What University Students Do (or Don't) Know about Security in their Mobile Phones

Iosif Androulidakis, *Member, IEEE* and Gorazd Kandus, *Senior Member, IEEE*

***Abstract* — We surveyed a pool of 433 students at the University of Banja Luka in Bosnia and Herzegovina during April 2010, examining users' perceptions about mobile phones security. The main research hypothesis validated was that users are unaware of the necessary measures to avoid a possible unauthorized access and/or sensitive data retrieval from their phones and that they lack proper security education. Most of the results proved to be non-country specific, revealing that users feel mobile phone communication is not secure. We further present the results about users' security practices regarding mobile phone usage.**

***Keywords* — mobile phone security, mobile phone usage, security practices, user interface security, questionnaire survey.**

I. Introduction

MOBILE devices are becoming a critical component of the digital economy, a style statement and useful communication device, a vital part of daily life for billions of people around the world [1]. Used for personal entertainment or business purposes, the mobile phone has contributed to the growing momentum of the wireless revolution and the m-commerce explosion. Modern mobile phones' enhanced capabilities allow them to be almost as versatile as a computer becoming a valuable business (mobile applications, m-commerce) and entertainment tool (mobile games). At the same time users store and process more data including sensitive information in their phones (e.g. private life photos shot by the phone's internal camera or credit card numbers and PINs).

A few years ago the only concern of a mobile phone user would be his communication privacy. This is not the case anymore. Users have to be protected from unauthorized third party access to their data. It is logical that apart from the traditional security measures such as PIN usage and voice encryption, users have to take extra security measures and follow new best practices. Unfortunately they fail to do so as the results of this paper clearly show.

The main research hypothesis validated through the selection of 22 specially crafted questions was that users are unaware of the necessary measures they need to take in order to avoid a possible unauthorized access and/or sensitive data retrieval from their phones and that they lack proper security education. Proceeding one step further, we compared the results to a previous survey in the University of Ioannina, Greece [2]. The University of Banja Luka in Bosnia and Herzegovina was chosen as a typical Bosnian University with many similarities to the University of Ioannina, as to have the same distribution in the sample. However, the two cultures are different and the important finding of this comparison was that results are not "country" specific, but have the same, more or less, appearance among the two countries surveyed.

Iosif Androulidakis (corresponding author) is with the Jožef Stefan International Postgraduate School, Jamova 39, Ljubljana SI-1000, Slovenia, (e-mail: sandro@noc.uoi.gr)

Gorazd Kandus is with the Department of Communication Systems, Jožef Stefan Institute, Jamova 39, Ljubljana SI-1000, Slovenia, (e-mail: gorazd.kandus@ijs.si).

II. Related Work

Apart from quite many theoretical studies concerning mobile services, a significant means for investigating and understanding users' preferences is asking for their opinion via specific questioning techniques, as shown by several survey studies in this direction. The vast majority of these surveys indicate the growing importance of mobile phones in everyday life and the increased popularity of new features.

In any case, the security of mobile phones is proven not to be adequate in many research papers [3] – [6]. There also exist several survey studies in this direction. Some of these focus on mobile phone's security issues [7] while others focus on mobile phone services, touching also security issues [8] – [12].

A recent survey [7] published in November 2008 focused on mobile phones security issues and to the degree to which these issues concern the users. The conclusion was that a major part of the participants was extremely concerned about security and possible 3d party unauthorized access to their private data. As mentioned earlier, following the same rationale and based on the results of a similar survey [2] that took place last year at a Greek University we used the technique in order to understand users' security practices and to possibly compare the results among the users of the two countries.

It is interesting to note that according to other surveys [11], [12] a major part of the participants is interested in mobile services adoption only if the prices are low and the security framework is tight enough. This is why in the present paper we also try to address users' security awareness and practices, as an enabler for greater mobile services market penetration.

III. Methodology

In-person delivery of multiple-choice questionnaires is a very useful evaluation method for surveying user's practices [13], [14]. Our survey was conducted using such a delivery technique, with a total of 433 respondents participating in this survey. This method was selected instead of other alternatives (i.e. email or on-line survey) because it is more accurate and has a higher degree of participation from the respondents (e-mail questionnaires usually treated as spam mail from the respondents or they might misunderstand some questions). Data entry was handled using custom software [15].

The target group of the survey was university students aged mostly between 18 and 24 years. People of this age are more receptive to new technologies. They also understand better the technological evolution than older people who use mobile phones mostly for voice calls.

IV. Results

The questionnaire used consisted of two parts. In the first part we asked from the participants demographic data 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 we proceeded to our main contribution, the specific questions related with their practices and security perceptions regarding mobile phones' security issues.

