Where Security Meets Accessibility: Mobile Research Ecosystem

Radka Nacheva(✉), Snezhana Sulova, and Bonimir Penchev

University of Economics – Varna, Varna, Bulgaria
{r.nacheva,ssulova,b.penchev}@ue-varna.bg

Abstract. User-oriented approaches help teams develop digital products that will not only be functional, but will also help to enhance the emotional experience. The specifics of human beings, that are placed at the centre of the development, are determining the entire interaction flow with digital devices and software products. One of the topics that researchers' study in the field of human-computer interaction is accessibility. It is associated with the ability of a person to use barrier-free products or services. Accessibility, in turn, is also related to the user security such as attacks and vulnerabilities that often lead to a lack of access to digital devices. In this regard, the aim of our paper is to define a mobile research ecosystem for testing and evaluating secure and accessible mobile multi-device environments. The ecosystem should simultaneously implement the basic principles of accessibility and security of mobile applications. Thus defined aim determines the objectives of the paper, which are: to study the main problems of mobile applications' accessibility; to study mobile security frameworks; to test mobile accessibility and security. Design-thinking process flow is implemented in our approach. The accessibility and security of mobile operating systems Android and iOS are tested.

Keywords: Mobile accessibility · Mobile security · Research ecosystem · User experience

1 Introduction

The topic of cybersecurity is one of the leading in the last five years, along with others like artificial intelligence, machine learning, the Internet of Things, automation, automotive autonomy. In particular, privacy and confidential computing are enshrined in the Regulation (EU) 2016/679 General Data Protection Regulation (GDPR). Chapter 5 of the document regulates the terms of transfers of personal data to third countries or international organizations, including articles on: the general principle for transfers, transfers on the basis of an adequacy decision, transfers subject to appropriate safeguards, binding corporate rules, transfers or disclosures not authorized by union law, derogations for specific situations and international cooperation for the protection of personal data [1]. The document regulates the conditions under which personal data must be processed by the so-called data processor, ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services, as well as the encryption of personal data [1].

© Springer Nature Switzerland AG 2022
A. V. Chugunov et al. (Eds.): EGOSE 2021, CCIS 1529, pp. 216–231, 2022.
https://doi.org/10.1007/978-3-031-04238-6_17

Despite the efforts of cybersecurity experts, malicious individuals discover security vulnerabilities in software products and take advantage of them when committing illegal acts. This is also proved by the statistical data. A McAfee report from the beginning of 2021 shows that the pandemic situation has had a negative impact on cyber security. In 2020, the most affected are scientific and educational institutions, public administrations and IT companies. The most common security issues were vulnerabilities, targeted attacks, malware and account hijacking [2]. According to McAfee data, publicly disclosed incidents surged 100% in Europe from Q3 to Q4 2020. Incidents in Asia increased by 84% and those in North America rose by 36% [2]. There are approximately 3.1 million external attacks on cloud accounts from more than 30 million users worldwide during Q4 of 2020 [2]. There has been a significant increase in attacks on all families of operating systems from Q3 to Q4 of 2020: PowerShell threats grew to 208%; MacOS malware increases by 420%; Linux malware increased to 6%.

Another company, Norton, also provides a complete picture of cybersecurity globally. According to statistics published by the company, for 2020 over 75% of cyberattacks are launched via email [3]. Last year, the FBI received 15,421 internet crime complaints from 60 countries around the world. The first half of 2021 saw a 102% increase in ransomware attacks compared to the same period in 2020 [3]. Norton also confirmed that the COVID-19 pandemic had a negative impact on cybersecurity, stating that the FBI had reported a 300% increase in reported cybercrimes [3]. Users report an increase in fraudulent emails, spam, and phishing attacks from their corporate email.

Mobile users are also affected by cyberattacks. According to the statistical portal Statista.com for the last quarter of 2020 the number of malicious installation packages was over 2,106 million, which is over one million compared to the first quarter of 2020 and over 600 thousand more than the first quarter of 2021 [4]. In comparison, many malicious installation packages reported in 2019 equal those reported in Q4 of 2020. iOS users are less affected by malware than those of Android [5]. It is reported that mobile malware worldwide in 2020 were AdWare (57,26%), RiskTool (21,34%), trojan (4,46%), backdoor (1,49%), etc. [6]. Kaspersky shares 2020 statistics according to which 87% of Android mobile phones are exposed to security risks [7]. According to the company, the most common types of malwares faced by Android users are banking malware, mobile ransomware, mobile spyware, MMS malware, mobile adware and SMS trojans. To them, for 2021 open WiFi, phishing attacks, spyware, poor password security can be added [8].

As can be seen from the cited sources, the pandemic situation has significantly affected the committed cybercrimes. A breach of the security of individual and corporate users is reported. On the other hand, the problems that these cyberattacks create for people with special needs must also be taken into account. This is mainly due to their inability to access or make full use of digital devices. The consequences of disrupted cybersecurity are also at odds with the policies and strategies for people with disabilities developed by global organizations such as United Nations and the World Health Organization (WHO), as well as the European Union.

