2014

The Significance of Mobile Security Breaches in Terms of Their Economic Impact on Users

Christos Georgiadis
University of Macedonia, geor@uom.edu.gr

Emmanouil Stiakakis
University of Macedonia, stiakakis@uom.gr

Anna Andronoudi
University of Macedonia, it1141@uom.edu.gr

THE SIGNIFICANCE OF MOBILE SECURITY BREACHES IN TERMS OF THEIR ECONOMIC IMPACT ON USERS

Georgiadis, Christos K., University of Macedonia, Egnatia Street 156, 54006 Thessaloniki, Greece, geor@uom.edu.gr

Stiakakis, Emmanouil, University of Macedonia, Egnatia Street 156, 54006 Thessaloniki, Greece, stiakakis@uom.gr

Andronoudi, Anna, University of Macedonia, Egnatia Street 156, 54006 Thessaloniki, Greece, it1141@uom.edu.gr

Abstract

The issue of security in mobile devices and applications has been mostly examined from a technological perspective but not adequately from an economic point of view. In particular, the opinions of users in terms of the economic impact of mobile security breaches on them would be of great interest. This paper firstly analyses the basic mobile user types and classifies mobile services (except for phone calls) into these types. The basic user types are: (i) sporadic users, (ii) socializers, (iii) entertainment type, (iv) instrumental, and (v) advanced users. Through a survey conducted among mobile users, it is shown that the mobile user type is determined by the frequency and the variety of use of mobile services. It is also demonstrated that the perceptions of users with regard to the economic impact of mobile security breaches on them differ. These perceptions are dependent on how security breaches should be grouped. These groups are: (a) the breaches strictly related to device loss/theft, (b) those strictly related to malware attacks, and (c) those pertaining to both previous cases. This work falls in the efforts that have been made to assess the economic implications of mobile security breaches for different types of users.

Keywords: Mobile services, Mobile security breaches, Mobile user typology.

1 Introduction

In the past ten years, the rapid development of mobile technology resulted in the domination of mobile devices as the main channel through which we conduct most of our day-to-day communication, business and leisure activities (Ramu, 2012). The increasing capabilities that mobile technology offers is also the reason for increasing security threats, risks and needs for end-users, manufacturers, and service providers (La Polla et al., 2013). It is true that the world of smart devices has been adopted not only by personal users, but a large number of organizations as well. Movements, such as the "Bring Your Own Device" (BYOD) have embraced new mobile prospects in the working environment (Keyes, 2013). Unlike the benefits of this pioneering technology of mobile devices, huge amounts of money are lost due to security breaches in devices and applications. The economic impact of all the above is amplified by lack of information (Microsoft, 2013) and education of mobile users (Morrow, 2012), resulting in additional financial costs.

The purpose of this paper is to investigate the significance of mobile security breaches in terms of their economic impact on users. A detailed literature review on selected papers has led to classification of mobile users into distinct types, as well as suggestions on how mobile security breaches could be grouped. Secondary data from recent studies have confirmed the findings of our literature review. In the context of the methodological part of this study, a survey was conducted among mobile users with the aid of a number of undergraduate students as researchers. The main objective was to further investigate the economic implications of security breaches in mobile devices and applications; however, in this paper we focused on issues concerning mobile user types, as well as types of mobile security breaches which occur to a large extent.

