Imperial Journal of Interdisciplinary Research (IJIR)
Vol-2, Issue-11, 2016
ISSN: 2454-1362, http://www.onlinejournal.in

Risks Management of IT Smart Software and Hardware Controlling Daily Activities

Adriana Grigorescu[1], Razvan Ion Chitescu[2] &
Aurelia Aurora Diaconeasa[3]
[1]Ph.D. Professor, National University of Political Studies and Public Administration, Bucharest, Romania; Associate member of Academy of Romanian Scientists, Splaiul Independentei 54, 050094, Bucharest, Romania
[2]Ph.D. Associate Teacher, National University of Political Studies and Public Administration, Bucharest, Romania
[3]Ph.D. Student, Valahia University from Târgovi □te, Târgovi□te, Roma

Abstract: *The explosion of smart devices along with the numerous applications which connect us and make our life easier/embellish our life haven't passed unnoticed by the malware creators. In the context of smart devices' growing popularity while containing various important information and having low Security levels and many users, data theft for creating growing data bases seems to become a real "opportunity" for hackers.*
Our study aims to analyse the Security culture of smart devices users on a quota sample and to provide an idea about the dimension of risk associated with the personal smart devices' lack of security, ways of managing their risk when used daily, along with improvement proposals for this state of affairs.

1. Introduction

When talking about Smartphone, we can say that the mobility of a tiny-computer that uses a large number of applications without having an appropriate security, promotes cybercrime. Over the last ten years, the threat landscape of this field suffered major changes and, in the present, the cybercrime is speculating and identifying new vulnerabilities. Meanwhile, the Internet has connected people, objects, systems and processes, almost everything we can imagine. Cisco and General Electric estimates that these connections will sustain a market of over 10.000$ billions and International Data Corporation claims that by 2020, more that 40% of the transited data worldwide will be made on unsecured services via smart devices. The reports of different main actors of Romania's IT market , for example, Romanian National Computer Security Incident Response Team CERT_RO's which announces the appearance of a Trojan virus that targets Romania's' 12 banking institutions and another one used for mobile operating system.

The same institution has reported a number of 68 million of cyber alerts alone in 2015 which involved 2.3 million of IP addresses (approximately 24% of the entire Romanian cyberspace). Nearly 78% refers to vulnerable systems and 17.000 of .ro domains have been compromised.

A common way of attacking smart devices users is by creating the so-called "social bots" that can perfectly imitate the behaviour of social network users or of smart devices applications users but , in the same time , secretly promoting products or ideas in order to obtain private information . For example, in 2015, Facebook has reported the identification of over 170 million of fake accounts, most of them being social bots.

The big companies have made huge investments in securing the online world and in the Security infrastructure, not only in fields like e-Commerce or banking, but also in retailing. Due to the technological development, the virtual communication will escalate and the security breaches could mean huge losses both personally and on a larger scale (regionally, globally).

2. Literature review

Global leaders in security solutions constantly warn the smart devices users about the dangers they are exposing themselves to when using the devices without a proper protection from those who want to harm them. The smart devices are ubiquitous, multi-tasking devices which face both types of threats – those typical of devices and those regarding security [25]. A Smartphone is considered to be an

information system on a smaller scale which covers different assets [13] but which is, due to its portability and capacity to store huge volumes of data, one of the most hunted devices by hackers.

An analysis reported by the Bitdefender specialists in cyber security underlined how easily wrongdoers can steal personal information or even compromise one's physical safety through smart devices found at home.

Although specialists in cyber security frequently deliver this kind of data, certain smart software creators can't make their applications secure enough. The Kaspersky Lab specialists share the same concern, drawing attention to the vulnerability of the smart household appliances.

There is an increasing resistance to adopting smart solutions for delicate services, such as banking [24]. Considering the fact that risks cover a wide range of data – from private ones, to business and governmental ones--, a very important key concept is prevention, which implies that the user participates in the initial process of risk assessment, going from the punctual risk calculating to the global risk calculating [25]. This evaluation must be based on real, active information and there must be used a number of convincing criteria— disclosing personal information, damaging reputation and the public image, breaking the law or a contract, affecting economical and financial interests, affecting the affairs policy, home policy and even the internal policy [16].

