Users' perceptions about mobile security breaches

Stiakakis, E., Georgiadis, C., and Andronoudi, A.

University of Macedonia

Abstract Apart from the technological perspective of security in mobile devices and applications, the economic perspective has been increasingly attracting the academic and business interest. This paper aims to investigate the perceptions of mobile users about the economic importance of security breaches. Instead of considering mobile users as a whole, they were examined as distinct user types based on Brandtzæg's mobile user typology. These types are: (i) sporadic users, (ii) socializers, (iii) entertainment type users, (iv) instrumental users, and (v) advanced users. In the context of the research part of this study, a survey was conducted in a sample of smartphone and tablet owners. The five user types were identified in our sample by setting specific classification rules, based on the frequency and the variety of mobile services used. Mobile users' perceptions were assessed in terms of ten different kinds of security breaches. The findings indicated that the user types perceive differently the economic importance of security breaches, implying that the design of security policies and/or the development of tools totally for the community of users are not the appropriate practices. Our research could contribute to the knowledge considering mobile users and their perceptions about security breaches. Mobile content providers and developers could use the findings of this study to evaluate and redesign, if needed, their current strategies so as to meet users' needs regarding security.

Keywords Mobile security economics · Mobile security · Mobile security breaches · Mobile user typology · Mobile user perceptions · Mobile Internet

1 Introduction

The volume of data and users in mobile Internet is a continuously increasing number, which stresses the need for efficient methods of securing mobile applications, services, and devices. The importance of efficient mobile security becomes more urgent due to the habits of numerous mobile users who usually download a great number of applications in their devices. In addition, the abundance of different devices for mobile access, such as smartphones or tablets, leads many developers or companies to implement more and more applications for mobile systems. But, in parallel with the increase of mobile applications, there is an equivalent growth of malicious applications (Dini et al. 2013). Malicious software (malware) could be embedded to the downloaded software and thus, when the users install it to their device, it seeks to find a security gap to cause abnormal behavior, such as to track user's sensitive personal information. Apart from downloading, another aspect of mobile device usage, which is vulnerable to security attacks, is communication and file sharing (Kim et al. 2010). Mobile communication and sharing of sensitive personal or business data require a high level of security (Asokan et al. 2013). Moreover, mobile transaction systems, as for instance in banking or healthcare systems (Oh et al. 2011), require strong authentication techniques to isolate mobile viruses (Dmitrienko et al. 2014).

Huge amounts of money are lost due to security breaches in mobile devices and applications, and the economic impact is amplified by lack of information (Microsoft Corporation 2013) and education of mobile users (Morrow 2012), resulting in additional financial costs. The economic consequences of mobile security attacks may considerably be reduced by maintaining proper antivirus software. We have to underline though, that the complexity of the design of useful antivirus is a big challenge due to the size of mobile devices. There is a majority of proposed frameworks for the development of successful antivirus software in the classic computers, such as desktops and laptops. However, when we talk about mobile devices the task becomes harder due to their limitations (Li and Clark 2013). The size, for instance, does not allow security software developers to use the same (or even similar) antivirus methods, so they need to implement new techniques and methodologies in order to encounter all possible threats (Rhee et al. 2013). Moreover, mobile users tend to adopt free trial solutions that are offered with limitations to functionality, availability or usage convenience until a full paid licence is purchased (Wang et al. 2013).

Notwithstanding that the technological perspective of security in mobile devices and applications has been examined to a significant extent, the perspective of user's behavior, as for instance the factors that influence their intention to use mobile applications (Noh and Lee 2015), needs much further investigation. According to Tu et al. (2014), behavioral research on mobile security is very limited since most of mobile security studies focus on technical issues or organizational perspectives. With the increasing use of mobile digital content, it is of high importance to understand the behavior and the adoption of the mobile world by users so that optimum value can be delivered and revenue objectives can be achieved (Liu et al. 2014). It should be noted that, nowadays, practitioners and academics point out the economic aspect of security since they gradually realize that it is very difficult to achieve an adequately secure environment simply through technology (Gao et al. 2013). However, this aspect has been examined in m-commerce related articles to an extremely low degree (Kourouthanassis and Georgiadis 2014). The purpose of this paper is to investigate the perceptions of mobile users concerning the economic impact that security breaches have upon them; and will attempt to do that, focusing on specific mobile user types rather than seeing the users as a whole. The findings of this research could contribute to the comprehension of how mobile users react to the various kinds of security breaches, as well as to assist software

companies to develop more effective tools per user type, and companies which introduce new technologies in their workplace to adapt their security policies to the user type of their staff.

The rest of the paper is structured as follows: Section 2 provides an overview of mobile user typologies and security breaches in mobile devices and applications. The methodological approach followed in this study is presented in Section 3. A description of the survey which was conducted to serve the purpose of this study is given in Section 4, while our findings are presented in Section 5. Finally, we conclude in Section 6.

2 Literature review

2.1 Mobile user typology

In order to understand the security needs and vulnerabilities of users, it is indispensable to identify a unified comprehensive user typology. Moreover, a mobile user typology is a prerequisite to measure the economic impact of security breaches on the corresponding mobile users. There are several mobile user typologies due to the rapid increase of users and the advances in mobile technology (e.g. Mort and Drennan 2005; Kietzmann et al. 2013). Mobile phones have a general user typology that falls into three categories of users (Webliquid 2012): i) voice users, who only take advantage of the communication features that mobile devices offer, (ii) SMS users, who utilize mostly the texting capabilities of their device, and (iii) mobile media users, who exploit every possible innovation and feature that either devices or applications provide.

Brandtzæg (2010) reviewed 22 studies by comparing different media user typologies and models with each other as they had different research methodologies, research areas, and design. Brandtzæg noticed that previous studies ignored crucial factors and led to oversimplified explanations of how users employ media and how they are affected by the rapidly changing technology. In terms of creating a common framework to understand media behavior in the same way, Brandtzæg (2010) proposed a unified media user typology (MUT) concerning the 22 studies. According to Brandtzæg (2010; 2012), there are four main criteria for defining user types by media behavior. These are: frequency of use, media platform, variety of use, and content preferences. The initial typology consisted of eight different user types: (i) non-users, (ii) sporadic users, (iii) debaters, (iv) entertainment type users, (v) socializers, (vi) lurkers, (vii) instrumental users, and (viii) advanced users. In 2012, Brandtzæg managed to specify the initial MUT model in the mobile era. He noticed that the MUT model connects well with the mobile world since five of the initial user types corresponded to the types identified in mobile technology. Regarding the above mentioned criteria, a unified mobile user typology was introduced, which is the typology adopted in our study. Mobile users can be grouped into five major types, namely, (i) *sporadic users*, (ii) *socializers*, (iii) *entertainment type users*, (iv) *instrumental users*, and (v) *advanced users* (Brandtzæg 2012).

Sporadic are the users who do not frequently use smart devices due to lack of knowledge to do so. Sporadic users' major concern is communication through phone calls or texting (SMS, MMS). Socializers constitute the second user type; many mobile users make use of their devices primarily as a means of interaction and bonding with friends and family by accessing social media networks, such as Facebook and Twitter. Socializers also include the bloggers and in general all users involved in various social activities (e.g. generating, sharing, syndicating, and disseminating information); it is worth mentioning that they spend considerable time for building and retaining a personal profile (Huang and Benyoucef 2013). The entertainment type users employ

mobile devices as a means of amusement, mainly gaming and video viewing, but also browsing the Web and visiting information based sites in order to 'infotain' (inform plus entertain) themselves.

Instrumental users are interested in e-government, e-banking, and office applications, not only for personal use but also for matters related to their workplace. The activities of instrumental users are utility oriented, well organized, and purposeful (Brandtzæg 2012). For example, instrumental users are those who implement *Bring Your Own Device* (BYOD) policies in their workplace. BYOD movement is an emerging business strategy that permits employees, partners, and other users to carry out enterprise applications and access business information through their personally owned devices (Calder 2013; Pillay et al. 2013). Finally, advanced users exploit most of mobile device capabilities since they are well informed about the features of their smart devices and generally about the innovations in mobile industry and new technologies. Advanced users are regarded as a mixture of the aforementioned user types. This means that an advanced user can act as a sporadic user in his personal relationships, an instrumental user at work, a socializer when communicating with their social environment, and even as an entertainment type user when they relax and 'infotain' themselves. The mobile user typology analyzed above and the four main drivers that led to the user types are summarized in Table 1.

