Accessing Information Systems with Mobile Devices and Information Security

Blaž Markelj, Igor Bernik

***Abstract*—**The most technologically advanced mobile devices are changing communications and the way we access data and information. The number of people who use mobile devices is rising exponentially, even in countries of the third world – at the same time, information security is decreasing (Best, Smyth, Etherton and Wornyo, 2010; Goodman and Harris, 2010). Mobile devices are under attack from various threats. These threats can act individually or in combinations (blended threats). The risk is greatest, when a user accesses corporate information systems via mobile devices and public networks. Users are becoming more aware of the importance of information security. Providers of security software have already perceived the need to implement control over the transfer of data from the Internet to mobile devices. Users are usually the weakest link in information security. Each corporation with its own information system should implement internal safety standards and regulate the use of mobile devices, software, protocols and public networks. It is crucial to constantly educate users about information security and measures to protect private and corporate data.

***Keywords*—Blended Threats, Information Security, Mobile Devices.**

I. Introduction

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 data bases 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 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 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 user name, 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 and Matorord, 2008), and special equipment which prevents invasions into information systems (Scarfone and 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, 2011). 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, 2010). Some corporations implemented their own rules for maintaining information security in the process of acquiring the ISO 27001 certificate (Calder, 2006; Bernik and Prislan, 2011).

II. Safe Usage of Mobile Devices

As said, the number of mobile device users is rising. The most ubiquitous are relatively simple devices, developed from mobile telephones, which can also be used for browsing the Internet, e-mail, 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 an intrusion into 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, and this is a risk to the whole information infrastructure of an organization. Data and information that is being transferred (i.e. e-mail, documents, log-on data, client-server traffic, etc.) thus becomes relatively easily accessible to anyone interested in acquiring them, and, as protection is weak, they 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 and Matorord, 2008).

III. Software for Mobile Devices

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. To make use of certain programs (i.e. synchronization of e-mail), 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 (i.e. blue-tooth connections) when they are not in use, because this minimizes opportunities 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.

IV. Safety Standards and Regulations for Safer Use of 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 to 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.

V. 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 and Bernik, 2011). When a connection with the Internet is established, (and through this with a corporate network) the organization is immediately in severe risk. Threats can be direct or indirect and can be combined. The most direct threat is theft of the mobile device. If the owner of the device saved crucial information and documents on the device, but hasn't used even the most basic protection (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.

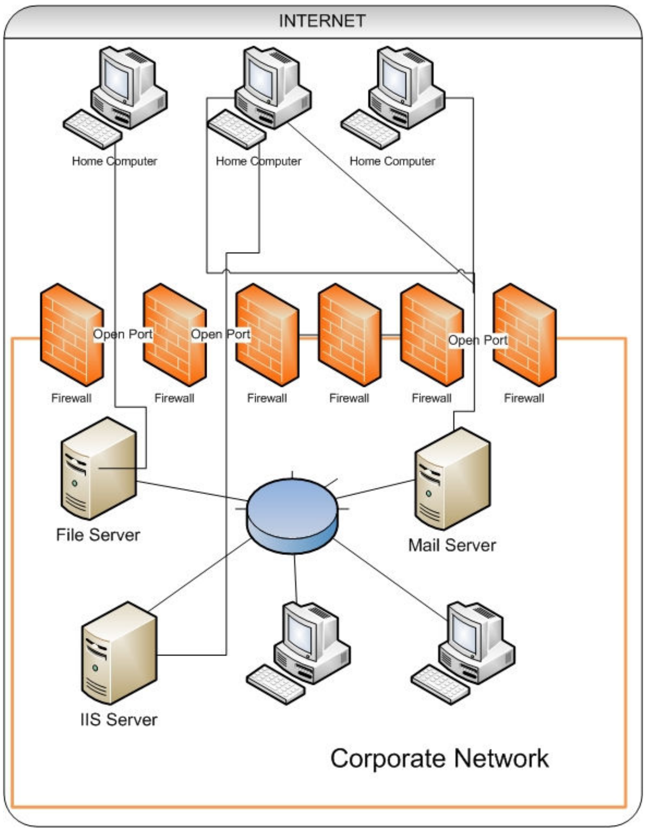

Fig. 1 Communication between a corporate information system and the Internet via firewall, as in the past.

Since the mobile device communicates with several networks simultaneously, and the firewall allowed access to the corporate information system, the user is in a position where his mobile device is open to blended threats (Fig. 2). The mobile device is a gateway to the "treasury" of the corporation – data and information stored in its information systems.

Threats that usually lurked on the communication pathway (which the user 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. In the past the need for information safety of an organization 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 from blended threats (International Data Group Company, 2011).

