Evaluating the Information Security Awareness of Smartphone Users

Ron Bitton, Kobi Boymgold, Rami Puzis, Asaf Shabtai
Department of Software and Information Systems Engineering
Ben-Gurion University of the Negev
Beer-Sheva, 8410501, Israel

Abstract—Information security awareness (ISA) is a practice focused on the set of skills, which help a user successfully mitigate a social engineering attack. Previous studies have presented various methods for evaluating the ISA of both PC and mobile users. These methods rely primarily on subjective data sources such as interviews, surveys, and questionnaires that are influenced by human interpretation and sincerity. Furthermore, previous methods for evaluating ISA did not address the differences between classes of social engineering attacks. In this paper, we present a novel framework designed for evaluating the ISA of smartphone users to specific social engineering attack classes. In addition to questionnaires, the proposed framework utilizes objective data sources: a mobile agent and a network traffic monitor; both of which are used to analyze the actual behavior of users. We empirically evaluated the ISA scores assessed from the three data sources (namely, the questionnaires, mobile agent, and network traffic monitor) by conducting a long-term user study involving 162 smartphone users. All participants were exposed to four different security challenges that resemble real-life social engineering attacks. These challenges were used to assess the ability of the proposed framework to derive a relevant ISA score. The results of our experiment show that: (1) the self-reported behavior of the users differs significantly from their actual behavior; and (2) ISA scores derived from data collected by the mobile agent or the network traffic monitor are highly correlated with the users’ success in mitigating social engineering attacks.

I. INTRODUCTION

Social engineering (SE) is the process of exploiting human vulnerabilities in order to penetrate to a computerized system. This is usually accomplished by manipulating a user to perform actions such as installing software, granting privileges, or revealing confidential information. According to the Internet Security Threat Report (ISTR) published by Symantec in 2018[52], the chance that SE methods will be selected as an attack vector is greater than any other advanced technical exploit. Hence, SE attacks pose a significant security threat to society.

Social engineering attacks are not limited to PC users. In fact, in the past five years the number of SE attacks targeting mobile devices users is rapidly increasing[52]. According to Avast and McAfee mobile threat reports (2019) the majority of attacks on mobile devices exploit human factor vulnerabilities (such as downloading applications from unknown sources, clicking on suspicious links, granting unnecessary permission). Furthermore, according to Checkpoint’s security report, every organization had suffered a mobile malware attack during 2018[1]. When SE is the most popular way for spreading malware in mobile platforms[52], SE attacks targeting mobile users become a major concern to both individuals and organizations.

Information security awareness (ISA) is a practice focused on the set of skills which help a user to successfully mitigate SE attacks. Since most SE threats are not covered by technological countermeasures, ISA is the most effective method to prevent SE attacks. Thus, assessing the ISA level of employees and thereby identifying those who are more vulnerable to SE attacks is extremely important for organizations. Early identification of such employees can be used to improve the security level of the organization, for example, by updating their security policies[49] and implementing personalized security awareness programs[12], [33], [53].

Previous studies have presented various methods for evaluating and increasing the ISA of PC users[53], [33], [12], [57], [36], [49]. However, the challenges in evaluating the security awareness of smartphone users are different from PC users for several reasons. First, smartphones are equipped with unique/different functionalities that are less common in PCs (location services, motion sensors, SMS, application stores and etc.) Second, smartphone users consume content and services mostly via apps, opposed to browsers in PCs. Third, some security safeguards are less common on smartphones than on PCs (e.g., antivirus or IDS), while others are implemented and used differently (permissions, certificates handling, encryption storage, authentication mechanism). Finally, the threats are different. According to the Internet security threat report (ISTR)[52], the top threat categories for smartphone users are fake apps, spyware, SMS messages, and permission abuse; in contrast PC users top threats are spear phishing, malicious websites, Trojans, and web-server exploits. These main differences clearly indicate that different security awareness skills are required by a mobile user for operating safely mobile devices, compared to a PC.

Most current studies on ISA assessment depend excessively on the subjects’ response to questionnaires[42] or surveys[8]. These methods rely on the subjects’ self-reported behavior, and thus, tend to be subjective and biased[50]. Moreover, these methods require the subjects’ active involvement and
collaboration, thereby consuming significant human resources.

Other methods are based on measuring the momentary behavior of subjects during specific events (e.g., by monitoring their reaction while facing a simulated SE attacks) \cite{4,31,59,23}. These methods, however, tend to be sensitive to environmental/contextual factors and therefore cannot provide a reliable ISA score \cite{15}. For these reasons, previous studies have argued that in order to reliably assess the ISA, continuous measurement of the subjects’ actual behavior must be considered \cite{56,37,59}. Although such measurements were developed for the PC \cite{24,56}, the criteria for a security aware smartphone user are different from those of a PC user \cite{13}. To the best of our knowledge, a comprehensive ISA assessment method, which encompasses the various aspects of mobile security and is based on continuous measurement of users’ actual behavior has not yet been developed for mobile platforms.

In this paper, we suggest a novel framework for assessing the ISA of smartphone users. The framework utilizes data collected and analyzed from three different data sources to derive/measure a set of criteria for a security aware smartphone user: (1) a mobile device agent, which is installed on the subjects’ devices and measures the subjects’ actual behavior (e.g., applications installed, security settings, connectivity management, and browsing history), (2) a network traffic monitor, which analyzes the network traffic sent to/from the subject’s devices, and (3) a security questionnaire, specifically designed to assess the self-reported behavior of smartphone users.

The expert-based process suggested in \cite{13} is utilized for deriving an ISA model that is specific to an SE attack class. We define a SE attack class as the set of SE attacks that exploit similar human vulnerabilities (e.g., phishing, application-related, and MITM attacks). Each model defines the contribution (i.e., weight) of each criterion to the overall ISA score of a specific SE attack class and can be applied for deriving the ISA score from the measured criteria. The ISA score provides an indication of the ability of the user to mitigate a particular class of SE attack.

In order to evaluate the proposed framework we conducted an empirical experiment involving 162 smartphone users for a duration of seven to eight weeks each. In addition to the data collected from the three data sources mentioned above, the participants were exposed to four different security challenges that resemble real-life SE attack scenarios: a phishing attack, an eavesdropping attack, a certificate manipulation attack, and a privilege escalation attack.

To validate the proposed framework, we tested the correlations between the derived ISA scores and the results of the challenges. We also analyzed the correlation between ISA scores derived by the different data sources. In addition, we systematically compared the data extracted by the mobile agent, network traffic monitor and challenges with the questionnaire results in order to examine the bias in the questionnaires compared to objective measurements within the context of information security.

The results of the experiment show that measurements of the subjects’ actual behavior using the mobile agent/network traffic monitor produce ISA scores that correlate with the subjects’ success or failure in the challenges. Our findings also question the reliability of assessing the ISA of smartphone users based on their self-reported behavior. In our experiment, subjects who reported to behave cautiously with respect to smartphone security failed in multiple social engineering challenges, while subjects who acknowledged their unsafe behavior successfully mitigated most of the challenges.

Moreover, we show that the ISA scores derived from the mobile agent are highly correlated with the ISA scores derived from the network traffic monitor. In contrast, the ISA scores derived from the questionnaire data source were found to have a very little correlation with the scores derived from the mobile agent and network traffic monitor data sources.

In summary, the contribution of the proposed research are two fold:

- **A framework for evaluating the ISA of smartphone users.** The first contribution of this research is a framework that can automatically detect users who are more vulnerable to social engineering attacks. The proposed framework relies on actual user behavior as observed from multiple data sources, as opposed to commonly used subjective self-reported behavior methods which were found to be unreliable in some cases. Moreover, in contrast to previous works, which explore the ISA of smartphone users with respect to a specific information security aspect (e.g., permissions, lock screen, etc.), the proposed method integrates multiple mobile security aspects into a single ISA score per attack class.

- **A comprehensive user study.** The second contribution of this research is a comprehensive and very unique user study. Within this study we monitored, using four different information sources (questionnaire, mobile agent, network traffic and challenges), the behaviour of 162 users while using their own smartphones, as opposed to previous works that either measure the momentary behavior of the subjects during specific events, or performed the assessment in a controlled environment, by using some dedicated device/platform. This unique user study allow us to explore the bias in questionnaires compared to objective measurements with respect to multiple behaviours within the context of information security.

**II. BACKGROUND**

Kruger and Kearney developed a prototype for assessing the ISA in organizations \cite{57}. The authors suggest that stakeholders define focus areas, i.e., primary technological issues related to the organization’s information security, and explore them within the context of three psychological dimensions: knowledge, attitude, and behavior. Each dimension addresses a specific psychological aspect of the focus area and contains factors that assist in the quantitative measurement of the dimension.
Bitton et al. [13] redefined and adjusted the prototype presented by Kruger and Kearney for the mobile platform. The authors presented an extensive list of measurable indicators, also referred to as criteria, for a security aware smartphone user. In addition, the authors introduced the concept of deriving the ISA level of a user with respect to a given class of SE attacks i.e., attacks that exploit similar human vulnerabilities. The motivation behind this concept is that the skills required to mitigate one class of attacks may differ from the skills required to mitigate another class of attacks.