Table 1 Mobile user typology (Brandtzæg 2012)

Mobile users	Frequency of use	Media platform	Variety of use	Content preferences
Sporadic user	Low	All	Low	Low use-low interest-low experience tasks
Socializer	Medium	Social media networks	Low	Keep in touch with friends, less organized and purposeful
Entertainment type	Medium	New media in general	Medium	Gaming, video watching, infotainment, programming & e-shopping
Instrumental user	Medium	New media in general including Internet and e-shopping	High	Low entertainment use, e-shopping, e-government apps, social media marketing, work related content
Advanced user	High	All	High	All the above mentioned

2.2 Security breaches

Even though users might have different incentives, as discussed in Section 2.1, they all store data in their personally owned smart devices. These data can be classified into four groups, namely, sensitive personal data, multimedia material, passwords, and confidential documents. Notably, the majority of mobile users store sensitive personal data in mobile devices, such as personal identification data, e-mail and home addresses, health records, as well as personal information of all the contacts they have in their mobile address book. A separate data group is related with multimedia material; approximately 50% of users have multimedia material stored in their devices, such as photos, videos, and music, according to the results of a survey conducted by the Ponemon

Institute (2012). This can be explained by the fact that smartphones nowadays replace devices (e.g. video cameras) by offering multiple services in one device.

The third data category includes personal passwords not only for the particular device that the user owns but also for other devices. Moreover, users store passwords for credit/debit cards, social media, and other e-services that require password in order to gain access. Not surprisingly, taking into consideration that smart devices are also well-known for their 'electronic wallet' dimension with which financial transactions take place, one out of three users, according to the survey of the Ponemon Institute (2012), store passwords of credit cards in their device. Additionally, a great proportion of mobile users have in their devices confidential documents that can be either personal or work-related (Jech 2012). Technology in mobile security is still in its infancy, putting individual's privacy at high risk (Li and Clark 2013). The data categories in mobile devices and their relevant content are mentioned in Table 2.

Table 2 Mobile data categories

Data categories in mobile devices	Relevant content
Sensitive personal data	Personal identity card's number E-mail & home address Health records Address book-contacts' personal information
Multimedia material	Videos Photos Music
Passwords	Credit/debit cards' PINs Various passwords in e-services Passwords related to social media accounts
Confidential documents	Personal documents or documents related to working purposes

The great variety of features that smart devices offer has resulted in a robust growth of the mobile industry. The main idea for understanding the various offered services and applications in a context of mobility is to analyze and understand in depth the differences amongst them and the kind of value that they offer (Bouwman et al. 2009). The rise in popularity and functionality of smart devices and applications has also drawn illegal/fraud activities (La Polla et al. 2013). Jech (2012) asserts that the advent of mobile applications and tools from a lot of companies and private users has improved, from the one hand, firms' profitability and facilitated the operation of functions, and from the other hand, created the need for more effective security policies.

According to Cate (2008), security breach or violation is any incident that results in unauthorized access of data, applications, services, networks, and devices by bypassing their underlying security mechanisms. More specifically, mobile security breaches can be classified into two main categories. The first category occurs during a loss/theft of a device while the second includes all the incidents of malware attacks in devices and applications. Regarding both categories, their main outcome is data leakage (Milligan and Hutcheson 2008). Data leakage implies personal data loss that could guide the attacker to several kinds of financial fraud (Chun 2011). Data leakage in a business environment refers to obtaining information about enterprise transactions, secret business policies, strategic plans, innovations etc. (Jech 2012). It should be noted that the cost of mobile security breaches in many business domains (e.g. health organizations) can be extremely high (Collier 2012).

The loss and theft of a mobile device are security risks which are unique to mobile devices (Scott 2004). When a device is lost or stolen there might be many security issues: to begin with, a notable feature is that 66% of all mobile users utilize a PIN authentication for switching on the device but only 18% of them also utilize this kind of security for other functions of the device (Clarke and Furnell 2005). As a result, mobile devices can be stolen without any difficulty and the users not only will have lost their device and the data stored in it but they will also have to buy another one as well. The survey of the Ponemon Institute (2012) also reveals that 51% of users do not have keypad locks or passwords to secure their device. In that way, the attackers gain access to the device and they can do illegal actions, such as processing financial transactions, making phone calls, and sending messages that exceed the normal cost of the user's bill. Also, it is estimated by the same survey that 52% of users never check their mobile bill for unidentified charges. The attacker can use the data stored in the device in order to gain access to social media and other services and then use techniques, such as cyber-bullying, as according to Dimensional Research (2012), personal information obtained from smart devices can be sold in the market at a premium.

With respect to the second category of security breaches, their main outcome is mobile malware attacks. There are many ways malware attacks can occur. One way is through infected programs received via Bluetooth and other ways that the Bluetooth technology supports (Sharma 2008). A second way is through telephony when unauthorized phone calls are made with high costs or illegal recordings (Pocatilu 2011). Another infection route is the messaging area where short and/or multimedia messages (SMS or MMS) are sent. Lumsden (2012) reports that there have been hidden charges due to short messages, which mislead users with their actual (not free) content. Mobile users usually realize the real cost too late. This is because the messages do not charge users a lot per month but their aggregation turns out to be a considerable amount of money. Moreover, these messages steal confidential content (e.g. phonebooks), charge the mobile user's bill and can additionally provide to attackers access to paid numbers, e-services including social media, and multimedia content. Wireless networks, which offer malicious downloads of games-applications and data transport (Pocatilu 2011), and malicious codes in webpages accessed by users though their mobile phone browsers (Shih et al. 2008) constitute another path for the attackers. Security breaches can also occur through near field communication (Ondrus and Pigneur 2009), widely used for unauthorized payments leading to financial frauds. Ramu (2012) points out that the contemporary nature of mobile devices and applications, along with the ongoing interest in mobile technology, will lead to the appearance of more weaknesses and risks.

3 Methodology

3.1 Mobile user types and security breaches

As already mentioned, this paper aims to investigate how the various mobile user types perceive the economic impact that security breaches have upon them. In the context of this investigation, we make use of the mobile user typology of Brandtzæg. The reason for choosing this typology is the included content that is offered for current and future use. In other words, the five distinct types can support future emerging trends and characteristics of the end-users. Firstly, we should focus on the kinds of security breaches that each mobile user type is mainly exposed. Since each mobile user type has its own characteristics which discriminate it from the

other types, security breaches have a different impact on each type. Moreover, each user is characterized by their content preference which is exploited, either through a data loss/theft or a malware attack, by the attackers.

In the case of a sporadic user, the attacker can only exploit his address book as the main activity of such users is communication through phone calls or texting messages (SMS, MMS). Socializers tend to have their social media passwords stored in their mobile devices. As a result, the attacker can easily gain access in their account and gather useful information, such as personal identity data and multimedia material, either personal or concerning the user's friends. After this, the attacker will be able to complete financial transactions or apply cyber-bullying techniques with or without money demand.

Entertainment type users prefer gaming and generally amusement activities. They usually have passwords and sensitive data stored in their devices as such kind of information is often required from gaming platforms and other applications. Moreover, some amusement activities include e-transactions. To this end, entertainment type users can store in their smart devices passwords which will lead a potential attacker to illegal transactions through identity theft.

Instrumental user is probably the user who is mostly exposed. As analyzed in Section 2.1, instrumental user's major activities are work related, utility oriented, and purposeful. They use applications and tools in order to achieve business goals. These users store confidential documents and passwords in their devices which are mainly related with their working environment. When a security breach occurs, there is high risk of exposing not only personal information but also confidential data concerning an enterprise with its clients, suppliers, and working force. Competitive advantages, strategic plans, and business secrets might also be at risk (Gest 2013). It is no coincidence that BYOD users were classified as instrumental users since the most important challenges of BYOD movement are data loss risk, lack of control, and increased security costs (Pillay et al. 2013). Finally, advanced users are exposed to all security breaches as they are a mixture of the above types and they have occasionally all their characteristics.

3.2 Classification of security breaches

In order to investigate the economic implications of mobile security breaches and how mobile users perceive their importance, we first analyzed the two main categories of security breaches, i.e. device loss/theft and malware attacks in devices and applications, into their most usual incidents. Malware attacks usually include malicious programs that either run without legal permission (from the owner in this case) or do not reveal their entire function and the related features from the beginning. In particular, such malicious sources usually pretend to be something useful and safe; however, as soon as they overtake the installed security mechanisms, they infect the devices and the data stored in them with undesirable consequences for the users. The usual incidents of security breaches, which were identified, were further classified into three groups, as presented in Table 3: (i) breaches belonging to device loss/theft, (ii) breaches belonging to malware attacks in devices and applications, and (iii) breaches belonging to both main categories. The rationale of classification is shortly analyzed below.