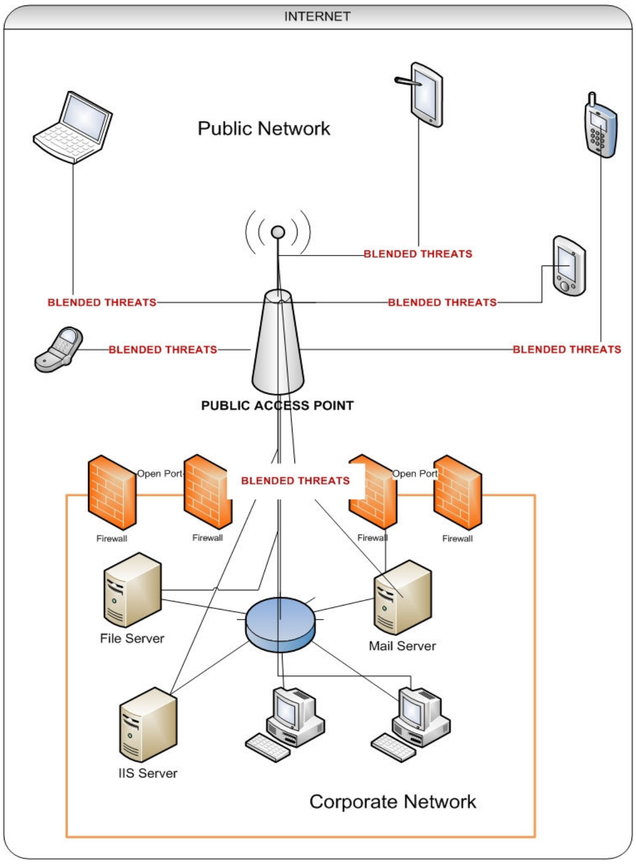

Fig. 2 Communication between a corporate information system and mobile device, and communication between mobile device and the Internet, as currently possible.

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 maintaining information safety (Bernik and 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).

VI. Conclusion

Technological development in information security is focused on analyzing Internet traffic and the behavior of information systems. Development is based on discovering discrepancies in 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 ever 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.

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

References

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

[2] Arbaugh, W. (2003). *Wireless Security Is Different*. Pridobljeno 5. 3. 2011 na svn.assembla.com/svn/odinIDS/Egio/artigos/.../Firewall/01220591_IMP.pdf.

[3] Best, M. L., Smyth, T. N., Etherton, J. in Wornyo, E. (2010). Users of Mobile Phones in Post-Conflict Liberia. *Informational Technologies & International Development, 6*(2), 91-108.

[4] Bernik, I. in Prislan, K. (2010). Proces upravljanja s tveganji v informacijski varnosti. V P. Umek in T. Pavšič Mravlje (ur.)*, Smernice sodobnega varstvoslovja [Elektronski vir]: zbornik prispevkov.* 11. slovenski dnevi varstvoslovja, Ljubljana, 3.-4. junij 2010. Ljubljana: Fakulteta za varnostne vede. Pridobljeno 1.3.2011 na http://www.fvv.uni-mb.si/DV2010/zbornik.html.

[5] Bernik, I. in Prislan, K. (2011). Information Security in Risk Management Systems: Slovenian Perspective. V B. Dobovšek in A. Sotlar (ur.), *Varstvoslovje, 13*(2), 208-222.

[6] Boudriga, N. (2010). *Security Of Mobile Communications*. New York: Auerbach Publications.

[7] Calder, A. (2006). Implementing Information Security Based on ISO 27001/ISO 17799: A Management Guide. Hogeweg: Van Haren Publishing B. V.

[8] Chickowski, E. (2009). *10 Mobile Security Best Practices*. Pridobljeno 10. 1. 2011 na http://www.baselinemag.com/c/a/Mobile-and-Wireless/10-Mobile-Security-Best-Practices.

[9] Endait, S. (2010). *Mobile Security – The Time is Now*. Pridobljeno 5. 3. 2011 na http://www.authorstream.com/Presentation/snehaendait-477029-mobile-security.

[10] European Network and Information Security Agency (ENISA). (2010). *The New User`s Guide: How to Rise Informations Security Awareness*. Luxembourg: Publications Office of the European Union.

[11] Goodman, S. in Harris, A. (2010). Emerging Markets - The Coming African Tsunami of Information Insecurity. *Communications of the ACM, 53*(12), 24-27.

[12] International Data Group Company. *Security for Mobile Devices on the Corporate Network*. Pridobljeno 15. 1. 2011 na http://www.networkworld.com/newsletters/2010/032210wan1.html.

[13] Markelj, B. in Bernik, I. (2011). Kombinirane grožnje informacijski varnosti pri rabi mobilnih naprav. *Nove razmere in priložnosti v informatiki kot posledica družbenih sprememb [Elektronski vir]: zbornik konference / 18. konferenca Dnevi slovenske informatike,* Portorož, Slovenija, 18.-20. april 2011.

[14] Mottishaw, P. (2010). *Policy Management Will Be Critical to Mobile Operators as Data Traffic Grows*. Pridobljeno 6. 3. 2011 na 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.

[15] Saksida, M. (2008). *Preprečite uhajanje podatkov iz omrežja*. Pridobljeno 17. 1. 2011. na http://dne.enaa.com/Racunalniska-oprema/Racunalniska-oprema/Preprecite-uhajanje-podatkov-iz-podjetij.html

[16] Scarfone, K. in Mell, P. (2007). *Guide To Intrusion Detection and Prevention System*. Pridobljeno 4. 3. 2011 na http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

[17] Schechtman, D. (2011). *IPad Security from En Pointe and McAfee's Mobile Security Practice*. Pridobljeno 5. 3. 2011 na http://www.enpointe.com/blog/ipad-security-en-pointe-and-mcafees-mobile-security-practice.

[18] Shilton, K. (2009). Four Billion Little Brothers? Privacy, Mobile Phones, and Ubiquitous Data Collection. *Communications of the ACM, 52*(11), 48-53.

[19] Simt (2009). *Upravljanje, nadzor in varnost informacijskih sistemov.* Pridobljeno 11. 10. 2011 na http://www.simt.si/informacijski_sistemi.html.

[20] Whitman, M. E. in Matorord, H. J. (2008). *Management of Information and Security, 2nd edition.* Boston: Course Technology Cengage Learning.