To assess the ISA of users for a specific class of attacks, Bitton et al. suggested the expert-based process presented in Figure 1 (in blue). As can be seen, the inputs to this process are: (1) an attack class (denoted by $a$), and (2) a list of criteria for a security aware smartphone user (listed in the ISA taxonomy [13]). Security experts utilize the analytic hierarchy process (AHP) [51] to efficiently estimate the contribution of each criterion to the ability of users to mitigate SE attacks of particular classes. The outcome of this process is a security awareness model, which is a set of weights $w_i(a)$ that reflect the contribution of each criterion $i$ to the ability of users to mitigate attack class $a$.

With the assistance of 17 security experts from both academia and industry, Bitton et al. applied the process and derived security awareness models three attack classes: Man-in-the-middle attacks such as session/signal hijacking, SSL strip, eavesdropping, and rogue access point; Application related attacks such as application phishing, malicious notifications (e.g., error messages), in app pop-ups, malicious advertisements, clicking fraud, Trojan applications, and rootkits; and Phishing attacks such as social network fraud (e.g., fake links, friend/game requests), phishing emails, websites, URL, SMS, IRC, forums.

In this paper we extend the work presented in [13] by introducing a comprehensive framework for measuring the criteria for a security aware smartphone user and computing the ISA score of smartphone users to different classes of SE attacks. The process of computing the ISA score of a smartphone user (denoted as $u$) for a specific class of SE attack (denoted as $a$) is presented in Figure 1 (in red). As can be seen, there are two inputs to the computation process: (1) the security awareness model for the particular class of attacks as defined by Bitton et al., and (2) an estimation of all criteria for a particular user (i.e., the set of measured values for each criterion $i$ for user $u$), as measured by the proposed framework.

III. RELATED WORK

The domain of ISA has been researched extensively in the past. In this section, we describe previously suggested methods for assessing the ISA of mobile users. Specifically, we present related work that used questionnaires as the data source (Section III-A), research that used software agents as a passive measurement data source (Section III-B), and related work that applied active challenges, either for evaluating a proposed method of ISA measurement or as a tool for training users (Section III-C). In addition, we summarized all relevant papers in the domain of ISA assessment in Table I.

A. The Assessment of ISA Using Questionnaires

PC users. A popular method for assessing the ISA of PC users is the Human Aspects of Information Security Questionnaire (HAIS-Q) [47], which aims to measure the knowledge, attitude, and self-reported behavior of employees regarding information security. The external validity of HAIS-Q was examined in previous studies, by using the test-retest method [42] and conducting phishing tests [46]. Onarlioglu et al. studied the resilience of PC users to phishing attacks by asking participants to rank the potential risk resulting from certain scenarios [45].

While Parsons et al. [46], [45] focused on the PC domain and conducted an evaluation involving one attack vector (i.e., phishing tests), in this study we focus on smartphone users and evaluate the proposed method on multiple SE attacks. In addition, the evaluation presented in these works was performed in a controlled environment (by asking subjects to assess the safety of clicking links in a series of simulated phishing emails), which may not reflect the subjects’ behavior in a real attack scenario [14]. In this study, the various attack simulations are executed in the natural environment of the users, which totally reflects the subject’s behaviour in a real attack scenario. Furthermore, in contrast to the proposed research these studies do not validates the self reported behavior of the users using objective data sources (e.g., an agent which installed in the user’s PC and measure the actual behaviour of the user).

Mobile users. Androulidakis and Kandus studied the security awareness of smartphone users through questionnaires [10], [11], [9]. Based on their questionnaires, Esmaeli [20] suggested a model for assessing factors that affected information security behavior in smartphone networks. Mylonas et al. studied the ISA of smartphone users in the context of downloading applications from official application repositories (e.g., Google Play, and Apple’s App Store) [43]. Gkioulos et al. presented an analysis of a security questionnaire, designed specifically for assessing the ISA of smartphone users [27], [26]. Their results indicate that for several security topics, the security competence level of users does not affect the subjects self-reported behavior. Each of these works contributed sig-
First, prior works explore the ISA of smartphone users with respect to specific information security aspect. As summarized on Table I, many important aspects of smartphone security awareness (such as application usage, browsing, and account security) are not covered by these works. In addition, the integration of different information security aspects into a single comprehensive and complete framework for assessing the ISA of users was not presented in prior works. Second, these works do not validate the self-reported behavior of users using objective data sources (such as a mobile agent and network traffic monitoring). In this work, we address this gap by developing three orthogonal methods for assessing the ISA of users, a security questionnaire, mobile agent and network traffic monitoring. We also compared the results of the three assessment methods and provides meaningful insights with regards to their reliability and accuracy. Third, previous studies was mostly evaluated using very limited set of attack vectors (typically different levels of phishing emails), which in most cases was performed in a controlled environment (which may not reflect the subjects’ behavior in a real attack scenario). In this study we evaluate the framework by measuring his/her reaction when facing multiple real-life attack scenarios.

### B. The Assessment of ISA Using Passive Measurements

**PC users.** Forget et al. introduced the Security Behavior Observatory (SBO), a client-server architecture designed for long-term monitoring of client machines running the Windows operating system [24]. In follow-up research they utilized the SBO to validate the self-reported behavior of users, assessed through interviews [25]. Wash et al. also presented a data collection system to validate the self-reported behavior of PC users, assessed through surveys [56].

Redmiles et al. compared real measurement data to survey results with respect to a specific user behavior: software updating [50]. Their results indicate that for software updating the self-reported data varies consistently and systematically with measured data.

Although these studies included objective measurements and continuous monitoring of the subjects’ actual behavior, they focused on very specific user behaviors. In addition, they centered on PCs rather than smartphones. Hence, these studies did not cover technological aspect that are relevant for smartphone ISA, such as location-based services, motion sensors, microphones, permissions and etc. Furthermore, these studies was never evaluated using real-life attack scenarios. Nonetheless, their practical results support the findings presented in this paper, namely the reports of users regarding their behavior are unreliable.

**Mobile users.** The self-reported behavior of users tend to be biased [7], [23]. Consequently, ISA assessment based on users’ self-reported behavior tends to be inaccurate. Because of this, researchers have developed objective measurement tools for measuring the actual behavior of users. Egelman et al. developed and examined the validity of SeBIS [19], a security questionnaire intended to measure the attitude of users towards security-related topics [18]. In their study, Egelman et al. examined the validity of their questionnaire using three distinct experiments: (1) by requesting the subjects to suggest a strong password and identify phishing URLs, (2) by examining the operating system version of the subjects personal computer two weeks after a release of an update, and (3) by checking for the existence of a secure lock screen on the subject’s personal smartphone.
The authors of [54] also studied the ISA of smartphone users in the context of lock screen security (e.g., pattern, textual password). In their experiment, the authors provided smartphones to the subjects with unlimited data, SMS, and mobile-to-mobile use in exchange for being monitored while participating in the study. During the course of the experiment, the subjects also completed several surveys to assess the factors that influenced the subjects’ decision to use a lock screen code or share this code with acquaintances.

Wijesekera et al. studied the perception of smartphone users regarding permission [57]. In their experiment, the authors collected contextual information about the state of the device when permissions are requested. At the end of the experiment, they asked the subjects about the permissions granted and denied as well as their decision making in accordance to specific contexts.

These works have four main limitations. First, the above methods explore the ISA of smartphone users with respect to specific information security aspect. For instance, Egelman et al. [18] focused solely on password usage, OS version and lock screen; Van et al. [54] was also focused solely on lock screen security; and Wijesekera et al. [57] focused solely on application permissions. As summarized in Table II in Appendix II, many important aspects of smartphone security awareness was not covered by these works. In addition, the integration of different information security aspects into a single comprehensive and complete framework for assessing the ISA of users was not presented in prior works.

In this work, we address this gap by presenting a comprehensive and complete framework for assessing the ISA of smartphone users. Within this framework, we develop multiple sensors that collects device’s security attributes and monitor the behaviour of the user, with respect to multiple information security aspect (the complete list of sensors is summarized in Table II in Appendix II). In addition, based on an expert-based procedure, we integrate the various mobile security aspects into a single ISA score per attack class.

Second, previous studies are either measuring the behavior of the subjects within a specific context (e.g., updating a specific program) and in a controlled environment [19], or provide additional smartphone to the participant for the experiment period. Thus, may not reflect the actual behaviour of the user when using his own smartphone on his natural environment.

Third, previous studies were not evaluated using real-life social engineering attacks. Hence, it is hard to estimate their impact to the information security of an organization in a real-life deployment. In this study we evaluate the framework by measuring his/her reaction when facing multiple real-life attack scenarios.

Finally, to the best of our knowledge, the assessment of user’s ISA through network traffic was never presented in prior research. The contribution of this kind of assessment is numerous, since it provides a completely passive method for assessing user’s ISA (i.e., without any interaction with the subject or subject’s device).

C. The Assessment of ISA Using Attack Scenarios

Previous studies have developed methodologies for designing experiments that include security challenges. Dodge et al. [17] outlined the aspects to consider when designing a phishing experiment in which the efficacy of a security awareness program is evaluated. The authors of [30] utilized publicly available information on social networks to automatically execute spear phishing challenges. Their results show that the ability of subjects to mitigate phishing attacks decreases dramatically when the origin of the message is one of the subjects’ acquaintances.

Security challenges (i.e., security exercises) have also been used as a method for assessing the ISA of users. The authors of [23] utilized surveys, interviews, and phishing challenges to explore the factors that affect the ability of subjects to mitigate phishing attacks, as well as the correlation between self-reported and observed behavior. Although their study was not targeted at the mobile domain, their results support our conclusion that the self-reported behavior of subjects does not necessarily reflect their behavior when faced with a real attack scenario [14].