Table 3 Classification of the most usual incidents of mobile security breaches

Usual incidents of mobile security breaches	Device loss/theft	Malware attacks in devices and applications
Breach 1: Device theft compelling the user to buy a new device	✓	
Breach 2: Password interception leading to costly phone calls by unauthorized users	✓	
Breach 3: Unintentionally receiving or sending charged messages		✓
Breach 4: Unintentional Internet connection with charge		✓
Breach 5: Malicious software infection resulting in undesirable consequences for the user		✓
Breach 6: Unexpected charges due to unintentional phone calls		✓
Breach 7: Unauthorized access to multimedia material	✓	✓
Breach 8: Identity and personal data interception	✓	✓
Breach 9: E-banking and/or credit/debit cards' passwords interception	✓	✓
Breach 10: Cyber-bullying	✓	✓

When a mobile device is lost or stolen, a number of security breaches can occur. Firstly, the involved users have to buy a new device as they no longer can access their regular device. Security breaches that are related to password interception lead finally to high charges. The attacker uses the device for making phone calls and sending messages (SMS, MMS). Such security breaches occur only with the 'aid' of an unauthorized user and this is the reason for classifying them into the first group. The attacker is the unauthorized user who overtakes password mechanisms (if they exist), either with hacking or malware tools. In this case, the attacker acts purposefully whereas a typical malware attack takes place without user's concurrence. Correspondingly, the second group of security breaches is analyzed below. During a malware attack, the device, the legal owner, and their stored contacts are exposed to unintentional charges and other undesirable consequences. There are malware attacks whose major characteristics are the high charges due to sending or receiving messages unintentionally. Moreover, there are malicious applications and tools that charge users by fulfilling unauthorized Internet connections. The legal owner realizes these connections only when the charges become extremely high. The second group strictly includes the security breaches that contain malware software which infects afterwards the device. The user, in this case, downloads such software without knowing or even underestimating the risks and the malicious code that stand behind. Additionally, during a malware attack, unexpected charges due to unintentional phone calls can occur, as there are many malware techniques that can penetrate in the calling system.

There are security breaches that can take place either during a device loss/theft or due to a malware attack (third group). For example, access to multimedia material can be obtained not only from the attacker during a device theft but also from a malicious program during a malware attack. Regarding both categories of security

breaches, their major and highly concerned feature is identity and personal data interception. This interception refers not only to legal users but to their entire contact book maximizing the importance of such breaches. Identity and personal data interception can finally lead to other undesirable consequences as this valuable information can be used in order to accomplish financial transactions either through banking frauds or cyber-bullying actions. Security breaches that include cyber-bullying behaviors can also happen either through a device loss/theft or a possible malware attack. With respect to a possible device loss, the attacker who has the device and the data stored in it under their possession can proceed into cyber-bullying actions. The illegal user can take advantage of the multimedia material, social media accounts, and various passwords (e-banking, e-shopping, and e-service accounts in general). Similarly, a malicious tool can gain access to all the aforementioned sources. The related entity behind the malicious tool can finally demand money for not publishing or utilizing the valuable 'stolen' information.

The classification of mobile security breaches considers that during a possible malware attack, unintentional charges and undesirable consequences can occur. Malware attacks arise with the 'aid' of a malicious tool whereas breaches concerning a possible device loss/theft require an unauthorized user. In a device loss/theft, the attacker can employ malware techniques in order to have access to personal data; however, the attacker has usually limited time to act before the legal owner proceeds to law enforcing actions. As a result, such security breaches remain either unfinished or cause negligible charges to the legal owner and they have not been considered in our research. As mentioned earlier, there are breaches which have been classified into the third group. Such breaches include acts/techniques that can be done/used either by a possible attacker (group 1) or a malicious program (group 2).

4 Research

Based on the literature review of this study and our methodological approach concerning the analysis of mobile security breaches into their most usual incidents, as well as the identification of breaches that mobile user types are mainly exposed, the following research questions and resulting hypotheses are formulated:

RQ1: Is the typology proposed by Brandtzæg a trustworthy typology concerning mobile user types (so that it can be used for the evaluation of the economic impact of mobile security breaches upon users)?

H1: The five user types of Brandtzæg's typology reflect all possible types of mobile users.

RQ2: Can mobile security breaches be classified into specific groups with common characteristics?

H2: The most usual incidents of mobile security breaches can be classified into three groups, based on their common characteristics when occurring.

RQ3: Do the mobile user types (of Brandtzæg's typology) perceive differently the economic impact of security breaches?

H3: The five user types of Brandtzæg's typology perceive differently the economic impact that security breaches in mobile applications and devices have upon them.

In order to test the aforementioned hypotheses, a survey was selected as the research tool of this study. The sample included owners of smartphones and tablets and the survey was accomplished in a 6-month period in the broader area of Thessaloniki, the second largest city in Greece based on population. The sample size was 2,769

mobile users and the data were collected through personal interviews and online forms. The synthesis of the whole sample was as follows: 1,206 mobile users (43.6%) through personal interviews and 1,563 mobile users (56.4%) through online forms.

The use of both personal interviews and online forms provided us the possibility to increase the sample size and accomplish the survey without the collection process having been influenced by geographical restrictions. We used a structured questionnaire which consisted of scaled and multiple-choice, but not open-ended, questions. The personal interviews were conducted with the aid of the undergraduate students of our university department (an IT department), who played the role of the interviewer. The interviewees were mainly students from the university campus (located in the center of the city) and staff from the university, shops, and companies in the city of Thessaloniki. They were selected on the basis of having an approximately proportional representation from all the areas of the city. Our goal was to attain a dispersed sample with one single condition that the units of the sample would be necessarily owners of smartphones and tablets. Households were not selected since it was difficult to have a representative sample in terms of certain selection criteria.

The online forms were created with the aid of the Google forms tool that enabled us to develop this part of the survey online and share the link of the questionnaire via email. Online responses were mostly received by students and staff of technological institutions, as well as people working in enterprises, around the city of Thessaloniki (malls, business parks, industrial enterprises, etc.). The response rate in the online part of the survey was about 19%. Notwithstanding the low response rate, though expected, online forms were a very useful tool to approach mobile users in areas, where a personal interview would be difficult to take place. There were some differences between the two sub-samples which are indicated in Section 5 (Findings). However, what is important is that all user types of Brandtzæg's typology were identified in both sub-samples, meaning that both could be used for the purpose of our survey.

Some indicative demographic data of the whole sample are given below. There was an equal participation concerning the gender while most of the respondents belonged to the age categories of 18-24 (38%) and 25-35 years old (23%). Regarding the level of education, the major category comprised people who had obtained or were in progress of obtaining their bachelor's degree (57%). The major occupation category consisted of students in universities and technological institutions (36%). It is interesting to be noted that the operating system mostly used was Android (42%) and that the respondents stated that they were quite familiar (38%) and very familiar (29%) with their device, smartphone or tablet. However, they stated that they were quite and very informed only at 19% and 5% respectively, regarding security issues in mobile devices and applications.

In the questionnaire there was intentionally no question to ask directly about the type that each mobile user belongs. This was considered the right choice since mobile users are not aware of the names and/or the characteristics of the various types. The classification of the participants in the survey into each mobile user type was achieved based on: 1) which mobile services are used and 2) how often they are used. The most usual mobile services (except for phone calls) were matched with the five mobile user types, as given in Table 4. This was done considering the characteristics of the user types as analyzed in Section 2.1. As it can be seen, the sporadic user type mostly sends and receives SMS/MMS, while the advanced user type utilizes all the available services. The main services for each user type are underlined (except for the advanced user who acts as a mixed type since they may use all the services to a greater or lesser extent).

