Skendžić, A. (2014). Security policy and wireless computer networks in educational institutions in the Republic of Croatia. *Anali poslovne ekonomije, br. 10,* str. 69−81.

UDK: 727:004.7(497.13); DOI: 10.7251/APE1410066S

Naučna kritika

SECURITY POLICY AND WIRELESS COMPUTER NETWORKS IN EDUCATIONAL INSTITUTIONS IN THE REPUBLIC OF CROATIA

Aleksandar Skendžić[11]
Veleučilište Nikola Tesla u Gospiću

Summary

Security policy defines planning and describes goals or security procedures. Security policy can also be defined as declaration of goals to be reached by implementation of certain procedures. The conditions under which security policy can be operational are not specific. Rather they are general. Implementation of security policy is not described as a part of the procedure and it is as a matter of fact a draft of secuity within a certain system. According to Peltier information security program shoud be a part of security program protecting the entire property of an organization. Security program is not created to meet security needs or requirement of revisions, but as a process providing the management with processes necessary for managing management's responsibility. The management is responsible for securing appropriate means to control protection of property owned by a company or institution in which security policy is implemented. This work describes security policy wifi networks situation in Croatian academic institutions (members of CARNet).

Key words: security policy, wifi, networks, education.
JEL classification: L, L4

Security policy

Security policy is not explicitly connected with business organizations, such as companies. It can also be defined in any type of organization and thus also in educational institutions. The goal of any security policy is to prescribe rules that govern management of all applicable aspects of information security systems. It defines users' rights and obligations, division of responsibility, maintenace plan, system documentation, etc. Furthemore security policy has to encompss risk management, control of incidents and procedures for damage control.

[11] 53000 Gospić, Hrvatska, Telefon: ++385(91)8823-413; E-mail: askendzic@velegs-nikolatesla.hr

Security policy in educational insitutions in the Republic of Croatia – Introduction

This chapter gives review of security policy in educational institutions of Croatia. There are some difference between security policies for schools and for academic institutions in way of security standards.

Secuity policy for schools

CARNet has developed a proposal referring to security policy for schools, under the heading *Acceptable use of computers in schools.* The idea underlying this document is to be exemplary experiment for schools to adopt security policies. The document contains a part relating to the use and security of wireless network in the institution: *… In order to facilitate maintenance it is necessary to document the appearance of network. The document can contain a graphic presentation of physical placement of computers in schools including basic properties (IP computer address) or listing of computers with information on places where the computers are placed and their IP adresses...*

It is evident from the Proposal that the security standard of wireless network opens with the documentation process of the appearance of wireless local network, in other words with the documenting process of network topology. It is also necessary to document data on network addresses of the computers, the protection walls, accessiblity points with information on the places where the computers stand.

…Wireless network (WiFi) should be adjusted in such a way that only legitimate users can access and use the network. Legitimate users can be teaching and administrative staff and students. None of the aforementioned users is allowed to hinder or make impossible operation of school wireless network. Adequate protection of wireless network requires introduction of WPA/WPA2 standard on wireless access points….

In addition, the Proposal emphasizes the need for adjustment of wireless network for use only by registered (authorized) users (students, teaching and administrative staff) and explicit ban on hinder and making impossible use of wireless network by the users. Additional security aspects of wireless network are very general and do not state an optimal protection model, recommending only use of WPA/WPA2 encryption/certification on wireless access points. On the basis of presented information one can conclude that an officially recommended model of optimal protection of wireless network is still lacking. Such a model, based on appropriate value parameters or on network topology, has not yet been proposed. Therefore it is necessary to suggest an opitimal solution.

… When accessing internet from school computers, this should be done exclusively by security protocols. Servers using secure protocols recommended for web access form school computers, are SSH v.2 service, web interface which enables user to access, and makes use of only HTTPS or VPN protocol….

In order to make (more) secure connection of users to school computers the use of secure protocols of the type Secure Shell - SSH[12], Hyper Text Transfer Protocol Secure – HTTPS[13] and VPN is recommended. Security policy includes implementing and monitoring changes in the properties of network equipment so as to enable network administrators to react faster and more efficiently to security incidents at any given moment. Draft form for recording properties change in wireless network euipment is presented in Table 1.

