Threat model of the testing subsystem for rare mobile device owners

Tatiana Rein*, *Vladimir* Torgulkin, and *Mikhail* Trefelov

Federal State Budgetary Educational Institution of Higher Education «Kemerovo State University», Digital Institute, Kemerovo, Russia

Abstract. Testing mobile applications for owners of rare mobile devices is a complex task because of the diversity of devices. The goal of this study is to create a threat model of the testing subsystem for owners of sparse mobile devices. The authors of the paper describe step by step the classes of users and the key components of the subsystem. The article defines the level of security and the dominant classes of subsystem vulnerabilities. The authors created an intruder model for the testing subsystem, defined the security class, and planned measures to protect the testing subsystem.

1 Introduction

One characteristic of the modern mobile device market is its fragmentation [1]. Many companies produce a variety of devices that differ in both hardware and software characteristics, such as screen size or operating system version. This is especially true for Android devices. The diversity of devices affects mobile app development, particularly the testing process.

The major consequence of fragmentation is the inability to test apps on all devices. Developers for this purpose purchase only the most popular models usually. On less popular, rare devices, app failures occur more frequently and they have more vulnerabilities. We should not neglect rare devices, because users of such models leave the most negative feedback, thereby damaging developers' reputations.

Table 1 shows the shares of brands of the most purchased Android devices in the world in 2022 [2]. The total share of rare brands is about 30%, which exceeds the share of the most popular brand, Samsung. Such brands as Huawei, Honor, and Vivo occupy a small share of the market, so we can also call them rare.

Table 1. Shares of mobile device brands on the Android platform.

№	Brand	Share, %
1	Samsung	25,3
2	Xiaomi	15,7
3	Oppo	10,8
4	Vivo	9,6
5	Honor	6,1

* Corresponding author: tsrein@mail.ru

Continuation of Table 1.

6	Huawei	2,4
7	Others	30,1

The purpose of this paper is to create a threat model of the testing subsystem for rare mobile device owners. Objectives of the work:
- describe the classes of users and the key components of the subsystem;
- determine the level of security of the subsystem;
- create an intruder model for the testing subsystem;
- identify the dominant classes of vulnerabilities in the subsystem;
- identify the primary security threats to the subsystem;
- to propose measures to protect the subsystem from the found threats.

2 Subsystem description

The testing subsystem is an information system for controlling the passage of test scenarios on mobile devices with the Android operating system, including its derivatives.

Two classes of users use the testing subsystem: testers and performers. Testers are users who create test scenarios (tasks) for performers and receive test artifacts from them - the results of passing the scenario. Executors are users who can pass test scenarios received from testers, and send them passing results. Executors can be notified of new scenarios available.

Figure 1 shows a diagram of the scenarios for using the subsystem.

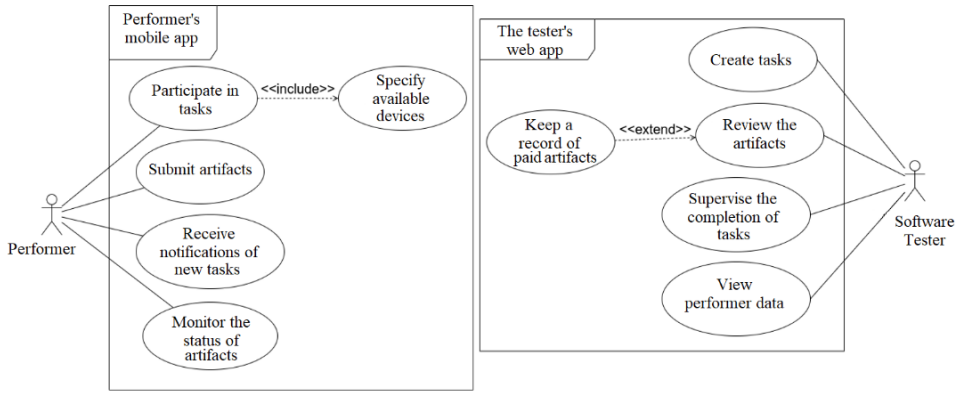

Fig. 1. Diagram of subsystem usage scenarios.

The subsystem operates according to the "client-server" model. The server part of the subsystem runs on a virtual server under Ubuntu Server 22.10 operating system. The main software that implements the functionality of the server part is Node.js web server version 19.8.1, Express framework version 4.18.2, DBMS MySQL version 8.0.32.

The client part comprises a mobile application of the executor and a web client of the tester. The mobile application is implemented in the Kotlin 1.8.10 programming language using the Jetpack Compose user interface library and the local SQLite3 DBMS. The web client is implemented in JavaScript using the React library version 18.2.0.

