Differences in Users' State of Awareness and Practices Regarding Mobile Phones Security Among EU Countries

IOSIF ANDROULIDAKIS

Jožef Stefan International Postgraduate School
Jamova 39, Ljubljana SI-1000, Slovenia
sandro@noc.uoi.gr

GORAZD KANDUS

Department of Communication Systems
Jožef Stefan Institute
Jamova 39, Ljubljana SI-1000, Slovenia
gorazd.kandus@ijs.si

Abstract: - As a style statement and useful communication device, the mobile phone has become a vital part of daily life for the majority of population in the developed world. While we are enjoying the technological advances that mobile phones offer, we are also facing new security risks coming as a cost of our increasing dependence on the benefits of wireless communications. In order to investigate users' security awareness and practices with regard to security in mobile phones, in this paper, we present the results of a survey conducted in 17 Universities of 10 Eastern and Southern Europe countries. 7172 questionnaires were gathered and processed with the results showing that users feel that mobile phone communication is moderately secure. The survey further showed 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. It is unquestionable that since users fail to secure their phones, industry and academia should proceed in educating them and designing better user interfaces in order to mitigate the risks

Key-Words: - mobile phone security, security practices, user interface security, questionnaire survey, mobile phone usage, user awareness, security education

1 Introduction

With the growing momentum of wireless technologies, offering among other things m-commerce capabilities, it is evident that 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. Used for personal entertainment or business purposes, the mobile phone has made a huge difference in how we do things nowadays. It is a safe prediction that in the near future the security of our mobile phones will affect our wellbeing in the broadest sense [1].

On the technological end, data and information security concern has been fiercely discussed along with the progress of wireless technology, as a result of wireless communications nature as a broadcast-based medium. For a mobile phone network, security should be an issue critically important to end-users and service providers from various perspectives. On the one hand, consumers need to be assured levels of trust to embrace wireless services; on the other hand, service providers benefit from wireless security in protection from fraudulent use of services, protection from unauthorized use of mobile devices, managing the distribution of digital rights (i.e. distribution of audio and video files under license arrangements), and possibly as a competitive advantage relative to other service providers [2].

We realized this survey in order to investigate users' security awareness and practices with regard to security in mobile phones. Results show that users feel that mobile phone communication is moderately secure. They are unaware of the necessary measures to avoid a possible unauthorized access and/or sensitive data retrieval from their phones and they lack proper security education. Despite the fact that we focused on students (who are usually living on a limited budget), there was a wide range of devices in use, varying from simple ones to smart phones (24% of devices had an advanced Operating System).

ISBN: 978-1-61804-018-3

2 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].

There also exist several survey studies researching security issues. Some of these surveys studies focus on mobile phone's security issues [8][14] while others on mobile phone services, touching also security issues [4]. In any case, the security of mobile phones is proven not to be adequate in many research papers. Modern smart phones, specifically, are vulnerable to more security risks [17].

A survey [3] published in November 2008 focused on mobile phones security issues and in which degree these issues concern the users. The conclusion was that a major part of the participants is very concerned about security and don't want any of their private data to be available to 3rd party unauthorized users. Furthermore, users are interested in mobile services adoption only if the prices are low and the security framework tight enough [5].

Another study of mobile users focused on their awareness and concerns related to security threats, from security vendor McAfee, indicated that more than three quarters of respondents don't have any security at all [7]. In other words, despite of 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 [8][9][10]), users don't see security strengthening of their phone as a critical concern.

In addition to the above, mobile security is not considered a critical issue by companies. Cell phone security for enterprise devices is seriously lacking, and a little misunderstood as well [11], while the majority of companies do not have a security policy that addresses mobile devices [12]. However, some initiatives are taken in the direction of protecting mobile phones against threats like viruses policies, tools and recruiting technically skilled personnel [13].

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 [14]. While users are not receiving proper cyber security and training education from schools [15], they are lacking the security awareness and proper etiquette [16].

This presents a vast opportunity for carriers and service providers to play a proactive and strategic role in protecting their subscribers, both through education and also through the security software they deploy across their networks.

3 Methodology

A very useful evaluation method for surveying user's practices is the use of multiple-choice questionnaires [6]. Our survey was conducted using in-person delivery technique (researchers approached students and asked them to participate by filling the paper questionnaires) to 7172 recipients in 17 Universities in 10 countries and is interesting to note that such a procedure could be of interest to mobile phone operators or the industry.