TABEL 1. DRAFT FORM FOR RECORDING CHANGES IN WIRELESS NETWORK EQUIPMENT IN INSTITUTION „X“

Access point Edimax EW-7228Apn	Factory properties (or after restore procedure)	User properties 1 Date of change : 07.4.2013.	User properties 2 Date of change:
Physical location of access point	Object A-East wing, corridor next to Dean's office	Objekt A –South wing, corridor next to administrative department	
IP address access point (LAN)	192.168.1.1	192.168.2.1	
Network Subnet	255.255.255.0	255.255.255.0	
Password for web access (configuration)	(none) or user: 1234	Te$205La	
Wifi network name (SSID)	VELENT_3	VELENT_5	
Network visibility (SSID Broadcast)	On/Visible	On/visible	
Type of encription (Security)	Disabled	Enabled/ WPA2+PSK	
(Pre-shared key)	none	1black2nokia3	
MAC filtering (On/Off)	Off	Off	

For efficient implementation of security policy and more efficient response to possible risks in wirelees network, it is of paramount importance to update daily or periodically changes in network or communication equipment.

[12] Secure Shell (SSH) is a cryptographic network protocol for secure transmission of data between two networked computers that are connected via a secure channel over an insecure network (usually the Internet).

[13] HTTPS - is a protocol that allows encrypted communication and secure identification of the web server network.

Security policy for academic institutions

The second CARNet document", bearing the title „Security policy of information systems for CARNet memebers[14]- A proposal" form December 2003 does not precisely state optimal solutions for wireless networks security. It rather dwells on general security policy of member institutions, users' rights and obligations and on responsiblity. Under the heading dealing with network managment, the document stresses the obligation to elaborate rules for accessing the network by guest computers. A patr of the document runs as follows:

…The institution is obliged to elaborate rules for accessing the network by guest computers, brought in by external colleagues, lecturers, bussines partners and service personnel. They should not be allowed to access the insitutions' network at will due to the danger of spreading viruses or committing deliberate aggressive acts such as intercepting network traffic or gathering of information, etc. The institution can designate access points, for example in lecture rooms where it is allowed to connect guest computers, and prevent by network configuration access from that network segment other computers in the institution ….

A part of the document refers to wireless network :

…If the institution uses wireless network, it should make sure that anybody cannot connent to a private network and record the traffic. This is done by the methods of encryption and authenication of equipment and users, to be fixed by a separate document. In order to protect confidential information in the network, it is desirable to encrypt such traffic. The institution will in such cases issue a book of rules which defines the sort of encryption, compulsory software, procedures for assigning and care of cryptographic key, and the like …

The document underlines the importance of institutions' security policies, the importance of network traffic encryption, but the details relating to implementation (the methods of encryption and authentication) and choice of security mechanisms are the task of the institution itself, i.e. IT department (service engineers).

The academic community is much more liberal than business organization (or the world of business in general) when it concerns definiton and implementation of security policy. Radojević (2011, pg. 196) argues that this is the case because the academic community belongs to open an culture oriented to communication, research and teaching inside academic circles. According to research results from 2011 cited by Radojević, only 20% of all school system institutions surveyed, have determined their security policies, while only 6% of the total also implement it. Radojević also reminds of the Law on information systems security (Zakon o informacijskoj

[14] Available at: http://www.cert.hr/sites/default/.../sigurnosna_politika_ustanove.pdf (06.4.2013)

sigurnosti, NN 79/07[15]) which obliges all public institutions to introduce security policy, either/or to define procedures of security accreditation. Bearring in mind that the present-day information systems both in companies and in educational institutions, are based on computer networks and the Intrnet, it is necessary to formulate security policy and to pass a system of recommendations and rule so as to make its efficient functioning possible. Otherwise is such a sysyem as a homogeneous totality unsustainable. Organized acitivity within information systems is necessary due to the importance of data carried by that very system, and also to the unreliability of the human factor. Both affect confidedentiality, acessibility and completeness of data.