Figure 2 shows a container diagram of the testing subsystem.

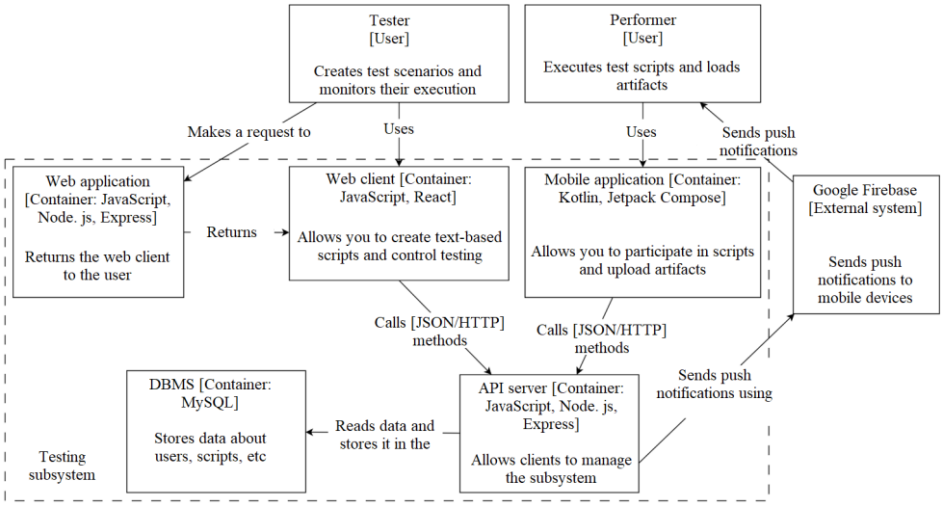

Fig. 2. Container diagram of the testing subsystem.

3 The security level of the subsystem

The subsystem processes public and other personal data of less than 100,000 subjects, who are and are not employees of the organization where the subsystem exists [3].

General personal data includes the names of testers and performers, and e-mail addresses of all users.

Other personal data include profile identifiers in the social network "VK", nicknames in the messenger "Telegram", date of registration in the subsystem, information about the devices, sent results of passing scenarios, and information about the amount of remuneration of performers for passed scenarios.

Threats of the 3rd type, not related to undocumented features of the application software used, characterize the subsystem.

Under Russian Government Decree No. 1119 of November 1, 2012, the testing subsystem corresponds to Security Level 4 [4].

4 Intruder model

An external intruder is outside the information system at the start of the threat [5]. An external intruder will not affect the testing subsystem, because the subsystem stores a volume of information insufficient to motivate such an intruder.

By an internal intruder, we mean an intruder within the information system at the time the threat begins [5].

We can refer the following groups of people to internal intruders: subsystem users, database administrators, information security administrators, and subsystem developers.

Database and information security administrators and developers understand subsystem processes and also have direct access to protected information. We must make special arrangements for recruiting, assigning, and monitoring the responsibilities of these individuals.

4.1 Intruders according to the FSTEC of Russia threat Databank

The FSTEC of Russia (Federal Service for Technical and Export Control) threat databank defines three types of external and internal intruders: low, medium, and high potential [6]. Table 2 describes each potential.

Table 2. Description of the potential of information security attackers.

Potential	Description
Low	Availability of capabilities at the level of one person to gain (freely available on a free or paid basis) and use special means of exploitation of vulnerabilities.
Medium	Availability of capabilities at the level of a group of persons/organization to develop and use special means of exploitation of vulnerabilities.
High	Availability of capabilities at the level of an enterprise/group of enterprises/state to develop and use special means of exploitation of vulnerabilities.

Intruders with low potential characterize the testing subsystem.

5 Subsystem vulnerability classes

According to the standard GOST R 56546-2015 "Information Security. Vulnerabilities of information systems. Classification of vulnerabilities of information systems", the following vulnerabilities by the area of origin are typical for subsystem testing [7]:
- code vulnerabilities;
- configuration vulnerabilities.

By the type of deficiencies in the information system:
- associated with the incorrect configuration of the software parameters;
- related to the incomplete check of the input data;
- related to the possibility of crossing the links;
- related to implementing arbitrary code;
- related to cross-site scripting;
- related to spoofing cross-site requests;
- related to authentication.

According to the place of occurrence (manifestation):
- vulnerabilities in system-wide software;
- vulnerabilities in application software.

6 Threat model

We determine the initial security level under the "Methodology for determining current threats to the security of personal data during its processing in personal data information systems" of the FSTEC of Russia [8]. Technical specifications with security levels listed in Table 3 characterize testing subsystems.