The target group of the survey was university students from ages mostly up to 23 years old because these ages are more receptive to new technologies. They also understand better the technological evolution than older people and are always keeping pace with technology, being always informed.

The construction of the questionnaire was based in 2 sets of questions. The first contained demographic and economic questions and it was followed by the security specific part. There were questions about security knowledge and best practices, as well as about users' behaviour in regards to mobile phones usage. Special care was given in order not to "guide" the respondents into answering in a "researcher favourable" way. As such, in most questions the user was free to chose a "don't know what it is" option.

The translated questionnaires were transformed to special forms, which were tested to be compatible with our patented optical mark reading methodology [18] and software. Using just 100dpi resolution and 1bit black & white configuration settings the researchers scanned the filled questionnaires and emailed back the scanned images.

Finally, the statistical process was carried out using SPSS software, where data were processed and analyzed, as presented in the following sections.

ISBN: 978-1-61804-018-3

4 Results

All of the results in the following sections are significant in the p=0.05 level (Pearson's Chi-Square)

4.1 Demographics and hardware

7172 participants from 10 countries (BG, CZ, EE, GR, HU, LT, LV, RO, SI, SK) were asked about their gender, age and field of studies. 53% of the participants were females and 47% were males while most of the respondents (~80%) were aged up to 23 years old. The subjects were studying various subjects 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. Most Bulgarians actually use 2 phones instead just one that the rest of participants use.

Nokia is the favourite brand (Figure 1), reaching 39% of students followed by Sony-Ericsson (25%) and Samsung (15%). This general trend changes only for Greeks and Slovenians. The former prefer Sony Ericsson (46%) and then Nokia (26%) while the latter prefer Samsung (41%), then Nokia (29%). As it was expected Lithuania, Latvia and Estonia being closer to Finland have the highest Nokia penetration ranging from 50%-55%. Apple's iPhone seems to be scarce among students with less than 4% of penetration (8% for Hungary). 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. We must note here that 24% of devices had an advanced Operating System, i.e. SymbianOS , Windows Mobile, Android or iOS.

4.2. Economics

Proceeding to economics, we asked participants whether they are using a pre-paid (card) or post-paid (contract) mobile phone connection. The differences in pricing options and available connection types immediately manifested in the results. Half of countries prefer pre-paid while the others post-paid. Countries with stronger preference to pre-paid are Greece, Czech Rep. and Slovakia with Greek pre-paid students surpassing 69%. On the other hand, Slovenia Estonia and Bulgaria lead the contract-based countries. Bulgarians were able to possess both types of connection (with a relatively high percentage of 28%).

Answering how much money they spent monthly, student mobile phone users have as it was expected limited budgets. The dominant 2/3 spend less than 20 Euros per month (currency converted) while most of them fall in the 11-20 Euros range (37%). Hungarians appear to spend considerably more, followed by Greeks.

Following, with a question of both security and economic importance, almost half of participants (47%) don't 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%.

Sorting the results, in Figure 2, we can see Slovenia and Bulgaria being the champions of downloading (with more than half users actively downloading) while in the antipode Czech Rep, Greece and Slovakia show around 20% penetration of mobile downloading. Of course, getting familiar with downloading users are being more vulnerable to downloading and using unauthorised software that can harm their phone.

Closing this section with a sensitive question, of indirect Economic character, 35% of users reported the loss of a mobile phone (possibly attributed to theft) with some 17% having lost it more than once. Greeks and Slovenians have had the less impact (circa 70% have never lost a phone) while Bulgarians and Romanians mostly impacted (65% lost once or more times their phone)

4.3. Security Questions

4.3.1 General feeling

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 dominant response was "moderately" with 31% while a significant 38% said not too much or even not at all (Figure 3). Czechs and Slovaks and Romanians feel more informed. 62% of Bulgarians said they are not much or not at all informed followed by Latvians, Greeks and Estonian that each one have sums of 46%-48% in the same two categories. In absolute terms, 30% of Bulgarians and 25% of Greeks are not at all informed.

ISBN: 978-1-61804-018-3

In the general question about how safe (in regards to communication security) mobile phone users feel (Figure 4), the majority (almost 37%) replied "moderately". Czechs and Slovaks consider mobile phone communication very much or much secure in percentages of 87% and 84% followed by 67% of Romanians. On the other hand, Slovenians, Bulgarians and Greeks appear more "suspicious" with percentages of 40%-43% believing that communication is not too much or not at all secure. The most "reserved" ones were Greeks with 21% feeling not at all secure.