The WHO said the pandemic has led to an urgent need for scale up disability services, including healthcare. According to the organization, people with disabilities are unable to use different services due to prohibitive costs and inadequate skills and knowledge

of the people who offer these services [9]. The facts reported by WHO are worrying - the percentage of people with some kind of disability is growing. This is about 10% of the world's population, and the share of young people is even higher - 30% [10]. The United Nations has an even higher share - 15% of the world's population lives with some form of disability, with 80% of people living in developing countries where their care is extremely low [11]. WHO cites UNESCO as saying that 9% of children in low-income countries do not attend school [10]. The United Nations has set 7 targets of the Sustainable Development Goals entirely aimed at people with disabilities [11]. These focus on: no poverty (Goal 1), zero hunger (Goal 2), good health and well-being (Goal 3), quality education (Goal 4), gender equality (Goal 5), reduced inequalities (Goal 10), peace, justice and strong institutions. (Goal 16) [12]. The 2030 Agenda for Sustainable Development was adopted in 2015 by all members of the United Nations [12]. It is an act of partnership between nations around the world to share common goals and strategies to reduce inequalities between people, improve health and education, and spur economic growth. In this regard, technological progress should be helpful in achieving the United Nations Sustainable Development Goals. Researchers are working on problems related to the practical application of business intelligence in education [13], the impact of social media [14] and e-learning methods [15] in education, the methods and tools for processing big data [16], the Internet of Things [17], the programming and database issues of web and mobile applications' development [18–20], the human resource management practical aspects [21–23]. All these topics are part of the overall view of providing quality digital products through which to achieve end-user satisfaction with the services they use [24].

The presented facts give us a reason to direct the **aim of this paper** as defining a mobile research ecosystem for testing and evaluating secure and accessible mobile multi-device environments. The ecosystem should simultaneously implement the basic principles of accessibility and security of mobile applications.

Based on the goal we can formulate the following research questions:

- (RQ1) What are the standards and good practices for bettering the mobile accessibility and security?
- (RQ2) What tools can be used to test the accessibility and security of mobile applications?

To answer research questions, the paper should meet the following objectives:

- to study the main issues of mobile applications' accessibility;
- to study mobile security frameworks;
- to examine mobile accessibility and security.

2 Related Work

To answer the RQ1, we must explore the international standards about accessibility and security. In addition, researches related on these problems should be explored too. In order to find the intersection between the major topics of security and accessibility, it

is necessary to look for the unifying link between them – human beings. The ways in which people use digital devices and machines are explored by the scientific field human-computer interaction. The efforts of specialists and scientists who work in that area are aimed mainly at minimizing the barriers between people's mental models in terms of fulfilling their goals and technological support of their tasks. Device access and information processing are essential for building multi-channel consistency within multi-device environments.

In the last two decades, the philosophy of user-centered design (UCD), also known as human-centered design (HCD), has emerged. According to ISO 13407: 1999 - now it is recognized by ISO 9241-210:2019(en), UCD is defined as an approach to developing interactive systems that focuses on creation of usable systems [25]. HCD is described as a multidisciplinary activity that includes human factors and ergonomics, techniques to increase efficiency and productivity, to improve human well-being, user satisfaction, accessibility and sustainability, the working conditions of people with a system and neutralize the possible adverse effects of its use on human health, safety and productivity [26]. Accessibility is one of the areas defined by the standard for expanding the digital inclusion of a wide range of people with specific needs, characteristics and capabilities to achieve the goals in a particular context of use [26].

The standard provides guidance for the UCD throughout the life cycle of developing computer-based interactive systems, which is divided into four parts: rationale, principles, planning and activities. Our interest is targeted to the setting of its principles and activities. The principles of user-oriented design are four:

- active participation of the users of the system and clear understanding of the tasks they should perform;
- appropriate distribution of functions between users and technology;
- re-use of design solutions;
- multidisciplinary design.

The UCD process is built by four activities (Fig. 1):

- Specifying the context of use: this includes getting to know the user, the environment of use, as well as the targeted tasks.
- Specifying the user and organizational requirements: it includes determining the criteria for the success of the usability of the product in relation to user tasks, such as how quickly a typical user must be able to complete a task with the product. This includes setting design guidelines and imposing various restrictions.
- Developing of product design solutions: taking into account the knowledge of human-computer interaction (e.g., visual design, interaction design, usability), a variety of design solutions are created.
- Evaluation of designs in accordance with the imposed requirements: the usability of the designs is evaluated according to user tasks.

On the other hand, HCD is closely related to the so-called "design thinking". It is considered as an iterative process in which user needs should be understood and, on this basis, problem solving could lead to innovation and competitive advantage [27, 28].