Table 4 Matching of mobile services with mobile user types

Mobile user type	Mobile service
Sporadic user	SMS/MMS
Socializer	SMS/MMS, e-mail, social media, multimedia
Entertainment type	SMS/MMS, e-mail, social media, multimedia, games, information, browsing the Internet, e-shopping
Instrumental user	SMS/MMS, e-mail, social media, information, browsing the Internet, e-shopping, e-banking, file/software downloading, file/software uploading, office applications
Advanced user	SMS/MMS, e-mail, social media, multimedia, games, information, browsing the Internet, e-shopping, e-banking, file/software downloading, file/software uploading, office applications

After matching the most usual services with the user types, the identification of these types in our sample was based on the frequency of use of the main services. Regarding the frequency of use, there were the following choices in the questionnaire: (a) none, (b) rarely, i.e. few times per week, (c) moderately, i.e. about 1 hour per day, (d) often, i.e. about 1-3 hours per day, and (e) very often, i.e. more than 3 hours per day. We used this scale taking into consideration the respective scale in Brandtzæg's typology (see Table 1). However, we preferred to spread the scale of Brandtzæg by taking five, instead of three, points in the measurement scale. This choice provides more discriminating power to the 'frequency of use' variable. So, 'low' in Brandtzæg's typology corresponds to 'none' and 'rarely' in our scale; 'medium' in Brandtzæg's typology corresponds to 'moderately' in our scale; finally, 'high' in Brandtzæg's typology corresponds to 'often' and 'very often' in our scale. Moreover, regarding the 'variety of use' variable in Brandtzæg's typology, we can see in Tables 1 and 4 how the three points in the measurement scale of Brandtzæg ('low', 'medium', and 'high') correspond to the number and type of mobile services that we used to identify the five user types in our sample. The rules followed to classify each participant in our survey into the proper user type are summarized below:

- Those who use SMS/MMS often and very often are *sporadic users*. Since we are talking about owners of smartphones and tablets, the consideration of an individual who only sends or receives SMS/MMS less than 1 hour per day in this user type does not make sense. If someone uses SMS/MMS not so much, but also makes use of e-mail (which is not the main service of the next user type) often and very often is a sporadic user as well.
- Those who use social media and/or multimedia (photos, videos, music) often and very often belong to *socializers*. Someone, for example, who uses SMS/MMS plus e-mail plus social media (all of them, often and very often) is a socializer.
- The often and very often use of games, browsing the Internet, and e-shopping is the criterion to classify a respondent as an *entertainment type user*. Even if someone uses only one of the main services of this type to a large extent is also an entertainment type user. For example, if someone uses SMS/MMS plus multimedia plus games (one of each aforementioned user type) has entertainment as their main activity in their mobile devices.
- Office applications, downloading and uploading of files and software, and e-banking are the main services of an *instrumental user*. The often and very often use of either one or more of these services classifies a

respondent into this user type. For example, if someone mostly uses office apps, as well as social media plus games to a lesser extent is an instrumental user.

- As already mentioned, the *advanced user* is a mixed type. This implies that the classification of the respondents into the other four user types should be completed before identifying the advanced users. These are the users who employ the most of the mobile services to a small or medium extent and the users who employ the main services of two or three of the other user types (the sporadic user type is not taken into account) to a large extent. If someone mostly uses both social media and office apps is an advanced user.

5 Findings

Based on the classification process described in the previous section, we tried to identify the five distinct types in our sample and study their perceptions regarding mobile security breaches. In other words, we tried to develop their profile in order to firstly identify the five types and then concentrate on the behaviors, motivations, and intentions of each category regarding mobile security breaches. The use of profiles (or personas) enabled us to better understand the users, their needs, how they react on certain incidents, and in our case how they perceive the economic importance of security breaches.

The respondents in our survey were classified into the five mobile user types as follows: 521 sporadic users, 383 socializers, 643 entertainment type, 345 instrumental, and 758 advanced users, in a total of 2,769 individuals. It was not possible to classify 119 mobile users (4.3%), mostly because the use of all the services in those cases was very low. The percentages of the mobile user types according to the survey results are shown in Fig. 1. Comparing the percentages of the two sub-samples, in relation to the data collection method, there were some noteworthy differences. The percentage of sporadic users was much higher when the data were collected through personal interviews, while socializers prevailed, as it was expected, in the sub-sample of online forms. In the other three user types, there were not significant differences. It should be noted that, despite the smaller or bigger differences, all the five user types were identified in both sub-samples with adequate (non-trivial) percentages. In this way, the resulting sample was appropriate to be used in order to draw conclusions about how the mobile user types perceive the economic importance of security breaches. Hypothesis H1 is confirmed since all the user types of Brandtzæg's typology, as they arose after matching services with user types, were identified in our sample.

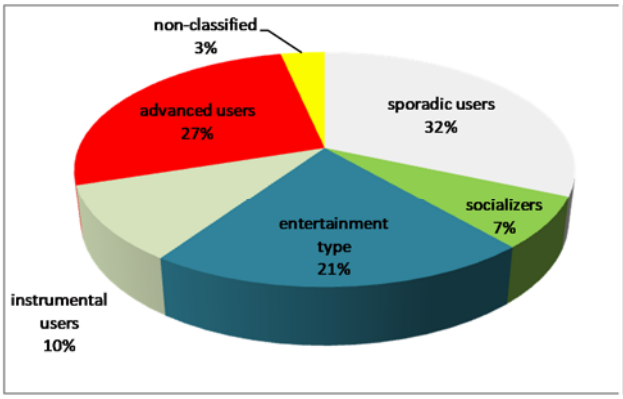

Fig. 1a Percentages of the mobile user types (personal interviews)

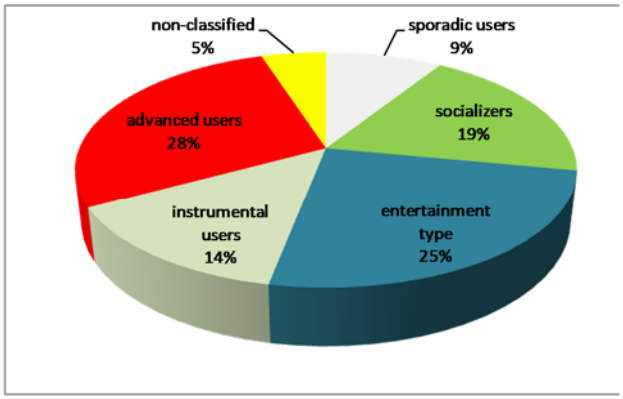

Fig. 1b Percentages of the mobile user types (online forms)

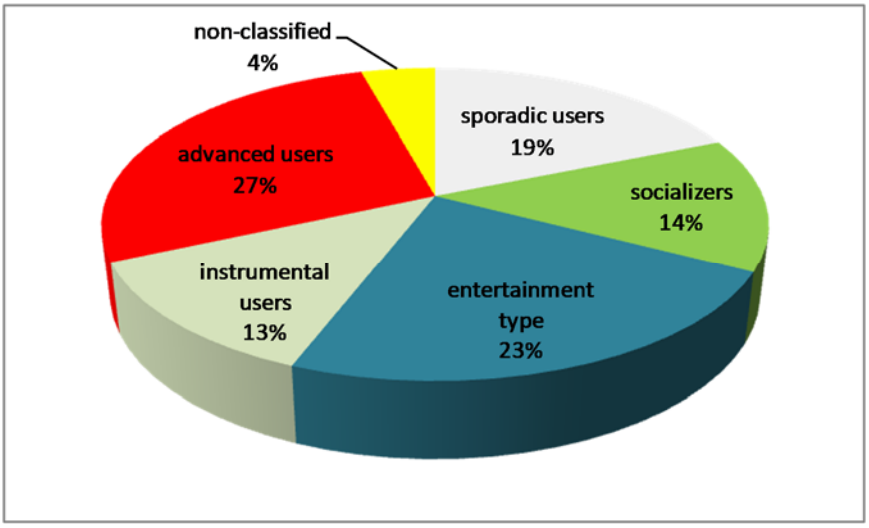

Fig. 1c Percentages of the mobile user types (whole sample)

The participants in the survey were asked to select and rate the five more important security breaches according to how they perceive the economic impact of breaches upon the user. They were given the ten breaches included in Table 3. Therefore, a breach could be rated as the most important, more important, moderately important, less important, and the least important (out of the five selected) or non-selected. The results for each mobile user type are illustrated in Fig. 2.