3. Study objective and Research methodology

Are we, as individual but also as informational community, prepared to face these challenges? Do we have the necessary culture to identify them or even eliminate them? Do we know the risks that are out there? Do we continue the technological boom or not? Do we follow the great companies' example to protect ourselves from the cyber-attacks? Do we get any help? Here are some questions that our study is planning to answer in order to meet its main goal: establishing the extent of people's trust in the online environment, what needs to be developed and where is recommended to invest.

Hypothesis 1: The smart devices are highly used in accessing personal or financial information

Hypothesis 2: The smart devices and the soft they use represent vulnerabilities for a network, with a wide range of danger to which they expose themselves. The users are aware of these risks.

Hypothesis 3: The users are informed about the dangers they expose themselves to by using these devices and there is an educational culture for personal data security.

Question Matrix:

For hypothesis 1:

1. Do you own a smart device through which you access applications for the financial - banking field, online shopping or E-mail?
2. Does your smart device contain important personal data?
3. Do you own applications which you share with other smart devices users?

For hypothesis 2:

1. Are you aware of the risks associated to using smart devices and certain other applications?
2. Are you aware of the dangers you expose the other users that share the network with you?
3. Is there a data back-up in case your device is compromised? Is there a way to fix that problem without further using smart devices or applications?
4. Which are the ways your device can be compromised?

For hypothesis 3:

1. When purchasing a smart device, have you been told how to use it and how to secure your data/information/applications?
2. Do you use authorised tools for securing your devices and data – antivirus software or advanced ways to secure your device (finger print)?
3. Can you access information on how to protect your device and your applications? Do you have to search for this information or are they given to you in a free and mandatory way?

The interview matrix has been sent via email to 600 people from the online world. The email addresses have been found through specialised search engines. The feedback was extremely low, mainly because there is a large number of unverified email addresses that send lots of unwanted emails containing questions and proposals on random subjects (mostly commercials), for this reason, people tend to be sceptical when it comes to this kind of messages.

The lack of feedback made it impossible to finish the analysis; as a result, the initial investigation method has been changed for the focus-group one. The meetings took place during the summer at the seaside, with the intention of meeting and interviewing people who don't know each other, with different educational levels and with a mixed territorial distribution.

As a consequence, two groups have been made-one, where the median age was 23, having boys and girls aged from 18 to 27, and another one, where the median age was 39, having men and women as well.

The age division has been made in order to its role in influencing the usage of smart devices and their applications as well as acknowledging the inherent dangers they imply.

The youngers' group was made out of 21 respondents, while the other had 17 members. Their gender was 14 females - 36.85% and 24 males, 63.15%. 86% of them were university graduates or

still students, 11% high school graduates, and 3% were vocational schools graduates.

4. Research results

Question 1: All of the respondents owned various smart devices – most of them had only smartphones—and all of them used the devices for different applications. The difference between the two groups was the following: the youngers' group uses a larger number of applications like email and online shopping while hardly ever using applications related to the financial or the banking field. Unlike it, the second group uses as often both the email applications and the banking ones, controlling other devices—the lighting, various automations, etc. The number of downloaded and used applications is overwhelmingly bigger for the youngers' group, and the main criteria of selecting the devices is actually the number of applications that can be downloaded/used. Data traffic is also far bigger for the youngers's group, which can be explained by the number of applications they use. Even though they use a larger number of applications, the members of the first group also know more about each application: how to use them, applicability, interconnection, functions, and dangers.

Question 2: All the respondents said that their smart devices contain important or very important information. The members of the first group had far more personal information stored on their smart devices. The difference between the two groups comes from the way each looks at the data sharing and the social networking communication. The members of the first group share most of their personal data with their friends, they share their private lives on social networks and their way of communicating must contain as much personal information as possible. They don't see their private information as being very important and losing or contaminating them doesn't have a big impact on them. Sharing most of the data gives them the possibility of taking the information back. The members of the second group said that they don't keep much vulnerable personal information in their smart devices, only those that are necessary and that their data is very important to them. From the smartphone's address book to the banking data, everything is considered very important and losing them has a great impact on the respondents.

