Establishing Effective Information Security on Modern Mobile Devices

BLAŽ MARKELJ, IGOR BERNIK
Faculty of Criminal Justice and Security
University of Maribor
Kotnikova ulica 8
SLOVENIA
blaz.markelj@fvv.uni-mb.si, igor.bernik@fvv.uni-mb.si http://www.fvv.uni-mb.si/en/

Abstract: - Ensuring information security for mobile devices (smartphones, tab computers, etc.) is and will be a problem for individuals and organizations. The problem is protecting data on mobile devices and during transmission of data between a device and secure data storage. Technological and other trends show, that increasing numbers of mobile devices are in use, therefore, ensuring information security is becoming even more important. It's also very important to educate users about safe usage and to increase their awareness of security issues. Ideally, users should follow technological trends and be well equipped with knowledge otherwise mobile technology will significantly increase security risks. It's crucial that we start educating youth so that our next generations of employees will live in a culture of secure data and information.

Key-Words: - Information Security, Blended Threats, Mobile Devices, Awareness.

1 Introduction

The purpose of technologically improved mobile devices is to better facilitate access to data which is vital for fast and efficient decision-making. It's therefore crucial that access to data is constantly available and unhindered. The evolution of the Internet, mobile devices, cloud computing, and software, is to maintain a constantly available connection to corporate data, no matter where decision-makers are based and when they need to tap into relevant data. Results of a study conducted by comScore [1] showed that in November 2011 the Internet was used by 380 million Europeans. Experts at MicrostoftTag [2] estimate that by 2014 the number of mobile connections to the Internet will surpass the number of connections made by stationary personal computers; the current ratio is 50:50. The ability to be uninterruptedly connected to the Internet is what makes constant access to data possible, and mobile devices are the connective elements between users and data storages.

But constant access to data also has its downsides. Users of mobile devices can become easy targets of numerous threats, which can be realized by deploying malicious code, intercepting communications, mobile device thefts and others. Numerous global manufacturers and providers of security software report that there are more and more virus infections, cases of unauthorized GPS location tracking of mobile device users, misappropriations of personal and confidential data (certificates, passwords, etc.), and automatic incorporations of bits of malicious code. These are only a few examples of attacks which are now frequently being directed at mobile devices. These can also be labeled as cybercrime. Cyberspace provides numerous beneficial opportunities, but also dangers [3]; and users' awareness of cybercrime is mostly influenced by media [4].

Such attacks can be deterred only if users know certain procedures (and sometimes also the functions of hardware and software) and act accordingly to protect data from being alienated when attacks are detected. Corporations should educate their employees and inform them about security measures and the basics of protecting digital evidence, in case they experience threats or attacks, to increase the likelihood that perpetrators will be caught.

The information infrastructure within which data is stored should be designed to be compatible with the functions of mobile devices, but data should be sufficiently protected. In the past, the remote access was facilitated by an »open door« in the system's fire wall through which communication could flow. Sophisticated mobile devices now constantly maintain connections with the Internet, and so communication mostly flows in a general way, as intended for web communications (browsing). This means that a door in the firewall is constantly left open and unprotected, thus increasing the possibility of a violation to the system.

In addition to their own information systems, more organizations are now storing and processing their

ISBN: 978-1-61804-127-2

data in a cloud. Because cloud technology works on an automated virtual plane the distribution of a system's resources is an automatic function of the system. It's necessary to provide sufficient protection from threats and see that digital evidence is properly collected in the event of a security incidence, so that the perpetrator can be detected and prosecuted. Detection is often difficult because a perpetrator's location is remote, and usually unknown. Users should also be careful when choosing their cloud provider. Increasing numbers of corporations are using cloud computing. This also means that the risk of experiencing threats is growing. TechNavio published a report on the current spread of cloud computing and the estimated future growth of these services – between 2010 and 2014 a 42 % growth rate is expected [5].