Security accreditation in the Republic of Croatia

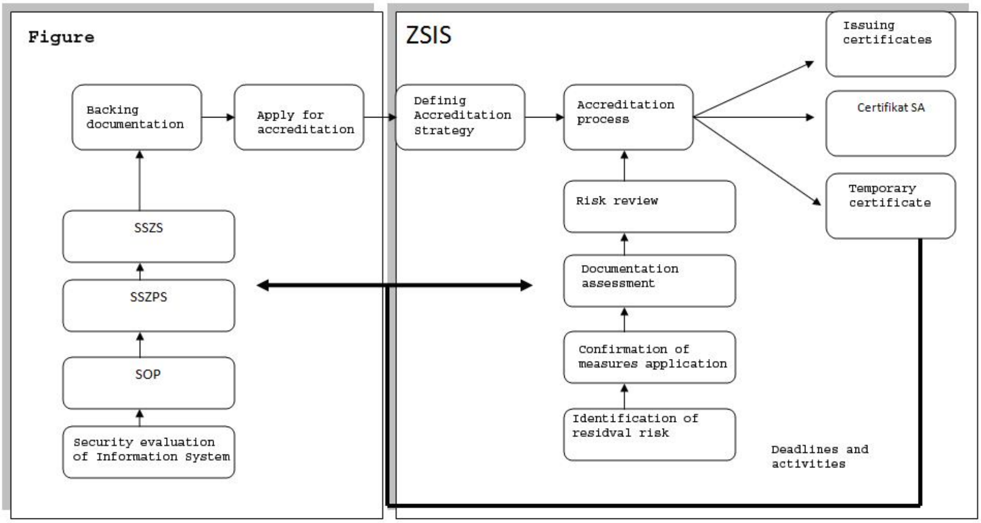
Security accreditation[16] is a procedure whose purpose is to warrant conformity of information system with laws and by-laws of the Republic of Croatia in the field of infomation security. This also includes managing bodies in the field of information security and refers to educational insitutions too. Security accreditation is carried out by checking implemented measures and information systems security standards and bringing them in accordance with laws and by-laws in the field of information and toese prescribed by the Croatian Institute for Normas. The purpose of the procedure is security, confidentiality, integrity and accessibility of classified information.

The accreditation procedure controls whether the desired level of protection has been reached and the manner in which it is maintained. Figure 1. presents the procedure of seccurity accreditation.

[15] Zakon o informacijskoj sigurnosti, Narodne novine, Zagreb, Hrvatska, http://narodne novine.nn.hr/clanci/sluzveni/298919.html (22.2.2013.)

[16] Source: http://www.zsis.hr/site/SigurnostISa/Sigurnosnaakreditacija/tabid/90/ Default.aspx

FIGURE 1. LAWS AND REGULATIONS RH - A PROCEDURE SECURITY ACCREDITATION.



Source: Zavod za sigurnost informacijskih sustava (zsis), ***www.zsis.hr***

Educational insitutions and security in the Republic of Croatia

Educational insitutions in Croatia react to damage in the sense of breach of security only after it had happened. Radojević (2011, pg. 196) draws attention to the fact that the security in educational institutions is marked by gross deviations: when disovered, it is a major problem, after solution to the problem, complete oblivion – until the next security incident.

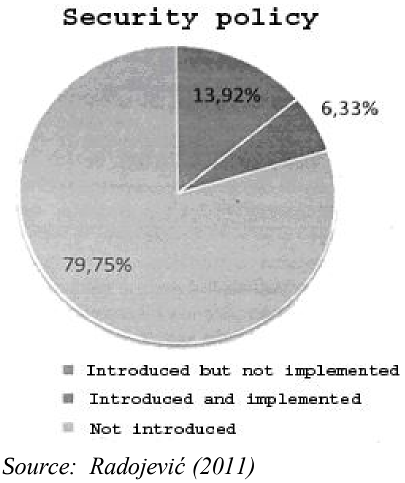
Furthermore, the academic community delegates system security to personal responsibility. Next to defining security policy, social factor is a very important one, i.e. personnel in need of training regarding the very importance of security of information systems. Besides, educational institutions, subjests of security measures, define and implement them in different ways. While such measures practically do not exist on elementary school level, subjects on academic level define and implement them as they please.

