Hindawi
Mobile Information Systems
Volume 2020, Article ID 8828078, 15 pages
https://doi.org/10.1155/2020/8828078

Review Article

Mobile Security: Threats and Best Practices

Paweł Weichbroth[1] **and Łukasz Łysik**[2]

[1]*Gdansk University of Technology, Narutowicza 11/12, Gdansk, Poland*
[2]*Wroclaw University of Economics, Komandorska 118/120, Wroclaw, Poland*

Correspondence should be addressed to Paweł Weichbroth; pawel.s.weichbroth@gmail.com

Received 5 September 2020; Revised 12 November 2020; Accepted 27 November 2020; Published 7 December 2020

Academic Editor: Quanzhong Li

Communicating mobile security threats and best practices has become a central objective due to the ongoing discovery of new vulnerabilities of mobile devices. To cope with this overarching issue, the goal of this paper is to identify and analyze existing threats and best practices in the domain of mobile security. To this extent, we conducted a literature review based on a set of keywords. The obtained results concern recognizable threats and established best practices in the domain of mobile security. Afterwards, this outcome was put forward for consideration by mobile application users ($n = 167$) via a survey instrument. To this end, the results show high awareness of the threats and their countermeasures in the domain of mobile applications. While recognizing the risks associated with physical and social factors, the majority of respondents declared the use of built-in methods to mitigate the negative impact of malicious software and social-engineering scams. The study results contribute to the theory on mobile security through the identification and exploration of a variety of issues, regarding both threats and best practices. Besides this, this bulk of up-to-date knowledge has practical value which reflects in its applicability at both the individual and enterprise level. Moreover, at this point, we argue that understanding the factors affecting users' intentions and motivations to accept and use particular technologies is crucial to leverage the security of mobile applications. Therefore, future work will cover identifying and modeling users' perceptions of the security and usability of mobile applications.

1. Introduction

Recent years have shown a significant increase in the popularity and ubiquity of mobile devices among users all around the globe [1]. These devices, based on a specific operating system, enable users to install a vast variety of applications, commonly referred to as "apps," from online sources called markets: Apple App Store, and Google Play [2]. The aforementioned apps are the essence of smartphones, enriching their functionality and enhancing the everyday lives of their users. The app markets allow users to perform a quick search and installation of new apps, but at the same time, they are also a source of different kinds of malware disguised as normal apps. Nowadays, mobile devices are subject to a wide range of security challenges and malicious threats [3].

The mobile revolution has empowered and influenced users to move almost all of their everyday operations into the mobile environment and so-called mobile applications. Hence, we can observe rapid growth in the domains of both mobile developers and users. Mobile devices are treated by their users as very personal tools, mainly used to facilitate everyday operations, but they also serve to store very sensitive personal information [4].

Contemporary mobile applications are ubiquitous and very easy to install on almost every mobile operating system: iOS, Android, Windows phone, etc. As a result of aggressive competition among application providers, we can observe more and more advanced and customized applications appearing on the market, resolving complex problems. These applications profoundly change a user's behavior by facilitating their day-to-day transactions [5–8].

In recent years, mobile applications have had to face a wide variety of external and internal security threats [9–12]. To address this growing issue, both research studies and business organizations have developed and promoted best

practices to this extent. However, to the best of our knowledge, there are few (if any) comprehensive studies which diagnose the status of knowledge within this domain from these two antagonistic objectives. Therefore, the goal of this study is to identify and analyze security threats to mobile applications on the one hand and contemporary best practices on the other hand. Therefore, we put forward the three following research questions:

RQ1. What are the security threats to mobile applications?

RQ2. What are the best practices to protect mobile applications?

RQ3. Which best practices are in use and to what extent by mobile application users?

To answer RQ1 and RQ2, we performed a literature review based on a combination of the keywords "mobile application," "threat," and "best practice" in an electronic search with Google web search engine and Google Scholar. These two platforms promptly rose to become dominant providers of information and scholarly literature. While the former, in 2019, was a search engine leader worldwide, accounting for 88.5 percent of global market share [13], the latter is claimed to be the most comprehensive academic search engine, with 389 million records indexed [14]. A critical analysis of the existing empirical evidence and state-of-the-art studies obtained results which contribute to a new understanding of mobile security threats and best practices.

To answer RQ3, we conducted an anonymous survey and asked mobile application users to fill in a questionnaire which was divided into two parts, where the first directly referred to the subject of the research and the second collected demographic data. In total, we examined the responses from 167 users regarding their adoption of ten mobile security best practices by users in Poland. The findings revealed a relatively high adoption level of security practices applied against a wide range of cyberattack vectors. Taking this into account, our contribution details the current state of the existing and applied security techniques, reflecting users' attitudes toward mitigating (ignoring) risks and eliminating (neglecting) hazards regarding mobile application threats and vulnerabilities.

The rest of the paper is structured as follows. Section 2 presents the research background and motivation. Section 3 provides a summary of the identified mobile security threats, whereas Section 4, in the same manner, reviews the best practices. Section 5 shows a comprehensive report from the conducted survey. Section 6 presents general discussion, along with the theoretical and practical implications, as well as the study limitations and future work agenda. Finally, Section 7 concludes the paper.

2. Research Background and Motivation

Mobile technology is a phenomenon which is strongly rooted in our everyday activity. More often than not, we are dependent on different kinds of applications, both for leisure (instant messaging, booking, maps, etc.) and for business (online banking, e-mail management, business functions, etc.). Users install mobile apps and provide their personal information while rarely thinking about security issues.

According to many researchers, the most influential factors which help the spread of mobile technology among customers are as follows [15, 16]:

(i) Gaining access to information which is up to date: there is no more information asymmetry; instead, we can observe information democratization

(ii) Lower production costs, granted by the technology revolution: thus, products/services offered on the market are easier to deliver to the end consumer and, at the same time, more customized to meet individual requirements

(iii) Fast access to less biased market research: the personal character of mobile technology allows real-time information to be gathered about consumers based on their actual behavior

(iv) A shift from accessing only local markets to a global economy and digital channels, yet at the same time, thanks to the personal character of mobile technology, consumers may be accessed in a personalized way

(v) A shift from mass markets to personal, one-2-one relations

(vi) A shift from "on time" to "right now" mobile technology which allows communication, no matter what localization and time and, at the same time, with customization of information observed never before

The other aspect which has created what we can observe nowadays as a new phenomenon, i.e., mobile communication, is the immanent characteristic of mobile/handheld devices, which will be discussed further. Consumers have gained access to a wide array of tools at their fingertips. In Figures 1 and 2, we can observe the market trend in the proliferation of mobile phone subscriptions. According to the Ericsson Mobility Report [17], we can observe a growth in mobile subscriptions starting in 2015 and predicted to reach nearly 9 billion mobile subscriptions in 2025.

The aforementioned report also shows the rapid increase in our consumption of information and points to constant growth in the number of mobile subscriptions and even quicker growth in the number of mobile broadband subscriptions (mobile broadband includes radio access technologies: 3G, 4G, 5G, CDMA20000 EV-DO, TD-SCDMA, and Mobile WiMAX).

According to researchers and agencies, mobile computing is the phenomenon worth observing since our habits as consumers, a few of which are listed in the following and are radically changing [17–19]:

(i) Over 73%, depending on the age group, of all emails are opened on mobile devices

(ii) Already in 2017, around 95% of Facebook users accessed the social network via mobile devices

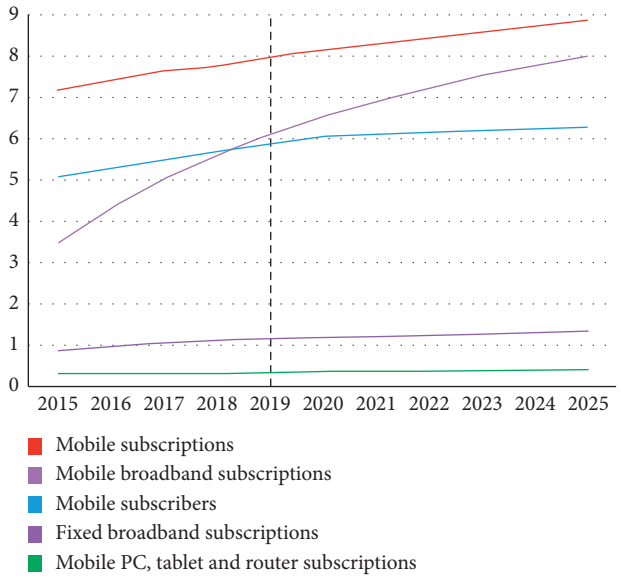

Figure 1: Global mobile subscriptions and subscribers (in billions) (source: [17]).