Kumaraguru et al. introduced PhishGuru, an embedded training system that teaches subjects how to mitigate phishing attacks [40]. In subsequent research, the authors performed a real-world evaluation of PhishGuru with 515 subjects for a period of 28 days. The results of their evaluation show that PhishGuru is effective [39]. The author of [31], implemented a phishing experiment based on the methodology presented in [17]. Their results show that phishing exercises can improve the subjects’ ISA with regard to phishing.

While SE challenges have been used in the past for assessing the ISA of users, the vast majority of them were focused solely on phishing attacks, and were not targeted at the mobile platform. In this study we implement four different challenges (Namely, phishing challenge, SPAM, Permission abuse and certificate manipulation).

IV. THE PROPOSED FRAMEWORK

The proposed framework encompasses three types of data sources: a mobile device agent, which is installed on the subjects’ smartphones and measures their actual behavior; a network traffic monitor which extracts a set of behavioral properties from the network traffic transmitted to/from the subjects’ smartphones; and a security questionnaire designed to measure the ISA of smartphone users. Each data source can be used separately to assess the ISA of a user; thus, the assessment process will result in three ISA scores for each user and attack class.

A. Mobile Device Agent

The first data source is implemented as a software application (agent) installed on the subjects’ smartphones.

Using a variety of dedicated software modules (i.e., sensors), the agent continuously monitors the actual behavior of the subjects while operating their smartphone. Thus, it
provides a complete, objective, and continuous record of the subjects’ actual behavior.

These dedicated sensors are used to estimate the ISA criteria presented in [13], which can later be used for assessing the ISA of a given subject for a specific class of SE attacks. The complete list of ISA criteria, as well as their indicators from the mobile agent is presented in Appendix VII-B.

The sensors implemented can be categorized into four groups: connectivity, applications, content, and device. The complete list of sensors is summarized in Table I.

1) Connectivity: The connectivity of a device can pose a threat to the user. For instance, the Bluetooth protocol has already been used many times as an attack vector [29], [9], [43], [41]. Similarly, untrusted Wi-Fi networks are fertile ground for network attacks such as eavesdropping and man-in-the-middle (MITM) [41].

Within the proposed framework, we developed software modules, which are used to monitor the behavior of the user while operating the device’s connectivity sensors (e.g., Wi-Fi, Bluetooth, GPS, and NFC), and collect statistical information regarding the incoming/outgoing network traffic of each application.

Specifically, we utilize the data extracted from these sensors to evaluate various criteria related to communication channels. For instance, to identify a potential risk of eavesdropping and content hijacking, we explore connections to unencrypted Wi-Fi networks to detect files and private data transmitted as plain-text over these insecure channels (N1, N2, N4 in Appendix VII-B). We also examine whether the user has privacy concerns with respect to connectivity, by observing whether the user manages the connectivity sensors cautiously, i.e., disables a connectivity when it is not in use (PC1 in Appendix VII-B).

2) Applications: The applications installed on the smartphone have the ability to access the user’s sensitive data, as well as to collect sensors’ data in real-time (e.g., camera, microphone, GPS, etc.); thus, malicious applications can pose a threat to the user.

The application sensors are used for collecting indicators of careless user behavior, with respect to installation and management of applications. As applications from dubious sources are more likely to be malicious [43], [22], [32], the source of the application is a very important indicator for the ISA of a user with respect to applications. For this reason, we search for such installation and use third party services (such as VirusTotal [5]) to identify malicious applications (AII in Appendix VII-B). We also search for applications that require root permission, since careless user behavior with rooted devices may permit applications to bypass the application’s sandbox mechanism [48], [16] (AIV in Appendix VII-B).

Since the permission mechanism can be easily exploited through SE [55], [59], [44], [28], we examine the permissions requested by applications with a low rating or low number of downloads in order to identify sensitive permissions granted to suspicious applications (AII2-AII3 in Appendix VII-B).

Figure 2: A distribution of the installation times of system and user applications for a specific sampled smartphone user.

The applications installed on a subject’s device can also indicate reckless behavior. Thus, we check for the existence of anti-virus software, as well as password management, backup and VPN services, since their existence corresponds to cautious user behavior (SS2, N3, and A3 in Appendix VII-B). Moreover, we continuously monitor updates and deletions of applications to validate that the user manages his/her applications carefully (AH1, AH3 in Appendix VII-B).

A challenging task with regard to the data mining of the application sensors was identifying the specific applications installed by the subjects themselves. As different vendors include different system applications on their devices, these applications, which typically require many sensitive and dangerous permissions, are mixed in with the users’ applications. Nonetheless, we noticed that system applications are usually installed in a burst that precedes the installation of applications by a user, sometimes many months before the first user-installed application. In contrast, user applications are installed gradually along a long period of time. Figure 2 presents a sample distribution of installation times for both user and system applications for a sampled smartphone user. We can clearly see the burst of system application installations that precedes the installations of the first user applications.

In addition, it can also be noticed that user applications are installed over a period of nine months (with a slight increase in the number of user applications installed at the beginning of this period).

For this reason, in order to filter out the system applications, we first sort the subjects’ application lists by the application’s installation time; then, we eliminate large installation bursts that appeared early in the installation timeline.

3) Content: Smartphones have changed the way we consume data and communicate with each other [34]. In 2018, 52.2% of all website traffic was generated by mobile phones[4]. Furthermore, 55% of all the emails opened, were opened through mobile devices[3] thus exposing smartphone users to additional threats such as spam, phishing, and account hijacking.

The content sensors monitor statistical information regarding the browsing history, email messages, and SMS messages. Specifically, we use the browsing data to identify malicious domains, e.g., by using VirusTotal [5]; and to detect expired and self-signed SSL certificates, e.g., by using OpenSSL [3].
A primary advantage of this data source is rooted in its passiveness. In contrast to questionnaires and mobile agents, which require some level of collaboration and interaction with the subject, network traffic monitoring is passive, taking place with no user interaction or involvement whatsoever.

The processes for extracting the behavioral attributes using a network traffic monitor can be divided into four categories: domain, application level protocols, deep packet inspection (DPI), and contextual analysis.

1) Domain: The domains exchanged within application layer protocols, such as the HTTP host and SSL server name, can provide indications regarding the users behavior. For instance, recurrent TCP sessions to anti-virus domain can indicate that the user has an anti-virus application.

2) Application level protocols: In this category we focus on two common application level protocols: HTTP and TLS. HTTP is an application level protocol widely used for hypertext information systems (e.g., Web applications). The header of an HTTP packet includes general information about the smartphone. Specifically, the user-agent field specifies the device model and OS version. We use this information to understand whether the user is constantly updates his/her device’s operating system(OS1 in Appendix VII-B).

The domain’s data was also used to identify the communication with common analytic services (such as ad.doubleclick.net), which provide indications about pop-up and advertisement clicks (AH2 in Appendix VII-B). In addition, we identify recurrent connections to domains that are associated with security applications (e.g., anti-virus, password management services, etc.) to detect the presence of security countermeasures (A3, SS2, SS3 in Appendix VII-B).

B. Network Traffic Monitor

The second data source is a network traffic monitor, which extracts a set of behavioral attributes from the Internet traffic of the subjects. These attributes are later used to evaluate the ISA criteria that serve as the input of the process of assessing a subject’s ISA for a specific SE attack class.

The primary advantage of this data source is rooted in its passiveness. In contrast to questionnaires and mobile agents, which require some level of collaboration and interaction with the subject, network traffic monitoring is passive, taking place with no user interaction or involvement whatsoever.

The processes for extracting the behavioral attributes using a network traffic monitor can be divided into four categories: Connectivity, Application, Content, and Device.
ital certificates which are transmitted from the server to the client during the handshake. TLS security is rooted in users' trust of the certificate authorities that issue these certificates. Accepting an untrusted certificate (e.g., self-signed, expired, invalid signature, etc.) is considered risky behavior, since it exposes the user to various attack vectors, such as phishing and man-in-the-middle (MITM) attacks. To identify this type of behavior, we monitor sessions that (a) included untrusted certificates, and (b) were not terminated immediately after the handshake with the RST flag. Such sessions strongly indicate that the user has accepted the untrusted certificate (B5 in Appendix VII-B).

3) Deep packet inspection: Transmitting private information via an unencrypted protocol can expose the user to eavesdropping. Thus, the existence of private content within the unencrypted network traffic of a user can be extremely indicative of the user’s ISA. Deep packet inspection is a type of data processing which provides in-depth inspection of the content of network traffic in order to extract meaningful patterns or insights. This includes protocol headers, data structures, as well as the payload of messages (i.e., layers 2 to 7 of the OSI model).

In order to determine the user’s likelihood of being the target of eavesdropping, we implement a dedicated DPI process. Specifically, we reconstruct the TCP session, decode GZIP/XML/JSON encoded traffic, and extract the content in a readable format. This content is then analyzed to identify personal information such as email addresses, passwords, credit card numbers, GPS coordinates, etc. (B3 in Appendix VII-B). We also identify file downloads and use third party services (such as VirusTotal [5]) to detect malicious files (B2 in Appendix VII-B). Furthermore, focusing on the downloads of Android application packages (APK), we identify installations of applications from dubious sources (A11 in Appendix VII-B).