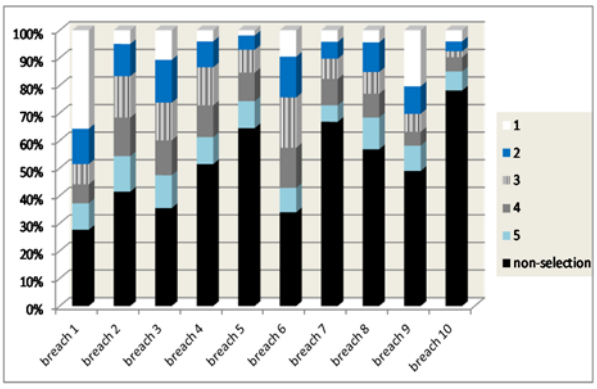

Fig. 2a Economic importance of security breaches on sporadic users

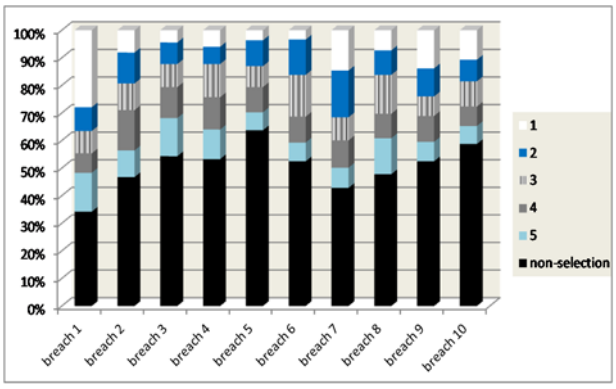

Fig. 2b Economic importance of security breaches on socializers

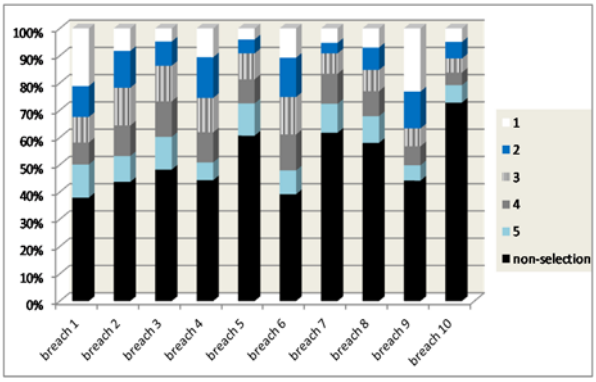

Fig. 2c Economic importance of security breaches on entertainment type users

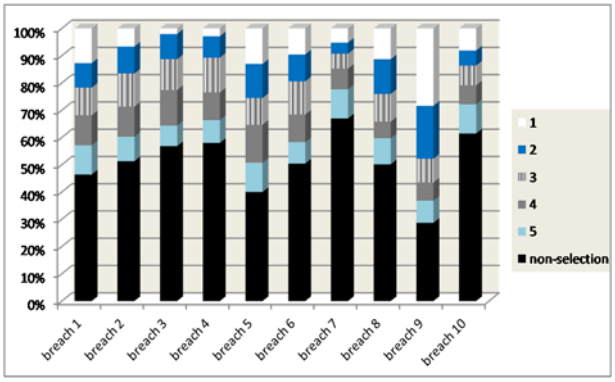

Fig. 2d Economic importance of security breaches on instrumental users

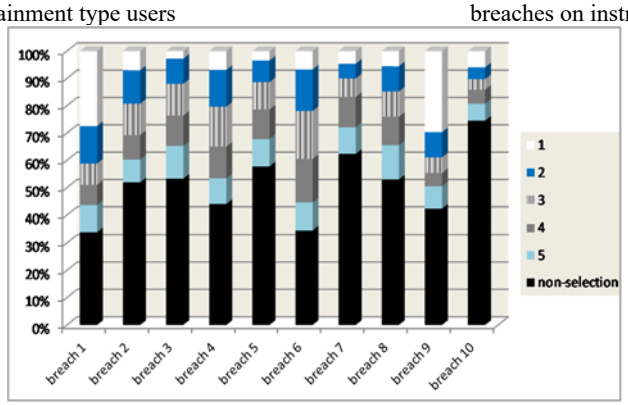

Fig. 2e Economic importance of security breaches on advanced users

where "1" corresponds to the most important breach till "5" to the least important (out of five breaches maximum selected).

Sporadic users perceive as most important the device theft (breach 1) and following that, breach 6, i.e. the unexpected charges due to unintentional phone calls (looking at the fewest non-selected responses). In order to compare easily and directly (through a perusal of the figures above) the results for all user types, the analysis which follows is based on the calculation of the sum of ratings "1" and "2" ("most important" and "more important"). This sum represents the percentage of respondents who consider a breach to be more important than the average score of importance, i.e. rating "3", with regard to its economic impact on the user. Apart from breaches 1 and 6, breach 9 (e-banking and/or credit/debit cards' passwords interception) has a high percentage (30.3%) in ratings "1" and "2", as well as breach 3, i.e. unintentionally receiving or sending charged messages (26.3%).

The results for socializers are quite different. The respective percentage for breaches 1 and 6 is smaller, whilst breach 9 has the smallest percentage compared to the other types of users (24%). This is noteworthy since breach 9 is a kind of breach in that a great number of users are generally involved. Socializers mostly worry about breach 7, i.e. the unauthorized access to multimedia material (31.6%) and breach 10, i.e. cyber-bullying (18.5%). It can be seen that in the other user types, cyber-bullying received a much lower percentage.

For entertainment type users, the economic impact of breaches 2 (password interception leading to costly phone calls by unauthorized users), 4 (unintentional Internet connection with charge), and 6 (unexpected charges due to unintentional phone calls) seems to be the highest, compared to the other user types. On the other hand,

they do not care so much about the interception of their personal data or cyber-bullying. Regarding the interception of passwords of their cards, they worry to a great extent just like the most user types do.

The perceptions of instrumental users differ in several cases as well. The results show that they do not pay much attention in device thefts; they do not also worry about unintentional Internet connections, at least to the extent the other user types do. However, they perceive as very important the malicious software infection (25.5%), as well as the interception of e-banking and/or credit/debit cards' passwords (47.8%). This percentage is much higher than the other user types and one of the largest for all the breaches. These findings are in agreement with the work related activities of instrumental users and the sort of data they usually store in their devices (mostly business data).

The advanced user is a mixed type and this is shown in their perceptions. There were not any very high percentages, always in comparison with the other user types, for ratings "1" and "2". This is because advanced users do not have any extreme preference for a breach, as it occurs with the other user types. Device theft received a high percentage (41.2%), as well as the interception of e-banking and/or credit/debit cards' passwords (38.9%). Generally, the advanced user perceives the economic importance of security breaches as the average user does. This implies that Fig. 2e provides also an overall view of the economic impact of security breaches on mobile users, independently of the specific user type examined.

A summary of the results is given in Table 5, which presents the weighted average and the ranking order of the breaches for each user type. The weighted average is calculated as follows: the breach which is assessed in the first position of importance is given 5 points, the second 4 points till the breach in the fifth position which is given 1 point. No points are given for non-selected breaches. Then, each number of points is multiplied by the corresponding frequency and their total sum is divided by the total of frequencies. In this way, the influence of a breach non-selection is taken into account in the calculation of the weighted average. If, for instance, we divided by the sum of frequencies, only for the selected breaches, then a breach, which would have been selected by a small number of respondents, could be assessed in a higher position. There are significant differences regarding how the five types of mobile users perceive the economic impact of security breaches, confirming hypothesis H3. If we wanted to have an overall view on the perceptions of mobile users for all the user types, we could say that breach 1 (device theft compelling the user to buy a new device) and breach 9 (e-banking and/or credit/debit cards' passwords interception) are assessed as the most important, while breach 10 (cyber-bullying) is assessed as the least important.

Table 5 Perceptions of the economic impact of mobile security breaches for each of the five user types

	Sporadic users		Socializers		Entertainment type users		Instrumental users		Advanced users	
	Weighted Average	Ranking Order	Weighted Average	Ranking Order	Weighted Average	Ranking Order	Weighted Average	Ranking Order	Weighted Average	Ranking Order
Breach 1	2.75	(1)	2.27	(1)	2.07	(2)	1.63	(3)	2.40	(1)
Breach 2	1.58	(5)	1.53	(4)	1.69	(5)	1.40	(6)	1.45	(5)
Breach 3	1.94	(3)	1.15	(9)	1.37	(6)	1.15	(7)	1.20	(7)
Breach 4	1.32	(6)	1.25	(8)	1.79	(4)	1.13	(8)	1.65	(4)
Breach 5	0.86	(9)	1.03	(10)	0.99	(8)	1.83	(2)	1.11	(8)
Breach 6	2.00	(2)	1.39	(6)	1.88	(3)	1.52	(5)	1.89	(3)
Breach 7	0.93	(8)	1.93	(2)	0.97	(9)	0.85	(10)	0.97	(9)
Breach 8	1.17	(7)	1.45	(5)	1.19	(7)	1.60	(4)	1.26	(6)
Breach 9	1.80	(4)	1.57	(3)	2.09	(1)	2.67	(1)	2.20	(2)
Breach 10	0.58	(10)	1.33	(7)	0.80	(10)	1.09	(9)	0.75	(10)

In another question, the participants were asked to evaluate the cost of breaches that had occurred to them. This is a different question compared to the previous one in which the user perceptions of the economic importance of security breaches were measured. In this question, only the individuals, who had experienced one or more incidents of a breach, were able to answer. If they had experienced more than one incidents of the same breach, they should have assessed the average cost. The results are presented in Fig. 3.

