VARSTVOSLOVJE, Journal of Criminal Justice and Security year 13 no. 4 pp. 406-417

Unlimited Access to Information Systems with Mobile Devices: Information Security Perspective

Igor Bernik, Blaž Markelj

Purpose:

Mobile devices have become an indispensible part of modern communications; they enable easy access to the Internet and also remote manipulation of data stored in corporate information systems. The number of mobile device users is on the rise, but most of them don't comprehend completely the less obvious functions of these devices. Users also have almost no control over background computer programs, because they run without their knowledge and volition. From the standpoint of information security, a lack of awareness of the risks can seriously compromise the integrity of corporate networks and information systems. The weakest links are users, but also the technology itself. To ensure the functioning and security of information systems, corporations and individual users should learn about protective mechanisms. It is also important that users adhere to implemented (internal) safety regulations.

Design/Methods/Approach:

We used descriptive and comparative methods, and made an overview of published literature, as well as processes pertaining to the use of mobile devices and related security issues. We compared general elements of information security in regard to the use of mobile devices.

Findings:

At present mobile devices are more and more frequently used to access information systems. The majority of users are concerned almost exclusively with the question, how to get uninterrupted remote access to data, but far less with security issues. This paper presents some guidelines for achieving and maintaining information security.

Research limitations/implications:

It has been noted, that this is a time of turbulent development and evolution in the field of mobile devices, and also related security issues, so best practices haven't been defined yet. Corporations and other organizations have just recently begun defining guidelines to eliminate security breaches through mobile devices, therefore a comparison of their implemented solutions is practically impossible.

Practical implications:

We propose guidelines, which can be used to: minimize information security risks posed by mobile devices; evaluate the current state of information security; and implement protective measures against cyber threats encountered by corporations and individual users of mobile devices.

Originality/Value:

Information security is a relatively new field because mobile devices and remote access to the Internet and data have just recently come into wider use. At the same time security issues and protective measures have stayed largely overlooked. Security threats are many, so it is impervious that users learn more about them and adopt some necessary security measures.

UDC: 004.056

Keywords: information security, blended threats, mobile devices, corporate information systems, business integrity

Neomejen dostop do informacijskih sistemov z mobilnimi napravami: informacijsko-varnostna perspektiva

Namen prispevka:

Mobilne naprave so postale stalnica vsakodnevnega komuniciranja, dostopa do omrežij in oddaljenega dela s podatki v zaprtih korporativnih informacijskih sistemih. Število uporabnikov se skokovito povečuje, malo uporabnikov pa delovanje naprav razume, prav tako pa nimajo pregleda nad delovanjem elementov naprave za komunikacijo v ozadju, kjer ni potrebna direktna interakcija z uporabnikom. Nepoznavanje, s stališča informacijske varnosti oziroma varne uporabe mobilnih naprav, lahko resno ogrozi informacijski sistem celotne organizacije. Šibka člena pri zagotavljanju informacijske varnosti sta uporabnik in tehnologija. Za zagotavljanje stalnega dela in ustrezno stopnjo varnosti je pomembno poznavanje varnostnih mehanizmov s strani uporabnikov in spoštovanje predpisanih omejitev za varno delo.

Metode:

Uporabljeni sta bili deskriptivna in primerjalna metoda. Narejen je bil pregled literature in postopkov, ki navajajo rabo mobilnih naprav in njihovo zaščito. Primerjani so bili elementi splošne in varne rabe mobilnih naprav z vidika informacijske varnosti.

Ugotovitve:

Uporaba mobilnih naprav za oddaljen dostop do informacijskih sistemov je v začetni fazi. Večina organizacij in uporabnikov se ukvarja zgolj z zagotavljanjem dostopa in delom, pozabljajo pa na informacijsko-varnostni vidik. Prispevek predstavlja smernice za vzpostavitev večje stopnje informacijske varnosti.

Omejitve/uporabnost raziskave:

Zaradi turbolentnega razvoja in sprememb na omenjenem področju je razumevanje uporabe mobilnih naprav v začetni fazi in dostopnost do uspešnih praks (angl. best practices) omejena. Izdelava smernic varne rabe mobilnih naprav

in njihovo udejanjanje v praksi je v začetni fazi, zato ni možna primerjalna analiza uspešnosti predlaganih ukrepov.