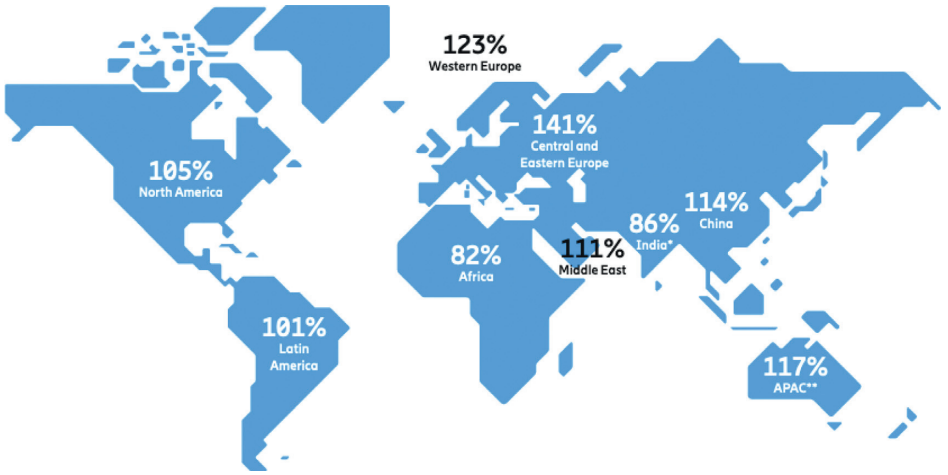

Figure 2: Subscription penetration Q3 2019 (percentage of the population) (source: [17]).

(iii) 80% of users used a mobile device to search the internet in 2019

(iv) 40% of online transactions are done using mobile devices

(v) More than 50% of websites now use responsive web design technologies that work for all devices

(vi) More than 75% of shoppers use mobile devices along with physical shopping

(vii) Global mobile data traffic is more than 30 exabytes per month

(viii) Mobile devices now account for half of the web traffic globally, and this grew 68% between Q3 2018 and Q3 2019

Our consumption of information is growing exponentially. We have, as users, changed our search and information consumption habits—we are able to search for information whenever and wherever we want, depending only on signal availability.

All these data suggest that users are gladly installing mobile apps on their mobile devices, and their mobile data consumption is growing. This trend is visible not only to developers, who are constantly trying to offer a smooth and convenient app experience, but also to all sorts of hackers, who are interested in obtaining personal information to use in a malicious way against the unaware user.

2.1. Usability and User Experience vs. Security. The main reference definition of usability in both desktop [20] and mobile settings [21] is given by the ISO 9241-11 norm, which states that usability is "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use." [22] More recently, user experience (UX) has

become a vital reference for studying human-computer interaction. By definition, UX is a "person's perceptions and responses resulting from the use and/or anticipated use of a product, system, or service," including "all the user's emotions, beliefs, preferences, perceptions, physical and psychological responses, behaviors, and accomplishments that occur before, during, and after use." [23]

Firstly, it can be noticed that none of the usability and user experience definitions include or point to security. Indeed, in the light of the results from our latest study [20], security is barely discussed in the area of product quality. On the contrary, security requirements typically impose barriers to users (such as passwords or other authentication mechanisms), while designers and developers attempt to minimize their impact on both application performance and user experience.

Secondly, security is a subject of study from two perspectives: technical and human factors [24]. The former focuses on the development of the systems, methods, and techniques which aim at mitigating risks associated with application code, user data, network traffic, and others, as well as, on the contrary, testing and evaluating existing mechanisms and solutions. The latter examines the relationships between security and factors such as design [25], ease of use [26], and human disabilities [27]. Therefore, we distinguish between security, which is generally a technical concern, and privacy, which is mostly a social concern. Naturally, these two notions are often related and interdependent.

Last but not least, it is frequently suggested [28] that "users are hopelessly lazy and unmotivated on security questions," while, on the contrary, they "perform an implicit cost/benefit calculation when deciding whether to follow security advice or not." There is no tradeoff established, which means that, in order to design and develop both usable and secure mobile applications, we must first understand user attitudes toward security and privacy. We address this issue in further reflection and discussion, hoping to engage researchers and practitioners in a broader dialogue to this extent.

3. Mobile Security Threats

Users of mobile devices or so-called mobile users are increasingly subject to malicious activity, mainly concerning pushing malware apps to smartphones, tablets, or other devices using a mobile OS. These handheld devices, carried in our pockets, are used to store and protect sensitive information. Even though Google and Apple offer distribution environments that are closed and controlled, users are still exposed to different kinds of attacks. A few of them are given in the following [29]:

(i) Phishing in an app: we observed that one way criminals can bypass the app market source code checks was not by including anything malicious in the app itself, but rather by making an app that, in essence, is a browser window to a phishing site. Such apps, in this case, are designed in tandem with the phishing site so that the user has a seamless experience.

(ii) Supply chain compromise: it was observed that a trojanized version of a legitimate app had been included in the factory firmware from a small mobile phone manufacturer and shipped to customers on brand new phones. The original app, called Sound Recorder, was found to have been modified to include code that was not part of its stated purpose: it could intercept and send SMS messages secretly. The malicious version of the app could have been inserted into the supply chain in a number of different places. It was never made available through any app store, but only in a specific firmware image on a specific model of an inexpensive Android phone.

(iii) Cryptominer code in games or utilities: we encountered a significant jump in the number of apps that, without notification to the user, included cryptominer code in the app. The code would run whether or not the app itself was running and functioned as a constant drain on the phone's (or other device's) battery.

(iv) Click-fraud advertising embedded in apps: advertisement fraud is, surprisingly, one of the most profitable criminal enterprises nowadays, and mobile apps appear to be a key part of this subtle crime. The advertising industry estimates that, today, the cost to advertisers of fraudulently "clicked" ads, according to data published by the World Federation of Advertisers, tops US $19 billion each year.

According to Landmann [30], the unprecedented growth in the number of smartphones and mobile workers has a direct impact on the number of attacks deployed on mobile devices. Smartphones today store hefty amounts of data and operate over international cellular networks, WLANs, and Bluetooth PANs. They run a diverse set of complex operating systems such as Symbian, iOS, BlackBerry OS, Android, and Windows Mobile. Most smartphones also support the Java platform for mobile devices, J2ME, with a variety of extensions. All this network connectivity and diverse rich code makes these devices more vulnerable than traditional PCs, which typically run standard operating systems for which many security products are readily available [31].

It is also crucial to mention top 10 web application security risks according to the most prominent security community worldwide named OWASP Foundation. Mitigation of these threats would be the first step in the production of secure code of mobile apps [32]:

(i) Injection
(ii) Broken Authentication
(iii) Sensitive Data Exposure
(iv) XML External Entities (XXE)
(v) Broken Access Control
(vi) Security Misconfiguration

(vii) Cross-Site Scripting XSS

(viii) Insecure Deserialization

(ix) Using Components with Known Vulnerabilities

(x) Insufficient Logging & Monitoring

Conventional viruses have not been the major threat to smartphones that they have to PCs. More often, the threat is simply rogue code or malfunctioning applications that are not addressed by antivirus vendors focused on the more virulent and easily detectable PC viruses [30]. A threat also exists from lost/stolen devices or accidental/malicious misuse by end users. Administrators often cannot remotely audit the content of smartphones as mandated in the International Organization for Standardization (ISO) 27001 security requirements. They frequently do not know what information has been stored on a phone and may not be able to remotely delete data or "kill" the device [33].

The worldwide information security market is forecast to reach $170.4 billion in 2022 [34]; the most frequent mobile threats include the following [30, 35–38]:

(i) Data leakage: 71% of breaches were motivated by financial aspect and 25% by espionage

(ii) Malware or malicious software: among most malicious e-mail attachments are .doc and .dot which make 37%, and the second highest is .exe

(iii) Phishing and social engineering: 62% of business experienced this type of attack in 2018

(iv) Direct hacker attack: data breaches exposed 4.1 billion records in the first half of 2019

(v) Intercepting communication: hackers globally attack every 39 seconds which makes, on average, 2244 times per day

(vi) Stolen and lost phones: by 2020, the estimated number of passwords used by users will grow to 3000 billion

(vii) User behavior: 64% of Americans have never checked to see if they were affected by data breach

3.1. Malware. Smartphones are quickly approaching PC capabilities, and the same incentives exist for hackers: fraud, stealing personal and business information, and extortion—hackers are poised for the attack, with many different avenues available to spread malware [35]. The following brief review of smartphone malware shows that the malicious capabilities of hackers have been clearly demonstrated; these are just some of the malware threats listed in the report by MobileIron [39, 40]:

(i) Android GMBot—spyware, usually from third-party app stores, which tries to trick users into giving up their bank credentials

(ii) AceDeceiver iOS malware—malware that works to steal a user's Apple ID

(iii) Marcher Android malware—malware that pretends to be a bank website in the hope that users will give up their login credentials

(iv) Backdoor families—distributed via Google Play Store as trojanized apps hidden within different types of applications

(v) Mobile miners—distributed via spam e-mail or SMS, an application which uses processing powers of mobile devices

(vi) Fake applications—a malware category of apps that mimics popular and useful applications, once installed asks the user for mobile verification or redirects to a link with instructions

Last but not least, applications and the given OS should be kept up to date to maximize their protection, and running an antimalware app is also recommended.