A. Demographics

Participants were asked about their gender, age and field of studies. 58.2% of them were females and 41.8% were males while most of the respondents were aged 18-23 (74.3%). The main body of respondents was studying Economics-Business Administration (28.2%) followed by Law (27.5%). There were equal parts of students of Humanities-Philology and Medicine (15.5% and 15%) with the rest of respondents (~13%) studying Engineering-Computing or Maths and Natural Sciences. It is arguable that the sample was mainly studying "theoretical" sciences but as it will be seen from the comparison with the Greek sample (where 41.4% of students were in Engineering-Computing or Maths and Natural Sciences) the responses are essentially the same.

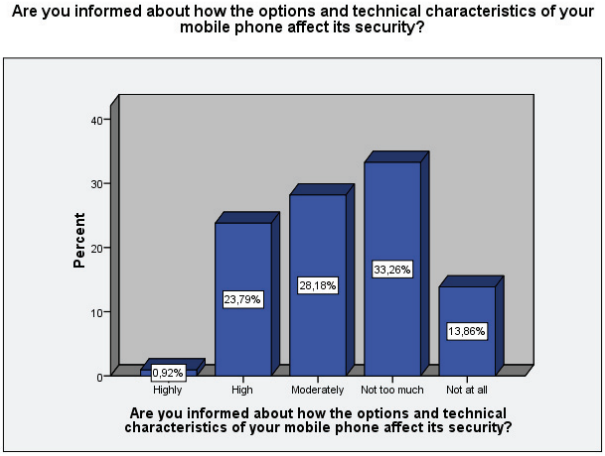

Fig. 1. Knowledge of mobile phone security aspects.

Our fundamental research question was whether students 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 results that follow are totally in line with the initial response of students that only 1% believe they are highly informed, with 47.1% stating that they are not much or not at all informed, Fig. 1.

In regard to mobile phone usage (Fig. 2), 82.2% of them are using a single mobile phone daily, with some 15.5% using two phones regularly (compared to 34% of Greek students). Nokia is the favourite brand, reaching 43% of students followed by Samsung (34%) and Sony Ericsson (15%). Greek students preferred Sony Ericsson (46%) and then Nokia (26%) and Samsung (9.5%). It is immediately apparent that focusing on Nokia and Samsung phones a security awareness campaign in Bosnia and Herzegovina would at once target almost 75% of users yielding a very high return of investment. Of course the brand itself is not enough to categorize attack vectors and practices, since there is also the feature of the specific operating system running on each phone.

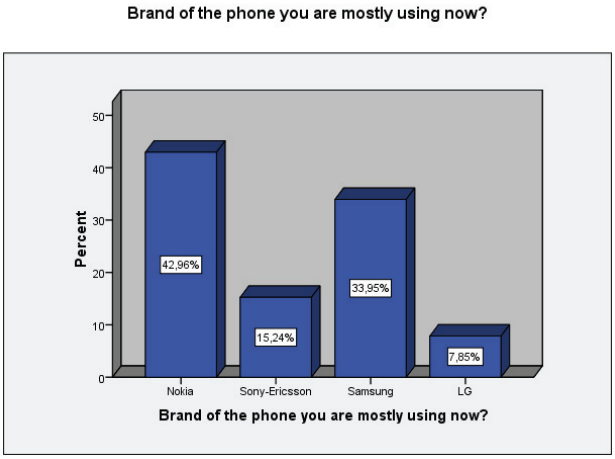

Fig. 2. Favourite brands.

B. Economics

Proceeding to economics, we asked participants whether they are using a pre-paid or post-paid (contract) mobile phone connection. 70.4% of students are using a pre-paid (card), a result seconded by the 69% of Greek respondents.

Answering how much money they spent monthly, student mobile phone users have, as it was expected, limited budgets. More than 70% spend less than 20 Euros per month (currency converted) while most of them fall in the 11-20 Euros range (43.2%). Greek students appear to spend slightly more, having 37% in the range of more than 20 Euros per month, compared to 29.6% of Bosnians.

C. Security Specific Questions

The main contribution of our research was to determine whether our participants acknowledge some security related features of their phone. This objective was achieved with the particular subsection questions and

results are analyzed in the following paragraphs. Starting with a generic question about how "safe" mobile phone users consider communications through mobile phones, the majority (37.2%) replied "moderately", with an alarming sum of 46.7% stating not too much or not at all. As a matter of fact 19.6% of users feel not secure at all, Fig. 3. Greek students reply the same, with some 40% that are not too much or not at all sure that they are safe.

