Chapter 2
A Multinational Survey on Users' Practices, Perceptions, and Awareness Regarding Mobile Phone Security

Abstract In this chapter, we will present some interesting findings from a large-scale empirical study. It was conducted in a sample of 7172 students studying in 17 Universities of 10 European countries, in order to assess users' levels of security feeling and awareness in regard to mobile phone communications. As this study revealed, there are categories of users who face increased security risks due to their self-reassuring feeling that mobile phones are per se secure. These users feel that mobile phone communication is secure and tend to be less cautious in their security practices. There was also a statistically backed correlation of an array of demographics and usage characteristics and practices to the overall security level of the user. As such, specific profiles of users were extracted according to their mobile phone objective and subjective security level.

Keywords Empirical study • Security survey • User awareness • Security awareness • Security perceptions • Mobile phone security • Security practices • User profiling • Mobile downloading • Ciphering indicator

2.1 Introduction

Mobile phones have become a vital part of daily life for billions of people around the world. Their presence is ubiquitous and most users report that their cell phone makes them feel safer, even sleeping with their phone on or right next to their bed [1]. As described in the previous chapter, this dependence on mobile phones is not free from security risks. In this chapter, we will present some interesting findings from a large-scale empirical study. It was performed in order to assess users' levels of security feeling and awareness in regard to mobile phone communications and the results were published in various academic conferences [2–7].

As this study revealed, there are categories of users who face increased security risks due to their self-reassuring feeling that mobile phones are per se secure. These users feel that mobile phone communication is secure and tend to be less cautious in their security practices. Moreover, there was a statistically backed correlation of an array of demographics and usage characteristics and practices to the overall security level of the user. This way, specific profiles of users were extracted according to their mobile phone objective and subjective security level.

I.I. Androulidakis, *Mobile Phone Security and Forensics*,
DOI 10.1007/978-3-319-29742-2_2

These categories of users need proper training and education; otherwise, a security incident will soon follow, harming in the long term the network operators too. They must be protected from unauthorized third party access to their data and from economic frauds. It is unquestionable that since users fail to secure their phones, reinforcing their security level should become a critical imperative.

2.2 Methodology

A very useful evaluation method for surveying user's practices is the use of multiple-choice questionnaires (i.e. in person delivery or e-mail questionnaires) [8, 9]. This empirical survey was conducted in the first half of 2010 using in-person (face to face) delivery technique, with a total of 7172 respondents participating (students in 17 Universities of 10 European countries).

This method was selected from other alternatives because it is more accurate and has a bigger degree of participation from the respondents (e-mail questionnaires usually are treated as spam mail from the respondents plus there is the risk of misunderstanding some questions). Indeed, the approximate ratio of participation was 80 % since the researchers were able to answer the questions of participants regarding the scope and the purpose of the survey. There was also a pilot study, conducted in the University of Ioannina, Greece, before the questionnaire was administered to the sample, to ensure the reliability and validity of the questionnaire [10]. At this point, it is interesting to note that there are not available already validated questionnaires for the subject.

The target group of the survey was university students from ages mostly 18–26, incorporating both younger and older youth segments because these ages are more receptive to new technologies. Given the fact that nowadays a very high percentage of young people is studying, the sample is not deemed limited and can be considered as representative of a large percentage of general youth population. Furthermore, since they are still studying, it would be easier to participate in security education programs, possibly implemented in Universities.

The English questionnaire was prepared, containing 22 questions, including the demographic ones. It was divided into two parts. In the first part, participants were asked demographic questions including gender, age, and field of studies as well as some economic data including mobile phone usage, connection type, and budget spent monthly on phone service. In the second part, specific questions related to their practices and security perceptions regarding mobile phones' security issues were researched. The questionnaire was translated to the corresponding languages. The translated text was reviewed by a third native language user to spot any translation errors or cultural misunderstandings. Data entry, finally, took place using custom software [11] while processing was done with SPSS.