4) Contextual analysis: The security awareness of subjects is also affected by the context of use. Therefore, some ISA criteria reflect the behavior of users in specific contexts. For instance, inserting private information into pop-ups (B4 in Appendix VII-B) and clicking malicious links while reading emails (VC2 in Appendix VII-B). These criteria, which are indicative of ISA, cannot be evaluated directly from the raw network traffic due to encryption. However, in some cases we can infer that such behavior takes place using indirect indicators. For instance, in order to directly infer that a user clicks on malicious links while reading emails, it is necessary to analyze the subject’s communication with email services which are typically encrypted. Nonetheless, instances in which communication with email services occurred around the same time as communication with a malicious domain can be used as an indicator that the subject tends to behave carelessly while reading emails. The values of the criteria measured through this method correspond to the number of appearances of the relevant attributes.

C. Security Questionnaire

Security questionnaires are the most common method for assessing ISA in the literature. The proposed security questionnaire was specifically designed to measure the self-reported behavior of subjects with respect to the security awareness criteria presented in [13]. When designing the survey, we followed the methodologies and questions presented in previous studies [11], [43], [20], [19], which pointed out two important aspects of behavior with respect to information security: preventive behavior i.e., actions that the user performs to reduce the risk of being exposed to an attack; and confronting behavior i.e., actions that the user performs when faced with a security risk.

Similar to previous studies, we formulated three type of questions:

1) Questions which focus on the likelihood of taking an action in the context of specific ISA criteria.
2) Questions which focus on the frequency at which the subject performs an action in the context of specific ISA criteria.
3) Questions which focus on management of the devices built-in connectivity.

The complete questionnaire, together with the distribution of each answer are presented in Appendix VII-A. In order to evaluate the questionnaire we conducted a pilot study, in which 20 users were requested to answer the questionnaire as well as participating in focus groups. The main insight from this pilot-study was that illustrations and snapshots need to be added in order to make the questions more clear (e.g., security alerts, popups, permissions, encrypted websites and etc.)

In order to evaluate the criteria using the security questionnaire, we created an ordinal five-level scale for each question, where the first level represents a very reckless behavior, and the fifth level represents the most cautious behavior. This scale was considered the raw value of a user for a criterion (because some criteria are evaluated using multiple questions, the values of these criteria were calculated by averaging the raw values of the relevant questions). Then, we calculated the normalized value of a user for a criterion by normalizing the raw values of all users for the same criteria. The normalized value was considered as the value of criteria for the specific user.

D. Computing the User’s ISA Score for an Attack Class

The process of computing the ISA score of a smartphone user for an attack class include two inputs (see Figure 1): (1) a security awareness model for the particular class of attacks as defined by Bitton et al. [13]; and (2) the values of criteria for a particular user as measured by the various data sources. The three security awareness models (referred to as application model, MITM model, and phishing model) are presented in Appendix VII-B. Figure 3, where we present the weight (y-axis) for each criteria (x-axis). In addition, for each model we map the three data sources to the criteria they measure. As can be seen, some of the data sources are able to measure only a partial set of criteria. We attribute this to the
fact that measuring the criteria is not a trivial task, especially when using a passive data source (such as the network traffic monitor). For instance, in the application model we can see that the network traffic data source can measure criteria that describe 62% of the model, where the mobile agent data source can measure criteria that describe 87% of the model. On the other hand, in the phishing model the most important criteria can be measured using all the three data sources. It is worth mentioning that the questionnaire data source can measure all of the criteria, however as previously mentioned, this data source tends to be very subjective.

The ISA score of a user \( u \) for an attack class \( a \), using data source \( d \) is denoted by \( s(u,a,d) \) and calculated as follows:

\[
s(u,a,d) = \frac{\sum_{i \in C_d} w_i(a) \cdot c_i(u)}{\sum_{i \in C_d} w_i(a)}
\]

(1)

where \( C_d \) denotes the set of ISA criteria measured using the data source \( d \), \( w_i(a) \) denotes the weight of criterion \( i \) in the awareness model \( a \) and \( c_i(u) \) represents the value of criterion \( i \) as measured using data source \( d \).

Given the ISA score, we can partition the users into groups according to three security awareness levels denoted as low, medium, and high as follows:

\[
L(u,a,d) = \begin{cases} 
\text{low,} & s(u,a,d) < \mu - \beta \cdot \sigma \\
\text{medium,} & \mu - \beta \cdot \sigma \leq s(u,a,d) \leq \mu + \beta \cdot \sigma \\
\text{high,} & \mu + \beta \cdot \sigma < s(u,a,d)
\end{cases}
\]

(2)

where \( \mu \) and \( \sigma \) denote the mean and the standard deviation of the ISA scores in the population and \( \beta \) is a hyperparameter which can be used to adjust the sizes of the groups within the partition.

V. Evaluation

The proposed framework computes the ISA score of a user for a given SE attack class. The main hypothesis of this research is that this score will indicate the ability of the user to mitigate SE attacks. In other words, we assume that subjects with a high ISA score will be less likely to fail in mitigating SE attacks, while subjects with a low ISA score will be much more vulnerable to these attacks. In order to evaluate the proposed framework, we conducted a long-term experiment involving 162 students who use their smartphones regularly. During the experiment, we monitored the network traffic of the subjects, measured their behavior while operating their smartphones, and asked them to answer the security questionnaire. Towards the end of the experiment we exposed the subjects to four SE attacks. Then, we used the framework to calculate the ISA score of each subject, and evaluated the correctness of the score by cross-checking the score with the subject’s performance in the challenges. In this section, we provide a detailed explanation of the evaluation process and results.

A. Social Engineering Challenges

In the interest of providing a practical evaluation of the proposed framework, we implemented security challenges that resemble different SE attacks. The primary advantage of this kind of evaluation is that it measures the ability of a subject to handle a real-life attack scenario. The challenges are: phishing, spam pop-ups, suspicious permission requests, and certificate manipulation. The last three challenges were implemented as part of the mobile agent, either by presenting a message or by presenting a pop-up Web-page. Only the first challenge (spear phishing) was initiated via an email. In order to validate that a participant completed the first challenge via the mobile phone, we checked on our phishing web page the user-agent field (in the HTTP request), which indicates whether the client is a mobile-client or pc-client. The users that complete the challenge using their PC were filtered out in the analysis of this challenge.

1) Spear phishing: One of the most common SE attacks is phishing. The spear phishing challenge (presented in Figure 4a) is a Web page that mimics a login page for student services. The attack scenario began by sending an email to the subjects that includes a message in which the subjects were asked to authenticate themselves using an attached link due to a problem with the university’s computer systems. The sender of the email was “STUDENT ADMINISTRATION,” a sender that the subjects are familiar with as emails associated with the university’s administration are sent by this entity. The email was sent to the participants during the academic semester, where administrative emails are more likely to be sent by the university’s IT department. Although the email looked like a legitimate email, there were several indicators that it was a phishing scenario. First, the phishing email was not
sent from the university’s mail system. Second, the attached URL was not associated with the university’s domain. Third, the phishing Web page was not connected via the HTTPS protocol. To preserve the subjects’ privacy, the authentication information was not transmitted to the server. Instead, we implemented a client side script that validates the username and ID number. Please refer to Section [V-B3] for further issues related to privacy and ethical considerations. Within this challenge, a subject who click on the malicious URL, and insert his/her private credentials in the phishing Web site was considered as failed in mitigating the attack.

2) SPAM pop-ups: Spam can expose the subject to privacy and security threats. The spam challenge (presented in Figure [4b]) is a Web page which offers a chance to win an iPad by answering a simple question; the subject is requested to expose personal information (such as their first name, date of birth, and email address). This attack scenario is executed when the user is within the context of mobile browsing, with a pop-up that was triggered by the mobile agent and appears on the subject’s screen. Similar to the phishing challenge, the personal information supplied by the subjects was not transmitted to the server. Within this challenge, a subject who insert his/her private information to the spam pop-up was considered as failed in mitigating the attack.

3) Suspicious permission request: Malicious applications can trick unaware users into granting dangerous permissions during runtime. In this challenge (presented in Figure [4c]), the Web page contained a request to grant superuser privileges for a "browser plug-in." The attack scenario was initiated when the user is within the context of mobile browsing; this triggered a "system alert" which was initiated by the mobile agent and appeared on the subject’s screen. The subject could reject the request, approve it forever, or approve it only for that time. Within this challenge, a subject who grant the superuser privileges to the browser plug-in was considered as failed in mitigating the attack.

4) Certificate manipulation: In this challenge (presented in Figure [4d]), the Web page contained a security warning about using a certificate that is signed by an untrusted certificate authority. The attack scenario was initiated when the user opened a secure connection to a website by using the browser. Then, triggered by the mobile agent, a "system alert" was issued and appeared on the subject’s screen. The subjects could accept the certificate, request more information, or cancel and navigate out of the suspicious website; the "more information" button provided information written in Chinese. Within this challenge, a subject who accept the untrusted certificate was considered as failed in mitigating the attack.

B. Data Collection

1) Recruitment: Collecting data from real subjects in their natural environment and for a long-term period is very challenging. In order to recruit a diverse population of subjects, we sent emails to active students and graduate students of two different academic institutes in Israel. The title of the email was “Invitation to participate in a study on Android smartphones.” Within the content of the email the potential subjects were told that the purpose of the study is to explore their browsing habits (we intentionally obfuscated the fact that the study is about information security to avoid Hawthorne effects, in which subjects modify their behavior in response to their awareness of being observed). About 1000 subjects were agreed to participate in the study, we invited 300 of them to our laboratory in order to sign in to the experiment, receive guidance, and install the data collection framework. About 250 of subjected received the guidance and 220 of them signed in to participate in the research. Upon signing the consent form, subject were requested to complete a demographic survey on Google Forms. Each one of them received a compensation of 200 USD.