1.1 Threats to Mobile Devices, to Data Accesses, and to Information

The weakest link in the whole process of storing and transferring data is the individual user, who is more or less educated about mobile devices, cloud computing, software, data transference, and the safe use of this technology. Increasing numbers of mobile devices were infected in the past few years. Both Lookout [6] and Juniper [7] regularly report more and more incidences of malware infections. The question is, why anyone would want to penetrate a corporate information system or cloud, since it's possible to get all data through mobile devices because these are so often used to access corporate systems via different networks. Because the number of mobile devices in use is steadily rising, threats are also proliferating. The IDC study [8] showed that, globally, sales of mobile smartphones are going up by 50 % per year. According to the CEE Telco Industry Report, carried out by GfKGroup [9] in 15 Central and Eastern European states, Slovenia is leading with the most smartphone users (27.8 % of Slovenians use smartphones). The second in line is Turkey (23.7 % use smartphones), followed by Lithuania (18.5 %). The more there are users of mobile technologies the greater is the exposedness of information systems to security risks. Threats are becoming more sophisticated and cybercrime is on the rise, because more mobile devices in use present more opportunities for perpetrators. As said, data which can be accessed by using mobile devices can be stored at different locations, that's why threats have to be categorized and each type tackled differently. Threats can act individually or in combinations [10], but always with the intent to alienate data. It is vital to identify: locations/points where threats could present themselves, the types of threats, and the possible misdeeds.

Corporate information systems and cloud computing can be especially vulnerable, even though indirectly, because of the use of mobile devices and (open) accesses to data, specifically when necessary security measures aren't used (e.g., authentication, encryption, tunnel protocols, secure Internet connections, etc.). Beckham [11] drew attention to five major information security risks connected to cloud computing, compounded by mobile device usage. First there is the transfer of data between a corporate information system, a mobile device and cloud. Especially risky is transferring data by using various different Internet providers and simultaneously not encrypting data or using authentication and secure Internet connections (http, etc.). The second problem is the software interface, and the way in which users are verified when they access data in a cloud. Next come dilemmas regarding how data is stored, how it is diffused and encrypted. Is data encrypted all the time, even while it's being transferred to a device and/or stored on a server? The need to maintain a constantly available access to data and therefore being dependant on Internet connections is quite a big security risk.

1.2 Security solutions - today

Mobile security threats come in many forms, and they are rapidly evolving. Many corporations now have mobility at the center of their IT strategy, and it will serve you well to put new emphasis on your mobile device security strategy [12]. Milligan [13] noted in his article that corporations and other organization can't monitor something that can't be identified. What the author had in mind, were threats endangering corporations, which come with the usage of the rapidly evolving mobile devices and information technology in general. Therefore, corporations should constantly upgrade their information security policies and assess the risk of having their system breached. Corporations minimize risk by implementing hardware, which checks for potential dangers at the level of Internet traffic [14], and special equipment, which prevents invasions into information systems [15]. Some companies that are developing security software are already providing advanced software solutions for mobile devices [16], and firewalls, which monitor Internet traffic on the mobile device and the information system [17]. Certain software enables corporations to define their own safety guidelines