Praktična uporabnost:

Predstavljene so smernice varne rabe mobilnih naprav, ocena trenutnega stanja informacijske varnosti in smernice za zaščito pred grožnjami, katerim so izpostavljeni organizacije in posamezniki ob uporabi mobilnih naprav.

Izvirnost/pomembnost prispevka:

Uporabniki so šele pred kratkim začeli množično uporabljati mobilne naprave za dostopanje do podatkov, zato so nova tudi informacijsko-varnostna vprašanja, vezana na mobilno tehnologijo. Širša raba oddaljenega dostopanja se šele uveljavlja, varnostni postopki in mehanizmi pa so zanemarjeni. Ker se kažejo možnosti zlorabe in uresničenja groženj, pa je pred udejanjanjem pomembno zagotoviti ustrezna znanja in postopke, da ne pride do tega.

UDK: 004.056

Ključne besede: informacijska varnost, kombinirane grožnje, mobilne naprave, poslovanje

1 INTRODUCTION

Mobile devices are a means of ensuring uninterrupted access to data and information, and are thus a basis for modern business practices. The fast pace of modern life, accelerated business processes and decision-making have all created the need for fast and reliable access to data and information. Due to the incredible development of technology and changing methods of communication, it is unimaginable that one wouldn't have constant access to data and information. Mobile devices, which have recently become ubiquitous, offer easy connections to the world of information. Recent development (wireless technology) has also changed how we access the Internet and pushed corporations into centralizing their information systems. Thus users now have uninterrupted access to corporate databases and information, which speeds up the working process and decision-making. The knowledge how to use mobile devices safely and efficiently can be a competitive advantage in business and science. On the other hand there is the issue of information security. When corporations minimize the possibility of unauthorized and malicious access to their information system, theft and misuse of their data, they strengthen their business credibility. Maintaining information safety is therefore a necessity (Saksida, 2008).

Almost all mobile devices provide a wireless connection to the Internet and thus access to corporate information systems, manipulation and transfer of data. Some corporations intentionally have open ports, so that their employees can work in virtual environments. Such a practice is an opportunity for anyone on the Internet who wishes to access a corporation's information system unauthorized. From the safety viewpoint, besides individual and blended threats, the following pose the biggest risk: software for mobile devices, public networks, unprotected certificates and the loss or theft of a mobile device. Certain programs automatically

cyclically transfer data from a corporate information system to the user's mobile telephone – this happens as soon as the user types in his username, password and server data. It is questionable, if software running automatically can be at all trusted. What is a program running in the background actually doing? What happens, if our telephone gets stolen? Our telephone contains much information, including data to access the domain and server system (Chickowski, 2009). This means that anyone who penetrates the mobile devices, while it is connected to the Internet, can eavesdrop on all communication between the device and the corporate information system.

When we started using wireless mobile communication devices, we dismantled the "border" between internal information systems and the outer world. Today the world is covered by a communications web: everyone can communicate with anyone else, upload and transfer data. Access to crucial data has become far too easy. Developers of security software are looking for ways to analyze and monitor contents in communication channels. It is apparent that future technology will make it possible to analyze Internet traffic and information systems, based on detected deviations from the routine. Regrettably, we still don't have simple, transparent solutions (from the user's point of view) to protect information systems from cyber criminals.

Corporations minimize risk by implementing hardware which checks for potential dangers at the level of Internet traffic (Whitman & Mattord, 2008), and special equipment which prevents invasions into information systems (Scarfone & Mell, 2007). Some companies that are developing safety software are already providing advanced safety software for mobile devices (Schechtman, 2011) and firewalls, which monitor Internet traffic on the mobile device and the information system (Endait, 2010). Certain software enables corporations to define their own safety guidelines for the use of mobile devices (Mottishaw, 2010). Employees usually have passwords to wireless networks (Arbaugh, 2003). Some corporations implemented their own rules for maintaining information security in the process of acquiring the ISO 27001 certificate (Calder, 2006; Bernik & Prislan, 2011).

2 METHODS

For the purpose of this article, we use descriptive methods and made a thorough overview of the literature, relevant research and procedures that deal with the use of mobile devices, software, wireless Internet connections and the necessity of safety measures. We also used comparison method where we draw special attention to the most recent results of research projects in this field, which have confirmed that both the number of mobile device users and cyber threats are on the rise.