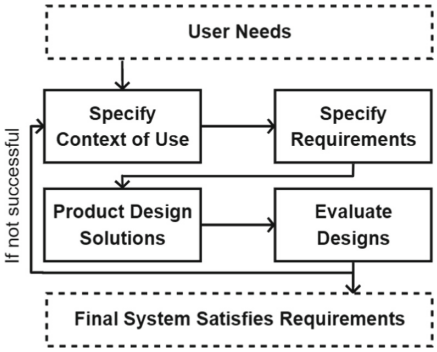

Fig. 1. UCD's activities adapted in accordance with [25].

The flow of the design-thinking framework is consisted of understanding, exploring, and materializing segments [27]. Within them five or six phases could be conducted. According to [28], these are: Empathize, Define, Ideate, Prototype, Test. [27] adds to them Implement stage. [27] states that the process starts with research about what users do, say, think, and feel. After that all observations are combined and problems are defined. These two stages are part of the understanding stage of the design-thinking framework flow. Next part of the flow – Explore, is formed by ideating and creating a prototype. Their task is to generate creative ideas and, on their basis, to build up tactile visual representations. The last part of the flow – Materialize, is related to collecting end user feedback and materializing user visions.

The most important factors that play significant role in building human-oriented technologies are: the audience, the context of use, the defined system requirements both by users and by the organization. Compliance with these criteria should lead to the creation of design solutions tailored to all levels' requirements.

Meeting the standards ensures quality development of UCD digital products. They can be related to any aspect of human-computer interaction, including accessibility. In terms of this paper's purpose, we are focusing on mobile accessibility standards.

Within the Web Accessibility Initiative (WAI) World Wide Web Consortium (W3C) supports the standard for application of Web Content Accessibility Guidelines (WCAG) to mobile. It's applicable to mobile web content, mobile web apps, native apps, and hybrid apps using web components inside native apps [29]. It provides only an informative guidance, but not any technical details that are useful for mobile development. The document includes four main principles as WCAG. Under the Perceivable principal guides related to user interface (UI) elements manipulations are formalized. The Operable principle defines recommendations for keyboard control, touch target size and spacing and touchscreen gestures. The Understandable principle is related to screen orientation, consistent layout and positioning important UI elements. The last one – Robust, is targeted to providing guides for using easy methods for data entry and supporting the characteristic properties of the platform. All the developer techniques that apply to mobile are summarised in another W3C document [30]. It includes an example code that visualizes the realization of WCAG to mobile.

Another international institution – the European Telecommunications Standards Institute (ETSI), supports accessibility standard EN 301 549 v2.1.2, that is applicable to mobile applications and "their compliance with the essential requirements of perceivability, operability, understandability and robustness defined in the Web and Mobile Accessibility Directive" [31]. It contains functional requirements and provides a reference document that can be followed by different stakeholders (e.g., managers, developers, UI designers, etc.). It includes WCAG recommendations too. The standard is based on the Directive (EU) 2016/2102 issued by the European parliament and the Council. The last one is targeted to accessibility of websites and mobile applications of public sector bodies [32]. It provides principles for digital inclusion of people with disabilities, but an example code is not included. Another European Union document that mentions mobile accessibility is Directive (EU) 2019/882. It is related to [30] and its purpose is more general – to document accessibility requirements for products and services and to contribute the proper functioning of the internal market by approximating laws, regulations and administrative provisions of the Member States [33].

There are national standards and guidelines. For example, Section 508, The Americans with Disabilities Act, New Zealand Web Accessibility Standard 1.1, etc. Some of them are also based on WCAG.

On the other hand, mobile operating systems' companies also form accessibility guidelines that are followed up by the developers. The most used are Google Android [34] and Apple iOS guidelines [35]. Companies provide complete guides for both designers and programmers, including principles, user interface elements patterns, programming code, and testing tools. They also have rapidly adopted the design thinking approach.

The combination of platform-specific standards and guidelines provides opportunities to fully address mobile accessibility issues. Closely related to the availability of digital devices and services is their security, which often predetermines the possibilities for their trouble-free use.

Unlike design thinking and user-centred design process, mobile device security research depends on the specifics of the platform. The development focus is not only on the interaction, but also on the approaches and standards for delivering better functionalities. Open Web Application Security Project (OWASP) Foundation works to improve the software security through various projects. It offers a Security Knowledge Framework, which is an expert system for applying the principles of secure coding in various programming languages [36]. It is based on the OWASP Application Security Verification Standard. It implements 4 phases of security research: defining the requirements for the project, defining security acceptance criteria, coding according to the established good security practices, testing according to the established requirements [36]. The testing is based on established security metrics and is conducted with the help of a wider range of specialists working on the project.

Similar to the W3C WCAG, OWASP defines a standard for mobile applications' security [37] and guidelines for testing mobile security [38]. Like WCAG, the OWASP mobile security standard sets out guidelines and principles for developing secure mobile applications. They are formed in two security verification levels and a set of reverse engineering resiliency requirements (RERR). The first level contains generic security requirements that are recommended for all mobile applications. Level two is aimed at

applying principles for handling highly sensitive data. RERR covers additional protection mechanisms that can be applied in the prevention of threats. Security verification is most fully accomplished when combining both levels with RERR. This ensures the security resiliency of the project.