It should be mentioned that during the first week of the experiment 40 participant opted to withdraw from the experiment; this was due to a high battery consumption or incompatibility of the data collection framework (which resulted in repeating crashes of the agent). In addition, we filtered out 18 participants who did not activated the data collection framework regularly. Finally, 162 participants who use their smartphones regularly served as the subjects of the experiment and for the data analysis and evaluation.

Descriptive statistics of the population are presented in Figure [5]. As can be seen, the population consisted mainly of 19 to 30 year-old’s, almost half of which are students/university-graduated from the faculty of engineering. We also analyzed the distribution in the number of distinct application installations among the experiment population. As can be seen in Figure [6], most of the applications are installed on less than 20% of the devices and more than 40% of the applications are installed on one device only. On the other hand, popular applications such as Whatsapp, Chrome, Waze, Facebook, Shazam, Skype, GetTaxi, and Instagram were installed on more that 50% of the devices (see Figure [7]). This indicates that the population of participants in the experiment is diverse.

In order to validate that the users use their smartphone regularly throughout the study. We routinely sent a “keep-alive” message to our data collection servers every 30 minutes. If for a period of 6 hours such message was not received the participant was automatically notified via an email. We also routinely validated that the VPN connection is active. In the case that a user was not connected to the VPN for a period of six hours, he was automatically notified via an email. Nevertheless, by the end of the experiment we requested each participant to complete the missing days by extending the experiment period respectively. At the end, each participant was active for at least seven weeks.

2) Experiment setup: In the experiment, each subject was requested to install two Android applications: a dedicated Android application that was developed by the research group and...
and used to passively monitor the subjects’ behavior based on a set of sensors (as described in Section IV-A) and a commercial VPN client application that was used to redirect the subjects’ Internet traffic to the server used in the experiment. It should be mentioned that all of the data was transmitted securely to this server.

The experiment was conducted according to the following schedule:

- **Opening session:** At the beginning of the experiment the subjects were asked to install the applications on their personal smartphones and keep them there for a period of seven weeks.
- **Passive data collection:** During the first three weeks of the experiment, we passively monitored the subjects’ behavior and Internet traffic using the mobile agent and VPN applications. During this period the subjects were not exposed to any challenges.
- **Active probing:** From the fourth week on, each subject was exposed to a different challenge each week. To prevent the order of the challenges to influence the results, the order was based on the lattice square design [58].
- **Security questionnaire:** At the end of the seventh week, the subjects were requested to answer an online security questionnaire.

3) **Privacy and ethical considerations:** The experiment involved collecting sensitive personal information from real subjects for a long period of time, including their browsing patterns. We did our best to preserve the subjects’ privacy and reduce any risks associated with participating in the experiment. The experiment was approved by the institutional review board (IRB), subject to the following precautions:

1) The subjects participated in the experiments, freely, at their own free will, and provided their formal consent to
participate in the research. The subjects received a one-time payment as compensation for their participation. Although, at the beginning of the experiment the subject were not aware to its purpose, they were fully aware of the type of data that would be collected and were allowed to withdraw from the study at any time.

2) Anonymization was applied to the data. At the beginning of the experiment, a random user ID was assigned to each subject, and this user ID served as the identifier of the subject, rather than his/her actual identifying information. The mapping between the experiment’s user ID and the identity of the subjects was stored in a hard copy document that was kept in a safe box; at the end of the experiment we destroyed this document.

3) During the experiment, the communication between the agents and the servers was fully encrypted and the collected data was stored in an encrypted database. At the end of the experiment the data was transferred to a local server (i.e., within the institutional network), which is not connected to the Internet. Only anonymized information of the subjects was kept for further analysis.

C. Statistical Analysis

The main hypothesis of this research is that subjects with high ISA score are likely to mitigate SE attacks, while subjects with low ISA score will fail doing so. We evaluate this hypothesis with respect to the three data sources \(d \in \{\text{questionnaire, network, agent}\}\) using the four challenges presented in Section V-A \(a \in \{\text{phishing, spam, permissions, certificate}\}\). In order to evaluate the above hypothesis we start with the \(\chi^2\)-test to check whether the failure \(f(u, a)\) of the subject \(u\) in challenge \(a\) and his/her awareness level \(L(u, a, d)\) are statistically dependent. In a standard \(\chi^2\)-test the null hypothesis states that the two variables are independent. If the null hypothesis is accepted then the ISA score computed based on the specific data source does not reflect the subject’s ability to mitigate the challenge. If the alternative hypothesis is accepted, that is, success in the SE challenges and the level of security awareness are statistically dependent, then the latter can be used to guide security awareness policies.

However, \(\chi^2\)-test does not provide the complete picture. For example, if most people with high security awareness will fail mitigating the SE attacks and most people with low security awareness will succeed doing so, then both variables will be statistically dependent but the computed ISA score will be misleading. We will demonstrate such situation in Section V-D based on the data collected during our experiment.

In order to complement the statistical analysis we use Pearson correlation coefficient to check for trends and derive actionable insights. We define the average ISA score \(\bar{s}(l, a, d)\) of the subjects with security awareness level \(l \in \{\text{low, medium, high}\}\) as:

\[
\bar{s}(l, a, d) = \frac{1}{n} \sum_{u} u \in L(a, a, d) \{ s(u, a, d) \}.
\]

We define the success rate \(sr(l, a, d)\) of the subjects with security awareness level \(l\) as the fraction of the subjects that succeeded at mitigating the challenge out of all subjects with security awareness level \(l\):

\[
sr(l, a, d) = \frac{\{u : L(u, a, d) = l \land f(u, a) = \text{success}\}}{|\{u : L(u, a, d) = l\}|}.
\]

We examine the Pearson correlation coefficient between the two random variables \(sr(l, a, d)\) and \(\bar{s}(l, a, d)\) across different security levels. A high positive correlation along with significant statistical dependency according to \(\chi^2\)-test will suggest that the level of ISA computed based on the source \(d\) correctly reflect the ability of the subjects to mitigate SE attacks similar to \(a\). Ideally, the following inequality should hold for any \(a\) and \(d\): \(sr(\text{low}, a, d) < sr(\text{medium}, a, d) < sr(\text{high}, a, d)\).

D. Results

The statistical analysis described above was applied on the three data sources (questionnaire, network and agent). Success rates of subjects are presented in Figure 8 where each subfigure present the performance of the three data sources for a specific challenge. The \(p\)-values associated with the \(\chi^2\) tests for each data source are presented in the figure legend. The dashed lines indicate the overall success rate for each challenge.

As can be seen, in most of the challenges, the classification based on the mobile agent and network traffic analysis are statistically significant. In addition, in all of the challenges, the mobile agent and network traffic monitor classify the subjects to awareness groups that are correlated to the success rates for the challenge. This observation is also reflected in the correlation coefficient matrix presented in Figure 9a, since the

...
average ISA scores based on the mobile agent and network traffic analysis are linearly correlated with the success rates for the challenges. On the other hand, the assessment of ISA based on the security questionnaire produced a negative correlation; namely, the questionnaire classified the subjects into awareness groups that are not correlated to the success rates for the challenge.

This insight prompted us to further investigate the correlation between the ISA scores of different data sources. In Figure 9, we present the Pearson correlation coefficients for each pair of data sources (y-axis) and awareness model (x-axis). As can be seen, for the phishing and MITM models the ISA scores generated by the network traffic monitor and mobile agent are highly correlated. However, for the application model the correlation of the ISA scores generated by the network traffic and mobile agent is slightly lower. We attribute this to the fact that both the phishing and MITM models are based on criteria that can be measured precisely from the network and agent. However, for the application model the correlation of the ISA scores generated by the network traffic and mobile agent is slightly lower. We attribute this to the fact that some of the criteria are not measurable through the network. On the other hand, the ISA scores generated by the security questionnaire are not correlated with the ISA scores derived from the network traffic monitor or agent data sources.

The contradictions between the self-reported behavior of the subjects (measured by the behavioral questionnaire) and the actual behavior (measured by the mobile agent, network traffic, and the challenges) can be seen more clearly in lower resolution by analyzing subjects’ responses specific questions. The distribution of questionnaire answers is presented in Figure 10.

An interesting observation is that about 70% of the subjects have reported that they would never provide personal data in pop-up Web pages. However, as presented in Figure 11 when analyzing the actual behaviour of these subjects we noticed that almost 40% of them entered their private data in the SPAM website (our SPAM challenge). Similarly, almost 60% out of the subjects who reported that it is unlikely that they would provide personal data in a pop-up Web pages did entered their heir private data in the SPAM website (our SPAM challenge).

Similar findings were observed while investigating questions related to certificates, lock screen protection, and file downloads. For example, 50% of the subjects who claimed that would never enter a Website for which a security warning was displayed, failed in the certificate manipulation challenge; 35% of the subjects who claimed that they always use lock screen protection (e.g., password, PIN code, or pattern) did not use any method at all; and subjects who claimed that it is unlikely that they would download a file via (unsecured/unencrypted) HTTP protocol, downloaded on average executable files via HTTP during the experiment. On the other hand, subjects who reported that they always download files via HTTP, downloaded on average six executable files via HTTP during the experiment.