3 RESEARCH OF MOBILE DEVICES AND INFORMATION SECURITY

How useful a mobile device is, depends on its software and its capability to connect to and conform to bigger systems. The development of software for mobile devices

has largely followed the general trend in the development of information technology. More attention was channeled towards simpler programs or applications, which simplify access to data and information. These applications represent a new method of communication or can just enable faster service. It is questionable how safe these applications are, since the user often doesn't know their source and isn't fully aware how downloaded programs work in the background. Programs, which seem harmless, can be a means to achieve unauthorized access and to carry out malicious acts. A good example is software (downloaded from the Internet for free), which enables money transactions, payments by mobile telephone or transfer of data. Such software can also contain malicious code and cause great damage, such as loss of data and money (Leavitt, 2011). We know of software designed to change background graphics on mobile devices, which also functions as a secret program for dispatching personal data (photos, messages, contacts, etc.), and is secretly stored on the device (Lookout, 2011). A mobile device can also be under threat by software fragments transferred to the device by malware, spyware, botnets or Bluetooth connections and social networks (Leavitt, 2011). Research carried out by Lookout (2011), shows that the number of malware applications based threats have risen considerably in the past six months, especially in comparison to spyware threats (by 14%). It is likely that 1 to 4% of mobile devices are infected in this way (Lookout, 2011). Providers of software for mobile devices usually install "back doors", programs that manage settings and other software on the device without the knowledge of the user. Such programs automatically send GPS data to locate the user and/or device, and can even take control of the device (Lookout, 2010). Flores (2011) noted that the results of research recently carried out in different parts of the globe clearly show that anyone collecting and analyzing data automatically acquired from mobile devices can make assumptions about a user's lifestyle (his health, political preference, consumer habits, etc.). Known are incidences, when data was secretly collected, with the help of the GPS module in mobile devices, and stored in larger information databases. Such software can also monitor the frequency and methods of communication, which again uncovers a user's habits. Kučić (2011) commented on the matter of deleting personal data – when a user stops using certain software, an Internet browser or his mobile device, he assumes that he will be able to delete all personal data, and that no one will retain and manipulate it.

To make use of certain programs (e.g. software for email synchronization), a user must type in certain data (log-on to the corporate domain). It is important to perceive all software on a mobile device as a whole. A perpetrator needs only to "embed" a fraction of the malicious software in the mobile device to be able to tap into it. All software for mobile devices should be checked to determine if it is trustworthy. Even pre-loaded software should be tested so that it functions as expected. It is prudent to shut off certain programs and functions of the mobile device (e.g. Bluetooth connections) when they are not in use, because this minimizes the possibility of malicious intrusions (Shilton, 2009). It would be sensible, if developers and producers of mobile devices and software for these set some safety standards and certified their products. In addition, each organization

should define internal standards and rules for the use of mobile devices based on general standards for these and the software developed for them.

3.1 Mobile Devices and Safety Issues

As said, the number of mobile device users is rising. The most ubiquitous are relatively simple devices, developed from mobile telephones and Pads, which can also be used for browsing the Internet, email, etc. The rise and advancement of mobile technology was rapid, but little was done to ensure safe access and transfer of data. If mobile devices are used within an organization with defined safety standards, it is quite possible to achieve a high level of information security – this can be done by applying methods, developed in the last fifty years, to the information system as a whole.

The possibility of a breach of the system and misappropriation of data is greater when a mobile device is used outside the secure information environment of an organization – when the user connects to a public network and through that, using simple protocols, to the information system. Mobile devices connect and transfer data in several ways. Users should be aware that every time a connection is established there appears a "tunnel" through the security "shield" of a corporate network, which is a risk to the whole information infrastructure of an organization. Data and information that is being transferred (i.e. email, documents, log-on data, client-server traffic, etc.) thus becomes relatively easily accessible to anyone interested in acquiring them, and, as protection is weak, perpetrators even don't need special knowledge to do so. Mobile device users are still the weakest link in information security, because they use open ports to enter information systems. It is vital that users know about safety standards. Employers should provide training and education for their employees, and define standards, rules and the consequences of not applying to them. It should be clearly stated which hardware, software and protocols for establishing connections to networks can be used (Allen, 2006; Whitman & Mattord, 2008).

3.2 Blended Threats

Mobile devices are targeted by blended threats, with the goal to unlawfully acquire restricted information and profit from this. Threats act on various levels and can work simultaneously, thus the name blended threats. Blended threats are a significant danger to individuals and organizations (Markelj & Bernik, 2011). When a connection with the Internet is established, (and through this with a corporate network) the organization is immediately in severe jeopardy. Threats are direct or indirect and can be combined. The most direct threat is theft of the mobile device. If the owner of the device stored crucial information and documents on the device, but hasn't used even the most basic protection (e.g. PIN code), then he is responsible for the consequences. More sophisticated threats are interceptions of communication and implanted software, which automatically harvests information.