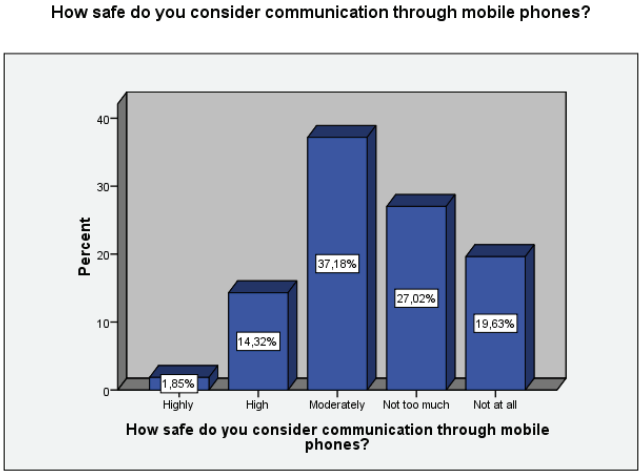

Fig. 3. How safe do you consider communication through mobile phones?

A considerable percentage of the participants (19%) don't know about the capabilities of their phone's operating system. Some 23% of students are using mobile phones with an advanced operating system, slightly more than Greeks (17%). In any case, the ignorance of the type of operating system renders users more vulnerable to hacker attacks with the use of exploits specifically targeted for their phones [4], [16].

Similarly, less than 18% know his/her phone's IMEI and have noted it somewhere. IMEI is very significant because if the phone is ever stolen, using this serial number the provider can block access to the stolen phone effectively mitigating stealing risks. Half of the students are completely unaware of its existence. Knowledge of this feature would have helped 34% of them (or 31% of Greeks) who unfortunately had their phone stolen or lost once or more.

At the same time, just 15% (Fig. 4) of users (exactly the same percentage of Greek students) are aware of the existence of the special icon that informs the user that his/her phone encryption has been disabled [5]. Ignorance of this security icon leaves users vulnerable to man in the middle attacks since they can't recognize the attack taking place. This was probably the most expected result as even professionals are not aware of this feature. It is also an indication that user interfaces instead of revealing security dangers, sometimes obscure them.

Unfortunately, almost half of the users (46.2%) do not activate the PIN code in their SIM card. One can argue that this is because they are using pre-paid phones so the financial losses can be rather limited. Quite contrary to Bosnians, almost 80% of Greek students are using SIM's PIN code.

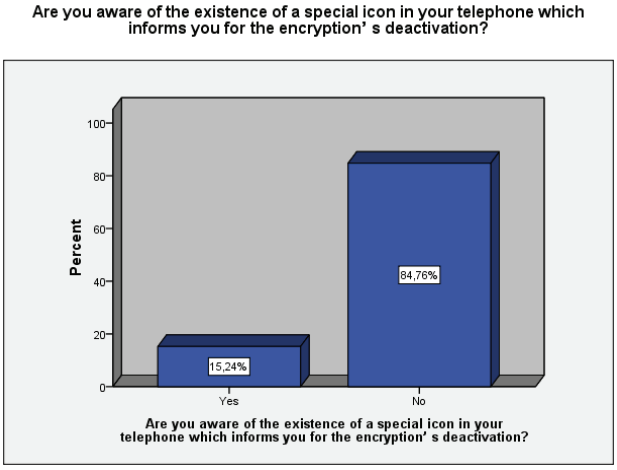

Fig. 4. Encryption icon knowledge.

The negative finding of the next question reveals that only a small percentage (10%) uses a screen-saver password while similar percentages do not know if their phone has such an option or are positive that their phone doesn't support the feature. That leaves 90% of users without a screen saver password and their phones ready to be manipulated by "malicious" hands. An attack can take place in a few minutes by downloading specific software to the phone; this is why it is not enough to protect the phone only by PIN but also by a screen saver password.

A great attack vector of the past, Bluetooth, seems not to be the problem any more. Just 6% have Bluetooth switched on and visible (leaving the phone vulnerable), while almost 73% of users have it switched off. It is not clear whether this is a security practice or a social practice that stemmed from the continuous harassements that messages over Bluetooth caused upon users. Greek students are a little more tolerant since 20% of them are still waiting for Bluetooth messages (while the remaining 56% have completely switched it off)

In a question that touches upon issues of politeness and openness, 55% of students are lending their phones, but only while they are present. This is a major factor that compromises the phone's security even if the participant is present, because a single minute is needed for someone to install malicious software in the phone. In that respect 37% of Greeks refuse to lend their phone in any case, being better safe and "impolite" than sorry.