ISBN: 978-1-61804-127-2

for the use of mobile devices [18]. Employees usually have passwords to wireless networks [19].
Corporations can protect their data by using encryption software, but this method of protection is only as strong as the encryption key itself. It is possible to encrypt only certain segments of data stored on a mobile device, or data transferred through the Internet, or an information system as a whole. The encryption should in no way hinder the functions of a mobile device. Gilaberte [20] wrote about various methods and algorithms, which can be used to encrypt certain data in certain ways. Corporations strive to achieve better information security, especially in regard to log-on procedures, and/or the transfer of crucial data and information. This can be accomplished by implementing safer »http« data transfer protocols, and by authentication with certificates, as well as by encrypting and decrypting data (SSL), and also by the use of virtual private networks (VPN). Good examples of how the above-mentioned technology is used are bank portals and portals used for managing email. Certificates are used to authenticate the identity of a user when he or she tries to access these portals. Corporations try to protect their data by using strong passwords and authentication by a smart-card. Smart-cards can function only, if supported by sophisticated »background« technology. Most organizations set up virtual private networks to enable direct communication between mobile devices and their corporate information system or systems. This technology functions on the principle of establishing a »channel« between the virtual private network software of the mobile device and the virtual private network server located within a corporation's information system. Verification between a mobile device and an information system is done by using certificates – entrance to the system is granted once the identity of the user is verified (username, password). Zheng Yan and Peng Zhang [21] noted that we should be aware of two crucial security weaknesses in the virtual private network technology. These are: (1) software for mobile devices and virtual private network clients are so diverse that it is impossible to guarantee that the technology will work flawlessly; (2) it is questionable, whether the software on a mobile device (including specific software used to establish a connection to a virtual private network) can be fully trusted.
As noted by Milligan [13] some security measures in use today are inadequate protection for mobile devices against blended threats.

2 Method

Understanding how smartphones are actually used is of crucial importance for technological development and the establishment of information security. It's undeniable that for students mobile devices have become an indispensable means of communication, so it's even more important that we find out with which elements of information security these users are familiar with, and use them, because this generation will soon be working in corporate environments and making use of different mobile devices. These issues were the basis for our online study conducted in December 2012. Our questionnaire was published on the web portal »1ka« (www.1ka.si) for 21 days. We alerted youth to our survey through e-mail, Facebook profiles, and in person. The questionnaire was designed so that we would discover how and why youth used their mobile devices; which devices and software solutions they preferred. The second part of the questionnaire was designed so that we could gauge users' knowledge and use of security measures, and awareness of threats that can endanger data security. The analysis of the compiled survey data was made with SSPS software tools.
Because some questionnaires weren't filled out completely, the sample population for some questions varies. Most of the respondents were aged between 21 and 25 years, in the next group were youth under 20 years of age. 61.5 % of the respondents were female, 63.2 % were male; all had secondary school level education. Table 2 shows what the respondents use their mobile devices for (in this case smartphones). More than a half of the respondents use smartphones for private purposes, while a quarter of them use them for private and work related purposes. Because of the chosen sample population, these finding were more or less expected (Table 1). It gives us concern that the percentage of users who used the same mobile device for private affairs and business purposes is relatively high.

Table 1: Characteristics of the sample population – users of the World Wide Web.

		N	%
Age (n=281)	Below 20 years	75	26.7
	21 to 25 years	133	47.3
	26 to 34 years	57	20.3
	35 to 44 years	2	4.6
	44 to 54 years	2	0.7
	Over 55 years	1	0.4
Gender (n=275)	Female	169	61.5
	Male	106	38.5
Education level (n=280)	Secondary school	177	63.2
	1st Bologna level	67	23.9
	2nd Bologna level	25	8.9
	3rd Bologna level	11	3.9

ISBN: 978-1-61804-127-2

Table 2: Smartphones are used for.

Sample (n=216)	N	%
Only for private needs	126	58.3
For private needs, occasionally also for business needs	56	25.9
For private and business needs	31	14.4
For business needs, occasionally also for private needs	1	0.5
Only for business needs	2	0.9

The question is if their habits are already such that they have difficulty drawing a line between private and business affairs. How will youth use mobile technologies in the near future? Is it possible to change the present trend and ensure better security of data and information? It's problematic when private and corporate data is indiscriminately mixed without ensuring sufficient security. The results derived from a study conducted by Ponemon (2011) also showed a high percentage (40 %) of people who used mobile smartphones for private and business needs. We can conclude, based on the finding of Ponemon's and our own survey, that, in the future, it will be increasingly difficult to delineate between the private and business usage of continuously improving mobile devices.