Answers in specific questions were correlated to the answers in question: "Are you informed about how the options and technical characteristics of your mobile phone affect its security?" which had the following possible answers: "A Very Much, B Much, C Moderately, D Not too much, E Not at all". Apart from the statistical interpretations, a simple mathematical formula was also developed in the analysis of the security knowledge to produce numerical values from the multiple choice questionnaires. Responses were weighted with these weights: Very Much: 4, Much: 3, Moderately: 2, Not much: 1, Not at all: 0 and then divided by the number of occurrences, in order to get a mean value that was called "Mean Security Feeling Value (MSFV)".

In addition to MSFV which was based on subjective answers, another, objective, metric was introduced, the "Mean Actual Security Value (MASV)". MASV was calculated by adding one point for each of the following practices, which are objectively correct: Having IMEI noted down, knowledge of lack of encryption icon, having SIM PIN enabled, using a screensaver password, having Bluetooth disabled, not lending the phone, not downloading software to the phone, using antivirus, not saving passwords in the phone, and not saving personal data in the phone. The maximum score would hence be 10, since there were 10 specific questions.

Similarly, an objective awareness metric was introduced, the "Mean Actual Awareness Value-MAAV". For this one, one point was added for each "I do not know" in the answers. The maximum score would hence be 7 denoting a highly lacking awareness profile while 0 would be the mostly security aware score (negative scale).

2.3 Results

2.3.1 In General

In the next sections we present the results of categorizing users in regard to their security knowledge using the correlation and the simple formula described earlier. All of the findings presented are statistically significant at the Pearson's Chi-Square test $p<0.001$ level. As was found, there are many statistically significant correlations between the following parameters:

- Security feeling and awareness to {sex, age, field of study, brand, operating system of phone, monthly bill}
- Country to {downloading, security awareness, feeling, practices}
- Storing personal data to {security awareness, feeling, practices}
- O/S type (advanced or not) to {downloading, security awareness, feeling, practices}
- Bluetooth usage to {demographics, security practices}
- Downloading to {demographics, security awareness, feeling, practices}.

These findings are thoroughly presented in papers [2–7].

2.3.2 Demographics

Among the 7172 participants of Table 2.1, 53 % were females and 47 % were males while most of the respondents were aged 18–26 (75 %). The subjects were studying various sciences and were generally equally distributed.

Regarding mobile phone usage, almost 67 % of them are using daily a single mobile phone, with some 24 % using two phones regularly. Nokia is the favorite brand, reaching 39 % of students followed by Sony-Ericsson (25 %) and Samsung (15 %). Apple's iPhone seems to be scarce among students with less than 4 % of penetration. It is immediately apparent that focusing on Nokia and Sony-Ericsson phones, a security awareness campaign would immediately target almost 2/3 of users yielding a very high return of investment. The brand itself however is not enough to categorize attack vectors and practices, since there is also the feature of the specific operating system running on each phone.

The Mean Security Feeling Value MSFV was 2.26 in the scale 0–4 (0 not at all, 4 very much), with minimal differences among genders. Correspondingly, the Mean Actual Security value MASV was calculated to be just 3.55 out of maximum value 10. The MSFV was found to be somewhat higher in younger ages. Examining the field of study, we discovered that soon to be medical doctors are feeling the most secure (MSFV 2.69). Mathematics and Natural Science students with MSFV 1.89 were in the other end of spectrum the most worried ones. Engineers were in the middle of the range, with MSFV 2.24.

2.3.3 Economics

Proceeding to economics, participants were asked whether they are using a prepaid or post-paid (contract) mobile phone connection. 42.4 % of students are using a contract-based subscription, a rather high percentage, while 13.6 % have both prepaid and post-paid SIMs (Subscriber Identity Module). Users having both types of connection seem to be more worried about security issues. Answering how much money they spent monthly, student mobile phone users had a wide range of financial capabilities. The leading 36.7 % spends 11–20€ (currency converted) monthly while 30.5 % spend less than 10€. Only 9 % spend 31–40€ and some 6.3 % spend more than 40€ per month.

The MSFV shows an interesting trend. It progressively gets lower as the bills get higher, from 2.33 (≤10€ bill) to 2.05 (31–40€ bill). Then, for users who spend more than 40€, it grows a little to 2.12. This is quite logical, since the more users spend, the more are concerned about the security of communication and possible fraud.

