Standard

The OWASP MASVS (Mobile Application Security Verification Standard) is the industry standard for mobile app security. It can be used by mobile software architects and developers seeking to develop secure mobile applications, as well as security testers to ensure completeness and consistency of test results [17].

The standard is divided into various groups of security controls, labeled MASVS-XXXXX, that represent the most critical areas of the mobile attack surface:

- MASVS-STORAGE: Secure storage of sensitive data on a device (data-at-rest).
- MASVS-CRYPTO: Cryptographic functionality used to protect sensitive data.
- MASVS-AUTH: Authentication and authorization mechanisms used by the mobile app.
- MASVS-NETWORK: Secure network communication between the mobile app and remote endpoints (data-in-transit).
- MASVS-PLATFORM: Secure interaction with the underlying mobile platform and other installed apps.
- MASVS-CODE: Security best practices for data processing and keeping the app up-to-date.
- MASVS-RESILIENCE: Resilience to reverse engineering and tampering attempts.

To complement the MASVS, the OWASP MAS project also provides the OWASP Mobile Application Security Testing Guide (MASTG) and the OWASP MAS Checklist which together are the perfect companion for verifying the controls listed in the OWASP MASVS and demonstrating compliance.

4.2. OWASP Mobile Application Security Testing Guide

The OWASP Mobile Application Security Testing Guide (MASTG) is a comprehensive manual for mobile app security testing and reverse engineering. It describes technical processes for verifying the controls listed in the OWASP MASVS.

The MASTG contains descriptions of all requirements specified in the MASVS [18]. The MASTG contains the following main sections:

1. The General Testing Guide contains a mobile app security testing methodology and general vulnerability analysis techniques as they apply to mobile app security. It also contains additional technical test cases that are OS-independent, such as authentication and session management, network communications, and cryptography.
2. The Android Testing Guide covers mobile security testing for the Android platform, including security basics, security test cases, reverse engineering techniques and prevention, and tampering techniques and prevention.

3. The iOS Testing Guide covers mobile security testing for the iOS platform, including an overview of the iOS OS, security testing, reverse engineering techniques and prevention, and tampering techniques and prevention.

5. Case Study: Testing Postal Operator Mobile Application with OWASP MAS Methodology

In this section, we will showcase the outcomes of testing the postal service mobile application based on the guidelines from the OWASP Mobile Application Security Testing Guide.

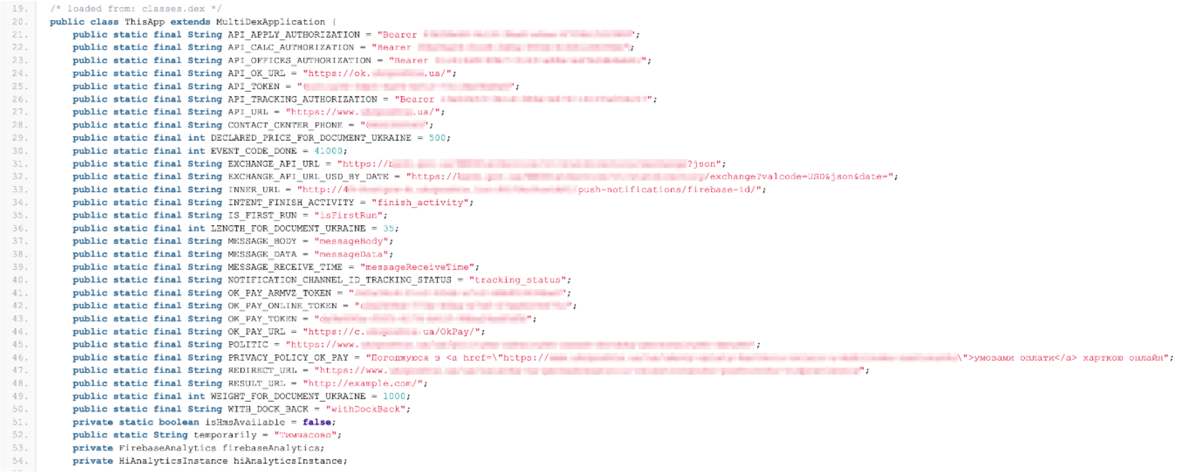
The test was concluded using the MobSF (Mobile Security Framework) Framework [19]. The researchers team executed static and dynamic binary analysis.