Following with a question of both security and economic importance, almost half of participants don't download any software at all. There is also 44.8% that actively download ringtones or logos, 6.2% that try applications and only 4.6% of "gamers". It is also interesting to note that the penetration is considerably higher than that of Greece's where 64.5% of users do not download at all (a somehow steady trend with results that haven't changed since a few years ago [8], [9]). In the antipode, getting familiar with downloading users are being more vulnerable to downloading and using unauthorised software that can harm their phone.

This is where a mobile phone antivirus would help. It is sad to see that both Bosnians and Greeks are still not using such products. In our case, 24.9% of users acknowledge

there exists such a product but don't use it, while almost half of them (41.8%) do not know whether such a product exists. That leaves just a fraction of 6.2% using it. Compared with PC users where nowadays everybody is using (at least) an antivirus, this shows a clear lack of security education and different mind-set.

Being young, 45.7% of university students (some 10% less than Greeks) keep sensitive information in their mobile phones. It seems that we consider our mobile phone to be a very personal device and we save equally important and sensitive information there. Such kind of information should be protected but again, the results from our survey show that users fail to do so. The consequences from a breach of data of this type could be devastating for the life of the victim.

In a rather positive finding, more than 77.6% of users are not saving important passwords in their phone. Almost 15% are using some form of encryption (i.e. letter scrambling) while only 7.5% keep their passwords saved in plain. These results are somehow better than the ones we saw in Greece's survey. Since users follow the notion of encryption in these saved passwords, it is expected that they would be able to do the same with private information (i.e. photos) kept in the phone, should they be provided with the necessary software. Once again, the issue of better designed user interfaces surfaces.

Closing our survey, we examined the issue of backup. As it was seen, a whopping percentage of the participants surpassing 88% never perform a backup of their phone's data. One can argue that this was one of the most expected findings since even PC users don't actively back their data up.

V. Conclusions and Future Work

Taking into consideration the answers given, we can deduce that users lack proper security education and are unaware of security measures and best practices, thus validating our research hypothesis. Conducting the survey in another country proved that the challenging findings of the previous survey were true. While the majority of the respondents care about security issues and are concerned about data interception and the fact that an intruder could gain unauthorized access to their devices, there is no culture of security and no advanced technical knowledge of their mobile phones. A very high percentage of users didn't know there was an icon that informs them about the phone encryption status. Most of them don't take backups at all while at the same time would lend their phone that contains sensitive data and passwords to somebody else. Contributing to the problem, badly designed interfaces are an additional factor of hindering the development of security culture.

In order to have comparative results, we have conducted a similar survey in more than 10 European countries reaching more than 7500 students and the results will soon be published. The preliminary findings however, show that users exhibit the same behaviour everywhere. Since students (who are young people and mostly receptive to technology and knowledge) do not actively follow most of security best practices then academia, phone manufacturers and operators must team up informing users, raising awareness level and building more secure systems and user interfaces.

APPENDIX

The questionnaire used:

1) Male (A) or Female (B)?

2) Age? (A < 18, B 18-20 , C 21-23, D 24-26 , E >26)

3) Are you studying: (A: Humanities-Philology, B: Medicine, C: Law, D: Engineering-Computer Science, E: Maths-Natural Sciences, F: Economics-Business Administration, G: Other)

4) How many mobile phones do you use (daily)? A) 1 B) 2 C) >2 D) None

5) Are you a contract subscriber or a prepaid subscriber? A) Pre-paid (Card) B) Post-paid (Contract) C) Both

6) Your average monthly phone bill? (A: up to 10 Euros, B: 11-20 Euros, C: 21-30 Euros, D: 31-40 Euros, E: >40 Euros)

7) Brand of the phone you are mostly using now? (A: Nokia, B: Sony-Ericsson, C: Samsung, D: Sharp, E: Apple iPhone, F: Motorola, G: LG, H: Other)

8) Does it have an advanced operational system (eg Symbian, Windows Mobile, Android)? (A: I don't know, B: yes, C: no)

9) Have you noted somewhere your mobile phone's IMEI? (A: I don't know what it is, B yes: C no,)

10) Was your mobile phone ever lost or stolen? (A: Never, B: once, C: more than once)

11) Are you aware of the existence of a special icon in your telephone which informs you for the encryption's deactivation? (A: Yes, B: No)

12) Do you have SIM card's PIN activated? (A: Yes, B: No)

13) Do you use password in your phone's Screen-Saver? (A: I don't know if it has such a feature, B: doesn't have such feature, C: Yes, D: No)