2 Mobile User Typology

The unexpected growth of the number of mobile users with the developments in mobile technology resulted in a distinct mobile user typology. According to the Webliquid enterprise (Webliquid, 2012), mobile users fall into three categories: i) voice users who do not fully exploit the increased capabilities provided by mobile technology since their basic concern is communication, ii) SMS users, whose preferences lie mainly into the texting capabilities of their mobile devices, and iii) mobile media users, who take advantage of innovations both in the devices and their applications. With respect to the determinant factors of mobile user typology, there are four main drivers (Brandtzæg, 2010): a) frequency of use, b) media platform, c) variety of use, and d) content preferences. Taking into consideration the mobile user behaviour and the aforementioned factors, mobile users can be classified into five types (Brandtzæg, 2010): first, sporadic users who do not use smart devices frequently due to lack of knowledge to do so. Sporadic users aim to communicate through phone calls or texting (SMS, MMS) mainly. Second, the socializer type makes use of his/her device as a means of interaction and bonding with friends and family by accessing social media, such as Facebook and Twitter. Third, the entertainment user type sees their devices as a means of amusement, such as browsing the Internet, downloading games and various applications, watching videos etc. Entertainment activities could also be considered shopping, programming tasks and visiting information based-sites to "infotain" themselves (inform plus entertain). Fourth, the instrumental user type makes advantage of e-government, e-banking, and e-shopping applications not only for personal use but also for matters concerning his/her workplace. The users belonging to the instrumental type surf in the Internet searching for relevant information, use social networks in order to exploit possible social media marketing techniques, and download useful software for working purposes. Finally, advanced users exploit most of mobile device capabilities since they are well informed about the features of their smart devices. Their prime concerns include gaming, e-shopping, e-government, programming, socializing, and numerous other services. The mobile user typology described above and the four main drivers that led to the user types are summarized in Table 1.

Types of Mobile Users	Drivers			
	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 Networking Services	Low	Keep in touch with friends, less organized and purposeful
Entertainment	Medium	New media in general (mobile phones, PCs, game consoles, etc.)	Medium	Gaming, video watching, infotainment, programming & e-shopping
Instrumental	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	High	All	High	All the aforementioned

Table 1. Mobile User Typology.

3 Mobile Data Categories

Even though users might have different incentives, as discussed in the mobile user typology section, they all store data in their personally owned smart devices. These data categories can be mainly sorted into four groups, namely, sensitive personal data, multimedia material, passwords, and confidential documents. First of all, 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 that the user has in his/her mobile address book. Approximately half of users have multimedia material stored in their devices, such as photos, videos, and music according to a recent survey conducted by the Ponemon Institute (2012a). The third category of data 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 and for social media and other e-services that require password in order to gain access. The same Ponemon survey shows that 29% of users store credit card's passwords in their device. Considering the fact that e-payments are the new trend in mobile community and the volume of these financial transactions in 2011 was in the range of 86 billion USD (Baig, 2011), it is not surprising that users like to have their passwords stored in mobile devices. Additionally, a great proportion of mobile users have in their devices confidential documents that can be either personal or work-related (Jech, 2012). The data categories in mobile devices and their relevant content are mentioned in Table 2.

Data Categories in Mobile Devices	Relevant Content
Sensitive personal data	• Personal identity card's number • E-mail & home address • Health record • 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

Table 2. Mobile Data Categories.

4 Security Breaches and Economic Implications

The great variety of features that smart mobile devices offer has led to a robust growth of the mobile industry. This rise in popularity of smart devices and applications has also drawn illegal/fraud activities (La Polla et al., 2013). Security breach or security violation is any incident that results in unauthorized access of data, applications, services, networks, and devices by bypassing their underlying security mechanisms (Cate, 2008). The advent of mobile applications and tools from a lot of companies and private users apart has, on the one hand, improved firms' profitability and facilitated operating functions better, and on the other hand, created the need for more effective security policies (Jech, 2012). The quite divergent use of smartphones from businesses and private users gives rise to different types of danger. Security breaches potentially lead not only to valuable personal data loss but also to business data loss, such as classified information on financial assets (La Polla et al., 2013). 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 of security breaches, their main outcome is data leakage (Milligan et al., 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). Furthermore, business data leakages can include important relevant information about clients, suppliers, and the related work force. In the case of a hospital, health records and sensitive information about patients might be intercepted. Considering the fact that e-health apps and services are considered to be a huge part of mobile technology innovations, the cost of security breaches in the mobile health community are turned out to be extremely high (Collier, 2012). In specific, the Annual Benchmark Study, published in 2012, reports that the average economic impact of data breaches from 2010 till 2012 was 2.4 billion USD for the interviewed health organizations (Ponemon Institute, 2012b).

When a device is lost or stolen there might be many security issues. To begin with, we take into consideration that 66% of all mobile users utilize a PIN authentication for switch on 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 level of difficulty and the users not only have lost their device and the data stored in it but they also have to buy another one as well. The survey of the Ponemon Institute (2012a) 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 move easily on

various actions, such as identity theft and processing financial transactions, making phone calls, and sending messages that outstrip the normal cost of the user's bill. It is further 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 with money demand in return for, as according to Dimensional research, personal information obtained from smart devices can be sold in the market at a premium (Dimensional Research, 2012).