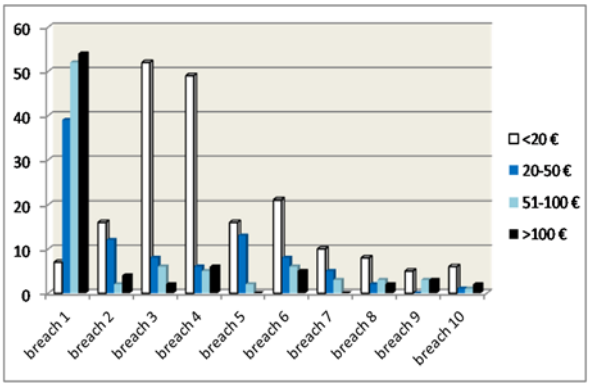

Fig. 3a Cost evaluation of security breaches occurred to sporadic users

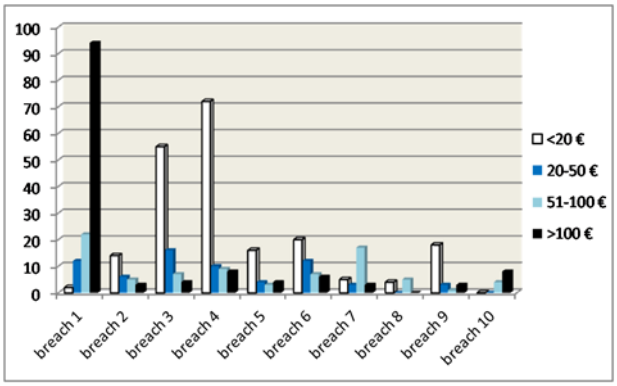

Fig. 3b Cost evaluation of security breaches occurred to socializers

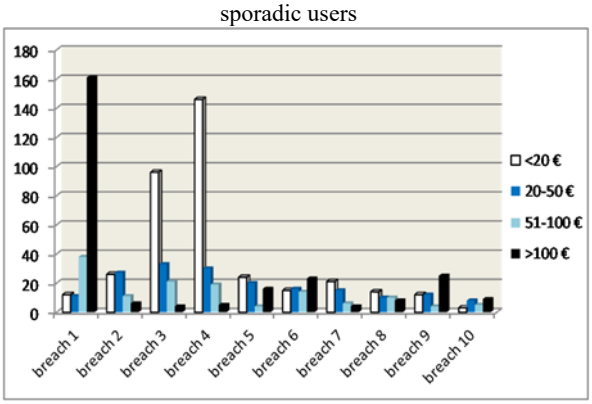

Fig. 3c Cost evaluation of security breaches occurred to entertainment type users

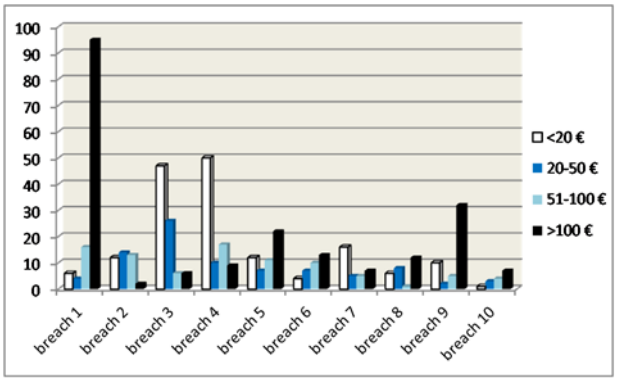

Fig. 3d Cost evaluation of security breaches occurred to instrumental users

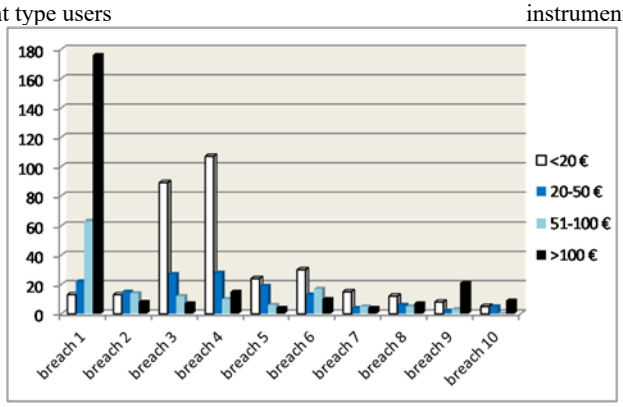

Fig. 3e Cost evaluation of security breaches occurred to advanced users

According to the findings relating to the question of cost evaluation of security breaches, the number of breach incidents per mobile user is as follows: (i) 0.85 (445 incidents / 521 users) for sporadic users, (ii) 1.27 (485/383) for socializers, (iii) 1.47 (944/643) for entertainment type users, (iv) 1.57 (543/345) for instrumental users, and (v) 1.13 (853/758) for advanced users. As it can be seen in Fig. 3, the cost is getting higher in the

cases of the instrumental (firstly) and the entertainment type user (secondly). For instance, an incident of interception of e-banking and/or credit/debit cards' passwords (breach 9) for the instrumental user costs mostly more than 100 €. Breach incidents for sporadic users generally have a low cost, which slightly increases when the users belong to socializers. For this user type, two breaches which have a higher cost are unauthorized access to multimedia material (breach 7) and cyber-bullying (breach 10). The cost of malicious software infection (breach 5), as well as the cost of unexpected charges due to unintentional phone calls (breach 6) increase for entertainment type and instrumental users. For these two user types, breach 9 is the one which causes a significant cost, while the device theft compelling the user to buy a new device (breach 1) has a constantly high cost for all the user types, as expected. Analyzing the graph for the advanced user, we can see why it is considered a mixed type. There are not so high costs as for the instrumental user but neither so low as for the sporadic user. Breaches 1, 9, and 10 (despite the small number of incidents for breach 10) generate a high cost to the user. Taking also into account the number of breach incidents per user (see the beginning of this paragraph), it can be deduced that the advanced user generally behaves like the average mobile user.

In order to compare the cost of breach across the five different types of users (for each breach), the Kruskal-Wallis test was used. This test is the non-parametric alternative to one-way analysis of variance. The reason for the use of a non-parametric test is that parametric assumptions, i.e. an interval-scale variable, approximately normally distributed, are not satisfied. The Kruskal-Wallis test is appropriate in our case since the test variable, i.e. the cost of breach, is an ordinal scale and we wanted to compare it for five different groups. Indeed, the possible values of the cost of breach are the following: (i) <20 €, (ii) 20-50 €, (iii) 51-100 €, and (iv) >100 €. We preferred this measurement of scale, firstly, because the respondents would not be able to give an exact amount of money for breach incidents that had occurred in the past, and secondly, because the determination of certain limits was necessary instead of using subjective value categories, such as low, medium, high, etc. Also, in this case there are five user types, i.e. sporadic users, socializers, entertainment type, instrumental users, and advanced users, which is in consistency with the fact that the Kruskal-Wallis test is used for three or more groups. Table 6 presents the Kruskal-Wallis test results. At the α=0.05 level of significance, we can conclude that there is a statistically significant difference in the cost of breach across the five mobile user types, for the breaches 1, 2, 3, 4, 5, 6, 9, and 10. For breaches 7 and 8, *p*-values are greater than 0.05, implying that there is no difference in the cost when comparing the user types.