Indirect threats are usually more severe, because they are unpredictable, and total protection from them is impossible.

Contemporary communications, access to corporate networks and methods of connecting to them have recently changed significantly. Fig. 1 shows the difference in communication between the central information system (Intranet) and the Internet.

It used to suffice that the information system was protected by a firewall, which monitored incoming communication. Until recently there were no external mobile devices that could connect to corporate networks and communicate with the world via WiFi, UMTS, etc. Users today use various mobile devices to establish connections and communication with different networks, regardless of firewalls. A firewall regulates communication between a mobile device and the information system it is protecting, but the weak link in the whole system is a mobile device that is connected to a public network. When a mobile device is invaded while it is connected to the Internet, an unprotected path to the central information system is opened. This happens because the firewall has already permitted communication between the device and system.

Threats that usually lurked on the communication pathway (which users learned how to master) are now, due to their variety and combined effects, a serious risk to corporate networks. Solutions are currently under development, but because there are no general standards, new safety measures will probably not be optimally effective, at least not in the long term. Constant changes and adaptations will be needed.

It is up to the individual user and organizations, how they ensure that they use safe connections to information systems and how they protect sensitive private or corporate data. Certain software solutions enable users, whose mobile device has been stolen, to remotely locate their device, lock it, erase crucial data and revert to the manufacturer's default setting (Phifer, 2009). In larger information systems, which permit their users to synchronize email on mobile devices, the above mentioned solution is already integrated into the system's software, but employees must be aware of this and know how to use it. In the past, the need for corporate information security was stressed, but now it is becoming evident that it is also vital to ensure safe usage of mobile devices (Boudriga, 2010). Any information system is as safe as its weakest link. Therefore it is important to focus on the least controllable elements, especially mobile devices. It is imperative to provide effective protection against blended threats (Metzler & Taylor, 2010).

A step towards better security is being aware of the various threats to information systems and their consequences (European Network and Information Security Agency [ENISA], 2010). One way for an organization to protect itself, is to put in place a solid policy for safeguarding its information system (Bernik & Prislan, 2010). A good safety policy encompasses standardized rules for the safest use of mobile devices. This is the basis for determining, which hardware and software are the most appropriate for the organization (Simt, 2009). Furthermore it is necessary to monitor network traffic, set up firewalls, encrypt data, and enable remote erasure of data from a stolen mobile device. Also authorization of access

to the system must be in compliance with standards and recommendations for ensuring the highest level of information security (Chickowski, 2009).

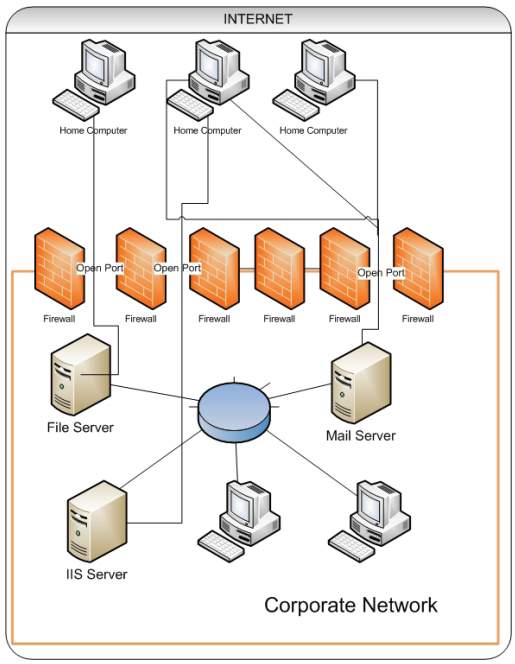

Figure 1: Communication between a corporate information system and the Internet via firewall, as in the past.

