Data Security of Mobile Phones, from the Aspect of University Students

Pál Fehér-Polgár

Óbuda University, Keleti Faculty of Business and Management
feherpolgar.pal@kgk.uni-obuda.hu

Abstract: The dramatic spreading of mobile devices (smartphones and tablets) brings new information security risks and threats. These have to be taken seriously because they are weakening not just our personal security but the security of the organisations too. The security of organisations is mainly based on the attitude for security of the organisational members. Accordingly, the exploration of their approaches of their mobile devices' security is a must. In my paper I have investigated the students of the Óbuda University to find out how they perceive the security of their smartphones. My hypothesis is that even those who use these devices a lot are still not aware of the security risks and threats and they do not have enough or any kind of countermeasure against these hazards.

Keywords: data security, mobile security

1 Introduction

1.1 Spreading of mobile devices

In the last few years the mobile phone market has seen a dramatic rise of the penetration of smartphones and tablets.

At the end of 2012 the top 5 mobile markets of the European countries had an average of 57% market share of smartphones. Spain leads in the ranking with a 66% penetration. UK follows with 64%, France and Italy are at 53-53% and Germany is at 51%.[1]

In the first quarter of 2013 google reported via think.withgoogle.com that the top 3 countries in the share of smartphones are the United Arab Emirates with the share of 73.8%, South Korea with 73.0% and Saudi Arabia 72.8%. In this report UK is the 9th (62.2%) Spain 15th (55.4%), while the USA is at the 13th position with the share of 56.4%.[2]

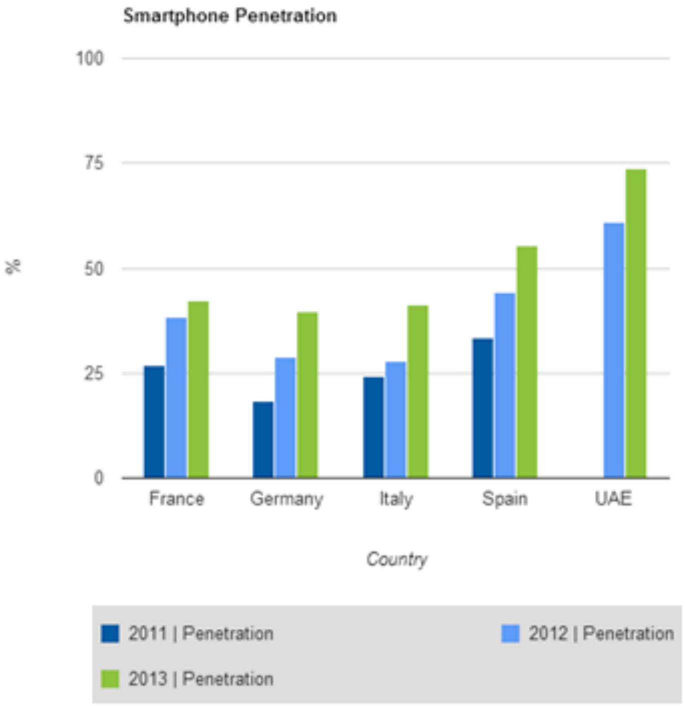

Figure 1
The penetration of smartphones in the selected countries[1] [2]

In Hungary at the end of 2012 the market share of smartphones was at 29% according to the report of eNET-telekom.[3] This report was based on a research of a representative questionnaire with 1000 answers.

On the other hand, another report by NRC reports a 45% penetration of smartphones in the Hungarian market in the first quarter of 2013. This report also covers tablets where it shows that the penetration of this kind of devices had quadrupled from the first quarter of 2012 to the first quarter of 2013. Also in this research NRC found that the penetration of these mobile devices (smartphones and tablets) has a cumulative penetration of 51% in the sample.[4]

If we look in to the data of the report, it is visible that the highest penetration is in the demographic group of highly educated young adults. This very group of twenty something people who are spending their first years at work or still are in the educational system.[3][4]

[1] Data was not available for the penetration in 2011 in the United Arab Emirates.

Accordingly in my research I concentrated on the very same young adult population, and focused on students in tertiary education. My research has been delivered at Óbuda University.

1.2 Security threats and risks of smartphones

The security threats and risks of smartphones are not a new concern for security personals. Although in 2004 Gareth James has written an article in Network Security about malicious threats to smartphones. He has stated that at that point of time no known malicious software existed, but vulnerabilities did.[5] In this paper he summarised that the number of smart phones is low, but the users of them are highly effective persons in the area of politics and business.