Following with a question of both security and economic importance, almost half of participants (47 %) do not download any software at all. There is also a 19 % that actively downloads ringtones or logos while some 16 % do not know whether their phone is able to download or not. The combined downloading mean including Ringtones/Logos, Games, and Applications is around 37 %. Of course, getting familiar with downloading users is being more vulnerable to downloading and using unauthorized software that can harm their phone.

Table 2.1 Sample distribution

	Country	City	Univ.	Students	University name			
1	GR	Ioannina	1	780	Univ. of Ioannina			
2	BG	Sofia	1	991	Univ. of Sofia			
3	RO	Iasi	3	994	Gheorghe Asachi Technical Univ.	Univ. of Medicine and Pharmacy "Gr. T. Poppa"	Alexandru Ioan Cuza Univ,	
4	CZ	Brno	2	633	Masaryk Univ.	Brno Univ. of Technologty		
5	SK	Bratislava	1	509	Comenius Univ.			
6	HU	Budapest	4	959	Semmelweis Unin.	Budapest Business School	Eotvos Lorand Univ.	Corvinus University
7	LT	Siauliai	1	759	Siauliai Univ.			
8	LV	Riga	2	620	Univ. of Latvia	Riga Technical University		
9	EE	Tallinn	1	829	Univ. of Tallinn			
10	SI	Ljubljana	1	98	Univ. of Ljubljana			
10		17		7172				

2.3.4 *Security-Specific Questions*

Our fundamental research question was how "secure" users feel that mobile phone communication is. The majority (36.9 %) replied "moderately" followed by 28.6 % "much" (Fig. 2.1). On the other hand, some 21.36 % felt not too much or not at all sure they are secure. Using the simple formula described in Sect. 2.2 the mean security feeling value (MSFV) was 2.26, in the 0–4 scale (0 not at all, 4 very much).

In addition, students answered whether they are informed about how the options and the technical characteristics of their mobile phones affect the security of the latter and whether they are taking the necessary measures to mitigate the risks. The majority (30.8 %) states that they are "moderately" informed while a large 15.8 % believes that they are "not at all" informed (Fig. 2.2).

Correlating MSFV value to awareness feeling (Fig. 2.3), an almost linear relationship between them manifested. Users who feel very much informed believe that communication is very much secure. On the other end, users who do not feel informed are afraid that communication is not at all secure. At this point, one can argue that excessive confidence can lead to "relaxation" of security practices. In addition, a campaign to enhance the security knowledge of users would lower their fear of communication insecurity, probably leading to greater phone usage and profits for the operators.

There was an even better (negative) linear association between the subjective security feeling and the objective mean actual security value (Fig. 2.4). Users who believe that mobile phone communication is very much secure have the lowest Mean Actual Security Value MASV (3.44). That shows a clear discrepancy between user opinions on security and actual security practices. The association grows linearly to the highest MASV of 3.84 for those that believe that communication is not secure at all. This group employs the most best practices, bit still fails in more than half (c.f. Methodology, where the maximum value of MASV is theoretically 10)

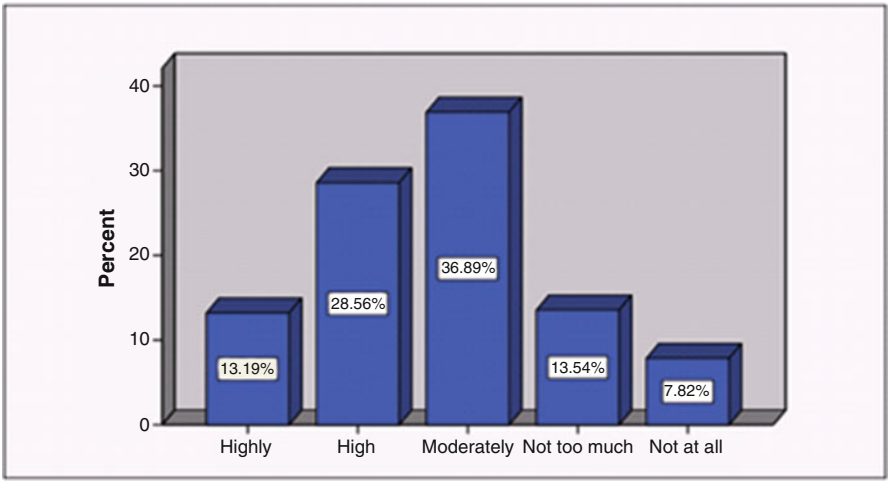

Fig. 2.1 How secure do you consider communication through mobile phones?