The OWASP Mobile Security Guidelines are divided into three main sections: general guidelines, Android guidelines, iOS guidelines. The general guidelines provide explanations for the place of security testing in the life cycle of software development. Depending on the development methodology, different methods for testing the security of applications are applied. It can be performed sequentially or iteratively; in both cases a risk assessment must be performed for the individual components of the applications as well as for the entire applications. The application of security techniques accompanies the entire life cycle - from defining the requirements to testing and implementation. OWASP takes into account the importance of human resources, seeing them as one of the weak links of security [38]. We can find similarities with the sources cited above, which put human beings at the centre of development and take into account their individual characteristics. [38] also offers specific coding techniques to follow when developing Android and iOS applications.

The major developers of mobile operating systems Google and Apple also offer complete guides for creating secure mobile applications that take into account the specifics of their platforms. They summarize good practices, principles and a sample code that can be put into practice in real mobile projects. Apple offers a security framework that implements different levels of security (Fig. 2).

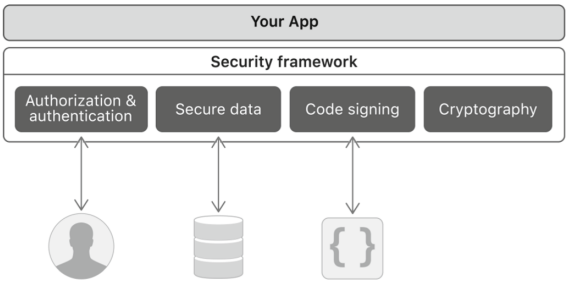

Fig. 2. iOS security framework by [39].

Authorization and Authentication, Secure Data, Secure Code, Cryptography and Result Codes [39]. They provide sample codes that can be used in iOS applications to increase security levels when performing: logging in, session management, network data exchange, malicious code isolation, encryption of user personal data, application security assessment.

Google's best practices for developing secure Android applications are similar to those of Apple. They are related to the security of user personal data, secure transmission over the Internet and storage of local devices, application of cryptographic techniques, user authentication, protection against malware [40].

Individual scientists and author teams study security in a specific context. Such are the developments in the field of m-learning [41, 42], finance [43], healthcare [44],

military training [45], machine learning [46], etc. Some also define frameworks [47] and general-purpose ecosystems [48]. Most of them are based on OWASP's mobile security projects and/or Apple's and Google's security guides. The ways of interaction with mobile devices, prevention of cyber-attacks and increase of security in data exchange are taken into account.

Based on the above mentioned, the main direction of the practical application of all frameworks, ecosystems, principles and standards can be outlined: user-oriented, a barrier-free digital experience, personal security.

3 Method

3.1 Material

Our research is aimed at defining a mobile research ecosystem for testing and evaluating secure and accessible mobile multi-device environments. In this regard, it is necessary to choose appropriate platforms for approbation of our approach. In particular, we used Android and iOS ones (Table 1).

Table 1. Specification of targeted mobile devices and platforms.

Characteristics	Device 1	Device 2
Operating System	iOS 14.7.1	Android 11
Device Brand	iPhone 12	Redmi Xiaomi Note 9
Year	2020	2020
CPU	Apple A14 Bionic six-core	Octa-core Max 2 GHz
RAM	4 GB	4 GB
Communication	Wi-Fi, Bluetooth, GPS, NFC, USB	Wi-Fi, Bluetooth, GPS, NFC, USB

Source: own elaboration

We would like to compare two different mobile platforms and the limitations that each of them imposes. On the first place, both devices were manufactured in 2020 with the same RAM capacity and the same hardware communication components. By specification, the main difference between the two stems from the technology used to develop the processor, which strongly affects the performance of the devices. According to tests, devices with Apple A14 Bionic processor are significantly more productive. According to some benchmark tests, Apple's CPU performance is much higher than Xiaomi's one – 93 overall scores versus 61 [49, 50]. Our research explored both platforms for passing the security and accessibility tests, including the overall performance point of view.

On the other hand, because of the platform-specific features each device security and accessibility were tested by different applications. Android accessibility is tested through Google Accessibility Scanner. As for the iOS accessibility testing, we used the Accessibility third-party tool. Security testing was performed by the following applications: MyTop Mobile Security (iOS) and WOT Security (Android).

The limitations of this paper are related to the versions of operating systems and hardware configurations of the devices used, as well as the accessibility and security testing software. We do not claim to be exhaustive of the types of devices and platforms. Our goal is put in practice the testing procedure described in Sect. 3.3.

3.2 Design

The study observes the following main factors: speed of testing; the number of security errors and the number of accessibility errors. These are the dependent variables. The independent variables are the mobile operating system of the devices and their hardware specifications.

3.3 Procedure

Based on the frameworks outlined in the previous two sections, we choose to follow an iterative procedure of exploring the security and availability of mobile applications. The procedure we followed consists of 5 phases: Define, Design, Test, Analysis and Implement (Fig. 3). They summarize the experiences of [25, 27, 28, 36]. We can define it as benchmarking approach too.