Question 3: All respondents share data with other smart devices users. The members of the first group share much more data with other users. The difference between the two groups is reflected by their far more aggressive behaviour in terms of demanding new data, connexions and applications used together with other people. The groups the younger members belong to are much larger but more compact in terms of sharing the same opinions, communication, hobbies, and age. The second group is more restrictive when it comes to sharing personal data, connecting with other unrecognised devices or having the same applications as other users.

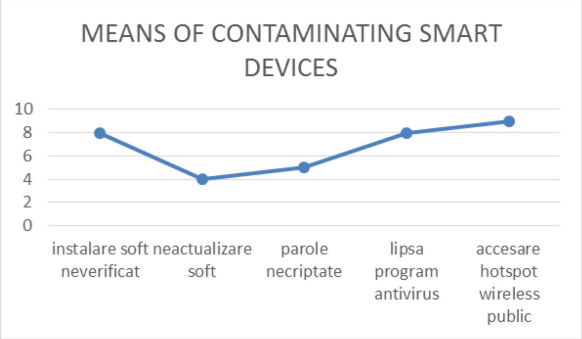
Question 4: The issue of risks was the most fiercely debated. Both groups reported that they know about the risks using smart devices imply, as well as about the antivirus and malware soft/applications. "According to Wikipedia, Malware is a type of software designed to harm a computer or to attach to it, or/and harm or attach to an entire computer network, without the owner's agreement. The notion is used by the IT specialists as a generalisation for any hostile, intrusive or harmful software or programme. The term 'virus' - when talking about computers - is sometimes used not only for computer virus, but also for any kind of malicious software." Their openness about this kind of discussion is very interesting. Although the respondents from the first group have a clearer idea about how malware application work and how to action against them, they have a more relaxed attitude towards this. The discussions led to an easier acceptance regarding the dangers of using smart devices. Many of them stated that this field-data security - is opposed to the idea of interconnection with other users and that the personal data theft is a risk taken when communicating online. The respondents from the other group are not as aware of the risks. They acknowledge the threat, the way a big loss of information could affect them, but they don't know how to better protect themselves from this. According to the way they responded to *question 5,* they are not aware of the losses they can cause by loosing/compromising personal/important data in the network they belong to. They believe that the losses are punctual, personally insignificant and that they can't echo in an entire user's community. On the other hand, they are the ones who identified greater risks, like those which can affect economically, socially or in fields like air transport or firms' databases. The respondents of the first group confine the influence of a smart device attack to the personal data shared within the network they belong to, that is, sentimental, image or financial, etc. losses only.

Question 6: The respondents of the first group don't see the data backup as a priority. Unlike them, the respondents of the second group believe it is of utmost importance and that it takes part of the Security actions they carry out. They create for themselves mini databases in order to diminish the risks of loosing/contaminating their own data. However, when asked, most of them were not aware that the data they stored on a hard drive can be contaminated by connecting with another infected smart device.

Question 7: The respondents from the two groups are partially aware of the ways a smart device can be

contaminated. The following means have been found:

- Installing an unverified soft
- Unchanged soft of the operating system or those adjacent to it
- Using the same passwords for different applications or unencrypted
- Not having an antivirus—the main cause of this is the price and the second is that it slows the device down by running in the background.



Question 8: most of the respondents reported that they were not informed about the data security when they bought a smart device. Some of them reported that they bought the devices online or that they couldn't test them. Most of the information about this kind of interventions was found out through other users or the Internet, after they have suffered different losses or when they didn't know how to use certain applications. Most of them reported that the information about Security can be found online, for free, even though they had never searched for it before buying a smart device, or even a long period after buying it. The interesting part is that, although they knew about that information, the users couldn't verify their efficiency because most of the malware applications are "invisible".

Question 9: From a total of 38 respondents, only 2 were using professional data security solutions for smart devices, the others being divided into two groups: the first one, in which people say they are not affected by the lack of security and the second one, in which the respondents are content with the free applications that promise security increase, even though these are not authorized by experienced or well-known producers. The respondents could have been reluctant in answering this question due to the illicit possession of false licenses.