In general, from the analysis of the gap between the self-reported behavior and the monitored behaviour (i.e., real

![Figure 8: The success rate of each awareness group (low, average, high) in each challenge; the dashed line represents the overall success rate for the challenge.](image)

![Figure 9: Results of the correlation tests.](image)
measurements) we conclude that security aware subjects less determined in their questionnaire’s answers, while subject that were found to be with a low security awareness level were more determined and reported a “safer” behavior. These conflicts supports the underlying assumption made in previous studies that the self-reported behavior is not reliable for measuring the behavior of subjects.

VI. DISCUSSION

In this paper, we develop a framework for assessing the ISA of smartphone users. The framework utilize three different data sources in order to evaluate an extensive list of criteria for a security aware smartphone user. Although in previous sections we showed that the mobile agent data source produced the best results, there are additional criteria that should be considered when selecting a data source in production. In this section we elaborate on those criteria.

A. Interactivity

A very important aspect to consider when selecting a data source in production is the level of interaction with subjects. A high level of interactivity requires more resources, hence, it is less likely to be performed on an ongoing basis. In terms of this criterion, the questionnaire requires the most significant amount of interaction with each subject. In contrast, measuring the ISA via a mobile agent requires a significantly lower level of interaction with the subjects as it requires a one-time installation of the application on their devices. However, in this category, the network traffic monitor data source outperforms all other data sources, as it does not require any interaction with the subjects.

B. Reliability

An unreliable data source will eventually produce an inaccurate assessment. Hence, reliability is an extremely important aspect to consider when selecting a data source. With regard to this criterion, the completion of a questionnaire, which is largely dependent on the subjects’ reliability, has inherent disadvantages. As presented in the previous section, when analyzing the security questionnaire we observed that subjects behaved differently than their stated behavior, as reported in the security questionnaire. The high performance of an ISA assessment based on objective data sources compared to performance of the security questionnaire data source, indicates that in terms of reliability, objective measures such as the network traffic monitor and mobile agent are superior.

C. Timeliness

Another important aspect to consider is the monitoring period required for a reliable assessment of the subject’s ISA. Although, this aspect is less relevant for a security questionnaire, it is crucial for the other data sources, since a data source that is based on behavioral monitoring is more likely to be inaccurate without a sufficient amount of data. With respect to this criterion, the mobile device agent is superior to the network traffic monitor. The main reason for this is that many types of security criteria can be measured.
by the mobile device agent immediately, at installation time, by observing device parameters, whereas measuring the same criteria solely by utilizing network traffic may take more time. A good example of such criteria are those criteria that are based on the list of installed applications (e.g., the presence of an anti-virus application). Obtaining such information by using the mobile device agent is as simple as calling an API function, whereas assessing such information from the network traffic depends upon the presence of communication between the anti-virus application and its server.

D. Intrusiveness

Preserving subjects’ privacy is probably the most important considerations when implementing such a framework in production. Especially, given the worldwide adoption of the General Data Protection Regulation (GDPR) [21]. With respect to this criteria, it is very important to mention that the data collection framework for conducting a user study (experimentation and research) are not the same as for a production system. Specifically, when conducting an exploratory experiment more data is collected because it is impossible to know in advance what are the exact parameters and data that are required for evaluating the security awareness. Therefore, in the experimental framework we collected raw network traffic and sensor data. This raw data was stored in an anonymized and encrypted form in an isolated environment, and analyzed by authorized users only. However, in a production environment the collected information can be dramatically minimized: (a) based on the research results and derived insights only the relevant data (that is required for the specific purpose) can be collected and analyzed; (b) analysis of most data can be done on the device and therefore, there is no need to store/transmit...
raw data out of the device (only aggregated data which does not contain any sensitive information).

Nevertheless, with respect to intrusiveness, the security questionnaire is the least intrusive data sources. This is followed by the network traffic monitor and mobile device agent which are more intrusive. However, in a production system, where the analysis are done on the device and only aggregated information is stored for a long period; the network traffic monitor and mobile device agent are not more intrusive than most of todays intrusion detection/prevention systems (IDS/IPSs), and mobile device management solutions.

VII. Conclusions

In this paper, we presented a novel framework for evaluating the ISA of smartphone users. The assessment is based on three data sources, each one of which requires a different level of interaction with the subjects. Our results shows that the mobile agent provides the most reliable information; the traffic monitor requires the least interaction with the subjects; and the security questionnaire is the least intrusive among the three.

We also conducted a comprehensive user study involving 162 smartphone users. Within this study we used the proposed framework to monitor the behaviour of users while using their own smartphones. In addition, all subjects were exposed to four simulated challenges that resemble real-life social engineering attacks. using Our results indicate that an ISA assessments, which are based on the mobile agent and on the passive traffic monitoring correctly reflect the ability of the subjects to mitigate SE attacks. In addition, multiple contradictions were observed between the self-reported behavior of subjects according to the security questionnaire and the actual measured behavior. These inconsistencies stress the necessity of acquiring objective measurements while assessing ISA of smartphone users.

The practical significance of this study are three-fold. First, the framework enable organizations to accurately and continuously assess the ISA of their employees without interfering with their everyday tasks. Second, the framework enable the early identification of users that are vulnerable to a specific SE attack class, and provide the organization with the exact factors that make a user vulnerable to those attacks. Knowing those factors enable an effective, targeted and efficient implementation of countermeasures, such as developing a focused security awareness programs, customize cyber security protection tools to the individual needs of employees, and etc. Third, because it does not require any interaction with the users, the proposed framework is also scalable and the assessment can be done automatically.

REFERENCES

[1] Android permissions overview. https://developer.android.com/guide/topics/permissions/overview
[2] Gmail api. https://developers.google.com/gmail/api/
[3] Openssl. https://www.openssl.org/
[4] Social engineering toolkit. https://www.trustedsec.com/
[5] Virustotal. https://www.virustotal.com
[6] Web of trust. https://www.mywot.com
[7] Icek Ajzen. The theory of planned behavior. Organizational behavior and human decision processes, 50(2):179–211, 1991.
[8] Eirik Albrechtsen and Jan Hovden. Improving information security awareness and behaviour through dialogue, participation and collective reflection. an intervention study. Computers & Security, 29(4):432–445, 2010.
[9] Iosif Androulidakis and Gorazd Kandus. Bluetooth® usage among students as an indicator of security awareness and feeling. In ELMAR, 2011 Proceedings, pages 157–160. IEEE, 2011.
[10] Iosif Androulidakis and Gorazd Kandus. Mobile phone security awareness and practices of students in budapest. In Proceedings of the 6th International Conference on Digital Telecommunications, pages 17–22, 2011.
[11] Iosif Androulidakis and Gorazd Kandus. A survey on saving personal data in the mobile phone. In Availability, Reliability and Security (ARES), 2011 Sixth International Conference on, pages 633–638. IEEE, 2011.
[12] Kregg Aytes and Terry Conolly. A research model for investigating human behavior related to computer security. AMCIS 2003 Proceedings, page 260, 2003.
[13] Ron Bitton, Andrey Finkelshtein, Lior Sidi, Rami Pazis, Lior Rokach, and Asaf Shabtai. Taxonomy of mobile users’ security awareness. Computers & Security, 73:266–293, 2018.
[14] Marilyn B Brewer and William D Crano. Research design and issues of validity. Handbook of research methods in social and personality psychology, pages 3–16, 2000.
[15] Dan Conway, Ronnie Taib, Mitch Harris, Kun Yu, Shlomo Berkovsky, and Fang Chen. A qualitative investigation of bank employee experiences of information security and phishing. In Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017), USENIX Association, pages 115–129, 2017.
[16] Dimitrios Damopoulos, Georgios Kambourakis, and Stefanos Gritzalis. isam: an iphone stealth airborne malware. In IFIP International Information Security Conference, pages 17–28. Springer, 2011.
[17] Ronald C Dodge Jr, Curtis Carver, and Aaron J Ferguson. Phishing for user security awareness. computers & security, 26(1):73–80, 2007.
[18] Serge Egelman, Marian Harbach, and Eyal Peer. Behavior ever follows intention?: A validation of the security behavior intentions scale (sebis). In Proceedings of the 2016 CHI conference on human factors in computing systems, pages 5257–5261. ACM, 2016.
[19] Serge Egelman and Eyal Peer. Scaling the security wall: Developing a security behavior intentions scale (sebis). In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, pages 2873–2882. ACM, 2015.
[20] Mohammadjafar Esmaeili. Assessment of users’ information security behavior in smartphone networks. Eastern Michigan University, 2014.
[21] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L119:1–88, May 2016.
[22] Adrienne Porter Felt, Matthew Finifter, Erika Chin, Steve Hanna, and David Wagner. A survey of mobile malware in the wild. In Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices, pages 3–14. ACM, 2011.
[23] Waldo Rocha Flores, Hannes Holm, Gustav Svensson, and Gran Ericsson. Using phishing experiments and scenario-based surveys to understand security behaviours in practice. Information Management & Computer Security, 22(4):393–406, 2014.
[24] Alain Forget, Saranga Komanduri, Alessandro Acquisti, Nicolas Christin, Lorrie F Cranor, and Rahul Telang. Security behavior observation: Infrastructure for long-term monitoring of client machines. Technical report, CARNEGIE-MELLON UNIV PITTSBURGH PA PITTSBURGH United States, 2014.
[25] Alain Forget, Sarah Pearman, Jeremy Thomas, Alessandro Acquisti, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, and Marian Harbach. Do or do not, there is no try: user engagement may not improve security outcomes. In Twelfth Symposium on Usable Privacy and Security (SOUPS 2016), pages 97–111, 2016.
[26] Vasileios Gkioulos, Gaute Wangen, and Sokratis K Katsikas. User modelling validation over the security awareness of digital natives. Future Internet, 9(3):32, 2017.
[27] Vasileios Gkioulos, Gaute Wangen, Sokratis K Katsikas, George Kavali-eratos, and Panayiotis Kotzanikolaou. Security awareness of the digital natives. Information, 8(2):42, 2017.