4.3.2. Security knowledge

In order to examine the security knowledge level of users, we asked two technical questions. The first was about the Operating System. We found out that a significant percentage of the participants (38%) doesn't know whether it has an advanced operating system or not. Ignorance of the type of operating system renders users more vulnerable to hacker attacks with the use of exploits specifically targeted for their phones.

At the same time, just 25% of users are aware of the existence of the special icon that informs the user that his/her phone encryption has been disabled. Most countries reached levels of around 80% of ignorance for the specific icon. This was probably the most expected result as even professionals are not aware of this feature and another hint that user interfaces should help and not obscure security.

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. Such an occurance can be attributed either to network's lack of encryption capability or to temporary failure/overloading. Unfortunately, the same can happen 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 false base station instead of the true one. The fraudster can then channel the communication through his own equipment, effectively intercepting it. Manufacturers use different icons to signal such a case, namely padlocks, exclamation marks, short informatory messages etc. As revealed by the survey, however, users are anware of them.

4.3.3 Security practices

In this section we examined Security practices, with some of the questions touching technical knowledge.

A small percentage of the participants (exactly 24%) knows his/her phone's IMEI and has written it down 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. Almost half of students (47%) are completely unaware of its existence. Knowledge of this feature and actual implementation of the white and black lists by the operators would help the 51% of users who unfortunately had their phone lost or stolen once or more.

Users, as expected, are actively (more than 67%) using SIM's PIN code. Slovaks and Czechs avoid the usage of PIN, while Estonians and Latvians are the ones using it the most. It is interesting to note that although Greeks are using prepaid cards with some 70% at the same time they have one of the highest percentages of PIN usage, while Slovenians on the other end, leaders in post-paid connections have a relatively low percentage of PIN usage.

Continuing, another negative finding is that more than 85% of users don't have a screen saver password, leaving their phones ready to be manipulated by "malicious" hands. Protecting the phone only by PIN is not enough since an attack can take place in a switched on phone in only a few minutes by downloading specific malware.

A great attack vector of the past, Bluetooth, seems not to be the problem any more. Just one out of five students has Bluetooth switched on and visible (leaving the phone vulnerable), while more than half of users have it switched off. It is not clear whether this is a security practice or a social practice that stemed from the continuous harassements that messages over bluetooth caused upon users.

In a question that touches upon issues of politeness and openness, more than 3 out of 4 students are lending their phones, while 56% does it only for a while and only when 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 and 36% of Hungarians refuse to lend their phone in any case being better safe and "impolite" than sorry. Baltic ones are the friendliest having the highest rates of lending (for a while or more) with percentages varying from 84% to 88%.

ISBN: 978-1-61804-018-3

As we have already discussed in Figure 2, downloading is moderately popular but is expected to grow. This is where a mobile phone antivirus would help. It is sad to see that 48% of respondents aren't aware of whether such a product exists. Some 20% of users acknowledge that such a product exists but don't use it. Excluding those that know that their phone doesn't support such software, we are left with a marginal 7% of users that use antivirus in their phones. Compared with PC users where nowadays more or less are using (at least) an antivirus shows a clear lack of security education and different mind-set. Bulgarians and Hungarians use it mostly (13% and 12% respectively) while in Romania we have a disappointing 1% penetration with 68% of users unaware of such a product.

Considering the mobile phone as a very personal device, 63% of university students keep sensitive information there. Such kind of information should be protected since consequences from a breach of data of this type could be devastating for the life of the victim. Again, results from our survey show that users fail to do so. Romania is leading with some 83% of its users keeping such information in their phones.

In contrast to personal data, and in a rather positive finding, almost 57% of users are not saving important passwords in their phone. Some 24% are using some form of encryption (e.g. letter scrambling) while only 19% keep their passwords saved in plain. Slovenians are again the most security minded, with 83% of them not saving at all passwords in their phone, in whatever form. Since users however generally follow the notion of encryption in these saved passwords, it is expected that they would be able to do the same with private information (e.g. photos) kept in the phone, should they were provided 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 very large percentage of the participants reaching 55% never performs a backup of the 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. Despite their security consciousness, Slovenians have the highest non-backup ratio of 85%, followed by 70% of Greeks. Slovaks and Czechs on the contrary take backups at least once per month (71% and 63%).