Question 10: Along with the answers to the previous questions, an incomplete one was given for this question. We tried to make them all aware of the great danger smart devices users expose themselves to and to propose ways in which their security could improve. They suggested that the Security culture of all users should be improved, as well as the smart devices producers and the applications developers' obligations to make known the main risks they expose themselves to when using them, along with ways to protect from them. Most of the respondents don't know which is the most effective antivirus for an application, how to buy it or the risks that are covered. It is commonly believed that certain operating systems are more vulnerable than others, although this aspect is not very important when buying a smart device.

5. Conclusions

Belonging to an informational community has both advantages and drawbacks, which are related to using smart devices on a large scale. Beyond the psychological implications of this type of communication, there are also the risks you expose yourself to as a user, or the risks you expose the entire group or community you are associated with.

The respondents have pinpointed several immediate risks of cyber-attacks - targeting bank accounts, personal data stored on mobile devices such as address, contacts, photographs, schedule, private conversations between life partners, business conversations or those related to minors. Risks related to the core competencies or to the working place of a user, as well as to its influence on others - politically, socially, judicially or that related to commercial or state espionage have been identified. This allowed them to realise the extent of a disaster which could affect the national security, only by contaminating a link in the chain of users of the same applications. The data security education shouldn't be optional but free and mandatory by simulating the tragedy their loss would create. Connecting to other people is not an obligation, but something spontaneous that comes from our ability to understand each other and to bond, creating groups which share the same destiny and goals.

Our study's assumptions have been partially confirmed: we have a big network of smart gadgets users, we use a great variety of applications for an increasing number of fields, and even though we know that these devices, their software and applications are not safe, we don't own a developed security culture.

We don't realize how dangerous data loss, using bad applications or a Trojan horse can be. What's more, even the companies that sell these devices or applications don't seem to be interested in their security. There are very few applications on the market that cannot be used without knowing their risks, as well as very expensive technologies that provide physical protection for devices - digital scanner, etc. Most of the applications don't have an initial cost-be it low or high. This allows the possibility of creating an extensive network in which users work with the same free application, thereby the possibility of a cyber-attack on the network and the associated risks grow exponentially.

Our study wants to be a red flag for those that can enforce certain obligations, too. We believe that a data security culture-regardless of the cost- must exist via schools, mass-media, study programs, trainings for employees of the private domain, etc. Although they are aware of the risks and dangers they expose themselves to, Romanians still have a high degree of confidence in their smart devices. A necessary measure could be the addition of the suitable antivirus to the price of an application, as well as physical securing the devices through efficient methods. Another measure could be the applications producers'/developers' obligation to reveal the associated risks and the way they can be prevented. This thing can be simply done when buying/downloading an application and before running it on the smart device by mandatory report/information. Another way of preventing this is by working together with institutions that can develop efficient measures in the cyber field. A first step has been already made by The Politehnica University of Bucharest - together with military and other specialised institutes - by realizing how important it would be to create a cyber security centre for civil society.

6. References

[1] Barbovschi, M.: Dealing with misuse of personal information online – Coping measures of children in the EU Kids Online III project. Communications: The European Journal of Communication Research, (2014).

[2] Becher, M., Freiling, F., Hoffmann, J., Holz, T., Uellenbeck, S., Wolf, C.: Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices. In: Proc. of the 2011 IEEE Symposium on Security and Privacy (SP 2011), pp. 96–111. IEEE Computer Society, USA (2011)

[3] Bertel, T. & Stald, G. (2013). From SMS to SNS: the use of the internet on the mobile phone among young Danes. In K. Cumiskey & L. Hjorth (eds) Mobile media practices, presence and politics. The challenge of being seamlessly mobile. New York: Routledge.

[4] Caldwell, T.: Smart security. Network Security 2011(4), 5–9 (2011)

[5] Dietz, M., Shekhar, S., Pisetsky, Y., Shu, A., Wallach, D.: Quire: lightweight provenance for smart phone operating systems. In: 20th USENIX Security Symposium, USA (2011)

[6] Dlamini, M., Eloff, J., Eloff, M.: Information security: The moving target. Computers & Security 28(3-4), 189–198 (2009)

[7] Enck, W., Octeau, D., McDaniel, P., Chaudhuri, S.: A study of android application security. In: Proc. of the 20th USENIX Conference on Security (SEC 2011), USA, p. 21 (2011)

[8] Faqih, Khaled M S., 2013, Exploring the Influence of Perceived Risk and Internet Self-efficacy on Consumer Online Shopping Intentions: Perspective of Technology Acceptance Model, International Management Review 9.1 (2013): 67-77,88.