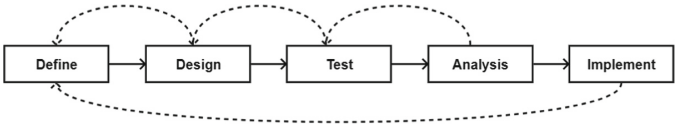

Fig. 3. Proposed benchmarking approach. Source: own elaboration.

- In the first phase - Define, the research of the project requirements is carried out, the peculiarities of the mobile platforms and the users who will use them are defined.
- In the second phase – Design, the project is planned, research questions, the metrics for success and milestones (if necessary) are determined. Possible metrics in accordance with the aim of the approach are: non-human traffic; mean time between failures; mean time to detect; mean time to acknowledge; mean time to contain identified attack vectors; mean time to resolve issue; mean time to recovery from error; security policy compliance; accessibility policy compliance; accessibility validation errors, etc. depending on the aim of the research. A weight of each of the metrics could be given to measure the overall accessibility and security level of mobile applications.
- In the third phase – Test, the testing of the security and accessibility of mobile platforms is performed according to the plan prepared at the previous stage.
- In the fourth phase – Analysis, an in-depth analysis of the test results is performed, a report with recommendations for improving security is formed.
- In the last phase – Implement, the recommendations from the report are put into practice.

If the recommendations cannot be implemented, the cycle is repeated until the recommendations are fully implemented in order to eliminate the weaknesses of the mobile platforms. The approach can be applied both at the application level and at the mobile platform level.

4 Results

In order to respond to RQ2, it is necessary to approbate our benchmark approach. Following the procedure described above, in the first phase, we determined that we would use Device 1 and Device 2 to perform our tests.

In the second phase of the research procedure, we defined the following metrics for test success: test speed, number of accessibility errors, number of security vulnerabilities. In the third phase of the procedure, we perform the tests of security and accessibility of the selected devices and platforms. More in-depth research should be done if specific problems are defined. Possible examples include: access by people with visual impairments to a specific mobile operating system or application; improving the security of banking mobile applications for people with visual or hearing impairments. In these situations, metrics and tests are adapted to the specifics of the problems. That is why in this paper the author's team only gives guidelines for performing a benchmark procedure without claiming to cover a wide range of cases.

Device 1 showed the following accessibility issues (Fig. 4).

Fig. 4. Device 1 accessibilities issues. Source: own elaboration.

There are mainly problems with the color scheme, contrast, size and thickening of the texts, sound alternatives to the interface elements for people with visual impairments; video alternatives for people with hearing impairments; assistive touch problems for people with motor disabilities.

Testing of Device 2 shows that it would create mainly problems for people with visual and motor impairments (Fig. 5). The problems with it are also with the colour scheme, text sizes, sound matching, touch and rotation problems, switch access.

Device 1 security testing shows that mainly network security and identity protection issues have been found (Fig. 6, on the left-hand side is MyTop Mobile Security). Only

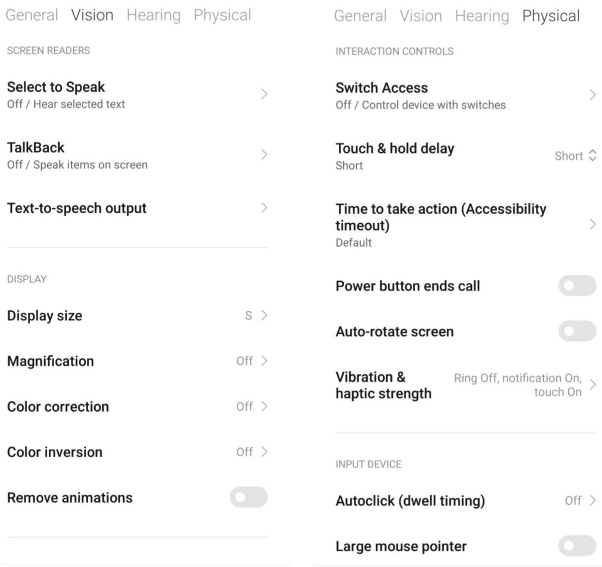

Fig. 5. Device 2 accessibilities issues. Source: own elaboration

one problem was found with Device 2 – Internet browsing protection (Fig. 6, on the right-hand side is WOT Security).

The test speed for both devices is fast:

- Device 1 accessibility test – 1 s.
- Device 2 accessibility test – 3 s.
- Device 1 security test – 10 s.
- Device 2 security test – 9 s.