5 Conclusion

Conducting the survey in such a representative target group of these 10 countries with a broad participating student sample proved that while the majority of the respondents considers mobile phone communication moderately secure, 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 is 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 lacking security features are an additional factor of hindering the development of security culture (especially regarding the lack of encryption icon, the password option in screen saver, the ability to save encrypted information and the antivirus integration).

Even without considering technical malicious acts, 51% of the sample had its mobile phone (containing sensitive data) lost or stolen, immediately being affected by security and privacy issues. On the positive side, Bluetooth security awareness has grown, while most users while still saving personal sensitive data, at least they refrain from saving passwords.

The use of mobile devices is here to stay. The number of devices, and more importantly, the types of devices, will only increase over time. There are undeniable cost benefits and increases in efficiency that can be derived from their use. But these benefits will only be actualized if a culture of privacy is developed. As wireless communication technology becomes fully integrated into information systems and business processes and m-commerce gains more momentum, it is inevitable that substantial amounts of personally identifiable information will flow over the airwaves.

Users therefore play a key role in protecting themselves and others. Since students (who are young people and mostly receptive to technology and knowledge) do not actively follow most of security best practices, service providers over time should be in a position to provide the means to increase their customers' awareness. Manufacturers on the other hand should proceed to better designed interfaces and mobile phones generally, richer in security features.

ISBN: 978-1-61804-018-3

References

[1] F-Secure , *"Wellbeing in a Mobile World",* F-Secure annual survey, 2010

[2] Krenik,W.,Wireless User Perspectives in the United States, *Wireless Personal Communications* [Online], vol. 22, issue, 2, pp.153-160,2002

[3] 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 (DNCOCO '08),* pp 130-135, Nov. 2008

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

[5] 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)

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

[7] McAfee, *"Mobile Security Report 2008"*, 2008

[8] Trend Micro, *"Smartphone Users Oblivious to Security",* Trend Micro survey, 2009

[9] CPP, *"Mobile phone theft hotspots",* CPP survey, 2010

[10] ITwire, *"One-third of Aussies lose mobile phones: survey",* ITwire article, 2010

[11] ABI Research, *"Study: Enterprises Need to Address Cell Phone Security"*, 2009

[12] TechRepublic, *"Survey respondents say companies are lax on mobile security",* TechRepublic article, 2007

[13] Darkreading, *"Survey: 54 Percent Of Organizations Plan To Add Smartphone Antivirus This Year",* Darkreading article, 2010

[14] Goode Intelligence, *"Mobile security the next battleground",* 2009

[15] National Cyber Security Alliance (NCSA), *"Schools Lacking Cyber Security and Safety Education"*, 2009

[16] Cable & Wireless, *"Workers lack mobile phone etiquette"*, 2009

[17] comScore M:Metrics, *"Smarter phones bring security risks: Study"*, 2008

[18] Androulidakis I., Androulidakis N. On a versatile and costless OMR system *Wseas Transactionson Computers* Issue 2, Vol 4, 160-165 (2005)

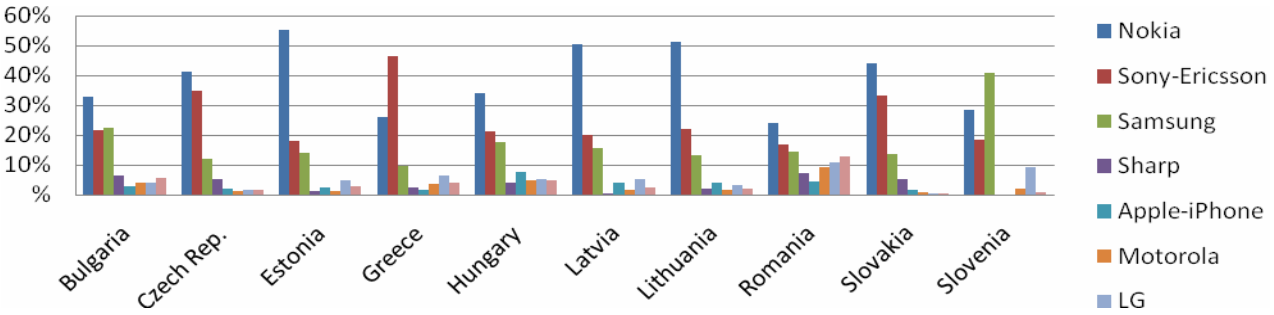

Figure 1. Mostly Used Brand.