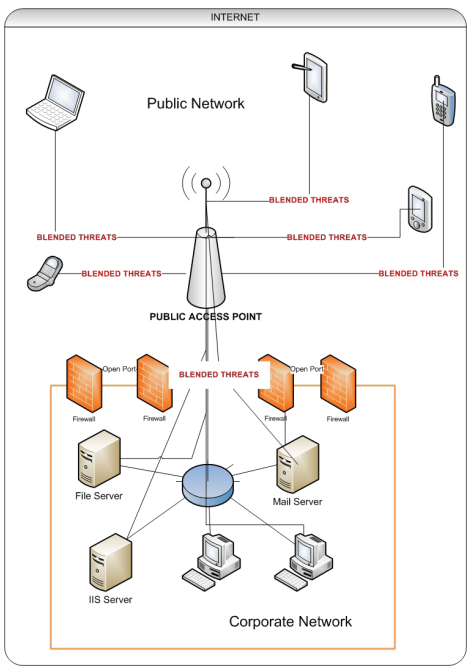

Figure 2: Communication between a corporate information system and mobile device, and communication between mobile device and the Internet, as currently possible.

Figures 1 and 2 are examples of the flow of communication. Not so long ago only computers communicated amongst themselves, and the Internet was a highway, "patrolled" by firewalls. In addition to this, we now use many different mobile devices, wireless connections and public networks. Currently, communication traffic commences without standardized security rules and is insufficiently monitored on almost all levels.

3.3 Security Regulations for Mobile Devices

Awareness of safety issues in regard to mobile devices can be a competitive advantage in business and/or science. Information security is the key to the integrity of any organization, its employees, business processes and compiled data. The lack of knowledge about the safety risks of mobile devices and internal safety standards can get an organization into serious trouble. An ignorant user is the first weak point in any information system; the second weak point, is the absence of standards for the use of hardware and software. Because of the rapid development of information technology, which is now used by the majority of employees, it is necessary to constantly inform and educate users of the pitfalls of modern technology. The goal of any organization should be to ensure that all information technology is used safely.

Mobile devices are safe, if they are used in compliance with safety regulations – these should be based on the following:

- Better information security can be achieved, if an organization defines its own safety standards and regulations.
- Safety regulations are a control factor, functioning as preventive measures in cases of irresponsible usage of mobile devices in the corporate environment.
- Safety regulations define how and why mobile devices and software can be used.
- Safety regulations also define legal responsibility of the user and/or the organization, if damages arise from irresponsible use of mobile devices.
- If an organization succeeds in getting their employees to comply with safety standards for the usage of mobile devices, then it has also successfully limited the risks of blended threats.

4 DISCUSSION

Technological development in information security is focused on analyzing Internet traffic and the behavior of information systems. Development is based on discovering discrepancies in the standard behavior of Internet traffic or the system. The human factor is still mainly overlooked. After all, people are the ones using and managing information technology, and thus represent the weakest link in information security. It is crucial for corporations to become aware that development of even more sophisticated mobile devices cannot be stopped. It is important for them to provide constant training and education for their employees,

and so lessen the risk to information security. It is necessary that corporations define internal regulations for the safest use of mobile devices and, based on their existing technology, determine, which mobile devices and software is most appropriate for them.

Mobile devices, and software for them, are being developed extremely fast; the process is unpredictable. It is crucial to maintain a flexible and safe information system. Current safety measures only partially cover mobile devices and their software. There is yet no system that enables corporations to monitor the performance of their information systems in regard to accessing and transferring data with the help of mobile devices.

Before employees are allowed to use mobile devices to connect to corporate information systems through public networks, they should be equipped with the appropriate software, which ensures that information security isn't compromised. Untested software for mobile devices should be prohibited. Employees should be taught how to use mobile devices safely. These measures can guarantee that only tried and approved (by the corporation) software for mobile devices is used, and that users comply with the implemented safety guidelines for mobile devices, software, Internet connections and accessing corporate data.

REFERENCES

Allen, M. (2006). Mobile security. *The Journal of International Security, 16*(6), 25-27.

Arbaugh, W. (2003). *Wireless security is different*. Retrieved March 5, 2011, from svn.assembla.com/svn/odinIDS/Egio/artigos/.../Firewall/01220591_IMP.pdf

Bernik, I., & Prislan, K. (2010). Proces upravljanja s tveganji v informacijski varnosti. In P. Umek, & T. Pavšič Mrevlje (Eds.), *Smernice sodobnega varstvoslovja: zbornik prispevkov*. Ljubljana: Fakulteta za varnostne vede. Retrieved March 1, 2011, from http://www.fvv.uni-mb.si/DV2010/zbornik/informacijska_varnost/Bernik_Prislan%20proces%20upravljanja.pdf

Bernik, I., & Prislan, K. (2011). Information security in risk management systems: Slovenian prespective. *Varstvoslovje, 13*(2), 208-222.