Today the penetration of smartphones is much higher, and is still growing. Nowadays the circle of users of these devices has widened. Not only businessmen but almost anybody can afford a smartphone and their devices need security also. The vulnerabilities still exists in the software of mobile devices whether they use Apple's iOS[6] or Android[7] but we have malicious softwares as well now.

The number of malicious softwares is growing fast. In a research of F-Secure they found 238 threats in 2012 and 804 new malware for Android operating system.[8]

According to the European Union Agency for Network and Information Security the top 3 risks for smartphone users are:

1. Data leakage resulting from device loss or theft
2. Unintentional disclosure of data.
3. Attacks on decommissioned smartphones.[9]

These risks are a concern for the data security of the data that stored on the device. Since the owners of smartphones are using their devices not just for business but for private reasons as well. Thus the security threats and risks are a concern not just for business but also for private security.

K. Parsonsa et al. also found that the security of organisations is highly affected by its member's attitude for security.[10] They found that, the knowledge and understanding of the security policies and processes is not enough, and the members of the organisation have to develop a good attitude for security with which they can provide a good foundation for the security of the organisation.

2 Research of the data security on mobile phones from the aspect of the students of Óbuda University

In my research I questioned the students of Óbuda University. Since they are already or will be working in the near future in organisations, their attitudes towards organisational, and in this case towards IT security is of high relevance. Accordingly, the exploration of their approaches of their mobile devices' security is very important.

My research is based on an online questionnaire that consisted of 42 questions generating 87 variables. I asked students from two faculties of the university, Keleti Faculty of Business and Management and John von Neumann Faculty of Informatics.

2.1 Demographic questions

The average age of the sample is 22.29 years. There were slightly more male than female respondents (55%-45%). The division of the faculties were 30%-70% for the faculty of informatics and the faculty of business and management.

Mostly (90%) these students were fulltime students, but almost half of them were already working besides their studies, (42% of the full time students).

2.2 Smartphone usage

The penetration of smartphones in the sample was 90%. This is twice as the penetration of what we could see in the Hungarian smartphone research for the whole market in 2013. Slightly more than 75% are using mobile internet with these devices and 90% of them using Wi-Fi. 16.4% have more than one mobile phone. The average age of their mobile phones is 16.68 months, and the distribution of the phones by age is displayed in the next graph.

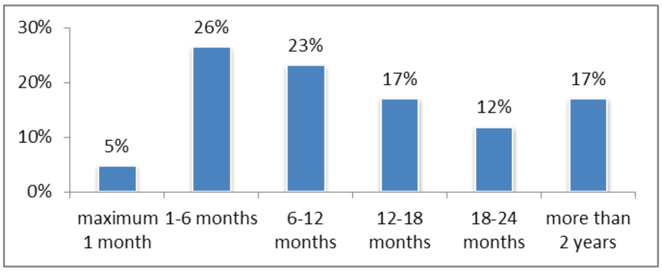

Figure 2
The distribution of the age of the respondents phones in months

They acquired their first phone at the age of 12.4 in average. However the older the respondents were, the later age they received their first mobiles (Pearson Correl.: 0,767, Sig.: 0,000). Interestingly the female respondents had their first phone at a younger age (in average 11.5), than the males (in average 13.1).

2.3 Security questions.

Almost 60% of the respondents stores important data on their phone and 62% are making backups from their phone. The most common stored contents are:

1. Contact list, 159
2. Memos, To-do list, 133
3. Private pictures, 123
4. Deadlines, 99
5. Data connected to their studies, 93

Most of them (41%) make backups more frequently than 3 months' time.

The distribution of the respondents by the frequency of their mobile backups is displayed in the next graph.

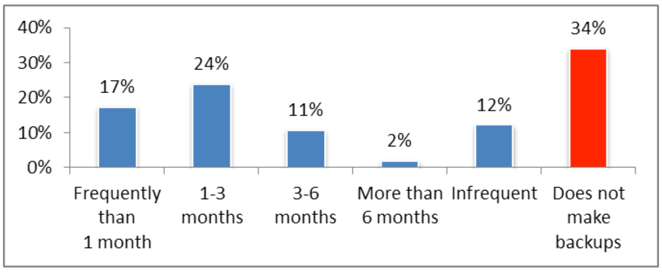

Figure 3
Distribution of the respondents by the frequency of their mobile backups

Although 86.4% of them have already installed some 3rd party softwares only 14.5% has installed any kind of security tool on their mobile phones.

2.4 Hypothesises about the questionnaire

H1. Those who store important data on their phone make backups more frequently.