As a result of the tests of the fourth phase of our proposed research procedure, an analysis of the accessibility and security of mobile applications or platforms is performed. It is also related to monitoring the success of the tests. The planned metrics are also taken into account. We observe the following results in terms of:

- Test speed: Device 1 is faster in performing accessibility tests, while Device 2 is faster in security testing. The differences are not significant, but it should be noted that the software used is different. This is also a prerequisite for the results of the speed of the tests to be accepted as conditional;
- Number of accessibility errors - 16 possible accessibility problems were found on both devices. In both types of tests, the software allows additional adjustments to be made to eliminate the detected problems. Both operating systems feature a wide range of settings for people with visual, hearing, motor and cognitive impairments. The specific features of the users also predetermine the settings of the accessibility of mobile devices;

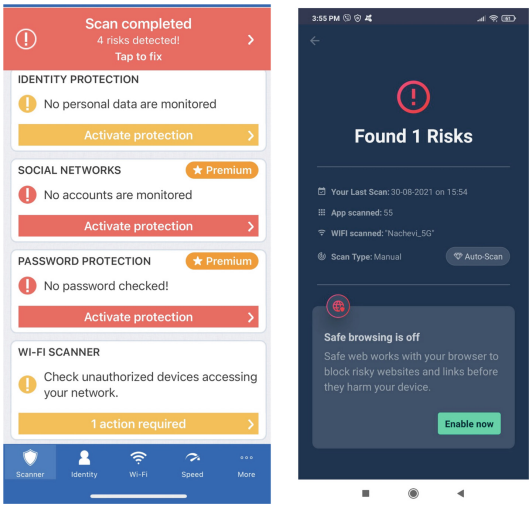

Fig. 6. Security issue of both devices. Source: own elaboration.

– Number of security vulnerabilities - in Device 1 4 security vulnerabilities were detected, while in Device 2 there is only one. As can be seen from Fig. 6, these are problems that can be solved by the user after raising awareness regarding cyber threats that may violate his privacy. Purely technical security breaches are established by testing the stability of the code to check for non-compliance with coding techniques.

5 Discussion

In view of the current paper's goal and the tests performed, we propose to unite the user expectations and experiences in a complete mobile research ecosystem for testing and evaluating secure and accessible mobile multi-device environments. It should meet some of the basic requirements set by the principles of user-oriented design [25], namely the active user participation and a functional design that meets their expectations. Activities related to the specification of: context of use, user and organizational requirements, the tools for developing product design solutions and the methods for evaluation of designs should also be defined. On the other hand, the security research phases proposed by the OWASP Application Security Verification Standard [36] should also be considered.

The study conducted in this paper gives us reason to propose a mobile research ecosystem (Fig. 7) that implements the procedure described in Sect. 3.3 and the features of mobile communication described in [48]. We need to keep in mind that there are limitations of interacting with individual devices in mobile contexts related to mobile multi-device environments [51]. These environments are a set of interacting devices that coordinate with each other. As stated in [52], more should be taken into account when defining such ecosystems: end-user privacy controls, self-regulation by platforms, legal regulation.

As a result of the first phase of the process, a summary report is generated for the individual characteristics of the users and the features of the tested platforms. For

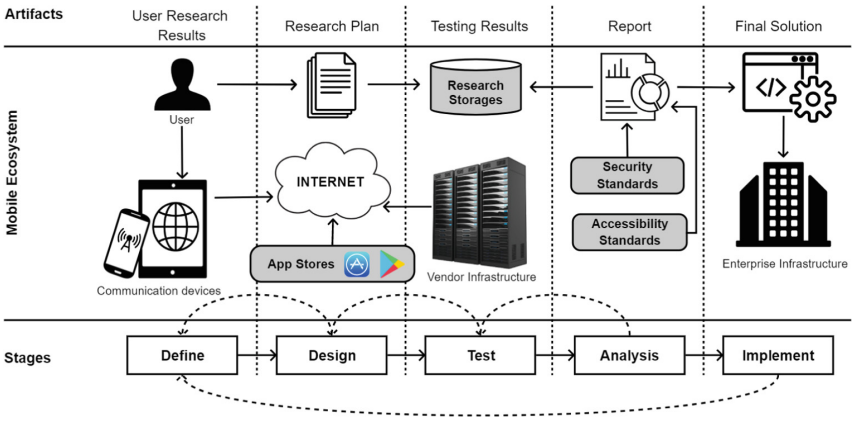

Fig. 7. Proposed mobile research ecosystem. Source: own elaboration.

example, type of disability, operating system. They provide a basis for preparing a study plan that provides guidance for conducting the design phase. As a result of the study of mobile accessibility and security, quantitative results are generated. For example, number of errors, internet speed and mobile connection. The result of the fourth phase is a report with recommendations for improving accessibility and security, and in the last phase - a working solution.

An important condition for the preparation of the reports is to comply with the standards for accessibility and security, which are formed by international organizations. Full coverage of the problems aims to achieve a better user experience.

6 Conclusions

As the capacity of mobile devices to process increasingly complex information increases, so do the requirements for the applications designed for them. As [53] points out, the mobile OS market is divided between Google Android and Apple iOS with respective market shares of roughly 70% and 30%. These two platforms also impose rules for the development of mobile applications, as well as much of the mobile ecosystem, including standards and applications. Development teams create a new generation of software in which users are placed at the centre of projects, and the products themselves must comply with the physical limitations imposed by devices and the specifics of the context of use, which changes frequently.