5.1. Static Analysis

Our goal is to research and comprehend the features of mobile applications and the libraries they employ. Through static analysis, we evaluated the security provisions put in place by the postal mobile app provider to counteract automated bot incursions, by scrutinizing libraries and remnants in the binary files. Furthermore, we delved into the architecture of mobile apps for a comprehensive functionality review. As such, we engaged in reverse-engineering the APK—a packed archive that includes a manifest detailing the package name, activity names, supported hardware attributes, permissions, and other settings. This APK also houses the app's certificates, a directory with the compiled libraries the app relies on, and a file with the app code index format. The latter can be processed by both the Dalvik Virtual Machine (DVM) and Android's runtime ecosystem.

The main outcomes from static analysis are:

- Hardcoded secret strings in source code. Fig. 1 shows sensitive strings found in decompiled application code. For privacy reasons, some keys and values are pixelated.
- The attribute android: usesCleartextTraffic in the Android app's manifest file is set to true, which means that the use of unencrypted network traffic in the app is permitted. This means the app can interact with the server by sending and receiving messages in plain text, which can be risky and lead to potential security threats, such as data interception.



```
/* loaded from: classes.dex */
public class ThisApp extends MultiDexApplication {
    public static final String API_APPLY_AUTHORIZATION = "Bearer [redacted]";
    public static final String API_CALC_AUTHORIZATION = "Bearer [redacted]";
    public static final String API_OFFICES_AUTHORIZATION = "Bearer [redacted]";
    public static final String API_OK_URL = "https://ok.[redacted].ua/";
    public static final String API_TOKEN = "[redacted]";
    public static final String API_TRACKING_AUTHORIZATION = "Bearer [redacted]";
    public static final String API_URL = "https://www.[redacted].ua/";
    public static final String CONTACT_CENTER_PHONE = "[redacted]";
    public static final int DECLARED_PRICE_FOR_DOCUMENT_UKRAINE = 500;
    public static final int EVENT_CODE_DONE = 41000;
    public static final String EXCHANGE_API_URL = "https://[redacted]?json";
    public static final String EXCHANGE_API_URL_USD_BY_DATE = "https://[redacted]/exchange?valcode=USD&json&date=";
    public static final String INNER_URL = "http://[redacted]push-notifications/firebase-id/";
    public static final String INTENT_FINISH_ACTIVITY = "finish_activity";
    public static final String IS_FIRST_RUN = "isFirstRun";
    public static final int LENGTH_FOR_DOCUMENT_UKRAINE = 35;
    public static final String MESSAGE_BODY = "messageBody";
    public static final String MESSAGE_DATA = "messageData";
    public static final String MESSAGE_RECEIVE_TIME = "messageReceiveTime";
    public static final String NOTIFICATION_CHANNEL_ID_TRACKING_STATUS = "tracking_status";
    public static final String OK_PAY_ARMVZ_TOKEN = "[redacted]";
    public static final String OK_PAY_ONLINE_TOKEN = "[redacted]";
    public static final String OK_PAY_TOKEN = "[redacted]";
    public static final String OK_PAY_URL = "https://c.[redacted]ua/OkPay/";
    public static final String POLITIC = "https://www.[redacted]";
    public static final String PRIVACY_POLICY_OK_PAY = "Погоджуюся з <a href=\"https://[redacted]\">умовами оплати</a> карткою онлайн";
    public static final String REDIRECT_URL = "https://www.[redacted]";
    public static final String RESULT_URL = "http://example.com/";
    public static final int WEIGHT_FOR_DOCUMENT_UKRAINE = 1000;
    public static final String WITH_DOCK_BACK = "withDockBack";
    private static boolean isHmsAvailable = false;
    public static String temporarily = "Тимчасово";
    private FirebaseAnalytics firebaseAnalytics;
    private HiAnalyticsInstance hiAnalyticsInstance;
```

Figure 1: Secret strings in code

5.2. Dynamic Analysis

We use dynamic analysis in tandem with our static analysis approach, ensuring a thorough and all-encompassing evaluation of every interaction and feature offered by the mobile application [20]. This dynamic examination is carried out via functionality analysis, logging user interactions, scrutinizing network traffic, and observing changes in the system's state.