H2. Those whose phones have been stolen or lost are not storing important data on their phones, or are making backups more frequently.

H3. Those who use internet banking on their phone are actively updating their phone's software and have some kind of security software installed.

H4. Those who use mobile internet or Wi-Fi connection on their phone are updating their mobile phones operating software.

H1. Those who store important data on their phone make backups.

Interestingly, there was not any kind of correlation between storing important data and making backups, or the frequency of it. This means, most of the mobile owners/users are not aware of the threats that they are facing when storing data on mobile devices.

H2. Those whose phones have been stolen or lost are not storing important data on their phones, or are making backups more frequently.

There was no correlation between having experienced the loss of a mobile device with all of its content and making updates more frequently, or at all of the data presently stored on the new device. Additionally, only a weak correlation was found (Pearson Correl.: -0.200, Sig.:0.003)This means, that those experiencing the loss of important personal data are a bit less probable to store such data on mobile devices again.

H3. Those who use internet banking on their phone are actively updating their phone's software and have some kind of security software installed.

Using internet banking means sharing and transmitting financial data, and security information via the mobile device. I hypothesised that those, using such applications are more aware of security risks, and try to deal with them accordingly, either by frequently updating their software or installing specific security measures. There was an extremely weak, but significant correlation between the updating habits of the respondents and the use of internet banking on their mobile phone (Pearson Correl.: 0.197, Sig.:0.000). However, there was no correlation between the use of internet banking and security measures on their phone.

H4. Those who use mobile internet or Wi-Fi connection on their phone are updating their mobile phones operating software.

Using of internet on mobile means connection with remote websites via the software of the mobile phone. Last year's Mobile Pwn2Own competition has ended with founding such of software errors that could lead to remote code execution via the web browsers of smartphones.[11] Thus the continuous updating of the software is a must. I hypothesised that who are actively using internet on their phones are updating their software too in order to minimize the security risks of software vulnerabilities. I have found a week correlation between usage of internet via mobile net and updating the mobile's software (Pearson Correl.: 0.231, Sig.:0.000). On the other hand there was a week correlation between the usage of internet via Wi-Fi and updating the mobile's software (Pearson Correl.: 0.315, Sig.:0.000).

Conclusions

The aim of my research was to investigate the security attitude of students of the Óbuda University for their smartphones as they are working or will be working for organisations in the near future. Since, their attitude is, or will affect the safety of the organisation where they work or will work.

My findings are that, only a fraction of them is using security tools on their mobile devices and thinking about the IT or data security of their devices. In general, their attitude towards mobile security is poor. Not even those, who have already experienced the loss of a mobile device with its total content, or those using internet banking are adequately prepared and/or consciously addressing threats and risks of their mobiles.

References

[1] Smartphones Reach Majority in all EU5 Countries http://www.comscoredatamine.com/2013/03/smartphones-reach-majority-in-all-eu5-countries/ 2014.04.30.

[2] Thinkinsights with Google http://think.withgoogle.com/ 2014.04.30.

[3] Már okostelefon-felhasználó a magyar lakosság több mint ¼-e http://www.enet.hu/hirek/mar-okostelefon-felhasznalo-a-magyar-lakossag-tobb-mint-%C2%BC-e/?lang=hu 2014.04.30.

[4] Kütyükörkép 2013Q1: Lassan már több az okos, mint a nem okos http://nrc.hu/hirek/2013/05/15/Kutyukorkep_2013Q1 2014.04.30.

[5] Gareth James ‚Malicious threats to Smartphones in Network Security Volume 2004, Issue 8, August 2004, Pages 5–7

[6] Iphone Os : Security Vulnerabilities http://www.cvedetails.com/vulnerability-list/vendor_id-49/product_id-15556/Apple-Iphone-Os.html 2014.04.30.

[7] Android Vulnerability Statistics http://www.cvedetails.com/product/19997/Google-Android.html?vendor_id=1224 2014.04.30.

[8] F-Secure: Android accounted for 97% of all mobile malware in 2013, but only 0.1% of those were on Google Play http://thenextweb.com/google/2014/03/04/f-secure-android-accounted-97-mobile-malware-2013-0-1-google-play/ 2014.04.30.

[9] European Union Agency for Network and Information Security Top Ten Smartphone Risks - https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/top-ten-risks 2014.04.30

[10] K. Parsonsa et al. Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q) in Computers & Security Volume 42, May 2014, Pages 165–176

[11] Safari, Chrome and Samsung Galaxy S4 taken down in Mobile Pwn2Own http://www.net-security.org/secworld.php?id=15952 2014.04.30