As a result of the research conducted in this paper, we can conclude that:

- accessibility is a context-sensitive concept that is determined by the individual needs of users;
- security issues are a prerequisite for restricting the personal freedom of people;
- availability and security testing of mobile platforms should be performed periodically in order to troubleshoot.

As a result of the experiments conducted in terms of security and accessibility of mobile platforms, as well as the definition of a mobile research system, we believe that we meet the goal of this paper. The need to apply the standards for accessibility and security, considered in the theoretical part, is taken into account. It is reflected that consumers are actively involved in the study of human-computer interaction in order to implement the principles of user-oriented design and development of digital technologies to help people.

We believe that in the future we can improve our proposed research procedure, which we can adapt to the specific needs of people with visual, hearing or motor impairments.

Acknowledgment. The study was supported by project NPI-36/2019 "Contemporary Approaches to The Integration of Mobile Technologies in Higher Education".

References

1. General Data Protection Regulation. https://gdpr-info.eu. Accessed 24 Aug 2021
2. McAfee ATR Threats Report. https://www.mcafee.com/enterprise/en-us/lp/threats-reports/apr-2021.html. Accessed 24 Aug 2021
3. Cybersecurity statistics and trends you need to know in 2021. https://us.norton.com/internetsecurity-emerging-threats-cyberthreat-trends-cybersecurity-threat-review.html. Accessed 24 Aug 2021
4. Number of detected malicious installation packages on mobile devices worldwide from 4th quarter 2015 to 1st quarter 2021. https://www.statista.com/statistics/653680/volume-of-detected-mobile-malware-packages. Accessed 24 Aug 2021
5. What systems have you seen infected by ransomware? https://www.statista.com/statistics/701020/major-operating-systems-targeted-by-ransomwar. Accessed 24 Aug 2021
6. Distribution of new mobile malware worldwide in 2020, by type. https://www.statista.com/statistics/653688/distribution-of-mobile-malware-type. Accessed 24 Aug 2021
7. Android Mobile Security Threats. https://www.kaspersky.com/resource-center/threats/mobile. Accessed 24 Aug 2021
8. Top Security Threats of Smartphones (2021). https://www.rd.com/article/mobile-security-threats/. Accessed 24 Aug 2021
9. Disability and health. https://www.who.int/en/news-room/fact-sheets/detail/disability-and-health. Accessed 24 Aug 2021
10. Fact sheet on Persons with Disabilities. https://www.un.org/disabilities/documents/toolaction/pwdfs.pdf. Accessed 24 Aug 2021
11. United Nation Inclusion Strategy. https://www.un.org/en/content/disabilitystrategy, Accessed 24 Aug 2021
12. The 17 Goals. https://sdgs.un.org/goals. Accessed 24 Aug 2021
13. Marinova, O.: Business intelligence and data warehouse programs in higher education institutions: current status and recommendations for improvement. Electron. J. Econ. Comput. Sci. **5**, 17–25 (2016)
14. Parusheva, S., Aleksandrova, Y., Petrov, P.: A study of the use of social media in higher education institutions in Bulgaria. In: 4th International Multidisciplinary Scientific Conferences on Social Sciences and Arts, SGEM 2017, Albena, vol. 1, pp. 19–26 (2017)
15. Todoranova, L.: E-learning at the University of Economics - Varna. In: Proceedings of Scientific Conference: TechCo - Lovech 2019, vol. 2, pp. 244–248 (2019)