Boudriga, N. (2010). *Security of mobile communications.* New York: Auerbach Publications.

Calder, A. (2006). *Implementing information security based on ISO 27001/ISO 17799: A management guide.* Hogeweg: Van Haren Publishing.

Chickowski, E. (2009). *10 mobile security best practices*. Retrieved January 10, 2011, from http://www.baselinemag.com/c/a/Mobile-and-Wireless/10-Mobile-Security-Best-Practices

Endait, S. (2010). *Mobile security - the time is now*. Retrieved March 5, 2011, from http://www.authorstream.com/Presentation/snehaendait-477029-mobile-security

European Network and Information Security Agency. (2010). *The new users' guide: How to raise information security awareness.* Luxembourg: Publications Office of the European Union.

Flores, M. (2011). *What your cell phone data reveals about you and your life.* Retrieved September 7, 2011, from http://www.intomobile.com/2011/04/25/your-cell-phone-data-reveals-you-and-your-life

Metzler, J., & Taylor, S. (2010). *Security for mobile devices on the corporate network*. Retrieved January 15, 2011, from http://www.networkworld.com/newsletters/2010/032210wan1.html

Kučić, L. J. (2011, July 12). Uporabniki hočejo imeti pravico do elektronske svobode. *Delo.si*. Retrieved September 12, 2011, from http://www.delo.si/druzba/infoteh/uporabniki-hocejo-imeti-pravico-do-elektronske-pozabe.html

Leavitt, N. (2011). *Mobile security: Finally a serious problem?*. Largo: University of Maryland. Retrieved September 7, 2011, from http://www.computer.org/portal/web/computingnow

Lookout. (2010). Zlonamerna koda nad zasebnost uporabnikov mobilnikov Android. *Racunalniske-novice.com*. Retrieved September 7, 2011, from http://www.racunalniske-novice.com/novice/mobilna-telefonija/google/zlonamerna-koda-nad-zasebnost-uporabnikov-mobilnikov-android.html

Lookout. (2011). *Lookout mobile threat report*. Retrieved September 10, 2011, from https://www.mylookout.com/mobile-threat-report

Markelj, B., & Bernik, I. (2011). 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, 18.-20. april 2011*. Ljubljana: Slovensko društvo Informatika.

Mottishaw, P. (2010). *Policy management will be critical to mobile operators as data traffic grows*. Analysys Mason. Retrieved March 6, 2011, from 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

Phifer, L. (2009). *Find remote mobile device wipe solutions on a budget*. Retrieved September 7, 2011, from http://searchmidmarketsecurity.techtarget.com/tip/Find-remote-mobile-device-wipe-solutions-on-a-budget

Saksida, M. (2008). Preprečite uhajanje podatkov iz omrežja. *DNE*. Retrieved January 17, 2011, from http://dne.enaa.com/Racunalniska-oprema/Racunalniska-oprema/Preprecite-uhajanje-podatkov-iz-podjetij.html

Scarfone, K., & Mell, P. (2007). *Guide to intrusion detection and prevention system*. National Intitute of Standards and Technology. Retrieved March 4, 2011, from http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

Schechtman, D. (2011). *IPad security from En Pointe and McAfee's mobile security practice*. En Pointe Technologes. Retrieved March 5, 2011, from http://www.enpointe.com/blog/ipad-security-en-pointe-and-mcafees-mobile-security-practice

Shilton, K. (2009). Four billion litlle brothers?: Privacy, mobile phones, and ubiquitous data collection. *Communications of the ACM, 52*(11), 48-53.

Simt. (2009). *Upravljanje, nadzor in varnost informacijskih sistemov.* Retrieved October 11, 2011, from http://www.simt.si/informacijski_sistemi.html

Whitman, M. E., & Mattord, H. J. (2008). *Management of information and security* (2nd ed.). Boston: Course Technology Cengage Learning.

About the Authors:

Igor Bernik, PhD, is Assistant Professor of Information Sciences and the head of the Information Security Department at the Faculty of Criminal Justice and Security, University of Maribor, Slovenia. His research fields are information systems, information security, and the growing requirements for information security awareness.

Blaž Markelj is Assistant Lecturer of Information Science at the Faculty of Criminal Justice and Security, University of Maribor, Slovenia. His research interests include blended threats to mobile devices, and information security.