Traffic analysis. While emulating user behavior and performing user actions, we capture the traffic generated by the mobile application to understand the information that is being sent and the interactions between the mobile application and the server similar to

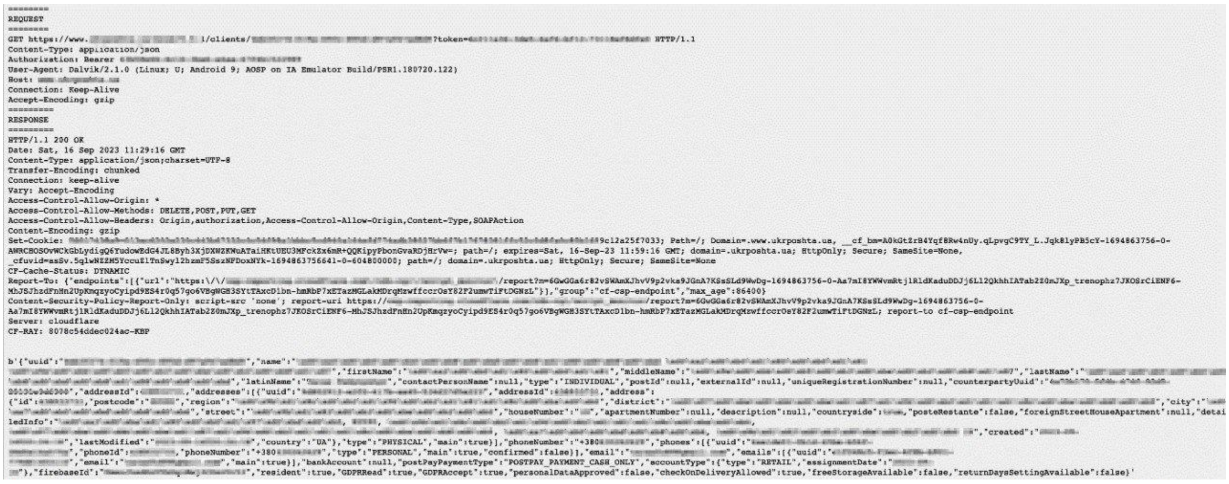
[21]. We trigger important functionalities of the application such as sign up/in and others. The application we analyzed does not use trusted Certificate Authorities to protect user privacy by encrypting the communication between the mobile application and the server side. To decrypt the communication we utilize an un-rooted device with the Android 7.

Dynamic Analysis tests the mobile app by executing and running the app binary and analyzing its workflows for vulnerabilities. For example, vulnerabilities regarding data storage might be sometimes hard to catch during static analysis, but in dynamic analysis, you can easily spot what information is stored persistently and if the information is protected properly. Besides this, dynamic analysis allows the tester to properly identify:

- Business logic flaws.
- Test environment vulnerabilities.
- Weak input validation and bad input/output encoding as they are processed through multiple services.

The main result of the dynamic analysis is the detection of a poorly protected mechanism for retrieving user data. Specifically, after authentication (entering the user's email and password), the app retrieves user information (name, surname, phone number, address, and other data) without using a user token.