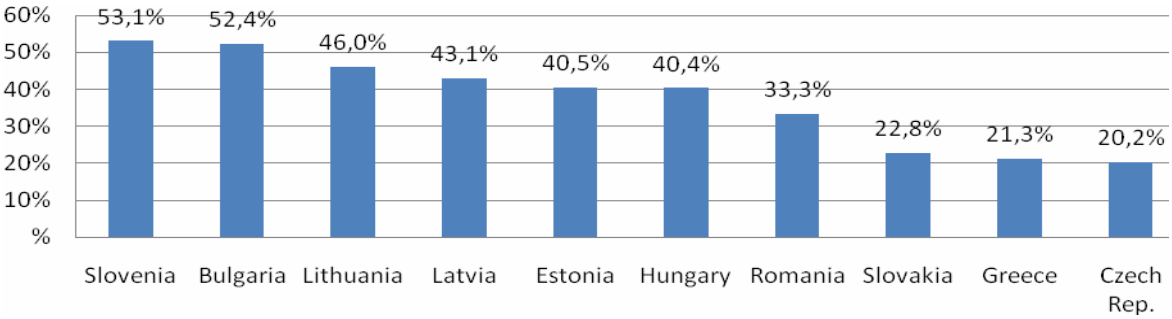

Figure 2. Mobile downloading

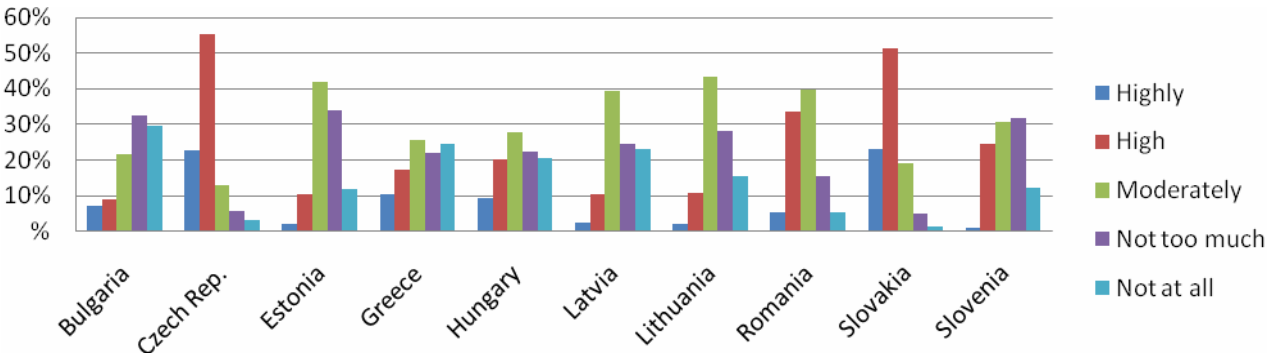

Figure 3. How much informed are you?

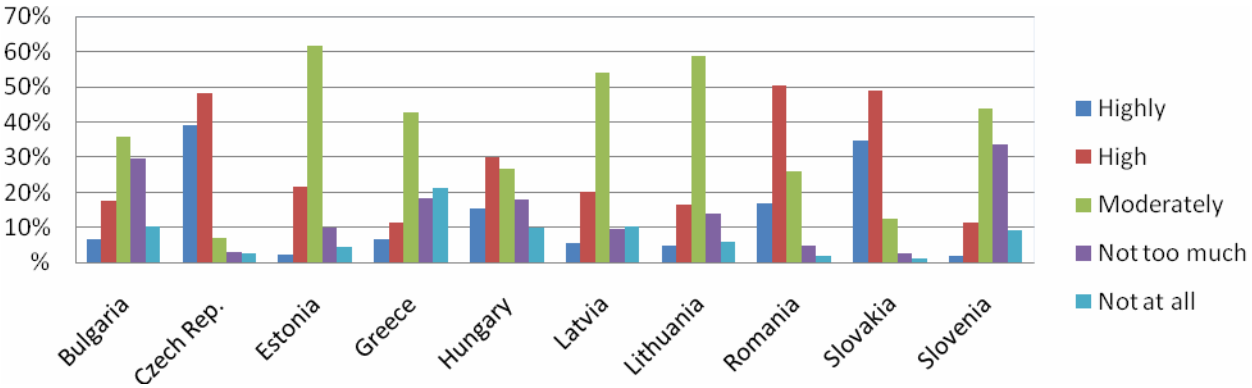

Figure 4. How secure do you consider mobile phone communication?

ISBN: 978-1-61804-018-3