With respect to the second category of security breaches, there are many ways malware attacks can occur. One way is through infected programs received via Bluetooth and other methods the Bluetooth technology offers (Sharma, 2008); also, 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) says that there have been hidden charges from short messages which mislead users with their actual not free content. Mobile users 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 (for example, 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), consist another malicious path for the attackers. Security breaches can also occur through the Near Field Communication (NFC), widely used for unauthorized payments, leading to financial frauds (Pocatilu, 2011).

5 "Bring Your Own Device" Movement

Recently, companies have started to increasingly implement the "Bring Your Own Device" (BYOD) initiative to reduce costs and improve productivity. BYOD is regarded a business strategy that permits employees, partners, and other users to carry out enterprise applications and access business information through their personal owned client devices (Keyes, 2013). The increase in BYOD policies benefits but also challenges the control of companies over sensitive data. The benefits can be summarized in cost reduction, better data accessibility, higher employee satisfaction, and productivity (Pillay et al., 2013). Particularly, according to Morrow (2012), BYOD policies reduce costs for organizations since they minimize investments on hardware equipment. Moreover, by allowing access to stakeholders through unmanaged devices, corporations support anywhere, anytime, and any endpoint working philosophy.

A recent research conducted by CISCO (2012a) shows that employees are satisfied with BYOD concept for they allowed choosing their device assorted applications and combining work and personal lives over the course of a day. The same study advocates that productivity and innovation are benefited by BYOD policies, for employees collaborate more and freely decide on the time, place, and tools to fulfil a task. Another research of CISCO (2012b) indicates that BYOD adoption can bring annual financial benefits to the company from 300 to 1,300 USD per employee, depending on the role of the employee.

With respect to challenges, these can be summarized in data loss risk, lack of control, and increased security costs (Pillay et al., 2013). Specifically, Calder (2013) argues that BYOD policies correspond to higher data loss risk, for the small size of unmanaged devices makes them easier to be robbed or lost. To this end, inseparability of device and data ownerships results in financial risks that involve timely breaches of competitive advantages (Gest, 2013) and data leakages when employees quit their workplace (Smith and Forman, 2014). The unrestricted freedom that is imposed by BYOD policies results to an increased number of employee misconducts and unsuspected malicious downloads (Pillay et al., 2013; Tzoumas, 2013).

The organizations that adopt this movement in order to offer high security take some cost measures, such as the creation of an IT-help-desk department which provides support to the employees (Keaney, 2012). Furthermore, proper software against malicious programs should be provided. There are various mobile security solutions offered by different service providers. Martin (2011) gives evidence on how much these solutions cost. As he says, the average cost of a security package is from 20 to 40 USD. A report sponsored by Checkpoint with 790 IT professionals in 2013 shows that 52% of large companies' security costs exceeded 500,000 USD and 45% of businesses with less than 1000 employees reported security costs over 100,000 USD (Checkpoint, 2013). Finally, although the number of threats continuously increases, the security budget of companies and the individual security actions of mobile users remain the same in most cases (Stammberger, 2010).

6 User Level of Concern

As discussed above, BYOD policies are extremely popular to organizations. Though, unlike this popularity the underlying risks that these policies create are highly neglected. A joint study by McAfee and Carnegie (2011) concludes that in 14 countries and 1,500 respondents, 95% of companies implement mobile device policies, while less than one out of three employees are aware of the policy in place. Moreover, less than half of the companies disclose that their employees fully comprehend the mobile device restrictions.

Generally, users care about the security of their devices but they do not adopt security practices until they experience a security breach (Bullguard, 2011). A recent report (Androulidakis and Kandus, 2011) stated that users mainly do not use PINs or passwords although the device has security possibilities. Bullguard discloses that only 29% of users have considered security software. The majority of mobile users feel that they have little or no control over the personal information stored in the devices and they have no knowledge over the data that companies gather while they are browsing the Web or using online services (Microsoft, 2013).