3.2. Phishing and Social Engineering. The main platform for phishing attacks is spam emails, which are sent out in mass quantities by cybercriminals. Recently, we have witnessed a new form of phishing, which is using SMS text messaging (so-called "smishing") to send a fraudulent link to a mobile device. Social media are also used by hackers to take advantage of mobile phone users.

This type of attack is aimed at users directly, most frequently exploiting human psychology rather than using technical hacking techniques. This aims to [41]

(i) make money from a small percentage of recipients who actually respond to the message

(ii) run phishing scams—in order to obtain passwords, credit card numbers, bank account details, and more

(iii) spread malicious code onto recipients' devices

Protection against this type of attack is common sense based and concerns mainly not responding to dubious messages, keeping applications up to date, etc. [42].

3.3. Direct Hacker Attack and Intercepting Communication. Contemporary users have access to sophisticated mobile devices which are part of their everyday lives, and this directly leads to an increase in the number of users. This rapid growth in users entices hackers to either intercept communication or directly attack mobile devices.

According to Bishop, there are three prime targets for hackers [43]:

(i) Data—mobile devices store data and may contain sensitive data of all types

(ii) Identity—mobile devices are customizable, so it is easy to associate a device with a specific person, so stolen identity may be used to commit other offenses

(iii) Availability—limiting access to a device or even depriving the owner of its use

Intercepting communication concerns a situation in which 2 mobile devices are communicating, usually via a public LAN—the users believe they are in direct communication. This interception of communication is called a man-in-the-middle attack (MITM); the perpetrator redirects the data route, either eavesdropping or impersonating one of the parties, to steal personal data. To prevent this type of attack, users should

(i) avoid public Wi-Fi or nonpassword-protected connections

(ii) pay attention to notifications in their browser

(iii) conduct sensitive transactions via secure connections

Taking into consideration the above rules, the user of a mobile device significantly reduces the likelihood of the interception of communication and the loss of sensitive data.

3.4. Stolen and Lost Phones. Mobile phones are considered to be personal devices on which users store lots of different types of data, either personal or business. Table 1 presents device loss case types. According to the research [42], mobile device users, most frequently, simply lose their devices.

Mobile device owners are themselves the greatest threat when it comes to losing sensitive data, yet, at the same time, their proper behavior can help protect such data. Implementing 2FA (two-factor authentication), avoiding automatic logins, and using password-lock applications can minimize the probability of losing sensitive data.

When the general public and the media picture the greatest threats to the loss of mobile devices, they usually depict muggers and pickpockets as the main suspects, while according to the research [41], users are twice as likely to lose their device (69%) than have it stolen (31%).

3.5. User Behavior. Mobile device users often create vulnerabilities due to the blurred line dividing personal and business use. Some of the blameworthy behaviors include turning off all types of security apps, downloading apps from third-party application stores, and sharing confidential information with unauthorized recipients. With smartphones, it becomes even easier to obtain sought-after information. Controlling user behavior is considered to be one of the greatest challenges in mobile device security [30].

Among the practices which are helpful to organize procedures regarding user behavior security issues, we can point to security awareness training [44], providing detailed information about the latest online fraud techniques [45], and reviewing existing security procedures [46]. One may also consider the adoption of collaborative games which, by design, stimulate creative thinking [47, 48] and therefore serve as effective learning tools [49].

4. Mobile Security Best Practices

Mobile security best practices are recommended guidelines and safeguards for protecting mobile devices and users' data [50]. In general, hardware and software vendors outline and promote procedures and instructions which, properly applied, should maintain or increase the security level. Although there is no way to 100 percent guarantee security, as unforeseen vulnerabilities can be discovered and exploited by attackers, let us take a look at some recently developed best practices for mobile devices and applications [51–55].

(1) Make user authentication the highest priority: most mobile devices can be locked with a screen lock and unlocked with a password, biometric (e.g., fingerprint and face recognition) or personal identification number (PIN) [56]. Nowadays, multifactor authentication is considered as the best practice to protect user's data [57]. On the contrary, security is entirely based on password complexity and the user's attention to its confidentiality.

(2) Update mobile operating systems and on-board applications with security patches: keeping the operating system (Android and iOS) and the installed applications up to date is a must. Both Google and Apple provide regular updates to users, which resolve recent vulnerabilities or other threats, as well as sharing additional performance and security features [58]. However, updating an app is a two-edged sword since a new release can decrease its overall performance and the user's productivity. From a security perspective, updates can trigger the revetting process to confirm security clearance. In order to ensure that a mobile application conforms to an organization's security requirements and is free from vulnerabilities, a series of rigorous and comprehensive analyses take place. One has to keep in mind that app vetting might also include updated external components (e.g., third-party libraries) and new mandatory versions of the operating systems.

(3) Back up user data on a regular basis: backing up is a basic method of preventing data loss or deletion. A backup schedule should be adapted to an increase in data over time. Examples of user data include individual user files (documents and spreadsheets), media files (e.g., pictures and videos), contacts, and other sensitive data [59]. In case of mobile devices, the obvious choice is a remote backup, which means copying and storing files in a private or public cloud. However, the main concern in this case is the transfer speed. Even if a high-speed connection is used to send the data, the upload limitations, antivirus scanners, and firewalls can slow down the speed considerably. Another limitation concerns

the cost of data uploading set by mobile internet providers. On the contrary, there is no guarantee that data stored in the cloud will be kept private. However, this can be easily overcome and most recommends that data files be encrypted which in turn might extend the overall backup task duration, if performed on the fly.

(4) Utilize encryption: data encryption translates data into another form, or code, so that only authorized parties can decrypt and read these data. The encryption feature is used for data stored on the mobile device as well as for data transmission over the network. Nevertheless, by default, encryption requires a password to encrypt and decrypt data files. If one forgets the password, the data recovery is usually problematic and not always successful. On the contrary, relying on the publicly available solutions could simply lull a user into a false sense of irrefutable security. Moreover, it is also strongly advised not to connect to and use a public and insecure Wi-Fi spot without using a secure transmission option such as a virtual private network (VPN) [60]. In this case, compared to regular internet connections, VPNs are still almost invariably slower, depending on the distance between the server and the client, the current server load, and the encryption level applied.

(5) Enable remote data wipe: in case a user has their device with sensitive data stolen and there is little chance of retrieving them in a relatively short period of time, one should consider turning on the device capability which allows a factory reset message to be remotely executed [59, 61]. Furthermore, remote data wipe is imperative in case of termination of employment or contracting a malware infection which cannot be uninstalled or deleted. While the existing solutions have clear advantages, they are not cure-all for mobile security. For instance, while some tools erase only part of the data, others erase the entire content, including applications and personal data. Therefore, one should consider deploying a secure container which, by design, separates the applications from personal data, enabling selective erasure in case of a security incident. Moreover, a proactive approach that tracks the use of sensitive data will improve security by early detection and prevention of its misuse or theft.

(6) Disable Bluetooth and Wi-Fi when not needed: minimizing both Bluetooth and Wi-Fi usage reduces exposure to having vulnerabilities exploited, although the flaws are not in these standards, but in their implementations [62]. Here, it should be noticed that the disabling action requires an intentional interaction from a user. However, there are tools (e.g., Auto-Bluetooth) that turn Bluetooth on or off without any user interaction, based on the rules defined by a user.

Table 1: Types of theft and loss by frequency (source: [42]).

Type of theft or loss	Frequency (%)
Misplaced	69.12
Pickpocketed	10.98
Home invasion	7.60
Robbery	6.76
Car break-in	2.77
Business break-in	2.77

(7) Be aware of social engineering techniques: social engineering is a term that encompasses a broad spectrum of malicious activity such as phishing, pretexting, baiting, quid pro quo, and tailgating ("piggybacking"). With this human-centric focus in mind, it is up to a user to be aware of malicious "actors" who engage in social engineering attacks hunting for human greed and ignorance [59, 63]. Organizations, in particular security analysts, might also consider conducting social engineering penetration tests (also known as social pen testing) among employees. By design, social pen testing is the practice of applying social engineering scams on an organization's employees to evaluate their capability to provide sensitive information. Such an assessment is beneficial by providing a real attestation on the level of adherence to the company's security policies by particular individuals.

(8) Be sure not to jailbreak your device: jailbreaking is a privilege escalation with the aim of removing software restrictions imposed by the device manufacturer. In other words, deploying a series of kernel patches permits a root access which allows software, not available and distributed via the app store, to be installed. Jailbreaking can seriously expose an operating system to additional vulnerabilities, effectively exploited by attackers [59, 64]. One should also keep in mind that, in case of removing manufacturer restrictions, the device's warranty will most likely be voided. Moreover, a decrease of overall system stability might occur since buggy apps tend to utilize substantial amounts of hardware resources.