Table 3. Technical and operational characteristics of the subsystem.

Characteristics	Value of characteristic	Security level
Location	Deployed within a single building	High
Connection to public networks	Has a single point of access to the public network	Medium
Built-in (legal) operations with personal database records	Modification, transfer.	Low
Delimitation of access to personal data	Only the organization's employees defined in the list have access	Medium
Availability of connections to other personal databases of other information systems	A single personal database is used, belonging to the organization that owns the information system	High
Level of generalization (depersonalization) of personal data	Data is not depersonalized (i.e., there is information that allows to identify the data subject)	Low
The volume of personal data, which third-party users of information systems receive without prior processing	Does not provide any information	High

Since there are characteristics corresponding to the low level of security, and the proportion of characteristics of medium and high levels is about 71%, the subsystem has a medium level of initial security.

6.1 Security threats according to the FSTEC of Russia threat Databank

Threats, the source of which is an internal intruder with low potential, are typical for the testing subsystem. Table 4 lists these threats according to the threat databank [9].

Table 4. Threats to the testing subsystem.

Threat ID	Threat	Information security properties to be violated
UBI.008	Recovery and/or reuse of authentication information	Confidentiality
UBI.012	Destructive change of configuration/environment of programs	Confidentiality Integrity Availability
UBI.030	Use of default identity/authentication information	Confidentiality Integrity Availability
UBI.034	The exploitation of weaknesses in network/local exchange protocols	Confidentiality Integrity Availability
UBI.074	Unauthorized access to authentication information	Confidentiality
UBI.086	Unauthorized changes to authentication information	Integrity Availability
UBI.091	Unauthorized deletion of protected information	Availability
UBI.100	Bypass of improperly configured authentication mechanisms	Confidentiality Integrity Availability

Continuation of Table 4.

UBI.113	Reboot of hardware and firmware of computer equipment	Integrity Availability
UBI.140	Putting the system into a state of "denial of service"	Availability
UBI.152	Deletion of authentication information	Confidentiality Integrity Availability
UBI.167	Infecting computers by visiting unauthorized sites	Confidentiality Integrity Availability

6.2 Defining protective measures

To draw up protection measures, we must determine the security class of the testing subsystem. For this purpose, we will use the Order of the FSTEC of the Russian Federation of February 11, 2013 No. 17 "About approval of requirements for the protection of information not constituting state secrets in state information systems". [10].

Let's find the security class of the testing subsystem by the level of importance of the information and the scale of the subsystem itself. Let's determine the level of importance of information by damage from violations of confidentiality, integrity, and availability of information. And the scale of the subsystem on the placement in one or more subjects of the Russian Federation.

Table 5 contains the results of the calculation of the level of significance of information. Based on these calculations, the information significance level is 1.

Table 5. Damage from the violation of the property of information.

Information Security Basics	Damage
Confidentiality	Low
Integrity	Low
Availability	Low

The testing subsystem has an object scale. Table 6 shows the basic protection measures for the security class.

Table 6. Measures to protect the testing subsystem.

Unit designation	A measure of protection
IAF.1	Identification and authentication of users who are employees of the operator
IAF.3	Management of identifiers, including creation, assignment, and destruction of identifiers
IAF.4	Management of authentication means, including storage, issuance, initialization, blocking of authentication means, and taking measures in case of loss and/or compromise of authentication means
IAF.5	Protecting feedback when entering authentication information
IAF.6	Identification and authentication of users, who are not employees of the operator (external users)
UPD.1	Management (activation, blocking, and destruction) of user accounts, including external users
UPD.2	Implementation of the methods (discretionary, mandate, role, or another method), types (read, write, execute, or another type), and access control rules
UPD.3	Control (filtering, routing, connection control, unidirectional transfer, and other control methods) of information streams between devices, information system segments, and information systems

Continuation of Table 6.