One of possible reasons for neglecting security policy as an important factor of information systems security in educational institutions is the assessment of importance of information needing protection. There is a deep-rooted opinion that educational institutions do not harbour information that require protection (Radojević 2011, pg. 197). Bearing in mind introduction of information systems in the school system on all levels, as well the already existing computer systems presently in use, the need is being felt for more quality in protection and security levels, involving existing and future systems. As an example one can cite present-day systems like

ISVU, Prehrana, IFIS, NISpVU and SmartX that exist primarily in academic institutions. We can add standard network services like Internet access, systems of distant learning, FTP, as well as various audio and video services, such as VOIP.

According to official report of member instututions of CARnet for 2009, only 45% of member institutions report prescribed security policy. The respondents were CARNet coordinators, i.e. persons representing institution's interests in the CARNet community. The results show that the CARNet coordinators are not professional computer or information specialists, but specialists in the profession that is essential for the institution that employs them. The survey executed among system engineers in November 2010 shows that only 20% of surveyed institutions have defined their security policy , and only 6% of the total surveyed respondents also implement it. Figure 2. shows the results of the survey of system engineers employed in academic institutions (61), research institutes (9), secondary schools (4) and other institutions (5). The Law on information security has suggested the need for security policy, but the surveys have shown that its implementation in all educational institutuons and institutes did not follow.

FIGURE 2. RESULTS OF CARNET SURVEY ON SECURITY POLICY IN EDUCATIONAL INSTITUTIONS



Source: Radojević (2011)

Radojević (2011, pg. 197) wonders why once adopted security policy is not applied in the practice and how institutions deal with security incidents? The results are presented in in Table 2.

TABLE 2. RESULTS OF GUESTIONNAIRE AMONG CARNET SYSTEM ENGINEERS IN NOVEMBER 2010. SAMPLE: 79 RESPONDENTS.

Question	Yes	No
Was there any security incident involving loss of classified data?	38	41
Is it possible to establish responsibility in case of security incidents?	14	65

Source: Radojević (2011)

Table 2 clearly shows that 48.1 % of respondents answered positively the question regarding occurrence of security incidents and, as a consequence, loss of important data in the institution where they are employed. Moreover, 82,2 % of respondents cannot without doubt ascertain the responsibility for the security incident. The results obtained can *per analogiam* be applied to security of local wireless networks in institutions. Bearing in mind exceptional „sensitivity“of wireless network communication and use of air as the transmitting medium of network communication equipment, security policy adds importance to the stated facts. The research further brings to light that system engineers at the surveyed institutions often occupy rather low positions on the hierarchy ladder in schools or academic institutions to be able to influence directly institutions' security policy. To be able to implement security policy system engineers should enjoy management's support. The reason for that is that an adequate system of protection requires financial resources, although these only are not a crucial factor in implementation of security rules. The question of justification for investment in security is also posed. The peculiar character of security policy is that means and effort in its conceptualization should be invested in advance in order to prevent risk and loss of classified data.

Personnls' professional expertise is one of key factors in implementation of securty policy. Earlier CARNet research shows that a consisderable number of member institutions do not have sufficient (or none at all) expert personnel. In accordance with business model, companies solve the signalled problem by hiring external firms (outsourcing) (Weidenbaum & Murray, 2004, pg. 23–37). This is not the case in academic institutions. The first reason for that is lack of financial means, while the second one could be availability of external firms in case of emergency. The consequence is that conceptualization and implementation of security policy in educational institutions is often delegated to system engineers in the institution. However, they need constant expert training in order to achieve higher levels of security.

In order to implement security policy conscientously Radojević (2011, pg. 199) stresses the need of urging responsible bodies to encourage institutions to activate security policy as soon as possible. In the first place Ministry of science, education and sport, Presidents and Senates of Croatian universities. That would be a good starting point for introducing and implementing security policy in educational institutions.