(9) Be sure not to grant unnecessary permissions to applications: app permissions are the privileges an app has—like being able to access peripherals such as the camera, contact list, or location. Current versions of operating systems come in a variety of flavors depending on the manufacturer. The major tenet is to grant only those permissions that are necessary for the application to work properly. In other words, a user should always employ the principle of least privilege (PoLP) [65]. On the contrary, granted permissions can be described as the keys that unlock the app's functionality. Therefore, a good design pins runtime permissions with specific actions and tasks, which justify the permission requests.

(10) Install mobile security and antivirus applications: since there is no additional protection by default, mobile security and antivirus real-time scanners safeguard against malicious applications and viruses, as well as identify theft, ransomware, and cryptominers. Moreover, some tools can also scan URLs and block dangerous sites, monitor links in text messages, and provide parental control [59, 66]. There is no doubt that experts highly recommend using such tools, but nothing comes for free. In their case, the side effects refer to additional hardware resource allocation and increased battery drain due to the processes executed in the background.

Naturally, following these ten best practices will not 100 percent guarantee mobile device security; however, it will leverage the security level by reducing the attack vector and lowering the risk of system outages and malformed requests.

5. The Survey Report

The data for this study were collected by using the survey instrument since our intention was to formulate a relevant answer for the third research question. We selected this type of research method for three reasons: first, due to the descriptive nature of the question, which simply aims to describe the variables intended to be measured. Second, the survey is claimed to be a good instrument for obtaining empirical descriptions about people's attitudes and opinions [67]. Third, our target respondents were geographically dispersed and working at home because of the restrictions in force due to the COVID-19 epidemic.

5.1. Design and Settings. The survey consisted of two parts. The first part included ten questions that addressed the best practice usage by the mobile application users. The second part, including five questions, aimed at collecting demographic data (gender and age), as well as the level of education, professional experience (in years), and the sector of professional activity (also in years). We used Google Forms to collect the data since they have the benefits of being user-friendly and free of charge.

The self-administered, anonymous form was disseminated by e-mail among mobile application users and published on forum groups available for students of the Gdańsk University of Technology (GUT) and the Wroclaw University of Economics (UE). Therefore, we applied convenience sampling, a nonprobability sampling, where members are willing to voluntarily participate in a study.

Before the final launch, the draft questionnaire was independently reviewed by three experts to ensure content reliability and validity. In particular, the evaluation aimed to assess the accuracy of the measurement scales (reliability) and to appraise the degree to which the scale measures what it is intended to measure (validity).

The survey was launched on 1st May and closed on 19th May 2020. Afterwards, the primary dataset was further processed in a spreadsheet editor that let us perform the necessary calculations and operations such as data aggregation, comparison, and visualization.

5.2. Respondents. In total, during the period of twenty days, we collected data from 167 respondents, of whom 63.5% (106) were male and 36.5% (61) were female. The age distribution shows that the majority (77%) were aged 20–29 years, 17.8% were aged 30 or more, and only 5.3% were 19 or under. Therefore, 59.9% of the respondents declared secondary education, whereas the rest (40.1%) had graduate degrees. The distribution of professional experience was relatively low, which is reasonable given the respondents' ages: 65.3% declared having two years or less, while the remainder (34.7%) could be said to have moderate professional experience. A summary of the demographic data is given in Table 2.

Finally, we would like to highlight the survey's diversity, as it broadly involved a wide range of respondents who not only represent the IT sector but also others. It is worth noting here that a more diverse sample brings the promise of less bias [68].

5.3. Findings and Discussion. As the data are quantitative in nature, each individual best practice, along with the findings and discussion, has been combined to complement and enrich argumentation driven by numerical data. Hence, the review and analysis of the existing knowledge in the field resulted in the qualitative information. We argue that the applied mixed-methods approach brings added value by highlighting other related issues which were not directly included in the survey question pool.

Q1. Which authentication method do you use to secure your smartphone?

(i) Fingerprint scanner: 53.3% (89)
(ii) PIN: 12.6% (21)
(iii) Pattern lock: 12% (20)
(iv) Facial recognition: 10.2% (17)
(v) Password: 4.8% (8)
(vi) Iris scanner: 1.2% (2)
(vii) None: 6% (10)

Over half of the respondents (53.3%) have declared using the fingerprint scanner method to recognizing their identity. The second most frequent (12.6%) authentication method was based on a PIN, which is relatively strong, as a typical four-digit option provides 10^4 possible combinations. Twelve percent of the users used a pattern lock method that relies on a preselected pattern on a grid of dots to unlock the mobile device. The second biometric method, namely, facial recognition, also based on "who the user is," was claimed to be used by over ten percent (10.2%) of the users. The "old standby" password was rarely used, as only 4.8% of users pointed to this method. Last but not least, iris scanning, with the angle and distance guided by on-screen feedback, was very rarely used (1.2%) by the users.

It is worth noting here that particular biometric methods are mandatory to use mobile applications that require a

higher level of security such as mobile banking (m-banking), online payments, and online financial transactions [69]. In addition, biometric methods are easy to use since users do not have to remember a PIN, pattern, or password. Moreover, since the PIN-, pattern-, and password-based security methods fail to address the requirements of the restricted and highly sensitive data in mobile applications, voice recognition systems are currently more often being implemented in a wide range of mobile services [70]. Obviously, an attack on voice is feasible since such systems can be deceived if an attacker records the user's voice and plays it back during the authentication time window [71].

Q2. Do you update the mobile applications installed on your mobile device?

(i) Yes, but at a convenient time for me (e.g., Wi-Fi availability): 50.9% (85).
(ii) Yes, immediately after being informed by the relevant notification: 21% (35).
(iii) Updates are automatically installed: 21% (35).
(iv) No. I intentionally block all updates: 5.4% (9).
(v) I do not know: 1.8% (3).

The vast majority of users (92.9%) declared to have their mobile applications updated, whereas 71.9% consciously granted the permission to the app update process. Notably, over five percent of users pointed to invoking the update process. A very small percentage (1.8%) was not able to give an answer.

The reasons for keeping the apps up to date might include expecting new features, as well as benefiting from performance improvements, and fixing to errors and security vulnerabilities [72]. Moreover, a developer can set up the priority for each update, considering three different types: low, medium, or high.

Q3. Do you perform backups of the app data collected on your smartphone?

(i) Yes, data backups are automatically performed: 47.3% (79)
(ii) Yes, I manually perform data backups: 19.2% (32)
(iii) No: 31.1% (52)
(iv) I do not know: 2.4% (4)

Almost two-thirds (66.5%) of respondents declared having data backups performed, either automatically (47.3%) or manually (19.2%). On the contrary, almost one-third (31.1%) neglected data backup as part of mobile device maintenance. The vast minority is not aware of the status of their data backups.

Here, another question arises, which (unfortunately) was not included in the survey: what do you back up? An undeniable approach is to copy everything, in particular user-generated content, such as documents, images, videos, and other content. On the contrary, a user may also consider backing up setting data to preserve their personalized preferences if their data are restored on a new device [73].

Q4. Do you use data encryption on your smartphone?

(i) Yes: 24% (40)

Table 2: Demographic profiles of the respondents.

Demographic variables	Frequency	Percentage (%)
Gender		
Male	106	63.5
Female	61	36.5
Age (x)		
$x < 20$	11	5.3
$20 \leq x < 30$	136	77.0
$x \geq 30$	20	17.8
Education		
Primary	0	0.0
Secondary	100	59.9
High	67	40.1
Experience in years (y)		
$y < 3$	109	65.3
$3 \leq y < 6$	30	18.0
$y \geq 6$	28	16.7
Sector		
IT	59	36.0
Non-IT	46	28.0
N/A	59	36.0

(ii) No: 50.3% (84)
(iii) I do not know: 25.7% (43)

Less than a quarter of the respondents admitted to using data encryption on their smartphones. On the contrary, over a half acknowledged not enabling any available feature or third-party app to encrypt data. Interestingly, over a quarter of users are not aware of the status of the data collected on their smartphones.

A Contractor Magazine forecast [74] that, in 2019, mobile platforms would be the largest cybersecurity threat turn out to be correct [75]. Moreover, infections from both Mac App Store and Google Play continue to increase. According to Hodge [76], for years, iOS has kept "an iron grip on its reputation as the most secure mobile operating system." However, the upcoming Android 11 shows Google's efforts focused around privacy features. Nevertheless, on iOS, drive encryption is a standard, while Android users must enable this feature [77].

Q5. Are you aware of the remote data wipe feature in your smartphone?