UPD.4	Division of powers (roles) of users, administrators, and persons ensuring the operation of the information system
UPD.5	Assignment of the minimum necessary rights and privileges to users, administrators, and persons ensuring the operation of the information system
UPD.6	Limitation of unsuccessful attempts to log on to the information system (access to the IS)
UPD.10	Blocking an access session to the information system after a set period of inactivity (inactivity) of the user or at the user's request
UPD.11	Permission (prohibition) of user actions permitted before identification and authentication
UPD.13	Implementation of secured remote access of subjects to objects via external information and telecommunication networks
UPD.16	Managing interaction with third-party information systems (external information systems)
OPS.3	Installation of only approved software and (or) its components
ZNI.1	Accounting for machine-readable media
ZNI.2	Managing access to machine storage media
ZNI.8	Third parties can repair or dispose of machine media and control its destruction (erasure)
RSB.1	Definition of security events to be logged and their retention periods
RSB.2	Determining the composition and content of the information about security events that must be recorded
RSB.3	Collection, recording, and storage of safety event information for the specified retention period
RSB.4	Responding to security event logging failures, including hardware and software errors, failures in information collection mechanisms, and reaching a memory limit or overflow (capacity)
RSB.5	Monitoring (review, analysis) of the results of security events logging and responding to them
RSB.6	Generation of time stamps and (or) synchronization of the system time in the information system
RSB.7	Protection of information about security events
AVZ.1	Antivirus protection
AVZ.2	Updating the database of signs of malicious computer programs (viruses)
ANZ.1	Detection, analysis of vulnerabilities of information systems and quick fixing of newly detected vulnerabilities
ANZ.2	Control over the installation of software updates, including software updates of information protection facilities
ANZ.3	Control of workability, setup parameters, and proper functioning of software and information protection facilities
ANZ.4	Control over the composition of hardware, software, and information security facilities
ANZ.5	Control over rules of generation and change of user passwords, creation and deletion of user accounts, implementation of rules of access differentiation, and user authorities in the information system
ANZ.3	Ensuring the ability to restore software, including information security software, in the event of abnormal situations
ZSV.1	Identifying and authenticating subjects and objects of access to the virtual infrastructure, including virtualization management administrators
ZSV.2	Management of subject access to objects in the virtual infrastructure, including within virtual machines
ZSV.3	Recording security events in the virtual infrastructure

Continuation of Table 6.

ZSV.9	Implementing and managing antivirus protection within the virtual infrastructure
ZSV.10	Partitioning of virtual infrastructure into segments (segmentation of virtual infrastructure) for information processing by an individual user and/or group of users
ZIS.3	Ensuring protection of information from disclosure, modification, and imposition (input of false information) when transmitting it (preparing it for transmission) via communication channels outside the controlled area, including wireless communication channels
ZIS.5	Prohibition of unauthorized remote activation of video cameras, microphones, and other peripheral devices and notification of users about activation of such devices

7 Conclusion

This work considered the characteristics of personal data processed in the subsystem, based on which the level of protection of the testing subsystem was determined. The article contains a model of an intruder and the dominant classes of subsystem vulnerabilities. The authors found the initial security level and listed the primary security threats according to the data bank of information security threats of FSTEC of Russia. The authors have also determined the security class and generated a list of protection measures for the testing subsystem.

The authors used the equipment of the Kemerovo State University Center for Collective Use of Scientific Equipment under the agreement № 075-15-2021-694 dated 05.08.2021, concluded between the Ministry of Science and Higher Education of the Russian Federation and the Federal State Budgetary Educational Institution of Higher Education "Kemerovo State University" (unique contract identifier RF----2296.61321X0032).

References

1. How to deal with Android Fragmentation. BrowserStack. https://www.browserstack.com/guide/what-is-android-fragmentation

2. Omdia: Apple, Samsung and Honor win in Q2, overall market lose. https://www.gsmarena.com/smartphone_shipments_in_q2__apple_samsung_and_honor_win_overall_market_loses-news-55233.php

3. Federal Law of the Russian Federation of July 27, 2006 No. 152-FZ "About personal data" (as amended on 14.07.2022). http://pravo.gov.ru/proxy/ips/?docbody=&nd=102108261

4. Order of the Government of the Russian Federation of November 1, 2012 No. 1119 "About approval of security requirements of personal data in case of their processing in personal data information systems" https://base.garant.ru/70252506/

5. Attacker (intruder, violator, troublemaker). https://bdu.fstec.ru/ubi/terms/terms/view/id/33

6. Attacker potential. https://bdu.fstec.ru/ubi/terms/terms/view/id/38

7. GOST R 56546-2015 «Information Security. Vulnerabilities of information systems. Classification of vulnerabilities of information systems». https://internet-law.ru/gosts/gost/60628

8. Methodology for determining current threats to the security of personal data during their processing in personal data information systems. https://fstec.ru/tekhnicheskaya-

zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380-metodika-opredeleniya-aktualnykh-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-fstek-rossii-2008-god

9. Data bank of information security threats. https://bdu.fstec.ru/threat

10. Order of the FSTEC of the Russian Federation of February 11, 2013 No. 17 "About approval of requirements for the protection of information not constituting state secrets in state information systems". https://fstec.ru/dokumenty