[28] Muhammad Haris, Hamed Haddadi, and Pan Hui. Privacy leakage in mobile computing: Tools, methods, and characteristics. arXiv preprint arXiv:1410.4978, 2014.

[29] Mikko Hypponen. Malware goes mobile. Scientific American, 295(5):70–77, 2006.

[30] Tom N Jagatic, Nathaniel A Johnson, Markus Jakobsson, and Filippo Menczer. Social phishing. Communications of the ACM, 50(10):94–100, 2007.

[31] K Jansson and Rossoouw von Solms. Phishing for phishing awareness. Behaviour & information technology, 32(6):584–593, 2013.

[32] Xuxian Jiang and Yajin Zhou. Dissecting android malware: Characterization and evolution. In 2012 IEEE Symposium on Security and Privacy, pages 95–109. IEEE, 2012.

[33] ME Kabay, Bridgett Robertson, Mani Akella, and DT Lang. Using social psychology to implement security policies. Computer Security Handbook, Sixth Edition, pages 50–1, 2002.

[34] Juuso Karikoski and Tapio Soikkeli. Contextual usage patterns in smartphone communication services. Personal and ubiquitous computing, 17(3):491–502, 2013.

[35] Patrick Gage Kelley, Sunny Consolvo, Lorrie Faith Cranor, Jaejeon Jun, Norman Sadeh, and David Wetherall. A conundrum of permissions: installing applications on an android smartphone. In International Conference on Financial Cryptography and Data Security, pages 68–79. Springer, 2012.

[36] Hennie A Kruger, Lynette Drevin, and Tjaart Steyn. A framework for evaluating ic security awareness. In ISSA, pages 1–11, 2006.

[37] Hennie A Kruger and Wayne D Kearney. A prototype for assessing security awareness. communications & security, 25(4):289–296, 2006.

[38] Ivar Krumpal. Determinants of social desirability bias in sensitive surveys: a literature review. Quality & Quantity, 47(4):2025–2047, 2013.

[39] Ponnurangam Kumaraguru, Justin Cranshaw, Alessandro Acquisti, Lor-rie Cranor, Jason Hong, Mary Ann Blair, and Theodore Pham. School of phish: a real-world evaluation of anti-phishing training. In Proceedings of the 5th Symposium on Usable Privacy and Security, page 3. ACM, 2009.

[40] Ponnurangam Kumaraguru, Yong Rhee, Alessandro Acquisti, Lor-rie Faith Cranor, Jason Hong, and Elizabeth Nunge. Protecting people from phishing: the design and evaluation of an embedded training email system. In Proceedings of the SIGCHI conference on Human factors in computing systems, pages 905–914. ACM, 2007.

[41] Mariantonietta La Polla, Fabio Martinelli, and Daniele Sgandurra. A survey on security for mobile devices. IEEE communications surveys & tutorials, 15(1):446–471, 2013.

[42] Agata McCormac, Draga Calic, Kathryn Parsons, Tara Zwaans, Marcus Butavicius, and Malcolm Pattison. Test-retest reliability and internal consistency of the human aspects of information security questionnaire (hais-q). 2016.

[43] Alexios Mylonas, Anastasia Kastania, and Dimitris Grizalis. Delegate the smartphone user? security awareness in smartphone platforms. Computers & Security, 34:47–66, 2013.

[44] Alexios Mylonas, Marianthi Theoharidou, and Dimitris Grizalis. Assessing privacy risks in android: A user-centric approach. In Thomas Bauer, Jürgen Großmann, Fredrik Seehusen, Ketil Stulen, and Marcel Florian Wendland, editors, Risk Assessment and Risk Driven Testing, pages 21–37, Cham, 2014. Springer International Publishing.

[45] Kaan Onarlioglu, Utku Ozan Yilmaz, Engin Kirda, and Davide Balzarotti. Insights into user behavior in dealing with internet attacks. In NDSS, 2012.

[46] Kathryn Parsons, Dragna Calic, Malcolm Pattison, Marcus Butavicius, Agata McCormac, and Tara Zwaans. The human aspects of information security questionnaire (hais-q): two further validation studies. Computers & Security, 66:40–51, 2017.

[47] Kathryn Parsons, Agata McCormac, Marcus Butavicius, Malcolm Pattinson, and Cate Jerram. Determining employee awareness using the human aspects of information security questionnaire (hais-q). Computers & Security, 42:165–176, 2014.

[48] Sancheng Peng, Shui Yu, and Aimin Yang. Smartphone malware and its propagation modeling: A survey. IEEE Communications Surveys & Tutorials, 16(2):925–941, 2014.

[49] James Reason. Managing the risks of organizational accidents. Rout-ledge, 2016.

[50] Elissa M Redmiles, Ziyun Zhu, Sean Kross, Dhruv Kuchhal, Tudor Dumitras, and Michelle L Mazurek. Asking for a friend: Evaluating response biases in security user studies. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pages 1238–1255. ACM, 2018.

[51] Thomas L Saaty. Decision making with the analytic hierarchy process. International journal of services sciences, 1(1):83–98, 2008.

[52] Symantec. Internet security threat report 2018. URL https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf, 2018.

[53] Mark E Thomson and Rossoouw von Solms. Information security awareness: educating your users effectively. Information management & computer security, 6(4):167–173, 1998.

[54] Dirk Van Bruggen, Shu Liu, Mitch Kajzer, Aaron Striegel, Charles R Crowell, and John D Arcy. Modifying smartphone user locking behavior. In Proceedings of the Ninth Symposium on Usable Privacy and Security, page 10. ACM, 2013.

[55] Timothy Vidas, Daniel Votipka, and Nicolas Christin. All your droid are belong to us: A survey of current android attacks. In Woot, pages 81–90, 2011.

[56] Rick Wash, Emilee Rader, and Chris Fennell. Can people self-report security accurately?: Agreement between self-report and behavioral measures. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, pages 2228–2232. ACM, 2017.

[57] Primal Wijesekera, Arjun Baokar, Ashkan Hosseini, Serge Engelman, David Wagner, and Konstantin Benosov. Android permissions remys-tified: A field study on contextual integrity. In Proceedings of the 24th USENIX Conference on Security Symposium, pages 499–514, Berkeley, CA, USA, 2015. USENIX Association.

[58] F Yates. Lattice squares. The Journal of Agricultural Science, 30(4):672–687, 1940.
A. The Security Questionnaire

What is the likelihood of you to perform the following actions?

| Action                                                                 | Never | Unlikely | Medium Likelihood | Very Likely | Always |
|------------------------------------------------------------------------|-------|----------|-------------------|-------------|--------|
| 1. Downloaded application from unofficial application store.          |       |          |                   |             |        |
| 2. Install application that requires permissions that are not necessary for its functionality (figure attached). |       |          |                   |             |        |
| 3. Install applications with a low rating (figure attached).          |       |          |                   |             |        |
| 4. Install application that requires root privileges (figure attached).|       |          |                   |             |        |
| 5. Approve an application update that requires permissions that are not necessary for the applications functionality (figure attached). |       |          |                   |             |        |
| 6. Verify an application update before approving it.                   |       |          |                   |             |        |
| 7. Enter an advertisement while using an application.                 |       |          |                   |             |        |
| 8. Enter an advertisement of a lottery.                               |       |          |                   |             |        |
| 9. Check which applications are installed on the device (figure attached). |       |          |                   |             |        |
| 10. Check which applications are running (figure attached).            |       |          |                   |             |        |
| 11. Close applications that are running in the background (figure attached). |       |          |                   |             |        |
| 12. Delete applications that are not in use.                          |       |          |                   |             |        |
| 13. Enter a website despite a security warning that this site is dangerous (figure attached). |       |          |                   |             |        |
| 14. Download file from a site that does not use an encryption protocol (figure attached). |       |          |                   |             |        |
| 15. Insert private information in a site which does not use an encryption protocol (figure attached). |       |          |                   |             |        |
| 16. Use your personal password in a site which does not use an encryption protocol (figure attached). |       |          |                   |             |        |
| 17. Enter private information (e.g., phone number, email address) into a pop-up that appears while using an application (figure attached). |       |          |                   |             |        |
| 18. Open an email classified as spam (figure attached).                |       |          |                   |             |        |
| 19. Enter a link sent from unknown party (e.g., via Facebook, WhatsApp, SMS). |       |          |                   |             |        |
| 20. Use a simple password that contains known personal details (e.g., name, date of birth, phone number). |       |          |                   |             |        |
| 21. Use a password that is constructed from many different digits and characters. |       |          |                   |             |        |
| 22. Use the same password for different services.                     |       |          |                   |             |        |
| 23. Save your password as plain-text on your device (e.g., in your contacts, document, notes). |       |          |                   |             |        |
| 24. Update your password in case you suspect that someone knows it.   |       |          |                   |             |        |
| 25. Update your password at least once a year.                        |       |          |                   |             |        |
| 26. Use two-factor authentication for email/Facebook (a service in which another authentication is used besides the password - figure attached). |       |          |                   |             |        |
| 27. Use password management services (figure attached).                |       |          |                   |             |        |
| 28. Jailbreak/root your device.                                       |       |          |                   |             |        |
| 29. Use embedded security systems (e.g., firewall, encryption).        |       |          |                   |             |        |
| 30. Install anti-virus application.                                    |       |          |                   |             |        |
| 31. Ignore a security alert (figure attached).                        |       |          |                   |             |        |
| 32. Use screen lock (e.g., PIN code, pattern, fingerprint).           |       |          |                   |             |        |
| 33. Use public (unencrypted) WiFi networks (figure attached).          |       |          |                   |             |        |
| 34. Download files while using a public network.                      |       |          |                   |             |        |
| 35. Use a VPN services while using the internet.                      |       |          |                   |             |        |
| 36. Use personal services (e.g., bank, online shopping, Facebook) while connected to a public Wi-Fi network |       |          |                   |             |        |
| 37. Auto-connect to Bluetooth devices.                                |       |          |                   |             |        |
| 38. Connect your smartphone to foreign device (e.g., a friends computer, wireless headphones). |       |          |                   |             |        |