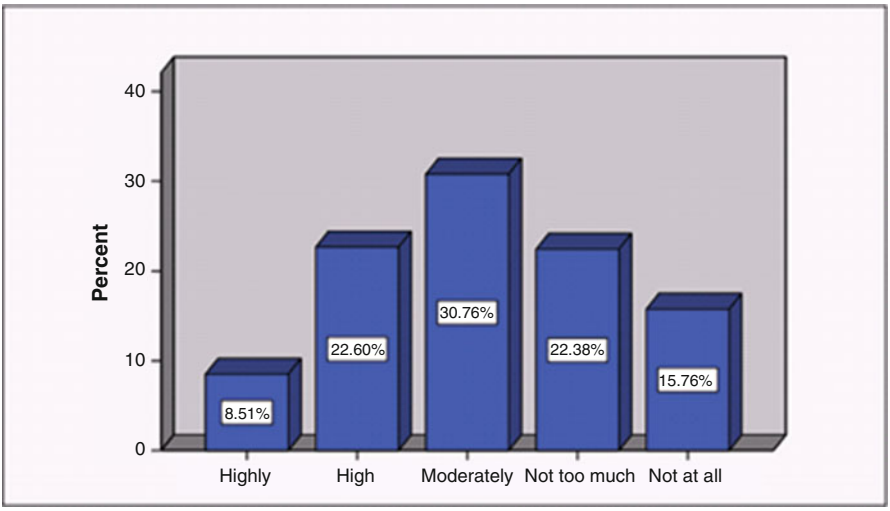

Fig. 2.2 Knowledge of mobile phone security aspects

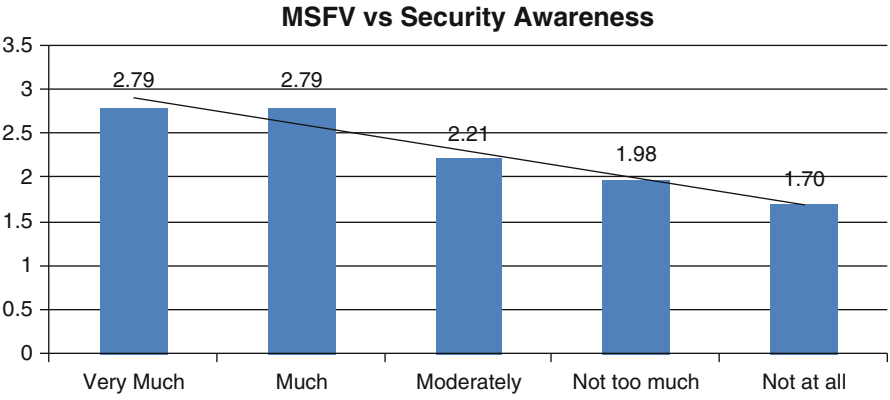

Fig. 2.3 Mean security feeling value vs. security feeling

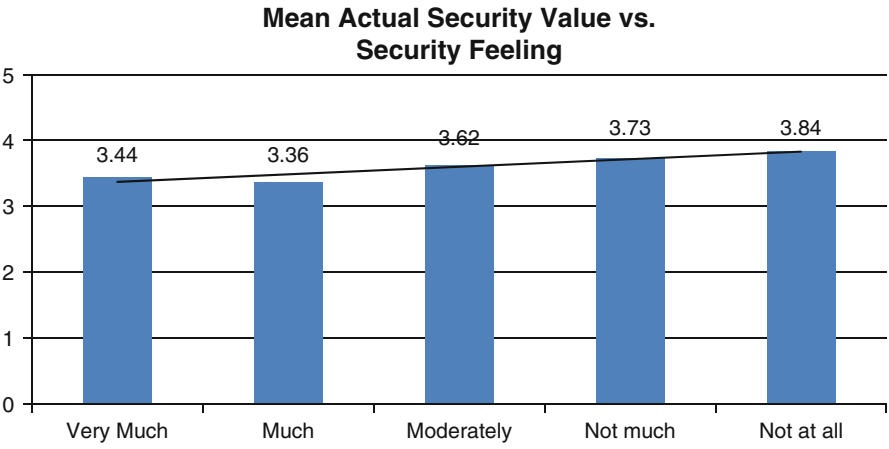

Fig. 2.4 Mean actual security value vs. security feeling

Further correlating the responses to the type of operating system (advanced or not) proved that students owning phones with an advanced operating system believe they are more secure than those who actually own a phone without advanced O/S. There was also a clear connection between increased backup frequency and security feeling.

At the same time, knowledge of the existence of the special icon that informs the user that his/her phone encryption has been disabled increased the safety feeling of users. In short, when A5 encryption is switched off or not supported, there is provision for handsets to display a special icon informing the user about the situation (it will be further explained in Chap. 3). Such an occurrence can be attributed either to network's lack of encryption capability or to temporary failure/overloading. The same icon can appear when a malicious attacker is launching a man in the middle attack, impersonating network's base stations to deceit the handset into connecting with the fake base station instead of the legitimate one. The fraudster can then channel the communication through his own equipment, effectively intercepting it [12]. This finding is a clear explanation of how better User Interfaces can help enhance the subjective security feeling via an objective method.

2.4 Related Work

Although there have been quite many theoretical studies concerning mobile services and mobile phones, a significant means for investigating and understanding users' preferences is asking their opinion via specific questioning techniques. The vast majority of these surveys indicate the growing importance of mobile phones in everyday life and the increased popularity of new features [1, 13]. In addition, with the apparent omnipresent availability of wireless devices, mobile services have a very promising prospect [13]. However, the success of those services (namely, m-commerce and m-payment) depends much on the security of the underlying mobile technologies [14], and mobile ubiquitous services pose great security challenges [15] Furthermore, users are interested in mobile services adoption only if the prices are low and the security framework is tight enough [16, 17].

A study of mobile users focusing on their awareness and concerns related to security threats, from security vendor McAfee, indicated that more than three quarters of respondents do not have any security at all [18]. In other words, despite acknowledging the wealth of threats—ranging from phishing scams to viruses—that could impact them (including concerns about losing or having their phone or personal data stolen [19–21]), users do not see security strengthening of their phone as a critical concern.