Admittedly, given the popularity of BYOD policies, the evolution of security threats and breaches is inevitable. Predestined security policies will be enacted but what is needed to be done is the proper education of mobile users in order to protect their privacy and the data stored in the devices, either they are personal data or work related information. To this end, Morrow (2012) suggests that organizations have to educate their employees in order to make them fully aware of the security policies. In a more general setting, the change in attitude toward security risk can be achieved through school-time education. Accordingly, Sangani (2013) maintains that BYOD in schools not only provides high level of education despite the decrease in the school budgets but also prepares future employees to take advantage of security policies and better manage security threats.

7 Research

In the context of the methodological part of this study, a survey was conducted among mobile users. The sample included only owners of smartphones and tablets, while owners of mobile devices of older generation were excluded. The survey was conducted in a 6-month period using as researchers the undergraduate students in the Department of Applied Informatics, in the city of Thessaloniki, Greece. The sample size was 2,769 respondents and the data were collected through personal interviews and a website constructed particularly for this survey. A structured questionnaire, containing scaled and multiple-choice questions but not open-ended questions, was designed following a systematic literature review of relevant issues. It should be noted that the participation of males and females was equal in numbers. Most of the respondents were aged 18-35 (61%). Regarding the level of education, 67% of the participants had obtained (or were in progress of obtaining their higher education degree (BSc, MSc, and PhD). The main subject of the survey was the investigation of the economic implications of security breaches in mobile devices. However, for the purposes of this study, only the

questions pertaining mobile user types, the data categories in mobile devices, and types of mobile security breaches are further analysed. The research hypotheses of the present study are cited below:

- The mobile user type is determined by the frequency of use in combination with the variety of use of the various mobile services.
- Mobile users perceive security breaches according to their economic implications on them.

In the questionnaire, mobile services (except for phone calls) were classified into categories according to their usage by the five types of mobile users given in Section 2. It is reminded that these types are: (i) sporadic users, (ii) socializers, (iii) entertainment type, (iv) instrumental, and (v) advanced users. The classification, which is presented in Table 3, was based on the characteristics of the users who belong to these types, according to the analysis of Section 2. Twelve types of the most usual mobile services were included in the questionnaire. The type of sporadic user utilizes mainly SMS/MMS, while the type of advanced user utilizes all kinds of mobile services.

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

Table 3. Classification of Mobile Services into Mobile User Types.

In order to investigate the economic implications of mobile security breaches, we first analyzed the two main categories of security breaches into the most usual incidents (second level of security breaches). It is reminded that the two categories are the breaches due to device loss/theft and the breaches due to malware attacks. The rationale of analysis is shortly mentioned below.

When a mobile device is lost or stolen, a number of security breaches can occur. Firstly, the involved legal user will have to buy a new device. On the other hand, the illegal or unauthorized user can easily gain access to the device and move on making charged phone calls and sending multimedia or short messages. Moreover, the attacker can have access to multimedia material either from the social media posts that are stored in applications of the device or the multimedia material that the user has also stored in various device locations. The attacker can easily pretend to be someone else as identity and personal data theft is easy to be achieved. Furthermore, this identity and personal data interception along with password theft can result in financial fraud, such as banking fraud through unauthorized access to bank accounts. Finally, the attacker, as long he has access to the personal data of the legal user, can use cyber-bullying techniques in order to threat and demand money from the legal user.

Correspondingly, the second category of security breaches is analyzed. Various incidents can occur herein, since malicious attacks do not have a stable form and evolve continuously. When a malicious attack takes place, a lot of unintended charges may happen, such as receiving or sending short and multimedia charged messages, Internet connections with high costs, and unauthorized phone calls. Similarly with the first security breach category, the malicious programs can easily gain access to multimedia material and generally to sensitive personal data and then can take advantage of this

information in order to accomplish financial transactions either through banking frauds or cyber-bullying actions.

The relevant classification of mobile security breaches into two major groups considers that during a possible malware attack, unintentional charges and undesirable consequences can occur. On the contrary, when a device is lost or stolen the attacker can exploit some malware techniques in order to gain access and personal data but in this case he/she acts intentionally and is aware of the possible charges. In most cases, the attacker has a limited time period to act before the legal owner proceeds into law enforcing actions. As a result, such malware attacks remain either unfinished or cause negligible charges to the legal owner and do not need to be considered in our research.