(i) Yes: 81.4% (136)
(ii) No: 18.6% (31)

More than three quarters of respondents (81.4%) are aware of the remote data wipe feature, available to use in the case of device loss (theft). On the contrary, the rest (18.6%) declared to be unaware.

By design, remote data wipe allows users to remotely delete data by sending a wipe command to the device through SMS or the internet. Other studies show differences in the extent of this awareness. In 2015, over forty percent of surveyed users (42.27%) based in the United Kingdom, when asked about the adoption of physical security controls in smartphones, declared using remote data wipe [78]. However, four years earlier, the results from another survey show that, in Greece, the adoption of preinstalled security controls

was poor. For example, remote data wipe was used by only 15.1 percent of the users [79].

Q6. Do you intentionally disable/enable Bluetooth or Wi-Fi on your smartphone?

(i) Yes: 85% (142)

(ii) No: 4.8% (8)

(iii) Occasionally, but I do not consider it as a habit: 10.2% (17)

The majority of the respondents (85%) intentionally used the Bluetooth and Wi-Fi settings, disabling or enabling these features according to the situation. Only 10.2% of the respondents switch on or off Bluetooth or Wi-Fi occasionally while not considering it as a habit. According to the survey, 4.8% declared they do not disable/enable the Bluetooth or Wi-Fi features.

According to the FCC (Federal Communication Commission) [80], both Wi-Fi networks and Bluetooth connections can be vulnerable points of access for data or identity theft. When transmitting sensitive information via Wi-Fi, it is recommended to use the cell phone's data plan instead of public networks. Turning Bluetooth off when not in use protects the device from being "visible" and therefore hacked. Additionally, turning off both these features guarantees longer battery life.

Q7. What is your knowledge regarding social engineering techniques?

(i) I have basic knowledge: 46.7% (78)

(ii) I have intermediate knowledge: 29.9% (50)

(iii) I have advanced knowledge: 9.6% (16)

(iv) I do not know: 13.8% (23)

Among the respondents, almost half (46.7%) declared they have basic knowledge regarding social engineering, 29.9% declared they have an intermediate level of knowledge, and 9.6% considered themselves advanced in the field.

The number of social engineering attacks is growing rapidly to weaken the cybersecurity chain, and they mainly aim at manipulating individuals and enterprises to divulge valuable and sensitive data [81]. Humans are more likely to trust other humans compared to computers or technology; therefore, they are the weakest link in the security chain [82]. The aforementioned is the reason why it is so important to educate users about what precautions they can take in order to protect their sensitive data. Finally, according to a study done by US telco Verizon [83], among 41,868 security incidents recorded, 33% concerned social attacks.

Q8. Have you ever used the root account on your smartphone?

(i) Yes: 32.3% (54)

(ii) No: 67.7 (113)

Over two-thirds (67.7%) claimed to use the root account, while the rest (32.3%) have never taken advantage of the root account on their smartphones.

As we can observe, mobile users are becoming more and more aware of technical gimmicks concerning their devices that can enhance their device speed, look and feel, and functionality. On the contrary, manufacturers do not want users to make modifications that could result in accidents beyond repair. It is noteworthy that rooted devices are more susceptible to attacks, especially iOS devices. In 2015, a piece of malware, known as KeyRaider, infected 225,000 iPhones, stealing personal data [84]. In case of Google, its app market does not allow users with rooted devices to download particular mobile applications [85].

Q9. Do you verify the permissions (e.g., GPS, camera, and microphone) requested by apps?

(i) Yes, I verify them all: 49.1% (82)

(ii) It depends on my familiarity with application: 44.3% (74)

(iii) Hard to say: 5.4% (9)

(iv) No: 1.2% (2)

Almost half of the respondents (49.1%) declared verifying all the permissions which apps notify to require. Over forty percent (44.3%) stated that they verify the requests based on the level of the application familiarity. Only 1.2% were not interested in checking the permissions granted to an application. Finally, over five percent (5.4%) were also not fully aware or willing to acknowledge their actions in this extent.

This type of permission usually pops up during the first use of the given application accordingly to gain access to the built-in hardware devices or data folders. These permissions exist to protect the smartphone resources against unauthorized access. Overprivileged applications introduce security threats to the mobile device ecosystem and pose various reputational risks to online markets such as the Android marketplace [86]. A study from 2016 demonstrated that users, in general, make the consistent choice to willingly grant access by default [87].

Q10. Which of the following safeguard apps have you installed on your smartphone?

(i) Antivirus: 27.5% (46)

(ii) Firewall: 10.2% (17)

(iii) None of the above: 47.9% (80)

(iv) I do not know: 12.0% (20)

(v) Others: 2.4% (4)

Over a quarter (27.5%) of respondents claimed to have antivirus software installed on their smartphones. A further ten percent (10.2%) added an extra layer of protection by using a firewall. However, almost a half (47.9%) stated that neither antivirus nor firewall software was currently in use, but 2.4% stated using other, undisclosed software. Interestingly, twelve percent did not actually recognize any safeguard apps being operational on a daily basis.

The experts argue that having antivirus software installed on smartphones is essential [88–90]. Indeed, mobile security apps offer protection with a raft of features including antitheft, antimalware capabilities, as well as real-time protection for web browsers, remote localization detection, and

lockdown features. An interesting one is the so-called autopilot, which is capable of making intelligent recommendations for security actions depending on the type of the operating system and frequent usage patterns.

Thinking in terms of security, mobile operating systems work differently than their desktop equivalents. In practice, it means that a user does not need to install a firewall on their mobile device to the same extent as on their PC. Due to its built-in power management functions, a mobile device is not constantly "open for traffic," and the risk of being attacked and hacked is greatly mitigated. However, over time, one can notice that more and more apps are demanding a permanent connection [91, 92].

Using a VPN client is a gateway to quickly add an extra layer of security to any network device, essentially including mobile computing. A VPN is also an answer to users' requests to maintain their online confidentiality and protect their online activities. In other words, at a basic level, VPN technology provides two major benefits [93]: privacy and security. The former concerns "hiding" the IP address, location, and browsing history, while the latter is associated with using an encrypted layered tunneling protocol. VPNs can also grant access to blocked websites. According to a Global Market Insights report from 2018, the cloud VPN market was worth $18 billion at that time and is projected to hit the $54 billion mark by 2024 [94].

6. Discussion

This is a follow-up study of an earlier and similar research regarding mobile security [3, 95–98]. We agree with Gkioulos et al. [95] in the area of security on contemporary mobile devices since both studies reveal that users, in general, tend to have increased confidence in their abilities to protect their mobile devices. However, we argue increased alertness when possible threats are common knowledge, or they become apparent for users. Yet, users remain unaware of specific risks and also of the available countermeasures which could significantly improve their security. Similar observations also concern the behavior of users who tend to prioritize access to particular applications over the security issues.

Amin et al. [96] proposed an automated procedure of vulnerability detection in mobile (Android-based) applications. The results achieved in the aforementioned research have a complementary nature to those presented in their study since the authors focus on the development of an automated model of finding flaws in mobile apps. What those investigations have in common are the aspects they focus on, which is detecting security threats, in general. Nevertheless, what separates them is that, in Amin et al.'s study [96], the main emphasis is put on the technological aspect of security issues, and it is based on the run-time behavior of an application. At the same time, the focus of our study is on the analysis of actual users' behavior and habits declared and collected via a questionnaire.

Mavoungou et al. [3], in their analysis, focused on vulnerabilities and attacks on mobile networks, which represent a significant concern for their security and performance. The study focuses on drawing an inventory of attacks while categorizing and classifying them with a strong focus on attacks based on IP, signaling, and jamming. Besides the proposed classification of threats, the authors suggested adequate countermeasures and mitigation solutions. Among the many discussed vulnerabilities, they also indicated a compromised mobile device, application security, and imperiled user identity confidentiality as those of high importance. Their study is a technically focused categorization of the possible dangers to the mobile network operator. However, it has corresponding value to that presented in this paper since the explosion of the number of mobile users/subscribers and their security habits influence the overall mobile security level.

Valcke [97] put forward a general examination of the banking sector and its flaws in the context of mobile security. Cybercriminals are targeting financial institutions via their mobile apps, which are gateways for different types of security abuse. The author advocates putting more emphasis on enhancing client-side protection (a variety of login methods), strengthening the security of the client-server communication, and being proactive with fraud prevention. Besides the stated security challenges, Valcke underlines the role of app developers who should pay close attention to the security aspect of mobile apps, while, at the same time, respecting user experience guidelines [95]. The similarities in these two studies concern user behavior as one of the essential factors of mobile security. A perfect summary of the article is the authors' statement: "You still have to balance security with ease of use, and you still have to ensure that your core business logic is not subject to any exploits too." [3]

Hatamian [98], in his paper, focused mainly on app developers as the first line of defense against frauds, threats, and attacks aimed at mobile users. The author proposes "a privacy and security design guide catalogue for app developers to assist them in understanding and adopting the most relevant privacy and security principles in the context of smartphone apps." [98] At the same time, the author points to the developers as those responsible for fulfilling privacy and security principles, making them an important factor in preserving mobile security guidelines.