Table 6 Kruskal-Wallis test results

Breach 1				Breach 2			
	User Type	N	Mean Rank		User Type	N	Mean Rank
Breach_Cost	sporadic users	152	315.79	Breach_Cost	sporadic users	34	96.29
	socializers	130	486.74		socializers	28	100.18
	entertainment type	222	485.66		entertainment type	66	100.66
	instrumental users	121	511.96		instrumental users	41	119.15
	advanced users	274	450.76		advanced users	50	129.65
	Total	899			Total	219	
	Breach_Cost				Breach_Cost		
Chi-Square	75.312			Chi-Square	10.383		
df	4			df	4		
Asymp. Sig.	0.000			Asymp. Sig.	0.034		
Breach 3				Breach 4			
Breach_Cost	sporadic users	68	233.43	Breach_Cost	sporadic users	66	294.61
	socializers	82	256.57		socializers	99	298.30
	entertainment type	152	265.45		entertainment type	200	291.01
	instrumental users	85	284.38		instrumental users	86	345.98
	advanced users	135	259.79		advanced users	160	312.72
	Total	522			Total	611	
	Breach_Cost				Breach_Cost		
Chi-Square	12.316			Chi-Square	9.895		
df	4			df	4		
Asymp. Sig.	0.036			Asymp. Sig.	0.042		
Breach 5				Breach 6			
Breach_Cost	sporadic users	31	93.29	Breach_Cost	sporadic users	40	112.86
	socializers	27	98.91		socializers	45	120.54
	entertainment type	60	96.40		entertainment type	76	134.38
	instrumental users	38	131.49		instrumental users	34	181.12
	advanced users	53	105.70		advanced users	70	127.64
	Total	209			Total	265	
	Breach_Cost				Breach_Cost		
Chi-Square	11.591			Chi-Square	19.402		
df	4			df	4		
Asymp. Sig.	0.021			Asymp. Sig.	0.001		
Breach 7				Breach 8			
Breach_Cost	sporadic users	18	62.17	Breach_Cost	sporadic users	15	50.30
	socializers	14	67.61		socializers	9	55.83
	entertainment type	46	70.20		entertainment type	42	61.02
	instrumental users	33	75.02		instrumental users	21	62.55
	advanced users	28	70.00		advanced users	30	58.98
	Total	139			Total	117	
	Breach_Cost				Breach_Cost		
Chi-Square	1.447			Chi-Square	1.571		
df	4			df	4		
Asymp. Sig.	0.836			Asymp. Sig.	0.814		
Breach 9				Breach 10			
Breach_Cost	sporadic users	11	67.23	Breach_Cost	sporadic users	10	28.30
	socializers	25	44.74		socializers	7	37.36
	entertainment type	46	77.83		entertainment type	25	32.34
	instrumental users	42	91.04		instrumental users	13	47.73
	advanced users	29	86.88		advanced users	19	42.18
	Total	153			Total	74	
	Breach_Cost				Breach_Cost		
Chi-Square	22.142			Chi-Square	11.707		
df	4			df	4		
Asymp. Sig.	0.000			Asymp. Sig.	0.039		

As analyzed in Section 3.2, the ten security breaches can be classified into three groups: (i) breaches 1 and 2, which constitute the “device loss/theft” group, (ii) breaches 3, 4, 5, and 6, being the group of “malware attacks in devices and applications”, and (iii) breaches 7, 8, 9, and 10, which belong to both previous categories and constitute a distinct group. To ascertain if the ten breaches were properly grouped, Principal Component

Analysis (PCA) was employed. It should be noted that the entire sample of mobile users was tested excluding only the non-classified data. PCA was performed through SPSS. According to the findings, the values of all the communalities were high since the minimum value was 0.467. Table 7 presents PCA results with the aid of the varimax-rotated component matrix. Its values are the component loadings, i.e. the correlations between each variable (breaches) and the corresponding component. The variables are sorted by highest loading on each component. Based on the scree test and the eigenvalues which were greater than unity, four components were extracted accounting for 58.14% of the total variance. As it can be seen in Table 7, breach 9 corresponds to a unique component, while according to hypothesis H2, it belonged to the group consisting of breaches 7, 8, and 10 (it is reminded that hypothesis H2 assumed three groups of breaches). If we also take into consideration the way that breach 9 varies in Fig. 2, it can be inferred that it would be preferable to treat this breach as a rather independent variable in forthcoming studies. Another choice would be to separate the breach into two parts, namely, e-banking passwords interception and credit/debit cards' passwords interception, and examine the two variables in forthcoming studies.

Table 7 Principal Component Analysis results

	Component			
	1	2	3	4
Breach 1	.741			
Breach 2	.693			
Breach 6		.675		
Breach 4		.627		
Breach 3		.515		
Breach 5		.426		
Breach 7			.714	
Breach 8			.687	
Breach 10			.567	
Breach 9				.771
% of Variance	16.577	15.678	14.046	11.841
Cumulative variance %	16.577	32.255	46.301	58.142

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
Rotation converged in 13 iterations.

6 Conclusions

In this work, a survey was conducted among mobile users aiming to investigate how different user types perceive the economic impact that security breaches have upon them. Firstly, we identified in our sample the five user types of the typology proposed by Brandtzæg. The five types are: (i) sporadic users, (ii) socializers, (iii) entertainment type users, (iv) instrumental users, and (v) advanced users. Noteworthy is that the participants in the survey were not asked to select their own user type. Instead, they were classified into the five types based on the frequency and the variety of mobile services in use. In addition, the most usual incidents of security breaches in mobile devices and applications were identified. Our findings indicate that the above user types perceive differently the economic impact that security breaches have upon them. Generally, they pay attention mostly to the breaches which are more related with the characteristics of their type. For instance, the interception of e-banking and/or credit/debit cards' passwords has a very strong impact on the instrumental user. The findings for the advanced user reveal that they behave as the average mobile user. There are also significant differences on how mobile users evaluate the cost of breaches actually occurred to them. The cost seems to be higher in the

cases of the instrumental and the entertainment type user. Another finding was that PCA did not validate the proposed classification of the ten braches into three groups. However, this deviation was due to a unique breach, i.e. the interception of e-banking and/or credit/debit cards' passwords, implying that more attention should be paid to the economic importance of this breach in forthcoming studies.

Through our research, mobile content providers and mobile developers can better understand what users really want and design their products according to targeted users' needs. Developers can address the needs for security and design applications and software that will be offered as response to the users' fears against security breaches. By knowing the users' personas, meaning motivation, behaviors, and intentions, developers will obtain the competitive advantage of realizing what the user wants. Mobile content providers can then design their strategies by taking advantage of all this knowledge. In the end, they will have the ability to be one step ahead of their competitors since the users will be engaged to providers as a result of their feelings of safety and trust towards them. The key idea of approaching different types of users is the possibility to study these types more carefully. Mobile content providers and mobile developers need to consider not merely the general description of each type but mostly their detailed characteristics and concerned activities. Our research could contribute to the knowledge considering mobile users and their perceptions about security breaches. Companies could use the findings of our research to evaluate and redesign, if needed, their current strategies so as to meet users' needs regarding security. Strategies that will help addressing mobile users should be interactive. Users should have the ability to express their opinions regarding their preferred activities, which is also a kind of evidence of the type they belong. In terms of considering different strategies for each user type, the involved parties need to design customized patterns and frameworks to meet each type's characteristics. They can develop different approaching practices (for example, SMS for sporadic users, social media polls for socializers, advergaming tools for entertainers, interactive blogs and forums for instrumental and advanced users) to get users' feedback and also establish a close relationship with users, which might be the starting point for developing new ideas and products.

Moreover, a company which implements a BYOD policy (so that its employees are regarded as instrumental users) could focus on this specific mobile user type's perceptions about security breaches; it should design an appropriate security policy giving emphasis in providing adequately tailored guidelines to its employees for taking measures of protection to minimize the risk of security breaches. There are also significant benefits for the simple users. If they are able to identify the user type they (or younger family members) belong to, they could recognize the dangers that exist in each circumstance and choose the right software to protect. They could also inform the family members, friends etc., who are not familiar with mobile technology, in order to minimize the possibility of a security breach occurrence (and the consequences that follow). Certainly, the way mobile users perceive the economic impact of a security breach is a reliable indication of their awareness level regarding this particular security risk.

In our study, two criteria were used for classification purposes, i.e. kind of mobile services and frequency of use; both are important aspects of usage of mobile services. However, there are other criteria, such as demographic factors, cultural factors, mobility preferences, that could also be used. As our purpose was to identify the five distinct user types of Brandtzæg's typology in the sample used for this survey, in order to investigate how these types perceive the economic importance of security breaches, we focused specifically on the aforementioned criteria; this is a limitation of our study. If the classification of mobile users was the principal

issue, the development of a framework of multiple criteria which represent all the possible categories of criteria pertaining to mobile users (not only usage) would be an interesting proposition for future research. In addition to that, it should be noted that the findings of this study are apparently related to the specific characteristics of the survey conducted in the context of our research methodology. The findings should be generalized with care if extrapolated to other economic and socio-cultural settings.

With respect to the academic contribution of this paper, researchers can utilize not only our findings, as presented in Section 5, but also the classification rules used to identify mobile user types in our sample and in general the approach that this paper implemented. Moreover, the most usual security breaches that are presented in this study can be further used or even modified with additional breaches that the digital era will introduce in the future. More importantly, the user typology that Brandtzæg proposed is a tool that we highly support and recommend. The five distinct user types along with the security breaches and the classification rules that our research revealed could be the basis for upcoming studies. Besides, we believe that the idea to investigate the user's perspective as regards the economic impact of mobile security breaches upon users will attract soon the interest of academic community worldwide.