The security breaches at second level, classified into the two main categories (device loss/theft and malware attacks in devices and applications), are given in Table 4.

Security breaches at second level	**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	✓	✓

Table 4. Classification of Security Breaches at Second Level.

8 Findings

The frequency of usage of the various mobile services is depicted in Figure 1. However, according to Table 3, there is overlapping between the mobile user types concerning the usage of mobile services. For instance, the socializer type includes the usage of SMS/MMS, email and social media, whereas the sporadic type uses only SMS/MMS. To conclude about the frequency of mobile services, it is necessary to focus on the most characteristic service(s) for each user type.

For sporadic users, the main characteristic is the high frequency of SMS/MMS ('very often' usage which, in our survey, is more than 3 hours per day). Therefore, 15.4% of the respondents belong to the sporadic user type. For socializers, the main service used is 'social media'. Taking again into consideration the 'very often' usage, 14.7% of users belong to the socializer type. Entertainment type users are those who indicated that they play games, and/or surf the Web, and/or use multimedia material over 3 hours per day. Since there is the possibility this type users not to utilize all three services, we considered their percentage in the range from 14.7% (the percentage of the service which is mostly used) up to 30.3% (the sum of the 'very often' usage of the three services). The basic feature of instrumental type users is their working related activities. The main services that they use are office apps, downloading and uploading of files and software (for tax purposes, e-health activities, etc.), and e-banking. The percentage of instrumental type users ranges from 10.7% (the percentage of the service which is mostly used) up to 21.3% (the sum of high usage of the four services). This is a low percentage which is due to the fact that the participants in the survey are mainly young people who do not have an adequate level of working experience. Despite the low percentage, instrumental users constitute a significant mobile user type, since BYOD users are undoubtedly instrumental users. Advanced users are all those who have the knowledge and experience to deal with any type of service more than 3 hours per day. This implies that the advanced user can exploit any combination of mobile services and this is the basic difference from the other user types, which are characterized by specific groups of services.

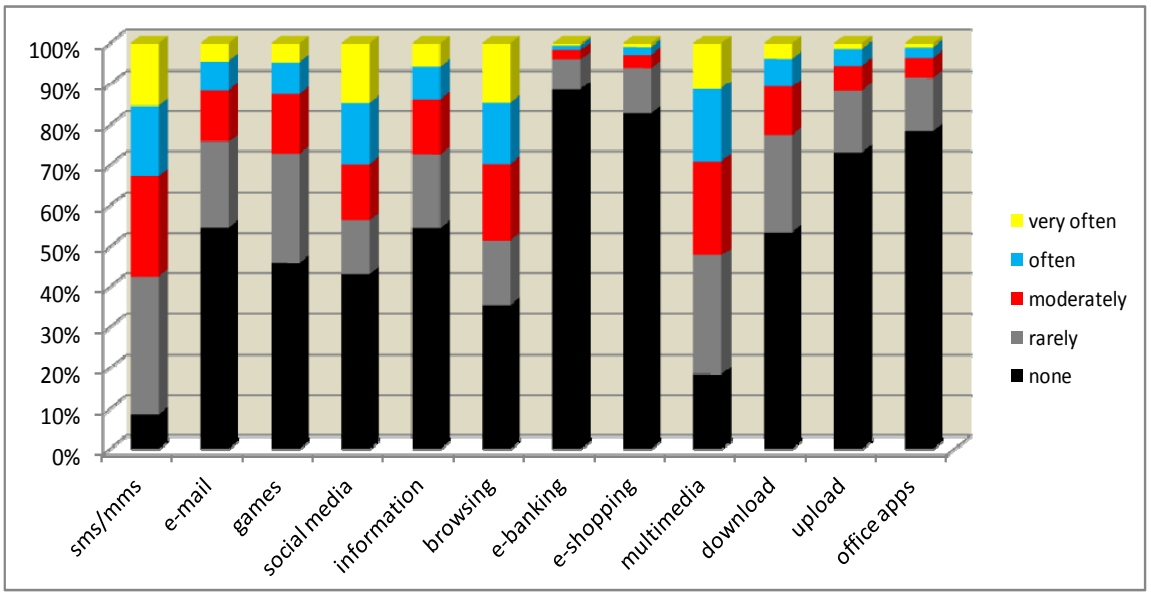

Figure 1. *Frequency of usage of mobile services.*

where:

none	the service is not used
rarely	few times per week
moderately	almost 1 hour per day
often	about 1-3 hours per day
very often	more than 3 hours per day.