In any case, the security of mobile phones is proven not to be adequate [12, 22]. Several survey studies exist that indicate in this direction. Some of these surveys studies focus on mobile phone's security issues [23] while others on mobile phone services, mentioning also security issues [16, 17, 24]. Modern smart phones, specifically, are vulnerable to more security risks [25].

As previous work has shown [2, 26], users exhibit different levels of knowledge in regard to security. Starting from the young age, they are not receiving proper cyber security and training education from schools [27], and they are lacking the security awareness and proper etiquette [28]. A method to pinpoint specific user categories and present them the right amount of information and dialogs [29] is needed in order to restore their security level.

In regard to awareness systems, there have been efforts to create a sense of accountability in a world of invisible services that we will be comfortable living in and interacting with [30] as well as mechanisms for managing security and privacy in pervasive computing environments [31] but they still focus mostly in privacy issues and not actual security enhancement through education. In any case, there are also significant legal questions as presented in [32].

In addition to the above, mobile security is not considered a critical priority by companies. Cell phone security for enterprise devices is seriously lacking, and a little misunderstood as well [33], while the majority of companies do not have a security policy that addresses mobile devices [34]. However, some initiatives are taken in the direction of protecting mobile phones against threats including policies, tools, and recruiting technically skilled personnel [35].

2.5 Conclusion

The findings of the survey that were briefly presented support the hypothesis that users can be grouped in well-defined categories according to the subjective statement of how secure they feel mobile phone communication is. These categories exhibit different values of a metric named “mean security feeling value”. Further introducing a “mean actual security value”, “good” security practices they follow were counted. Comparing this (objective) value to their subjective security feeling revealed interesting results. There was a clear negative connection between feeling secure and actually being secure. Users that feel that mobile phone communication is secure, tend to be less cautious in their security practices, being actually less secure than they feel. This discrepancy between user opinions on security and actual security practices is a fact that should be addressed in order to minimize vulnerabilities and user exposure.