By design, mobile devices tend to be relatively small which makes them easily misplaced or lost. Therefore, one should also take into account the physical security that currently is a major concern for mobile devices [99]. The most obvious issue is not only the loss of the device itself but also the data what it stores in its memory, as well as any additional credentials used to gain access to internal and external sources of information (e.g., e-mail or bank account, corporate intranet, and social media). In this case, the risk is much higher and relates to blackmail and ransom demands, directed against individuals and organizations alike. The countermeasures discussed in this paper are

intended to mitigate the risks related to the loss of the physical device. However, with the ongoing progress of cyber attacker tools, there are no universal methods to preserve mobile security against such threats.

The recent efforts of the combined research and business communities in the extent of mobile security have succeeded in developing innovative solutions by adopting and adapting artificial intelligence (AI) methods. For instance, RGS Nordic has deployed IBM MaaS360 with the Watson client (a cognitive system with complex natural language processing capability [100]) on all its mobile devices in Denmark to gain tighter control over the users' data, as well as to detect and remediate potential security threats [101]. Indeed, when considering certain facets of cybersecurity that benefit from embedded AI, one can definitely refer to the protection of endpoints. AI-driven endpoint protection establishes a baseline of behavior for the endpoint through a recurrent training process [102]. If an unusual event occurs, then AI will flag it and take relevant action. Moreover, in order to detect and protect against potentially harmful activities, including zero-day threats (also referred to as zero-hour [103]), machine learning models are able to determine the most relevant features, eventually classifying malign and benign actions.

Moreover, in the face of legal regulations, organizations might find themselves maladjusted in terms of applied security measures for mobile devices, and, in particular, sensitive data (e.g., personal data). While some decision makers might neglect to implement relevant solutions and corresponding procedures, it does not mean that security violations will pay off. For instance, the University of Rochester Medical Center (URMC) identified a lack of encryption as a high risk to electronic protected health information (ePHI), and the accountable individuals permitted the continued use of unencrypted mobile devices for over three years. Then, the Office for Civil Rights (OCR) conducted an investigation of the URMC and revealed that the organization failed to employ a mechanism to encrypt and decrypt electronic protected health information (ePHI), when it was reasonable and appropriate to do so. Eventually, URMC agreed to pay $3 million to the U.S. Department of Health and Human Services and take substantial corrective action to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules [104]. Obviously, there are many more examples showing that human ignorance has led to substantial financial losses.

It is worth noting that mobile security threats and best practices are quite similar worldwide, whereas security policy management is very much local, and, for this reason, specific to different business scenarios and application settings [105]. Therefore, at the beginning of our study, we assumed to identify and analyze only generic knowledge which contributes to the topic of the research. Having said that, as a consequence, explicit know-how represents an understanding of the generative processes that constitute the domain of mobile security.

The theoretical implications concern the identification and analysis of a plethora of issues, with regard to the threats and the best practices in the mobile application domain. Furthermore, our findings give rise to other research topics worth undertaking both for academia and practitioner communities. The practical implications include the non-limited application of the specified set of ten best practices at the individual or enterprise level since their specifications are both hardware and software agnostic.

Nevertheless, this study has its limitations and areas for potential improvement as well as future work. First, the results would be more conclusive if more factual data and experimental results were included. Second, cognitive biases, including the individual perception of the research problem, should be minimized through an open discussion with experts from the mobile security area. Third, the granularity of our analysis was based on the retrieval of general artifacts, neglecting sparse issues and specific case studies.

Nonetheless, the nature of this study was exploratory; thus, the results reveal empirical evidence showing both threats and best practices which currently exist in the extent of mobile security. The greater reliability and validity of the findings require the involvement of security practitioners in a greater number to confirm the results of the present study on the one hand and exploring the problem in-depth with different groups of users in a quantitative manner on the other hand.

The current advanced security technologies, available from either the level of the operating system or application, reveal a low level of vulnerabilities and weakness. Therefore, the overall security depends on the demonstrated user behavior and arbitrary undertaken efforts. Having said that, we argue that understanding factors affecting users' intentions and motivations to accept and use particular technologies is crucial to raising security and privacy concerns at the individual level. Hence, future work will cover identifying and modeling users' perceptions of security and usability of mobile applications.

7. Conclusions

Security is always an arms race between attackers and defenders. Since the mobile application market is growing, at the same time, mobile security will continue to deliver a plethora of issues to face. In other words, security is often a matter of balancing risk and reward, defense versus convenience. In this line of thinking, the potential risks and benefits, and their tradeoffs, undoubtedly deserve further and deeper investigation. The outcome of this paper is a holistic picture of this phenomenon, which examines the negative events, conditions and circumstances that have the potential to cause the loss of assets, and the countermeasures that aim to eliminate them and provide adequate and effective protection for a user.

During the World Economic Forum of 2019 [106], the participants came to the conclusion that the past ten years mark only the start of the global cybersecurity journey. New architectures and cooperation are still required as we stand at the brink of a new era of cybercrime, which will be empowered by new and emergent technology. These three technologies, namely, 5G networks and infrastructure

convergence, artificial intelligence, and biometrics, are going to define the next ten years of global cybersecurity.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This project was financed by the Ministry of Science and Higher Education in Poland under the programme "Regional Initiative of Excellence" 2019–2022 (project no. 015/RID/2018/19).

References

[1] Statista, *Smartphones—Statistics & Facts*, Statista, Hamburg, Germany, 2020, https://www.statista.com/topics/840/smartphones/.

[2] B. Guo, Y. Ouyang, T. Guo, L. Cao, and Z. Yu, "Enhancing mobile app user understanding and marketing with heterogeneous crowdsourced data: a review," *IEEE Access*, vol. 7, pp. 68557–68571, 2019.

[3] S. Mavoungou, G. Kaddoum, M. Taha, and G. Matar, "Survey on threats and attacks on mobile networks," *IEEE Access*, vol. 4, pp. 4543–4572, 2016.

[4] A. Papageorgiou, M. Strigkos, E. Politou, E. Alepis, A. Solanas, and C. Patsakis, "Security and privacy analysis of mobile health applications: the alarming state of practice," *IEEE Access*, vol. 6, pp. 9390–9403, 2018.

[5] W. Song, D. Tjondronegoro, and M. Docherty, "Exploration and optimization of user experience in viewing videos on a mobile phone," *International Journal of Software Engineering and Knowledge Engineering*, vol. 20, no. 8, pp. 1045–1075, 2010.

[6] M. Hernes, M. Maleszka, N. T. Nguyen, and A. Bytniewski, "The automatic summarization of text documents in the cognitive integrated management information system," in *Proceedings of the 2015 Federated Conference on Computer Science and Information Systems (FedCSIS)*, pp. 1387–1396, IEEE, Lodz, Poland, September 2015.

[7] Y. Chen, W. Xu, L. Peng, and H. Zhang, "Light-weight and privacy-preserving authentication protocol for mobile payments in the context of IoT," *IEEE Access*, vol. 7, pp. 15210–15221, 2019.

[8] J. Korczak, M. Hernes, and M. Bac, "Collective intelligence supporting trading decisions on FOREX market," in *Proceedings of the International Conference on Computational Collective Intelligence*, pp. 113–122, Springer, Nicosia, Cyprus, September 2017.

[9] G. Delac, M. Silic, and J. Krolo, "Emerging security threats for mobile platforms," in *Proceedings of the 34th International Convention MIPRO*, pp. 1468–1473, IEEE, Opatija, Croatia, May 2011.

[10] D. Mikhaylov, I. Zhukov, A. Starikovskiy, S. Kharkov, A. Tolstaya, and A. Zuykov, "Review of malicious mobile applications, phone bugs and other cyber threats to mobile devices," in *Proceedings of the 5th IEEE International Conference on Broadband Network & Multimedia Technology*, pp. 302–305, IEEE, Kyoto, Japan, December 2013.

[11] D. He, S. Chan, and M. Guizani, "Mobile application security: malware threats and defenses," *IEEE Wireless Communications*, vol. 22, no. 1, pp. 138–144, 2015.

[12] M. Wazid, S. Zeadally, and A. K. Das, "Mobile banking: evolution and threats: malware threats and security solutions," *IEEE Consumer Electronics Magazine*, vol. 8, no. 2, pp. 56–60, 2019.

[13] Statista, *Online Search Usage—Statistics & Facts*, Statista, Hamburg, Germany, 2020, https://www.statista.com/topics/1710/search-engine-usage/.

[14] M. Gusenbauer, "Google Scholar to overshadow them all? Comparing the sizes of 12 academic search engines and bibliographic databases," *Scientometrics*, vol. 118, no. 1, pp. 177–214, 2019.