Mobile security economics is a research area that requires continuous and multifaceted investigation. The relationships among users, providers, software developers, security breaches, and their economic consequences should be studied from different perspectives in order to obtain a satisfactory level of knowledge in this research area. The emerging technologies can undoubtedly change many things concerning mobile users, their characteristics, and their perceptions regarding security breaches. New concepts will introduce new actors and activities. Still, the typology used is valuable as it presents five generic user types that in the future can be modified and enriched with additional characteristics. Moreover, there is the potential to move one step ahead by considering these five types as main actors that are inherited in specialized sub-types. We believe that these ideas could contribute for future research directions in this topic.

References

Asokan N, Dmitrienko A, Nagy M, Reshetova E, Sadeghi A-R, Schneider T, Stelle S (2013) CrowdShare: secure mobile resource sharing. In: Jacobson M, Locasto M, Mohassel P, Safavi-Naini R (eds.) Applied cryptography and network security, Lecture Notes in Computer Science 7954. Springer, Berlin, pp 432–440

Brandtzæg PB (2012) MUT and the mobile Internet: applying the approach to other domains. University of Oslo, Norway. http://www.slideshare.net/PetterB/user-types-of-the-mobile-internet. Accessed 27 December 2013

Brandtzæg PB (2010) Towards a unified media-user typology (MUT): a meta-analysis and review of the research literature on media-user typologies. Comput Hum Behav 26(5):940–956

Bouwman H, Carlsson C, Walden P, Molina-Castillo FJ (2009) Reconsidering the actual and future use of mobile services. Inf Syst E-Bus Manage 7(3):301–317

Calder A (2013) Is the BYOD movement worth the risks?. Credit Control J 34(3):65–70

Cate FH (2008) Information security breaches. Faculty Publications. http://www.repository.law.indiana.edu/facpub/233. Accessed 29 December 2013

Chun SH (2011) Smart mobile banking and its security issues: from the perspectives of the legal liability and security investment. In: Proceedings of the 6th international conference in future information technology, Loutraki, Greece, pp 190–195

Clarke N, Furnell S (2005) Authentication of users on mobile telephones – a survey of attitudes and practices. Comput Secur 24(7):519–527

Collier R (2012) Medical privacy breaches rising. Can Med Assoc J 184(4):E215–E216

Dimensional Research (2012) The generation gap in computer security: a security use survey from GEN Y to baby boomers. http://www.zonealarm.com/products/downloads/whitepapers/generation_gap_research_2012.pdf. Accessed 2 March 2014

Dini G, Martinelli F, Matteucci I, Saracino A, Sgandurra D (2014) Introducing probabilities in contract-based approaches for mobile application security. In: Garcia-Alfaro J, Lioudakis G, Cuppens-Boulahia N, Foley S, Fitzgerald WM (eds.)

Data privacy management and autonomous spontaneous security, Lecture Notes in Computer Science 8247. Springer, Berlin, pp 284–299
Dmitrienko A, Liebchen C, Rossow C, Sadeghi A-R (2014) On the (in)security of mobile two-factor authentication. Technical Report TUD-CS-2014-0029. Technische Universität Darmstadt, Germany. https://www.informatik.tu-darmstadt.de/fileadmin/user_upload/Group_TRUST/PubsPDF/TR-Dmitrienko-2FA-analysis-v2.pdf. Accessed 31 March 2014
Gao X, Zhong W, Mei S (2013) Security investment and information sharing under an alternative security breach probability function. Inf Syst Front 17(2):423–438
Gest J (2013) Managing BYOD: How to mitigate the risks of using personal devices in the workplace. http://www.smartbusinessemag.com/may2013/Houston/10/0#&pageSet=10&contentItem=0. Accessed 10 January 2014
Huang Z, Benyoucef M (2013) From e-commerce to social commerce: a close look at design features. Electron Commerce Res Appl 12(4):246–259
Jech V (2012) Smart mobile devices in corporate and business practice. In: Proceedings of IMEA, University of Hradec Králové, Czech Republic, pp 30–35. http://is.muni.cz/repo/977628/IMEA_2012_Sbornik.pdf#page=34. Accessed 27 March 2014
Kietzmann J, Plangger K, Eaton B, Heilgenberg K, Pitt L, Berthon P (2013) Mobility at work: a typology of mobile communities of practice and contextual ambidexterity. J Strategic Inf Syst 22(4):282–297
Kim C, Tao W, Shin N, Kim KS (2010) An empirical study of customers' perceptions of security and trust in e-payment systems. Electron Commerce Res Appl 9(1):84–95
Kourouthanassis PE, Georgiadis CK (2014) Analyzing m-commerce research: technology, applications and research themes. Int J Mob Commun 12(1):1–11
La Polla M, Martinelli F, Sgandurra D (2013) A survey on security for mobile devices. Commun Surv Tutor 15(1):446–471
Li Q, Clark G (2013) Mobile security: a look ahead. IEEE Secur Priv 11(1):78–81
Liu AX, Wang Y, Chen X, Jiang X (2014) Understanding the diffusion of mobile digital content: a growth curve modelling approach. Inf Syst E-Bus Manage 12(2):239–258
Lumsden E (2012) Securing mobile technology & financial transactions in the United States. Berkeley Bus Law J 9(1):139–185
Microsoft Corporation (2013) Survey shows people need more help controlling personal info online. http://www.microsoft.com/en-us/news/press/2013/jan13/01-23dpdpr.aspx. Accessed 10 April 2014
Milligan PM, Hutcheson D (2008) Business risks and security assessment for mobile devices. Inf Syst Control J 1:1–6
Morrow B (2012) BYOD security challenges: control and protect your most sensitive data. Netw Secur 12:5–8
Mort GS, Drennan J (2005) Marketing m-services: establishing a usage benefit typology related to mobile user characteristics. J Database Mark Customer Strategy Manage 12(4):327–341
Noh MJ, Lee KT (2015) An analysis of the relationship between quality and user acceptance in smartphone apps. Inf Syst E-Bus Manage. doi: 10.1007/s10257-015-0283-6
Oh T, Choi YB, Ryoo J, Stokes K (2011) Security management in wireless sensor networks for healthcare. Int J Mob Commun 9(2):187–207
Ondrus J, Pigneur Y (2009) Near field communication: an assessment for future payment systems. Inf Syst E-Bus Manage 7(3):347–361
Pillay A, Diaki H, Nham E, Senanayake S, Tan G, Deshpande S (2013) Does BYOD increase risks or drive benefits?. http://sitic.org/wp-content/uploads/Does-BYOD-increase-risks-or-drive-benefits.pdf. Accessed 23 February 2014
Pocatilu P (2011) Android applications security. Inform Economica 15(3):163–171
Ponemon Institute (2012) Confidential documents at risk study. Ponemon Institute Research Report. http://www.ponemon.org/local/upload/file/WatchDoxWhite_Paper_FINAL.pdf. Accessed 12 March 2014
Ramu S (2012) Mobile malware evolution, detection and defense. EECE 571B, Term Survey Paper. http://blogs.ubc.ca/computersecurity/files/2012/04/SRamu_EECE572_SurveyPaper-SrikanthRamu.pdf. Accessed 19 April 2014
Rhee K, Won D, Jang S-W, Chae S, Park S (2013) Threat modeling of a mobile device management system for secure smart work. Electron Commerce Res 13(3):243–256
Scott JE (2004) Measuring dimensions of perceived e-business risks. Inf Syst E-Bus Manage 2(1):31–55
Sharma A (2008) Bluetooth security issues, threats and consequences. In: Proceedings of the 2nd national conference on challenges & opportunities in information technology, Mandi Gobindgarh, India, pp 78–80
Shih DH, Lin B, Chiang HS, Shih MH (2008) Security aspects of mobile phone virus: a critical survey. Ind Manage Data Syst 108(4):478–494
Tu Z, Yuan Y, Archer N (2014) Understanding user behaviour in coping with security threats of mobile device loss and theft. Int J Mob Commun 12(6):603–623
Wang T, Oh LB, Wang K, Yuan Y (2013) User adoption and purchasing intention after free trial: an empirical study of mobile newspapers. Inf Syst E-Bus Manage 11(2):189–210
Webliquid (2012) The surge: from communication to context. House of Kaizen. http://www.slideshare.net/Webliquid/the-surge-summary-of-mobile-in-europe. Accessed 27 March 2014