Information network systems and security

Information network systems are the main carriers of information transmitted by means of various communication channels like computer networks and Internet.There is in such environment a high risk of unauthorized access to information, of generating false and/or destruction of information. Therefore protection mechanisms, providing security of information network and computer systems. Security mechanisms can be classified as follows:

- protection of network systems form eternal influence
- protection of network systems by means of interface toward the user
- various internal protection mechanisma
- communication protection mechanisms

The protection of network systems from external influence refers to external influence like mechanical damage of communication equipment due to circumstances. The foreseen protection measures include mechanisms applied in protection of property in general, i.e. limited admittance to places where the communication equipment is placed, keeping backups in „safe" places, protection from unauthorized access by means of various control systems.

Protection of network systems by means of interface toward the user includes use of the system only by authorized persons and at the same time denial of access to those unauthorized. The right of access is determined by checking user's identity, i.e. authenticity of the user, performed at the first access to the system. In the distributive systems authentication is often double one in order to prove identity of both parties.

Internal protection mechanisms refer to allowing access to network system at the level for which the user is authorized. This is done by the process of authorization. In distributive systems information is transmitted by various (unsafe) communication channels, in particular by radio waves, since these can be eavesdropped (Čerić, Varga, Birolla 1998, pg. 345), without chance of being detected. In essence, wireless network protection mechanisms are based on transmitting radio waves have the task of protection sent and received messages. Therefore, the most efficient protection of messages is their encryption. There exsist several wireless network security mechanisms of the standard 802.11 that base their security on encryption of contents. They shall be dealt with below.

The forms of disturbing security

According to Budin (Čerić, Varga& Birolla, 1998, pg. 347) general forms of disturbing system security can be shown by a model in which the source of information is connected to its destination by means of a certain communication channel. The same model can direcly be applied to wireless network communication of the network 802.11, where the access point or router via a communication channel exchange messages with a client using radio waves. Considering that air is a free communication medium, the risk of unauthorized network incursion is at the same time increased. Possible forms of disturbing security are shown in Figures 3–7.

FIGURE 3. UNDISTURBED FLOW OF WIRELESS NETWORK DATA. UNDISTURBED FLOW OF WIRELESS NETWORK CONTENTS EXCHANGE BETWEEN SENDER AND RECEIVER COMMINICATON CHANNEL IS UNDISTURBED BY EXTERNAL SOURCE.

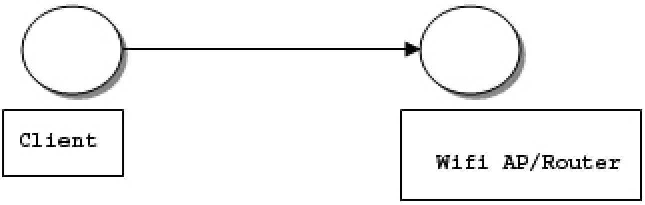


FIGURE 4. MODE OF EAVESDROPPING - „PASSIVE ATTACK“

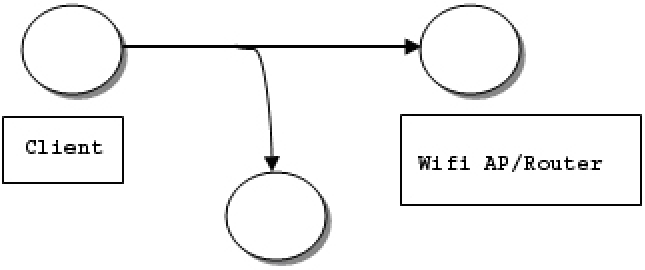


Figure 2 shows possibility of eavesdroppingin the wireless network communication channel. According to Budin (Čerić, Varga & Birolla 1998, pg. 347) this form of disturbin security is called *passive attack* because the intruderdoes not actively affect information. Passive attacks on wireless networks are used to intercept encrypted network packages that can later be used for *active attack* on wireless network. Active attacks require some sort of ctivity on attacker's part.