According to Section 7, security breaches constitute three groups: (i) the first group includes breaches 1 and 2 which strictly refer to device loss/theft, (ii) the second group consists of breaches 3, 4, 5, and 6 which are strictly related to malware attacks in devices and applications, and (iii) the third group includes security breaches 7, 8, 9, and 10 that can be encountered in both categories.

Figure 2 shows the importance of mobile security breaches according to the economic impact they have on users. As it can be seen, the percentage of the participants who did not select breaches 1 and 2

as important is about the same. Moreover, the percentages of those who rated these breaches as very important (rating as '1' and '2') are close (41.6% for breach 1 and 30.6% for breach 2 respectively). For breaches 3, 4, 5, and 6 the respective percentages are the following: 14.2%, 13.3%, 10.6%, and 22.3%. The slightly higher percentage of breach 6 (unexpected charges due to unintentional phone calls) is due to the fact that users are generally more sensitive to differences in phone call charges. Finally, for breaches 7, 8, 9, and 10 the respective percentages are: 10.2%, 15.3%, 35.5%, and 10%. There is a significant deviation for breach 9 (e-banking and/or credit/debit cards' passwords interception), which is probably due to the incorporation of passwords interception in this security breach.

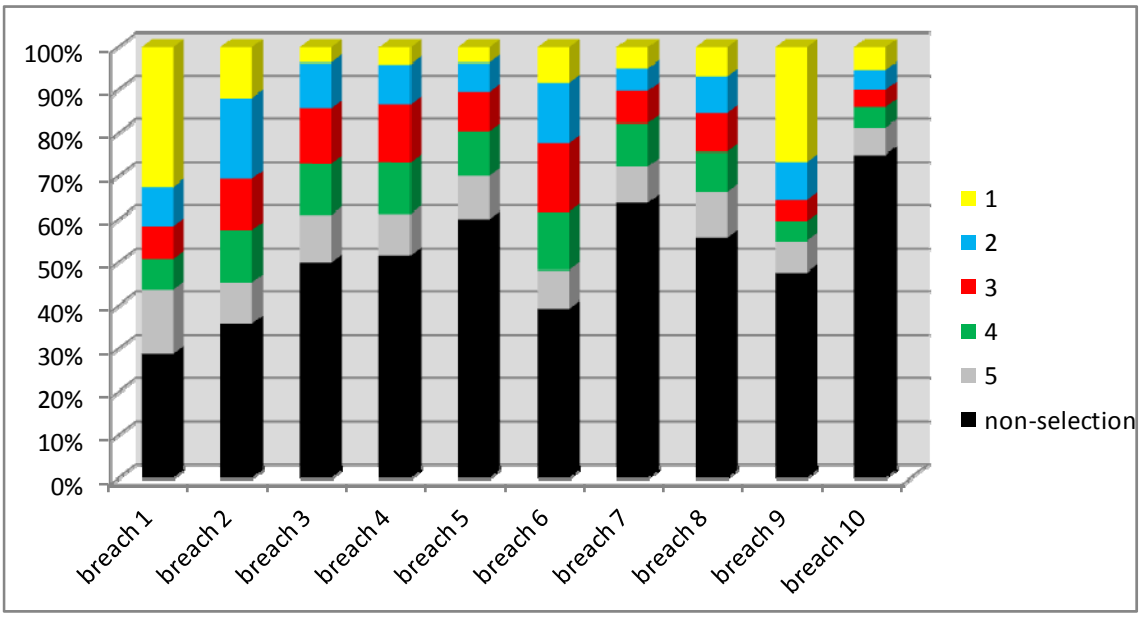

Figure 2. Importance of security breaches in terms of economic impact on users.

where 1 corresponds to the most important breach till 5 to the least important (the respondents had to select and rate the five more important breaches according to their economic impact on them).