[9] Gartner: Market Share: Mobile Communication Devices by Region and Country, 3Q11. Technical Report (2011)

[10] Grace, M., Zhou, Y., Wang, Z., Jiang, X.: Systematic Detection of Capability Leaks in Stock Android Smartphones. In: Proc. of the 19th Network and Distributed System Security Symposium, NDSS 2012 (2012)

[11] Hogben, G., Dekker, M.: Smartphones: Information security risks, opportunities and recommendations for users. Technical Report, ENISA (2010)

[12] Jansen, W., Scarfone, K.: Guidelines on Cell Phone and PDA Security. Recommendations of the National Institute of Standards and Technology, Special Publication 800-124 (2008) 456 M. Theoharidou, A. Mylonas, and D. Gritzalis

[13] Jeon, W., Kim, J., Lee, Y., Won, D.: A Practical Analysis of Smartphone Security. In: Smith, M.J., Salvendy, G. (eds.) HCII 2011, Part I. LNCS, vol. 6771, pp. 311–320. Springer, Heidelberg (2011)

[14] Kardefelt-Winther, D. (2014). A conceptual and methodological critique of internet addiction research: Towards a model of compensatory internet use. Computers in Human Behavior.

[15] Kaspersky Labs: IT Threat Evolution: Q3 (2011), http://www.securelist.com/ en/analysis/204792201/IT_Threat_Evolution_Q3_20 11

[16] Ledermüller, T., Clarke, N.L.: Risk Assessment for Mobile Devices. In: Furnell, S., Lambrinoudakis, C., Pernul, G. (eds.) TrustBus 2011. LNCS, vol. 6863, pp. 210–221. Springer, Heidelberg (2011)

[17] Mylonas, A.: Smartphone spying tools. MSc Thesis, Royal Holloway, University of London (2008)

[18] Mylonas, A., Dritsas, S., Tsoumas, B., Gritzalis, D.: Smartphone Security Evaluation: The Malware Attack Case. In: Samarati, P., Lopez, J. (eds.) International Conference on Security and Cryptography (SECRYPT 2011), pp. 25–36. SciTePress (2011)

[19] Nachenberg, C.: A Window Into Mobile Device Security. Technical Report, Symantec Security Response (2011)

[20] Oppliger, R.: Security and Privacy in an Online World. Computer 44(9), 21–22 (2011)

[21] Redman, P.: John Girard, L.: Magic quadrant for mobile device management software. Technical Report G00211101, Gartner (2011)

[22] Reisig M. D., Pratt T.C., Holtfreter K., 2009, Perceived Risk of Internet Theft Victimization: Examining the Effects of Social Vulnerability and Financial Impulsivity, Criminal Justice and Behavior April 2009 36:369-384

[23] Shabtai, A., Fledel, Y., Kanonov, U., Elovici, Y., Dolev, S., Glezer, C.: Google Android: A Comprehensive Security Assessment. IEEE Security and Privacy 8(2), 35–44 (2010)

[24] Tuire Kuisma, Tommi Laukkanen, Mika Hiltunen, Mapping the reasons for resistance to Internet banking: A means-end approach, 2007, *International Journal of Information Management*, Volume 27, Issue 2, Pages 75-85

[25] Theoharidou M., Mylonas A., Gritzalis D., A Risk Assessment Method for Smartphones, IFIP Advances in Information and Communication Technology, volume 376, pp 443-456

[26] ISO/IEC: Information technology – Security techniques - Information security risk management. ISO/IEC 27005:2008, 1st edn. (2008)

[27] OWASP: Top 10 Mobile Risks, http://www.owasp.org/index.php/WASP_ Mobile_Security_Project
https://ro.wikipedia.org/wiki/Software_r%C4%83u_inten%C8%9Bionat

www.avira.ro, Despre malware

http://www.microsoft.com/technet/security/alerts/info/malware.mspx

https://www.bitdefender.ro/news/

https://www.bitdefender.ro/site/view/e-threats_reports.html

http://www.kaspersky.com/news

http://www.kaspersky.com/about/news/virus

https://www.cert-ro.eu/stiri.php