[15] G. S. Mort and J. Drennan, "Marketing m-services: establishing a usage benefit typology related to mobile user characteristics," *Journal of Database Marketing & Customer Strategy Management*, vol. 12, no. 4, pp. 327–341, 2005.

[16] A. Carroll, J. Barnes, and E. Scornavacca, "Consumer perceptions and attitudes towards mobile marketing," in *Selected Readings on Telecommunications and Networking*, pp. 357–368, IGI Global, Harrisburg, PA, USA, 2005.

[17] Ericsson Mobility Report, https://www.ericsson.com/4acd7e/assets/local/mobility-report/documents/2019/emr-november-2019.pdf, 2020.

[18] 75+ Mobile Marketing Statistics for 2020 and beyond, https://www.bluecorona.com/blog/mobile-marketing-statistics/, 2020.

[19] 101 Mobile Marketing Statistics and Trends for 2020: https://quoracreative.com/article/mobile-marketing-statistics, 2020.

[20] P. Weichbroth, "Usability attributes revisited: a time-framed knowledge map," in *Proceedings of the Federated Conference on Computer Science and Information Systems (FedCSIS)*, pp. 1005–1008, IEEE, Poznań, Poland, September 2018.

[21] P. Weichbroth, "Usability of mobile applications: a systematic literature study," *IEEE Access*, vol. 8, p. 55563, 2020.

[22] ISO/IEC 9241-14, *Ergonomic Requirements for Office Work with Visual Display Terminals (VDT)s—Part 14 Menu Dialogues*, ISO/IEC 9241-14, Geneva, Switzerland, 1998.

[23] ISO 9241-210, *Ergonomics of Human-System Interaction—Part 210: Human-Centered Design For Interactive Systems*, ISO 9241-210, Geneva, Switzerland, 2010.

[24] P. Dourish, R. E. Grinter, J. Delgado de la Flor, and M. Joseph, "Security in the wild: user strategies for managing security as an everyday, practical problem," *Personal and Ubiquitous Computing*, vol. 8, no. 6, pp. 391–401, 2004.

[25] S. Chiasson, A. Forget, R. Biddle, and P. C. Van Oorschot, "User interface design affects security: patterns in click-based graphical passwords," *International Journal of Information Security*, vol. 8, no. 6, p. 387, 2009.

[26] M. Hertzum, N. Jørgensen, and M. Nørgaard, "Usable security and e-banking: ease of use vis-a-vis security," *Australasian Journal of Information Systems*, vol. 11, no. 2, 2004.

[27] J. van Heek, S. Himmel, and M. Ziefle, "Privacy, data security, and the acceptance of AAL-systems–a user-specific perspective," in *Proceedings of the International Conference on Human Aspects of IT for the Aged Population*, pp. 38–56, Springer, Vancouver, Canada, July 2017.

[28] C. Herley, "So long, and no thanks for the externalities: the rational rejection of security advice by users," in *Proceedings of the 2009 Workshop on New Security Paradigms Workshop*, pp. 133–144, Oxford, UK, September 2009.

[29] Sophoslabs Threat Report, 2020, https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophoslabs-2019-threat-report.pdf.

[30] M. Landmann, "Managing smart phone security risk," in *Proceedings of the 2010 Information Security Curriculum*

Development Conference, pp. 145–155, Kennesaw, GA, USA, October 2010.
[31] B. Potter, "Mobile security risks: ever evolving," *Network Security*, vol. 2007, no. 8, pp. 19-20, 2007.
[32] OWASP Top Ten, https://owasp.org/www-project-top-ten/, 2020.
[33] J. Fitzgerald, "Managing mobile devices," *Computer Fraud & Security*, vol. 4, pp. 18-19, 2009.
[34] E. Kim, D. Gardner, S. Deshpande, R. Contu, D. Kish, and C. Canales, "Forecast analysis: information security, worldwide, 2Q18 update," 2020, https://www.gartner.com/en/documents/3889055.
[35] Top 7 Mobile Security Threats in 2020, https://usa.kaspersky.com/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store, 2020.
[36] D. Emm, "Mobile malware-new avenues," *Network Security*, vol. 2006, no. 11, pp. 4–6, 2006.
[37] The TOP 10 Mobile Risks of 2016, https://www.techrepublic.com/article/the-top-10-mobile-risks-of-2016/last, 2020.
[38] R. Sobers, "110 must-know cybersecurity statistics for 2020," 2020, https://www.varonis.com/blog/cybersecurity-statistics/.
[39] New MobileIron Report Details Most Common Mobile Threats and Blacklisted Apps, https://www.techrepublic.com/article/new-mobileiron-report-details-most-common-mobile-threats-and-blacklisted-apps/last, 2020.
[40] A. Harkness, "Mobile malware threats," 2019, https://www.netmotionsoftware.com/blog/security/mobile-malware-threats.
[41] What Is Phishing Scam, https://usa.kaspersky.com/resource-center/threats/spam-phishing last, 2020.
[42] Mobile Theft Loss Report, https://preyproject.com/uploads/2019/02/Mobile-Theft-Loss-Report-2018.pdf last, 2018.
[43] M. Bishop, *Introduction to Computer Security*, Addison-Wesley Professional, Boston, MA, USA, 2004.
[44] T. Caldwell, "Making security awareness training work," *Computer Fraud & Security*, vol. 2016, no. 6, pp. 8–14, 2016.
[45] N. Gerber, B. Reinheimer, and M. Volkamer, "Home sweet home? Investigating users' awareness of smart home privacy threats," in *Proceedings of the An Interactive Workshop on the Human Aspects of Smarthome Security and Privacy (WSSP)*, Baltimore, MD, USA, August2018.
[46] K. O'Loughlin, M. Neary, E. C. Adkins, and S. M. Schueller, "Reviewing the data security and privacy policies of mobile apps for depression," *Internet Interventions*, vol. 15, pp. 110–115, 2019.
[47] A. Przybyłek and D. Kotecka, "Making agile retrospectives more awesome," in *Proceedings of the 2017 Federated Conference on Computer Science and Information Systems (FedCSIS)*, pp. 1211–1216, IEEE, Prague, Czech Republic, September 2017.
[48] A. Przybylek and W. Kowalski, "Utilizing online collaborative games to facilitate Agile Software Development," in *Proceedings of the 2018 Federated Conference on Computer Science and Information Systems (FedCSIS)*, pp. 811–815, IEEE, Poznań, Poland, September 2018.
[49] M. H. Hussein, S. H. Ow, L. S. Cheong, M.-K. Thong, and N. Ale Ebrahim, "Effects of digital game-based learning on elementary science learning: a systematic review," *IEEE Access*, vol. 7, pp. 62465–62478, 2019.
[50] Webopedia, "Mobile security best practices," 2020, https://www.webopedia.com/TERM/M/mobile_security_best_practices.html.
[51] F. Stroud, "Mobile security best practices," 2020, https://www.webopedia.com/TERM/M/mobile_security_best_practices.html.
[52] H. Dowden, "The 6 mobile device security best practices you should know in 2020," 2020, https://www.ntiva.com/blog/top-5-mobile-device-security-best-practices-2020.
[53] D. Hein, "7 essential mobile security best practices for businesses," 2020, https://solutionsreview.com/mobile-device-management/7-essential-mobile-security-best-practices-for-businesses/.
[54] S. Lerner, "Mobile device security best practices. How to protect portable technology," 2020, https://www.enterprisemobilityexchange.com/eme-security/articles/mobile-device-security.
[55] J. Mark, "8 best practices for mobile device security," 2020, https://www.jmark.com/8-best-practices-mobile-device-security/.
[56] A. D. Kent, L. M. Liebrock, and J. C. Neil, "Authentication graphs: analyzing user behavior within an enterprise network," *Computers & Security*, vol. 48, pp. 150–166, 2015.
[57] D. Dasgupta, A. Roy, and A. Nag, "Multi-factor authentication," in *Advances in User Authentication*, pp. 185–233, Springer, Cham, Switzerland, 2017.
[58] H. Patel, "14 best practices for your mobile app security," 2020, https://www.tristatetechnology.com/blog/best-practices-to-improve-mobile-app-security/.
[59] M. Ciampa, *Security Awareness: Applying Practical Security in Your World*, Cengage Learning, Boston, MA, USA, 2013.
[60] K. Lab, "Best practices. Encryption," 2020, https://media.kaspersky.com/pdf/b2b/Encryption_Best_Practice_Guide_2015.pdf.
[61] L. Phifer, "Best practices for improving mobile data security," 2020, https://searchmobilecomputing.techtarget.com/tip/Best-practices-for-improving-mobile-data-security.
[62] A. S. K. Pathan, M. M. Monowar, and Z. M. Fadlullah, *Building Next-Generation Converged Networks: Theory and Practice*, CRC Press, Boca Raton, FL, USA, 2013.
[63] S. Abraham and I. Chengalur-Smith, "An overview of social engineering malware: trends, tactics, and implications," *Technology in Society*, vol. 32, no. 3, pp. 183–196, 2010.
[64] D. Burley, R. Carpinella, D. Chesebrough et al., *Cybersecurity in our Digital Lives*, Vol. 2, Hudson Whitman/ECP, New York, NY, USA, 2015.
[65] V. K. Velu, *Mobile Application Penetration Testing*, Packt Publishing Ltd., Birmingham, UK, 2016.
[66] M. E. Vermaat, S. L. Sebok, S. M. Freund, J. T. Campbell, and M. Frydenberg, *Discovering Computers 2018: Digital Technology, Data, and Devices*, Nelson Education, Toronto, Canada, 2017.
[67] I. Illahi, H. Liu, Q. Umer, and S. A. H. Zaidi, "An empirical study on competitive crowdsource software development: motivating and inhibiting factors," *IEEE Access*, vol. 7, pp. 62042–62057, 2019.
[68] G. R. Murray, C. R. Rugeley, D.-G. Mitchell, and J. J. Mondak, "Convenient yet not a convenience sample: jury pools as experimental subject pools," *Social Science Research*, vol. 42, no. 1, pp. 246–253, 2013.
[69] Z. Siddiqui, O. Tayan, and M. Khurram Khan, "Security analysis of smartphone and cloud computing authentication frameworks and protocols," *IEEE Access*, vol. 6, pp. 34527–34542, 2018.
[70] E. Alepis and C. Patsakis, "Monkey says, monkey does: security and privacy on voice assistants," *IEEE Access*, vol. 5, pp. 17841–17851, 2017.
[71] Z. Rui and Z. Yan, "A survey on biometric authentication: toward secure and privacy-preserving identification," *IEEE Access*, vol. 7, pp. 5994–6009, 2018.