How often do you turn off the following components in your device?

| Component | Always off, unless needed | Turned on when needed, but often forget to turn off | Turned on if the battery allows | Always on | I didn’t know it could be turned off |
|-----------|---------------------------|-----------------------------------------------------|--------------------------------|-----------|-----------------------------------|
| GPS       |                           |                                                     |                                 |           |                                   |
| Wi-Fi     |                           |                                                     |                                 |           |                                   |
| NFC       |                           |                                                     |                                 |           |                                   |
| Bluetooth |                           |                                                     |                                 |           |                                   |

How frequently do you update the following services/applications on your smartphone?

| Service/application | I use auto-update | When I receive a notification | Once a month | Once in six months | Only when I must |
|---------------------|------------------|-------------------------------|--------------|-------------------|------------------|
| Operating system    |                  |                               |              |                   |                  |
| System applications |                  |                               |              |                   |                  |
| Security applications |                |                               |              |                   |                  |
| Other applications  |                  |                               |              |                   |                  |
### B. The Complete List of Security Awareness Criteria and the Indicators for Measuring Them

| ID | Topics                  | Description                                                                 | Network Indicators                                                                 | Mobile Agent Indicators                                                                 | Questionnaire Indicators |
|----|-------------------------|----------------------------------------------------------------------------|------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|--------------------------|
| **Focus Area: Applications** | **Sub-Focus Area: Application Installation (AI)**                          |                                                                              |                                                                                    |                          |
| AI1 | Untrusted Sources       | Download applications solely from trusted sources                        | Monitor accesses untrusted application sources, monitor downloads of APK files.       | Check the source of installed applications.                                           | Q1                       |
| AI2 | Permissions             | Does not install applications that require dangerous permissions.         | –                                                                                  | Monitor applications that require dangerous permissions and their Google Play ranking is less than 3.5 [1]. | Q2                       |
| AI3 | Rating                  | Does not install applications with a low rating.                         | –                                                                                  | Monitor installed applications with low Google Play rating (less than 3.5).            | Q3                       |
| AI4 | Root/Jailbreak          | Rarely installs applications that require root privileges.                | –                                                                                  | Monitor applications that require root privileges.                                    | Q4                       |
| **Focus Area: Applications** | **Sub-Focus Area: Application Handling (AH)**                              |                                                                              |                                                                                    |                          |
| AH1 | Application Updates     | Regularly update applications                                             | –                                                                                  | Check how many of the installed applications are not up-to-date.                      | Q5, Q6                   |
| AH2 | Advertisements          | Rarely clicks on advertisements                                           | Monitor communication with domains associated with monitoring advertisements clicks (e.g., ad.doubleclick.net). | Monitor communication with domains associated with monitoring advertisements clicks (e.g., ad.doubleclick.net). | Q7, Q8                   |
| AH3 | Application Management  | Properly manages running/installated applications                        | –                                                                                  | Monitor deletion of applications.                                                    | Q9, Q10, Q11, Q12        |
| **Focus Area: Browsing and Communication** | **Sub-Focus Area: Browser (B)**                                           |                                                                              |                                                                                    |                          |
| B1  | Malicious Domains       | Does not enter malicious domains                                          | Monitor accesses malicious domains.                                                 | Monitor accesses malicious domains.                                                   | Q13                      |
| B2  | File Downloads          | Refers to downloadable files via HTTPS.                                   | Monitor downloads of files via HTTP.                                                | Monitor downloads of files via HTTP.                                                  | Q14                      |
| B3  | Data Confidentiality    | Does not send sensitive information via HTTP.                             | Monitor personal information sent as plaintext (using Regex).                       | –                                                                                     | Q15, Q16                 |
| B4  | Pop-ups and Advertisements | Does not insert private information into popups.                       | Monitor transmission of private information around the time at which a pop-up was clicked. | –                                                                                     | Q17                      |
| B5  | Certificates            | Operates in accordance with system/browser alerts and does not use untrusted certificates. | Monitor sessions that include untrusted certificates that were not terminated immediately after the handshake. | Monitor accesses to domains with untrusted certificates.                             | Q13                      |
| **Focus Area: Browsing and Communication** | **Sub-Focus Area: Virtual Communication (VC)**                             |                                                                              |                                                                                    |                          |
| VC1 | Spam                    | Does not open emails/messages received from unknown senders (or spam).   | Monitor communication with spam domains around the time of communicating with email services. | Monitor opens spam emails.                                                          | Q18                      |
| VC2 | Malicious Attachments/URL | Does not download/execute attachments, or click on URL’s received from unknown senders. | Monitor communication with malicious domains around the time of communicating with email services. | Monitor clicks on links sent via SMS from unknown senders.                         | Q19, Q20                 |
| **Focus Area: Browsing and Communication** | **Sub-Focus Area: Account (A)**                                           |                                                                              |                                                                                    |                          |
| A1  | Password Management     | Updates passwords regularly, use unguessable and diverse passwords. Does not store passwords unsafely. | –                                                                                  | –                                                                                     | Q21, Q22, Q23, Q24, Q25, Q26 |
| A2  | Two Factor Authentication | Uses two-factor authentication mechanisms.                              | –                                                                                  | Monitor SMS with authentication codes (i.e., monitor messages associated with two-factor authentication mechanisms). | Q27                      |
| A3  | Keychain Services       | Uses password management services.                                        | Monitor accesses domains associated with password management services.              | Check for the existence of password management applications.                         | Q28                      |
| **Focus Area: Device** | **Sub-Focus Area: Operating systems (OS)**                                |                                                                              |                                                                                    |                          |
| OS1 | Updates                 | Uses an updated OS and configures auto-updates for critical services      | Monitor the device model and OS version (from HTTP user-agent string) and verify that this version is the latest. | Verify that the OS version is the latest.                                             | Q45                      |
| OS2 | Root/Jailbreak          | Does not root or jailbreak the device.                                    | –                                                                                  | Check whether the device is rooted.                                                  | Q29                      |
| **Focus Area: Device** | **Sub-Focus Area: Security Systems (SS)**                                 |                                                                              |                                                                                    |                          |
| SS1 | Embedded Security Systems | Uses embedded security systems.                                      | –                                                                                  | –                                                                                     | Q30                      |
| SS2 | Anti-virus              | Uses anti-virus application regularly to scan the device.                | Monitor accesses domains associated with anti-virus services.                      | Check for the existence of anti-virus applications.                                 | Q31                      |
| SS3 | Security Updates        | Updates security systems.                                                 | Monitor accesses to domains associated with anti-virus services                    | Monitor that security applications are up-to-date.                                  | Q47                      |
|   | Security Alerts | Operates in accordance with security alerts (i.e., does not ignore security alerts). | – | – | Q32 |
|---|----------------|-------------------------------------------------------------------------------------------------|---|---|-----|
| SS5 | Lock Screen | Uses PIN-code/pattern/fingerprint. | – | Check whether a lock screen PIN-code/pattern is defined. | Q33 |

**Focus Area:** Communication Channels  **Sub-Focus Area:** Networks (N)

| N1 | Wi-Fi - Unencrypted Networks | Does not connect to unencrypted networks. | – | Monitor connections to unencrypted Wi-Fi networks. | Q34 |
| N2 | Wi-Fi - Unencrypted Networks | Does not download files on unencrypted Wi-Fi networks | – | Monitor files downloaded while connected to unencrypted Wi-Fi networks. | Q35 |
| N3 | VPN | Uses VPN services on public networks. | – | Monitor VPN client applications installed to the device. | Q36 |
| N4 | Wi-Fi - Unencrypted Networks | Does not transmit private data via unencrypted channels. | – | Monitor private data transmitted while connected to unencrypted Wi-Fi networks. | Q37 |

**Focus Area:** Communication Channels  **Sub-Focus Area:** Physical Channels (PC)

| PC1 | Connectivity | Enables Bluetooth, Wi-Fi, NFC, and GPS while they are in use and only connects trusted Bluetooth and NFC devices, and trusted Wi-Fi networks. | – | Check whether the Bluetooth and/or NFC are turned on while no device is connected. Check whether the GPS is always turned on. | Q38, Q41, Q42, Q43, Q44 |
| PC2 | USB/Charging Connections | Does not use a USB to connect the device to unknown devices. | – | – | Q39 |