16. Stoyanova, M., Vasilev, J., Cristescu, M.: Big data in property management. Applications of mathematics in engineering and economics. In: Proceedings of the 46th Conference on Applications of Mathematics in Engineering and Economics (AMEE 2020), vol. 2333, no. 1, pp. 070001-1–070001-7. American Institute of Physics (2021)
17. Armiyanova, M.: IoT problems and design patterns which are appropriate to solve them. In: Proceedings of the International Conference Information and Communication Technologies in Business and Education, pp. 291–305 (2019)
18. Bankov, B.: Software evaluation of PHP MVC web applications. In: Proceedings of 19 International Multidisciplinary Scientific Geoconference, SGEM 2019, vol. 19, no. 2.1, pp. 603–610 (2019)
19. Sulov, V.: Iteration vs recursion in introduction to programming classes: an empirical study. Cybern. Inf. Technol. **16**(4), 63–72 (2016)
20. Kuyumdzhiev, I.: Comparing backup and restore efficiency in MySQL, MS SQL server and MongoDB. In: Proceedings of 19 International Multidisciplinary Scientific Geoconference, SGEM, vol. 19, no. 2.1, pp. 167–174 (2019)
21. Antonova, K., Ivanova, P.: Emerging or changing occupational hazards at the workplace. In: International Academic Conferences: Proceedings of IAC 2018 in Vienna Management, Economics and Marketing (IAC-MEM 2018), pp. 350–355. Czech Technical University, Prague (2018)
22. Veleva, M.: Best practices as opportunities for leadership soft skills improvement in human resource management in Bulgarian tourism organizations the four-season hotels example. Izvestia J. Union Sci. Varna Econ. Sci. Ser. **9**(3), 63–71 (2020)
23. Koleva, V.: Labor needs of IT specialists in Bulgaria. East. Acad. J. **1**, 51–62 (2018)
24. Sirendi, R., Taveter, K.: Bringing service design thinking into the public sector to create proactive and user-friendly public services. In: Nah, F.F.-H., Tan, C.-H. (eds.) HCIBGO 2016, Part II. LNCS, vol. 9752, pp. 221–230. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-39399-5_21
25. International Organization for Standardization. Human-centred design processes for interactive systems (ISO 13407:1999(en)). https://www.iso.org/obp/ui/#iso:std:iso:13407:ed-1:v1:en. Accessed 24 Aug 2021
26. International Organization for Standardization. Ergonomics of human-system interaction — Part 210: Human-centred design for interactive systems (ISO 9241-210:2019(en)). https://www.iso.org/obp/ui/#iso:std:iso:9241:-210:ed-2:v1:en. Accessed 24 Aug 2021
27. Design Thinking 101. https://www.nngroup.com/articles/design-thinking/. Accessed 24 Aug 2021
28. Design Thinking. https://www.interaction-design.org/literature/topics/design-thinking. Accessed 29 Aug 2021
29. Mobile Accessibility: How WCAG 2.0 and Other W3C/WAI Guidelines Apply to Mobile. https://www.w3.org/TR/mobile-accessibility-mapping/. Accessed 29 Aug 2021
30. WCAG 2.0 Techniques that Apply to Mobile. https://www.w3.org/WAI/GL/mobile-a11y-tf/MobileTechniques/. Accessed 29 Aug 2021
31. ETSI. Accessibility requirements for ICT products and services (EN 301 549 v2.1.2). https://www.etsi.org/deliver/etsi_en/301500_301599/301549/02.01.02_60/en_301549v020102p.pdf. Accessed 29 Aug 2021
32. Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L2102&from=en. Accessed 29 Aug 2021
33. Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0882&from=EN. Accessed 29 Aug 2021

34. Developing for Accessibility. https://www.google.ca/accessibility/for-developers/. Accessed 29 Aug 2021
35. Accessibility on iOS. https://developer.apple.com/accessibility/ios/. Accessed 29 Aug 2021
36. OWASP Security Knowledge Framework. https://owasp.org/www-project-security-knowledge-framework/. Accessed 29 Aug 2021
37. Holguera, C., et al.: OWASP Mobile Application Security Verification Standard. OWASP Foundation (2021)
38. Mueller, B., et al.: OWASP Mobile Security Testing Guide. OWASP Foundation (2021)
39. iOS Security Framework. https://developer.apple.com/documentation/security. Accessed 29 Aug 2021
40. Android Developers Guides: Security. https://developer.android.com/topic/security/best-practices. Accessed 29 Aug 2021
41. Shonola, S., Joy, M.: Security framework for mobile learning environments. In: Proceedings of ICERI2014 Conference, pp. 3333–3342 (2014)
42. Mahalingam, S., et al.: Learners' ensemble based security conceptual model for m-learning system in Malaysian Higher Learning Institution. In: Proceedings of 10th International Conference Mobile Learning, pp. 335–338 (2014)
43. Ambore, S., et al.: A resilient cybersecurity framework for Mobile Financial Services (MFS). J. Cyber Secur. Technol. **1**(3–4), 202–224 (2017)
44. Srivastava, M., Thamilarasu, G.: MSF: a comprehensive security framework for mHealth applications. In: 2019 7th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), pp. 70–75 (2019)
45. Hatzivasilis, G., et al.: Modern aspects of cyber-security training and continuous adaptation of programmes to trainees. Appl. Sci. **10**, 5702 (2020)
46. Sagar, R., et al.: Applications in security and evasions in machine learning: a survey. Electronics **9**, 97 (2020)
47. Ding, C., et al.: A hybrid analysis-based approach to android malware family classification. Entropy **23**, 1009 (2021)
48. Mitrea, T., Borda, M.: Mobile security threats: a survey on protection and mitigation strategies. In: Proceedings of International Conference Knowledge-Based Organization, vol. 16, no. 3, pp. 131–135 (2020)
49. Apple A14 Bionic. https://nanoreview.net/en/soc/apple-a14-bionic. Accessed 23 Oct 2021
50. Xiaomi Redmi Note 9. https://nanoreview.net/en/phone/xiaomi-redmi-note-9. Accessed 23 Oct 2021
51. Grubert, J., et al.: Challenges in mobile multi-device ecosystems. mUX: J. Mob. User. Exp. **5**, 5 (2016)
52. Binns, R., et al.: Third party tracking in the mobile ecosystem. In: Proceedings of the 10th ACM Conference on Web Science, pp. 23–31 (2018)
53. Kim, J., et al.: The Value of Technology Releases in the Mobile App Ecosystem. The Economic Impact of Software Developer Kits. Data Catalyst (2021)