3 Research: Security Aspects of Mobile Device

Data compiled in the course of our study showed us how the student population uses mobile devices and how they connect to the cyberspace. The goal of our study was to determine how well young users are aware of certain cyber threats (which can result in theft of data) and various protective measures which they could use to avoid security incidences. In our study the most commonly known threats are theft (89.4 %) and viruses (83.1 %) followed by bluetooth hacking, tracking, payment frauds, infections through applications, data alienation, interception of communications, automatic data transfer, browser infection, spyware infection, drive-by-downloads, malware infection, phishing, and rootkit infection. These findings aren't surprising, because these threats have been around for some time. It’s quite a big concern that the youth aren’t better informed about sophisticated malware which is steadily increasing in numbers. While bigger organizations regularly publish results of their monthly analyses, which show a steady rise in the number of mobile devices infected by malware, the results of our study showed that users aren’t well aware of these threats.
Table 3 shows some possible solutions which can protect mobile devices from cyber threats. Most respondents use standard PIN-code protection for their SIM-cards and antivirus software, but they aren't aware of more sophisticated tools, such as data encryption and remote deletion of data from mobile device.

Table 3: Protective measures for mobile smartphones in use.

	I use	I'm familiar with, but I don't use	I'm not familiar with
PIN-code for SIM-card	89.6%	9.9%	0.5%
Antivirus protection	29.5%	49.3%	21.3%
Education	26.0%	41.2%	32.8%
PIN-code for applications	21.4%	56.8%	21.8%
Smartphone tracking	20.3%	50.2%	29.5%
Archiving contents	19.5%	44.4%	36.1%
Authentication	13.0%	43.3%	43.8%
Remote content deletion	6.8%	40.8%	52.4%
VPN connection	6.8%	40.8%	52.4%
Central control	6.3%	40.5%	53.2%
Data encryption	5.8%	54.4%	39.8%

They do know about some other protective measures, e.g., PIN-codes, but they don't use them. It is a fact that young users aren’t well aware of threats to information security and don’t know enough about protective measures, therefore it’s hard to prevent certain security incidences, misusages of mobile devices and data theft, even though some good technical solutions are available.
On one hand many corporations monthly publish the results of their surveys which all show steadily increasing numbers of smartphones infected with malware, on the other hand our study showed that the student population is ill informed and little aware of these threats. It's a fact that the youth of today will soon join the ranks of employees in corporations and other organizations where they will access and manipulate (corporate) data by using various mobile devices.

4 Discussion

Mobile devices come with some protective measures preinstalled, but users often ignore these. Security depends on how much individuals know about the technology they use, therefore it's crucial to spread awareness and implement organizational policies to regulate the use of mobile devices, software, and accesses to corporate data in the central information system and/or cloud. It's necessary to evaluate which data can be stored on mobile devices, in the information system and cloud, and of course, if it's safe to access data from remote locations. Figure 1 shows possible security measures that can be implemented on connections

ISBN: 978-1-61804-127-2

between mobile devices and central information systems and/or cloud – but knowledge and awareness are still crucially important. Figure 1 is based on theory and insights gained from our study. The conclusions drawn from the results of our study show a rising trend in the number of threats endangering users of mobile devices and all who access corporate data from remote locations. All mobile devices users should be informed which threats they could encounter, what the consequences could be, and be told how to avoid them.

There are available different methods of protection against cyber threats, but one has to use them. On the other hand, there are many ways to alienate data. The most common are: theft of mobile device, interception of data, and direct breach of an information system. Systems can also be breached by using decoding methods or by stealing passwords. But there are even more sophisticated ways which can »open a system's back door« or retrieve data by infecting the system with malware. E.g., infected mobile devices can automatically pass on confidential information to unauthorized strangers. This information can also contain certificates, passwords, and the location of the user.