In regards to awareness, users that feel they are very much informed believe that communication is very much secure. On the other end, users that do not feel informed are afraid that communication is not at all secure. Excessive confidence could lead to “relaxation” of security practices while excessive fear certainly hinders technology adoption and especially mobile downloading.

It is more than clear that the mobile security area is going to be the next battleground since mobile security is an emerging discipline within information security arena and security levels are not high enough [36]. Users themselves are critically affected by security and privacy threats, and play a key role in protecting themselves and others. Since they do not actively follow most of security best practices,

academia and industry should focus their security awareness campaigns and efforts in order to combat the false sense of security that users have. In the following chapters of this book, we will hopefully help toward this direction, highlighting specific practical security problems.

Moreover, given the growing usage of mobile phones to access the Internet, it is of paramount importance to enhance the overall users' security levels that were found to be alarmingly low. This presents a vast opportunity for carriers and service providers too. They can play a proactive and strategic role in protecting their subscribers, both through education and through the security software they should deploy across their networks.

Manufacturers on the other hand should proceed to better designed interfaces and mobile phones generally, richer in security features. Special software could help users mitigate the security risks offering embedded encryption options for data stored in the phone as well as automated backup features and options.

Since users exhibit different levels of security feeling in regard to mobile phone communications, and since there are categories of users that face increased security risks due to their self-reassuring feeling that mobile phones are secure per se, research proposed in [37] describes a system that pinpoints and informs mobile phone users that have a low security level, thus helping them protect themselves. The system would consist of software application, installed in mobile phones as well as of software and data bases, installed in the mobile telephony operators' servers. Mobile telephony providers (by adopting this application), as well as manufacturers (by pre-installing it in their phones), could help mitigate the increased security threats effectively protecting the end users.

Software could help users mitigate the security risks associated with the usage of mobile phones. An array of tools could be implemented offering embedded encryption options for data stored in the phone as well as automated backup features and options. Of particular importance would be the implementation of software to inform the users about the encryption state of the phone, a task that seems to be a "taboo" in the mobile phone security ecosystem as we will further see in next chapter. Such software could be written either in Java, for lower-end mobile phones or in full SDK environments for the smart phones. It is also possible to collaborate with providers and implement solutions embedded in the SIM cards, using STK (SIM toolkit). The users of such a system can benefit from the following educational goals:

- Engagement and active participation in the mobile phone security field
- Understanding of the lurking dangers
- Learning how to assess the security level of the mobile phone
- Providing the tools to mitigate the dangers
- Promotion of security best practices
- Encouragement of supplying feedback
- Suggesting security actions to restore the security level

As Fig. 2.5 depicts, the system would consist of an application installed in mobile phones, and software and data bases installed in mobile operators' main servers. These applications communicate through the mobile telephony network in a

Fig. 2.5 System architecture

ciphered way. The mobile phone installed application (with minor differences in the array of services offered) would be able to function in all kinds of devices that have an advanced operating system (e.g. Windows Mobile, Symbian, Android, iOS). A lighter version could also be implemented for older and simple devices using J2ME (Java 2 Micro Edition).

Three main functions would be performed by the system. The first function allows pinpointing users, who have a low security level in their mobile phone, for whatever reason. The second function automatically suggests the proper methods, actions, and best practices the user has to follow in order to restore security in a higher level. Finally, the third function allows the encrypted communication and data exchange between mobile devices and provider's servers.

The device's security level evaluation function could be implemented automatically, manually, or with a combination of the two. Using the automatic method, the application transparently examines the device settings and informs the user about those that are in a state possessing security risk. In addition, by addressing questions to the user, the manual method can check aspects of his behavior that do not reflect directly to the device settings.

Furthermore, the user would be asked for his subjective opinion on how secure he feels his mobile is. As it is mentioned earlier, users can be grouped in specific security categories, based on demographical and other behavioral elements as well as on the way of using their mobile phones. Results from both the manual and the automatic method are transferred to the applications in the server, where using artificial neural networks and rules, conclusions would be extracted for the specific combination of user—mobile phone. Respectively, the answers to proper questions that examine the security practices that users follow can lead to a security behavioral prediction model of the users. It is also possible to record the hour where changes of security influencing settings take place, as to provide one more element that can help the security model.