It is worth mentioning some statistically significant correlations between selected pairs of security breaches regarding the economic impact they have on users. All the variables tested are ordinal, so Spearman's correlation coefficient was used. One of the relationships investigated was between breach 1 (device theft) and breach 2 (password interception) and a strong positive correlation was found at the 0.01 level of significance, indicating that the two breaches were properly grouped. In the second group of breaches, strong positive relationships were found between breach 3 (unintentionally receiving or sending charged messages) and breach 4 (unintentional Internet connection with charge), and between breach 4 and breach 6 (unexpected charges due to unintentional phone calls), at the level of 0.01 and 0.05, respectively. In the third group, which includes the breaches that belong to both main categories (device loss/theft and malware attacks in devices & applications), the strongest positive relationship found was between breach 7 (unauthorized access to multimedia material) and breach 8 (identity and personal data interception) at the 0.05 level of significance.

9 Conclusion

In this work, the mobile user typology was further investigated aiming to determine distinct mobile user types. These types are: (i) sporadic user, (ii) socializer, (iii) entertainment type, (iv) instrumental, and (v) advanced user. We classified the basic mobile services into the above types, indicated the main services for each type, and determined these mobile user types according to the findings of a survey.

In addition, we examined the significance of mobile security breaches in terms of their economic impact on users. Based on the classification of security breaches into two main categories, we proposed three groups of security breaches: (a) those strictly related to device loss/theft, (b) those strictly related to malware attacks, and (c) common security breaches belonging to both categories. We found that users perceive the economic impact of security breaches in relation to which group the breaches belong to. We also tested the relationships between the breaches in some selected pairs, trying to find indications for the suitability of the suggested grouping of breaches. A noteworthy limitation of this study is the composition of the sample, which included mostly young people. This is the reason why e-banking is the service which is used the least, although e-banking interceptions were considered one of the most important breaches in terms of their economic impact on users. Since the processing of data of the aforementioned survey is still in progress, we aim to further investigate how each mobile user type perceives the economic impact of specific breaches. This perspective seems to be very promising, because service providers and application developers may adjust their security policies according to the findings. It is also important to know how much each user type is willing to pay in order to ensure an acceptable security level in their mobile device, which depends on how the various user types perceive the significance of all possible security breaches. Moreover, it depends on the users' experience about breaches they are familiar with and the amount of money they probably had to pay to confront security problems. These are issues which need to be investigated more thoroughly regarding this topic.

References

Androulidakis, I. and Kandus, G. (2012). Feeling secure vs. being secure the mobile phone user case. In Proceedings of the International Conference in Global Security, Safety and Sustainability & e-Democracy 2011 (Georgiadis, C.K. et al. Eds), pp. 212-219, Thessaloniki, Greece.

Baig, E. (2011). When will we be paying for stuff with our smartphones?. USA TODAY, Available at: http://usatoday30.usatoday.com/tech/news/2011-07-25-mobile-payments_n.htm.

Brandtzæg, P.B. (2010). Towards a unified media-user typology (MUT): A meta-analysis and review of the research literature on media-user typologies. Computers in Human Behavior, 26 (5), 940-956.

BullGuard Ltd. (2011). Are Android users safe amidst the threat of mobile-based malware?. Available at: http://www.bullguard.com/bullguard-security-center/mobile-security/mobile-threats/mobile-security-the-deal-with-apps-for-android-phones.aspx.

Calder, A. (2013). Is the BYOD movement worth the risks?. Credit Control Journal, 34 (3), 65-70.

Cate, F.H. (2008). Information Security Breaches. Faculty Publications, Indiana University Maurer School of Law.

Checkpoint (2013). The impact of mobile devices on information security: A survey of IT professionals. A survey sponsored by Checkpoint and produced by Dimensional Research.

Chun, S.-H. (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, pp. 190-195, Loutraki, Greece.

Cisco (2012a). BYOD: A Global Perspective Harnessing Employee-Led Innovation. CISCO IBSG.

Cisco (2012b). BYOD and Virtualization Top 10 Insights from Cisco IBSG Horizons Study. CISCO IBSG.

Clarke, N. and Furnell, S. (2005). Authentication of users on mobile telephones - A survey of attitudes and practices. Computers & Security, 24 (7), 519-527.

Collier, R. (2012). Medical privacy breaches rising. Canadian Medical Association Journal, 184 (4), E215-E216.