Mark Fischetti [22] made a list of the most common methods of alienating data. At the top of his list are violations of corporate computers and server systems (16 %). We can immediately draw parallels with the results gained through studies carried out by Lookout [6] and Juniper [7], which indicate a significant increase of different infections; and our study from 2011 of how one in Slovenia use mobile devices, how well aware they are of the threats and possible protective measures. Obviously, all three studies show the increase of malware, which means increased possibilities that systems will get penetrated more frequently. The second most common method of data alienation is the direct »harvest« of data off the web. In this case also it's possible to compare the situation with an infection as perpetrators can access a user's data on the web only if they know his password to his profile or data storage in a cloud. It's interesting that in our study theft and viruses were at the bottom of the list of the data alienation methods most known by (young) users.

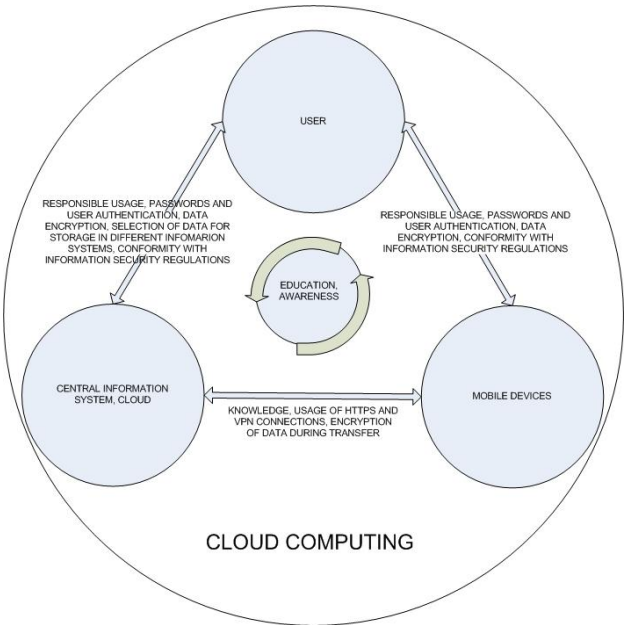

Fig. 1: Security measures implemented on connections between mobile devices and a central information system and cloud.

Studies don't show a decrease in the proliferation of cyber threats to mobile devices, and consequently, a decrease in the number of misusages and data thefts – quite the contrary. Manufacturers of information security products are well aware of this fact. Industry guidelines imply further evolution of security software, especially of software, which will be activated (by a password) whenever a user logs-on to an information system, and will be in compliance with a company's security policy. Trends in information security solutions point towards bettering users' awareness of cyber threats, promoting knowledge about new technologies, and informing people about available protective measures.

References:

[1] comScore, *In Europe, Apple iOS Eco system Twice the Size of Android When Accounting for Mobile Phones, Tablet sand Other Connected Media Device,*. http://www.comscore.com/Press_Events/Press_Releases/2012/1/Nearly_50_Percent_of_Internet_Users_in_Europe_Visit_Newspaper_Sites, downloaded: February 2nd 2012.

[2] MicrosoftTag, *Infographic: MobileStatistics, Stats&Facts 2011*, http://www.digitalbuzzblog.com/2011-mobile-statistics-stats-facts-marketing-infographic/, downloaded: February 2nd 2012.

[3] Bernik, I.; Prislan, K., *Kibernetska kriminaliteta, informacijsko bojevanje in kibernetski terorizem*, Faculty of Criminal Justice and Security, University of Maribor, Ljubljana, Slovenia, 2012.

[4] Bernik, I.; Meško, G. *Internetna študija poznavanja kibernetskih groženj*
in strahu pred kibernetsko kriminaliteto, Revija za kriminalistiko in kriminologijo, vol. 62, nr. 3, 242-252, 2011.

[5] Infiniti Research Limited, *Global Cloud System Management Software Market 2010-2014*, http://www.marketresearch.com/Infiniti-Research-Limited-v2680/Global-Cloud-Systems-Management-Software-6458283/view-stat, downloaded: September 7th 2011.