The system would maintain data bases from studies in large user categories that provide the proper body for the system's training. These data bases would constantly be updated with the results and the metrics from the system's operations. Finally, a very important function is the comparison of automated metrics to the user's answers. As it was previously mentioned, part of user's answers can be cross-checked from the data extracted automatically. Moreover, the system could compare the subjective security awareness and feeling (according to answers for questions fifteen (15)—sixteen (16)), with the objective indicators MAAV and MASV. In this way, the user can be protected from a false perception of security that he probably has, believing that he is secure, while in reality is not. These two methods, the automatic detection of settings and the conclusions extraction based on user's answers, complete the first stage of evaluating the security level.

At the second stage, the system would implement the functionality of informing the user. Examining the current state and user's profile, the application suggests proper methods, actions, and best practices the user has to follow in order to restore (if needed) the security in a higher level.

If the device allows it and if the user accepts it, device settings could automatically be changed. Depending on the device functionality, instructions are presented to the user, either as simple text documents or as multimedia material. The user can also configure different graphical user interface and setup elements.

For the proper operation of the system, encrypted communication and date exchange between the device's application and the servers of the provider's network would take place. This communication is essential for off-loading the resource intensive neural network classification to the servers, instead of running it in the mobile device. In that way, the mobile device only records settings and the whole process takes place in the servers. Moreover, this communication allows not only the disposal of new multimedia material whenever is available but also the enrichment of the manual evaluation method with new questions when new scientific data are presented. It could also upgrade the application itself so that it can examine and locate a greater array of mobile phone's settings that reflect to its security. In any case, the communication would take place in a ciphered way so that interception is not possible.

References

1. Lenhart A (2010) Cell phones and American adults. Pew Research Center, http://www.pewinternet.org. Accessed 10 Feb 2011
2. Androulidakis I, Kandus G (2011) A survey on saving personal data in the mobile phone. In: Proceedings of sixth international conference on availability, reliability and security (ARES 2011), pp 633–638, Sept 2011
3. Androulidakis I, Kandus G. Feeling secure vs. being secure, the mobile phone user case. In: Proceedings of 7th International Conference in Global Security, Safety and Sustainability (ICGS3), Lecture Notes of the Institute for Computer Sciences 2012
4. Androulidakis I, Kandus G (2011) Correlation of mobile phone usage characteristics, security awareness and feeling to the monthly bill. In: Proceedings of the 11th International Conference on Telecommunications, June 2011, pp 257–263