[72] Documentation for app developers. Support In-App Updates, https://developer.android.com/guide/playcore/in-app-updates, 2020.
[73] Documentation for App Developers. Data Backup Overview, https://developer.android.com/guide/topics/data/backup, 2020.
[74] Cyber Predictions for 2019, https://www.contractormag.com/technology/article/20883658/cyber-predictions-for-2019.
[75] Report Identifies the Most Dangerous Mobile App Store on the Internet. https://www.zdnet.com/article/report-identifies-the-most-dangerous-mobile-app-store-on-the-internet/, 2020.
[76] A. Hodge, "iOS 13 vs. Android 10: which OS is more secure?," 2020, https://www.cnet.com/news/google-postpones-android-11-beta-event-amid-protests-in-the-us/.
[77] D. Markuson, "Android vs. iOS: 2020 security face-off," 2020, https://nordvpn.com/pl/blog/ios-vs-android-security/.
[78] N. O. Alshammari, A. Mylonas, M. Sedky, J. Champion, and C. Bauer, "Exploring the adoption of physical security controls in smartphones," in *Proceedings of the International Conference on Human Aspects of Information Security, Privacy, and Trust*, pp. 287–298, Springer, Los Angeles, CA, USA, August 2015.
[79] A. Mylonas, A. Kastania, and D. Gritzalis, "Delegate the smartphone user? Security awareness in smartphone platforms," *Computers & Security*, vol. 34, pp. 47–66, 2013.
[80] Wireless Connections and Bluetooth Security Tips, https://www.fcc.gov/consumers/guides/how-protect-yourself-online, 2020.
[81] R. Kalnins, J. Purins, and G. Alksnis, "Security evaluation of wireless networks access points," *Applied Computer Systems*, vol. 21, no. 1, 2017.
[82] F. Salahdine and N. Kaabouch, "Social engineering attacks: a survey," *Future Internet*, vol. 11, 2019.
[83] 2019 Data Breach Investigations Report, https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf, 2019.
[84] L. Adams, *Q2 2017 State of Mobile Device Performance & Health Report Finds Android Devices Struggled to Keep Pace with iOS Devices*, https://www.blancco.com/blog-q2-2017-state-mobile-device-performance-health-report-android-devices-struggled-keep-pace/.
[85] S. A. Gordon, "Google play can now prevent rooted users from downloading certain apps," 2020, https://www.androidauthority.com/google-play-store-apps-download-block-root-users-773824/.
[86] P. Pearce, A. P. Nunez, and G. Wagner, "Android privilege separation for applications and advertisers in android," in *Proceedings of the 7th ACM Symposium on Information, Computer and Communictions Security, ASIACCS*, New York, NY, USA, 2012.
[87] P. Andriotis, M. A. Sasse, and G. Stringhini, "Permissions snapshots: assesing users' adaptation to android runtime permission model," in *Proceedings of the 2016 IEEE International Workshop on Information Forensics and Security*, Abu Dhabi, UAE, December 2016.
[88] D. Allan, "The best android antivirus app of 2020," 2020, https://www.techradar.com/best/best-android-antivirus-app.
[89] C. Li, K. Mills, D. Niu, R. Zhu, H. Zhang, and H. Kinawi, "Android malware detection based on factorization machine," *IEEE Access*, vol. 7, pp. 184008–184019, 2019.
[90] Z. Ma, H. Ge, Y. Liu, M. Zhao, and J. Ma, "A combination method for android malware detection based on control flow graphs and machine learning algorithms," *IEEE Access*, vol. 7, pp. 21235–21245, 2019.
[91] A. A. Albasir and K. Naik, "SMOW: an energy-bandwidth aware web browsing technique for smartphones," *IEEE Access*, vol. 2, pp. 1427–1441, 2014.
[92] G. Ortiz, A. García-de-Prado, J. Berrocal, and J. Hernandez, "Improving resource consumption in context- aware mobile applications through alternative architectural styles," *IEEE Access*, vol. 7, pp. 65228–65250, 2019.
[93] S. H. Sun, "The advantages and the implementation of SSL VPN," in *Proceedings of the 2011 IEEE 2nd International Conference on Software Engineering and Service Science*, pp. 548–551, Beijing, China, July 2011.
[94] Global Market Insights: GlobeNewswire. https://www.globenewswire.com/news-release/2018/12/04/1661379/0/en/Virtual-Private-Network-VPN-Market-to-hit-54bn-by-2024-Global-Market-Insights-Inc.html, 2020.
[95] V. Gkioulos, G. Wangen, S. Katsikas, G. Kavallieratos, and P. Kotzanikolaou, "Security awareness of the digital natives," *Information*, vol. 8, no. 2, p. 42, 2017.
[96] A. Amin, A. Eldessouki, M. T. Magdy, N. Abdeen, H. Hindy, and I. Hegazy, "AndroShield: automated android applications vulnerability detection, a hybrid static and dynamic analysis approach," *Information*, vol. 10, no. 10, p. 326, 2019.
[97] J. Valcke, "Best practices in mobile security," *Biometric Technology Today*, vol. 2016, no. 3, pp. 9–11, 2016.
[98] M. Hatamian, "Engineering privacy in smartphone apps: a technical guideline catalog for app developers," *IEEE Access*, vol. 8, pp. 35429–35445, 2020.
[99] Cybersecurity & Infrastructure Security Agency, *Protecting Portable Devices: Physical Security*, Cybersecurity & Infrastructure Security Agency, Arlington, TX, USA, 2020, https://us-cert.cisa.gov/ncas/tips/ST04-017.
[100] R. High, *The Era of Cognitive Systems: An inside Look at IBM Watson and How it Works*, IBM Corporation, New York, NY, USA, 2012.
[101] IBM, RGS Nordic, https://www.ibm.com/case-studies/rgs-nordic, 2020.
[102] A. Hurst, "Use cases for AI and ML in cyber security," 2020, https://www.information-age.com/use-cases-for-ai-ml-cyber-security-123491392/2020-10-21.
[103] K. Nakao, D. Inoue, M. Eto, and K. Yoshioka, "Practical correlation analysis between scan and malware profiles against zero-day attacks based on darknet monitoring," *IEICE Transactions on Information and Systems*, vol. E92-D, no. 5, pp. 787–798, 2009.
[104] US Department of Health & Human Services, *Failure to Encrypt Mobile Devices Leads to $3 Million HIPAA Settlement*, US Department of Health & Human Services, Washington, DC, USA, 2019, https://www.hhs.gov/about/news/2019/11/05/failure-to-encrypt-mobile-devices-leads-to-3-million-dollar-hipaa-settlement.html.
[105] S. Venkatraman, "A framework for ICT security policy management," in *Frameworks for ICT Policy: Government, Social and Legal Issues*, pp. 1–14, IGI Global, Harrisburg, PA, USA, 2011.
[106] W. Dixon and D. Samartsev, "3 technologies that could define the next decade of cybersecurity," 2019, https://www.weforum.org/agenda/2019/06/3-technologies-that-could-define-the-next-decade-of-cybersecurity/.