Dimensional Research (2012). The generation gap in computer security: A security use survey from GEN Y to baby boomers. Available at: http://www.zonealarm.com/products/downloads/whitepapers/generation_gap_research_2012.pdf.

Gest, J. (2013). Managing BYOD. Smart Business Houston, 7 (11), 20.

Jech, V. (2012). The use and security of smart mobile devices in corporate and business practice. Available at: http://www.ondrejsimpach.ic.cz/publikace/konference_mezinarodni/DOKBAT2012/prispevky/24.pdf.
Keyes, J. (2013). Bring Your Own Devices (BYOD) Survival Guide. CRC Press, Boca Raton, FL.
La Polla, M., Martinelli, F. and Sgandurra, D. (2013). A survey on security for mobile devices. Communications Surveys & Tutorials, 15 (1), 446-471.
Lumsden, E. (2012). Securing mobile technology & financial transactions in the United States. Berkeley Bus. LJ, 9, 139-142.
Martin, T. (2011). Are users willing to pay yearly subscriptions for mobile security?. Available at: http://www.phonedog.com/2011/09/30/are-users-willing-to-pay-yearly-subscriptions-for-mobile-security, [10 December 2013].
McAfee (2011). Mobility and Security: Dazzling Opportunities, Profound Challenges. A report commissioned by McAfee and produced by Carnegie Mellon University's CyLab. Available at: http://www.mcafee.com/us/resources/reports/rp-cylab-mobile-security.pdf.
Microsoft (2013). Survey Shows People Need More Help Controlling Personal Info Online. Microsoft Corporation. Available at: https://www.microsoft.com/enus/news/press/2013/jan13/01-23dpdpr.aspx.
Milligan, P.M. and Hutcheson, D. (2008). Business risks and security assessment for mobile devices. Information Systems Control Journal, 1, 24.
Morrow, B. (2012). BYOD security challenges: Control and protect your most sensitive data. Network Security, 2012(12), 5-8.
Pocatilu, P. (2011). Android applications security. Informatica Economica, 15 (3), 163-171.
Ponemon Institute (2012a). Confidential Documents at Risk Study. Ponemon Institute Research Report. Available at: http://info.watchdox.com/Ponemon.html.
Ponemon Institute (2012b). Third Annual Benchmark Study on Patient Privacy & Data Security. Ponemon Institute Research Report. Available at: http://www2.idexpertscorp.com/ponemon2012.
Pillay, A., Diaki, H., Nham, E., Senanayake, S., Tan, G. and Deshpande, S. (2013). Does BYOD increase risks or drive benefits?. Available at: http://sitic.org/wp-content/uploads/Does-BYOD-increase-risks-or-drive-benefits.pdf.
Ramu, S. (2012). Mobile malware evolution, detection and defense. Available at: http://blogs.ubc.ca/computersecurity/files/2012/04/SRamu_EECE572_SurveyPaper-SrikanthRamu.pdf.
Rice, R.E. (1984). The New Media: Communication, Research, and Technology. Sage, Beverly Hills, CA.
Sangani, K. (2013). BYOD to the classroom [bring your own device]. Engineering & Technology, 8 (3), 42-45.
Sharma, A. (2008). Bluetooth security issues, threats and consequences. In Proceedings of the 2nd National Conference on Challenges & Opportunities (Information Technology), Mandi Gobindgarh, India.
Shih, D.-H., Lin, B., Chiang, H.-S. and Shih, M.-H. (2008). Security aspects of mobile phone virus: A critical survey. Industrial Management & Data Systems, 108 (4), 478-494.
Smith, K.J. and Forman, S. (2014). Bring your own device – Challenges and solutions for the mobile workplace. Employment Relations Today, 40 (4), 67-73.
Stammberger, K. (2010). Mobile & smart device security survey 2010: Concern grown as vulnerable devices proliferate, smartphones are the tip of the iceberg. Mocana, San Francisco, CA. Available at: http://mocana.com/pdfs/mocana-summer-2010-dir_v8.pdf.
Tzoumas, C. (2013). The BYOD world. Business West, 30 (2), 45.
Webliquid (2012). The surge: From communication to context. House of Kaizen. Available at: http://www.slideshare.net/Webliquid/the-surge-summary-of-mobile-in-europe.