14) Do you have Bluetooth: (A: Switched on and visible, B: Switched on and invisible, C: Switched off, D: don't know the difference between visible and invisible, E: My phone doesn't have Bluetooth)

15) Do you lend it to others? (A: Never, B: Only for a while and if I am present, C: Yes)

16) Do you "download" software to your phone? (A: I don't know if my mobile phone can download, B: No, C: mostly Ringtones/Logos, D: mostly Games, E: mostly Applications)

17) Do you use Antivirus software in your phone? (A: Doesn't have the ability, B: Don't know if there is such a product for my phone, C: I know there is but I don't use, D: Yes)

18) Do you store important passwords in your phone (eg Credit cards passwords, ATM passwords)? (A: No, B: Yes and "encrypted", C: yes, without encryption)

19) How often do you create backup copies of your phone's data? (A: Never, B: >3 times per month, B: 2-3 times per month, C: Once per month, D: Less often)

20) Do you keep sensitive personal data in your phone (photos/videos/discussion recordings)? (A: Yes, B: No)

21) How safe do you consider communication through mobile phones? (A: Highly, B: High, C: Moderately, D: Not too much, E: Not at all)

22) Are you informed about how the options and technical characteristics of your mobile phone affect its security? (A: Highly, B: High, C: Moderately, D: Not too much, E: Not at all)

REFERENCES

[1] Measuring the Information Society, The ICT Development Index, ITU 2009.

[2] I. Androulidakis,V.Christou, N. Bardis, I. Stilios, Surveying users' practices regarding mobile phones' security features, Proceedings of 3rd International Conference on COMPUTATIONAL INTELLIGENCE (CI'09), pp 25-30, Jun. 2009.

[3] Rahman, M. & Imai, H., Security in Wireless Communication, Wireless Personal Communications [Online], vol. 22, issue, 2, pp.218-228, 2002.

[4] I. Androulidakis, "Security Issues in Cell Phones", article-interview into Magazine "Defence and Diplomacy", Issue 187, pp 100-102, November 2006.

[5] I. Androulidakis, Intercepting mobile phones and short messages, Computers and simulation in modern science, Selected papers from WSEAS conferences, Vol II, 2008, pp 320-321, Dec. 2008

[6] I. Androulidakis, Intercepting Mobile Phones, Article in «IT security professional» magazine, Issue 8, pp. 42-28, Jan-Feb 2009.

[7] I. Androulidakis, D. Papapetros, Survey Findings towards Awareness of Mobile Phones' Security Issues, Recent Advances in Data Networks, Communications, Computers, Proceedings of 7th WSEAS International Conference on Data Networks, Communications, Computers, pp 130-135, Nov. 2008.

[8] Androulidakis N., Androulidakis I. m-Business: The base for creating competitive advantage. The case of Vodafone-Panafon, Wseas Transactions on Information Science and Applications, Issue 5, Vol 1, 1309-1313, 2004.

[9] Androulidakis, N. and Androulidakis, I. Perspectives of Mobile Advertising in Greek Market, 2005 International Conference on Mobile Business (ICBM 2005), 2005.

[10] Vrechopoulos, A.P., Constantiou, I.D. and Sideris, I. Strategic Marketing Planning for Mobile Commerce Diffusion and Consumer Adoption, in Proceedings of M-Business 2002, July 8-9, 2002.

[11] I. Androulidakis, C. Basios, N. Androulidakis, Survey Findings towards Mobile Services Usage and M-Commerce Adoption, Proceedings of 18th European Regional ITS Conference, International Telecommunications Society, pp: CD-ROM, September 2007.

[12] I. Androulidakis, C. Basios, N. Androulidakis, Surveying Users' Opinions and Trends towards Mobile Payment Issues, Frontiers in Artificial Intelligence and Applications - Volume 169, pp. 9-19, 2008 (Techniques and Applications for Mobile Commerce - Proceedings of TAMoCo 2008).

[13] Dillman, D. A. Mail and Internet Surveys: The Tailored Design Method, John Wiley & Sons, 2nd edition, November 1999.

[14] Pfleeger, S. L. and Kitchenham, B. A. Principles of Survey Research Part 1: Turning Lemons into Lemonade ACM SIGSOFT Software Engineering Notes, vol. 26 (6), November 2001.

[15] Androulidakis I., Androulidakis N. On a versatile and costless OMR system Wseas Transactions on Computers Issue 2, Vol 4, 160-165, 2005.

[16] I. Androulidakis, "This is how hackers hack into our cell phones", article-interview into Sunday Newspaper "To proto thema", Issue 90, pp 40-41, November 12, 2006.