In Fig. 2, you can see that to retrieve information about the user, an HTTP GET request is made to an address with user id URL-parameter and token query-parameter and looks like https://server/path/clients/<userID>?token=<token1>. Also, the headers are passed and Authorization is among them with value: Bearer <token2>.



```
========
REQUEST
========
GET https://www.[redacted]/clients/[redacted]?token=[redacted] HTTP/1.1
Content-Type: application/json
Authorization: Bearer [redacted]
User-Agent: Dalvik/2.1.0 (Linux; U; Android 9; AOSP on IA Emulator Build/PSR1.180720.122)
Host: [redacted]
Connection: Keep-Alive
Accept-Encoding: gzip
=========
RESPONSE
=========
HTTP/1.1 200 OK
Date: Sat, 16 Sep 2023 11:29:16 GMT
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: DELETE,POST,PUT,GET
Access-Control-Allow-Headers: Origin,authorization,Access-Control-Allow-Origin,Content-Type,SOAPAction
Content-Encoding: gzip
Set-Cookie: [redacted]9c12a25f7033; Path=/; Domain=.www.ukrposhta.ua, __cf_bm=A0kGt2rB4Yqf8Rw4nUy.qLpvgC9TY_L.Jqk8lyPB5cY-1694863756-0-
AWRCHOSOvWCkGbLydigQ6YudowEdG4JL8Byh3XjDXWZKWuATaiHKtUEU3MFckZx6mR+QQKipyPbonGvaRDjHrVw=; path=/; expires=Sat, 16-Sep-23 11:59:16 GMT; domain=.ukrposhta.ua; HttpOnly; Secure; SameSite=None,
_cfuvid=asSv.5qlwNZZM5YccuZlTnSwyl2hzmF5SszNFDoxNYk-1694863756641-0-604800000; path=/; domain=.ukrposhta.ua; HttpOnly; Secure; SameSite=None
CF-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https:\/\/[redacted]/report?m=6GwGGa6r82vSWAmXJhvV9p2vka9JGnA7KSsSLd9WwDg-1694863756-0-Aa7mI8YWWvmRtj1RldKaduDDJj6Ll2QkhhIATab2Z0mJXp_trenophz7JKOSrCiENF6-
MhJSJhzdFnHn2UpKmqzyoCyipd9ES4r0q57go6VBgWGH3SYtTAxcD1bn-hmRbP7xETazMGLakMDrqMzwffccrOsY82F2umwTiFtDGNzL"}],"group":"cf-csp-endpoint","max_age":86400}
Content-Security-Policy-Report-Only: script-src 'none'; report-uri https://[redacted]/report?m=6GwGGa6r82vSWAmXJhvV9p2vka9JGnA7KSsSLd9WwDg-1694863756-0-
Aa7mI8YWWvmRtj1RldKaduDDJj6Ll2QkhhIATab2Z0mJXp_trenophz7JKOSrCiENF6-MhJSJhzdFnHn2UpKmqzyoCyipd9ES4r0q57go6VBgWGH3SYtTAxcD1bn-hmRbP7xETazMGLakMDrqMzwffccrOsY82F2umwTiFtDGNzL; report-to cf-csp-endpoint
Server: cloudflare
CF-RAY: 8078c54ddec024ac-KBP


b'{"uuid":"[redacted]","name":"[redacted]
[redacted]","firstName":"[redacted]","middleName":"[redacted]","lastName":"[redacted]
[redacted]","latinName":"[redacted]","contactPersonName":null,"type":"INDIVIDUAL","postId":null,"externalId":null,"uniqueRegistrationNumber":null,"counterpartyUuid":"[redacted]
[redacted]","addressId":[redacted],"addresses":[{"uuid":"[redacted]","addressId":[redacted],"address":
{"id":[redacted],"postcode":"[redacted]","region":"[redacted]","district":"[redacted]","city":"[redacted]
[redacted]","street":"[redacted]","houseNumber":"[redacted]","apartmentNumber":null,"description":null,"countryside":[redacted],"posteRestante":false,"foreignStreetHouseApartment":null,"detai
ledInfo":"[redacted], [redacted], [redacted],
[redacted], [redacted]","created":"[redacted]
[redacted]","lastModified":"[redacted]","country":"UA"},"type":"PHYSICAL","main":true}],"phoneNumber":"+380[redacted]","phones":[{"uuid":"[redacted]
[redacted]","phoneId":[redacted],"phoneNumber":"+380[redacted]","type":"PERSONAL","main":true,"confirmed":false}],"email":"[redacted]","emails":[{"uuid":"[redacted]
[redacted]","email":"[redacted]","main":true}],"bankAccount":null,"postPayPaymentType":"POSTPAY_PAYMENT_CASH_ONLY","accountType":{"type":"RETAIL","assignmentDate":"[redacted]
[redacted]"},"firebaseId":"[redacted]","resident":true,"GDPRRead":true,"GDPRAccept":true,"personalDataApproved":false,"checkOnDeliveryAllowed":true,"freeStorageAvailable":false,"returnDaysSettingAvailable":false}'
```

Figure 2: Retrieving user information without using a user token

Thus, security is ensured by using two tokens—token 1 and token 2, the values of which were discovered in the source code in plain view during the static analysis (see 5.1) of the app. Therefore, knowing the user's identifier, it is possible to obtain confidential user data, such as surname, first name, patronymic, phone number, email address, physical address, and others.

6. Results and Recommendations

The testing of the mobile application for the critical infrastructure information system revealed serious vulnerabilities in the app's security that allow access to private user data by knowing only their system identifier.

The authors have prepared two courses of action to address the identified issues. The first is technical and involves the meticulous application of technical recommendations and best practices described in the OWASP Mobile Application Security Design Guide (MASDG) [22]. The MASDG is a document aimed at establishing a foundation for designing, developing, and testing secure mobile applications on mobile devices, including evaluation criteria (a set of rules) and code examples in the OWASP Mobile Application Security Verification Standard (MASVS) and the OWASP mobile program. The second is organizational and revolves around the implementation of the DevSecOps methodology [23] by development teams. DevSecOps integrates advanced security measures into the DevOps process since ensuring data and application security must be a top priority for all organizations, especially for critical infrastructure systems. Besides enhancing security, DevSecOps maintains the speed and agility that DevOps brings to data and applications. Furthermore, DevSecOps continuously integrates, develops, and updates the latest security methodologies, providing reliable, effective, and efficient protection.