[6] Lookout, *Lookout mobile threat report*, https://www.mylookout.com/mobile-threat-report, downloaded: September 10th 2011.

[7] Juniper Networks, *Malicious Mobile Threats Report 2010/2011*, http://www.juniper.net/us/en/dm/interop/go, downloaded: September 10th 2011.

[8] IDC, *IDC – Press Release*, http://www.idc.com/getdoc.jsp?containerId=prUS22871611, downloaded: September 9th 2011.

[9] GfKGroup, *CEE Telco Industry Report 2011*, http://www.gfk.com/group/press_information/press_releases/008894/index.en.html, downloaded: June 6th 2011.

[10] Markelj, B.; Bernik, I., *Kombinirane grožnje informacijski varnosti pri rabi mobilnih naprav*. In Nove razmere in priložnosti v informatiki kot posledica družbenih sprememb, 18. konferenca Dnevi slovenske informatike, Portorož, Slovenija, 2011.

[11] Beckham, J., *The Top 5 Security Risks of Cloud Computing*, http://blogs.cisco.com/smallbusiness/the-top-5-security-risks-of-cloud-computing, downloaded: December 30th 2011.

[12] Mathias, C., *Mobile Security Threats*, http://searchmobilecomputing.techtarget.com/tip/Mobile-security-threats, downloaded: October 20th 2011.

[13] MayerMilligan, P., *Business Risk and Security Assessement for Mobile Device*. 8th WSEAS Int. Conf on Mathematics and Computers in Business and Economics: Conference Proceedings (pp 189-193). Stevens Point, Wisconsin: WSEAS, 2007.

[14] Whitman, M. E. in Mattord, H. J. , *Management of Information and Security, 2nd edition*, Course Technology Cengage Learning, Boston, 2008.

[15] Scarfone, K. in Mell, P., *Guide To Intrusion Detection and Prevention System*, http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf, downloaded: March 4th 2011.

[16] Schechtman, D., *IPad Security from En Pointe and McAfee's Mobile Security Practice*, http://www.enpointe.com/blog/ipad-security-en-pointe-and-mcafees-mobile-security-practice, downloaded: March 5th 2011.

[17] Endait, S., *Mobile Security – The Time is Now*, http://www.authorstream.com/Presentation/snehaendait-477029-mobile-security, downloaded: March 5th 2011.

[18] Mottishaw, P., *Policy Management Will Be Critical to Mobile Operators as Data Traffic Grows*. Acquired 6. 3. 2011 at http://www.analysysmason.com/About-Us/News/Newsletter/Policy-management-has-become-an-urgent-issue-for-mobile-operators-as-a-result-of-the-rapid-growth-in-mobile-data-traffic-increasing-availability-of-flat-rate-data-plans-and-new-regulations-in-Europe, downloaded: March 6th 2011.

[19] Arbaugh, W., *Wireless Security Is Different*, svn.assembla.com/svn/odinIDS/Egio/artigos/.../Firewall/01220591_IMP.pdf, downloaded: March 5th 2011.

[20] Lacuesta Gilaberte, R., *Encryption tools for devices with limite dresources*. 4th WSEAS Int. Conf. on AppliedInformaticsandCommunications: ConferenceProceedings (pp. 299-304). StevensPoint, Wisconsin: WSEAS, 2004.

[21] Yan, Z. andZhang, P., *Enhancing Trust in Mobile Enterprise Networking.* 5th WSEAS Int. Conf. On AppliedComputerScience: ConferenceProceedings (pp. 1057-1064).StevensPoint, Wisconsin: WSEAS, 2006.

[22] Fischetti, M., *Stolen data: How thieves get your identity and other information. Scientific American*, http://www.scientificamerican.com/article.cfm?id=data-breach-how-thieves-steal-your-identity-and-information, downloaded: December 30th 2011.