5. Androulidakis I, Kandus G (2011) Mobile phone downloading among students: The status and its effect on security. In: Proceedings of 10th International Conference on Mobile Business (ICMB2011), June 2011, pp 235–242
6. Androulidakis I, Kandus G (2011) differences in users' state of awareness and practices regarding mobile phones security among EU Countries. In: Proceedings of 15th WSEAS international conference on communications, pp 296-300
7. Androulidakis I, Kandus G (2011) Ramifications of mobile phone advanced O/S on security perceptions and practices. In: Proceedings of the 3rd International Workshop on Cyberspace Safety and Security (CSS2011), pp 33–38
8. Dillman DA (1999) Mail and Internet surveys: the tailored design method, 2nd edn. Wiley, New York
9. Pfleeger SL, Kitchenham BA (2001) Principles of survey research Part 1: turning lemons into lemonade. ACM SIGSOFT Software Engineering Notes 26(6):16–18
10. Boynton PM (2004) Hands-on guide to questionnaire research: Administering, analyzing, and reporting your questionnaire. BMJ 328:1372–1375
11. Androulidakis I, Androulidakis N (2005) On a versatile and costless OMR system. WSEAS Trans Comput 2(4):160–165
12. Androulidakis I (2011) Intercepting mobile phone calls and short messages using a GSM Tester. In: Proceedings of CN2011, vol 160, CCIS. Springer, Berlin, pp 281–288
13. Synovate (2009) Global mobile phone survey shows the mobile is a 'remote control' for life, Synovate survey. http://www.synovate.com. Accessed 9 Oct 2010
14. Siau K, Shen Z (2003) Building customer trust in mobile commerce. Comm ACM 46(4):91–94
15. Leung A, Sheng Y, Cruickshank H (2007) The security challenges for mobile ubiquitous services. Inf Sec Tech Rep 12(3):162–171
16. Androulidakis I, Basios C, Androulidakis N (2007) Survey findings towards mobile services usage and M-Commerce Adoption. In: Proceedings of 18th European Regional ITS Conference, International Telecommunications Society, CD-ROM, September
17. Androulidakis I, Basios C, Androulidakis I (2008) Surveying users' opinions and trends towards mobile payment issues. Front Art Intell Appl. 169: 9–19 (Techniques and Applications for Mobile Commerce—Proceedings of TAMoCo 2008
18. McAfee (2008) Mobile security report 2008
19. Trend Micro (2009) Smartphone users oblivious to security. Trend Micro survey
20. CPP (2010) Mobile phone theft hotspots. CPP survey
21. ITwire (2010) One-third of Aussies lose mobile phones: survey. ITwire article
22. Rahman M, Imai H (2002) Security in wireless communication. Wireless Personal Comm 22(2):218–228 [Online]
23. Androulidakis I, Papapetros D (2008) Survey Findings towards awareness of mobile phones' security issues, recent advances in data networks, communications, computers. In: Proceedings of 7th WSEas international conference on data networks, communications, computers (DNCOCO '08), Nov. 2008, pp 130–135
24. Vrechopoulos AP, Constantiou ID, Sideris I (2002) Strategic marketing planning for mobile commerce diffusion and consumer adoption. In: Proceedings of MBusiness 2002, July 8–9
25. comScore M:Metrics (2008) Smarter phones bring security risks: Study. http://www.comscore.com. Accessed 9 Oct 2010
26. Allam SA (2009) Model to measure the maturity of smart-phone security at software consultancies, Thesis, University of Fort Hare. http://hdl.handle.net/10353/281
27. National Cyber Security Alliance (NCSA) (2009) Schools lacking cyber security and safety education
28. Cable & Wireless (2009) Workers lack mobile phone etiquette
29. De Keukelaere F, Yoshihama S, Trent S, Yu Z, Luo L, Zurko ME (2009) Adaptive security dialogs for improved security behavior of users, human-computer interaction—INTERACT 2009, LNCS 2009, Vol 5726. Springer, Heidelberg, pp 510-523
30. Langheinrich M (2002) A privacy awareness system for ubiquitous computing environments. In: Proceedings of UbiComp, pp 237–245

31. Cornwell J, Fette I, Hsieh G, Prabaker M, Rao J, Tang K, Vaniea K, Bauer L, Cranor L, Hong J, McLaren B, Reiter M, Sadeh N (2007) User-controllable security and privacy for pervasive computing. In: Eighth IEEE workshop on mobile computing systems and applications, HotMobile 2007
32. Nancy J. King NJ, Jessen PW (2010) Profiling the mobile customer—Privacy concerns when behavioral advertisers target mobile phones. Computer Law Security Rev 26(5):455–478
33. ABI Research (2009) Study: enterprises need to address cell phone security
34. TechRepublic (2007) Survey respondents say companies are lax on mobile security. TechRepublic article
35. Darkreading (2010) Survey: 54 percent of organizations plan to add smartphone antivirus this year. Darkreading article
36. Goode Intelligence (2009) Mobile security the next battleground. http://www.goodeintelligence
37. Androulidakis I, Kandus G (2012) PINEPULSE: A System to PINpoint and Educate Mobile Phone Users with Low Security. In: Proceedings of 7th International conference in global security, safety and sustainability (ICGS3), Lecture notes of the institute for computer sciences, vol 99, pp 62–66

http://www.springer.com/978-3-319-29741-5

Mobile Phone Security and Forensics
A Practical Approach
Androulidakis, I.I.
2016, XI, 120 p. 47 illus., 34 illus. in color., Hardcover
ISBN: 978-3-319-29741-5