References

[1] Statista, Smartphones—Statistics & Facts (2020). URL: https://www.statista.com/topics/840/smartphones/

[2] B. Guo, et al., Enhancing Mobile App User Understanding and Marketing with Heterogeneous Crowdsourced Data: A Review, IEEE Access, 7 (2019) 68557–68571. doi: 10.1109/access.2019.2918325.

[3] P. Weichbroth, L. Lysik, Mobile Security: Threats and Best Practices, Mob. Inf. Syst. (2020). doi: 10.1155/2020/8828078.

[4] V. Grechaninov, et al., Formation of Dependability and Cyber Protection Model in Information Systems of Situational Center, in: Workshop on Emerging Technology Trends on the Smart Industry and the Internet of Things, vol. 3149 (2022) 107–117.

[5] V. Grechaninov, et al., Decentralized Access Demarcation System Construction in Situational Center Network, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3188, no. 2 (2022) 197–206.

[6] The Resolution of the Cabinet of Ministers of Ukraine from October 9, 2020, No. 1109 ”On Certain Issues of Critical Infrastructure Objects”. URL: https://ips.ligazakon.net/document/KP201109?an=506

[7] A. Papageorgiou, et al., Security and Privacy Analysis of Mobile Health Applications: the Alarming State of Practice, IEEE Access 6 (2018) 9390–9403. doi: 10.1109/access.2018.2799522.

[8] Critical National Infrastructure (2022). URL: https://www.npsa.gov.uk/critical-national-infrastructure-0

[9] Regulation on Protecting the Security of Critical Information Infrastructure (2021). URL: http://www.lawinfochina.com/display.aspx?id=36511&lib=law

[10] S. Mavoungou, et al., Survey on Threats and Attacks on Mobile Networks, IEEE Access 4 (2016) 4543–4572. doi: 10.1109/access.2016.2601009.

[11] A. Papageorgiou, et al., Security and Privacy Analysis of Mobile Health Applications: the Alarming State of Practice, IEEE Access 6 (2018) 9390–9403. doi: 10.1109/access.2018.2799522.

[12] H. Hulak, et al. Formation of Requirements for the Electronic Record-Book in Guaranteed Information Systems of Distance Learning, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS 2021, vol. 2923 (2021) 137–142.

[13] Critical National Infrastructure (2022). URL: https://www.npsa.gov.uk/critical-national-infrastructure-0

[14] Z. Brzhevska, et al., Analysis of the Process of Information Transfer from the Source-to-User in Terms of Information Impact, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3188 (2021) 257–264.

[15] V. Buriachok, et al., Invasion Detection Model using Two-Stage Criterion of Detection of Network Anomalies, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 2746 (2020) 23–32.

[16] M. Ogata, et al., Vetting the Security of Mobile Applications, NIST Special Publication 800-163 Revision 1 (2019). doi: 10.6028/NIST.SP.800-163R1.

[17] OWASP Mobile Application Security Verification Standard. URL: https://mas.owasp.org/MASVS/

[18] OWASP Mobile Application Security Testing Guide. URL: https://mas.owasp.org/MASTG/

[19] MobSF, Mobile security framework (MobSF) (2021). URL: https://github.com/MobSF/Mobile-Security-Framework -MobSF

[20] K. Sarieddine, et al., Investigating the Security of EV Charging Mobile Applications As an Atack Surface, ACM Transactions on Cyber-Physical Systems (2023). doi: 10.1145/3609508.

[21] W. Zhou, et al., Discovering and Understanding the Security Hazards in the Interactions Between iot Devices, Mobile Apps, and Clouds on Smart Home Platforms, 28th {USENIX} Security Symposium (2019) 1133–1150.

[22] Mobile Application Security Design Guide. URL: https://owasp.org/www-project-mobile-application-security-de si gn-guide/

[23] F. Lombardi, A. Fanton, From DevOps to DevSecOps is not enough. CyberDevOps: an extreme shifting-left architecture to bring cybersecurity within software security lifecycle pipeline, Software Quality J. 31 (2023) 619-654. doi: 10.1007/s11219-023-09619-3.