FIGURE 5. BREAKUP OF COMMUNICATION BETWEEN SOURCE AND DESTINATION

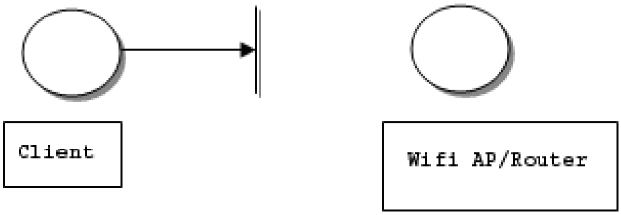
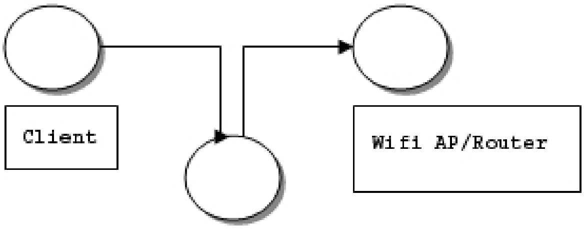


Figure 3. illustrates breakup in communication channel. Breakups are not divided into active and passive attacks on wireless network. They only refer to endangered availability of information, i.e. inaccessibility of wireless network service.

FIGURE 6. CHANGE OF CONTENTS IN WIRELESS NETWORK COMMUNICATION CHANNEL



Figures 4. i 5. illustrate change of contents in wireless network communication channel. The client sends data to access point/router, but the attacker modifies sent messages, forwards them in the form of ïnvented“ messages, being able to use them for active attack on wireless network. These forms of attack affect integrity of information. Figure 8. gives graphic presentation of possible security levels.

FIGURE 7. „INVENTED“ MESSAGES

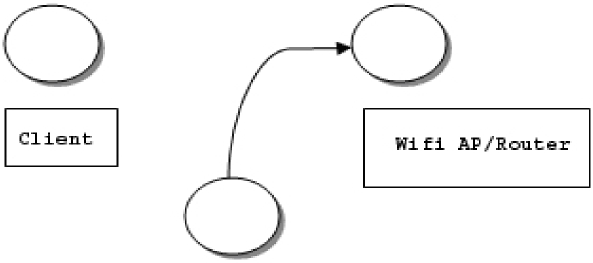
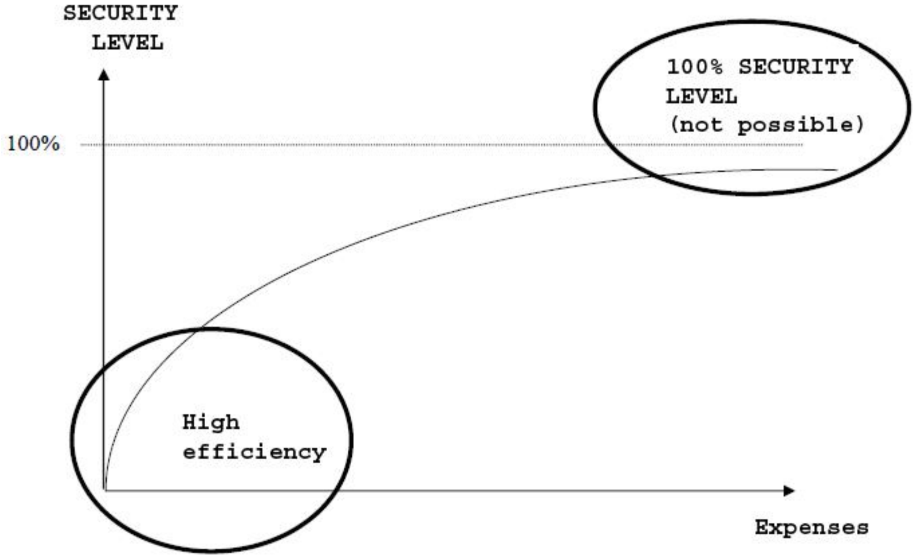


FIGURE 8. GRAPHIC PRESENTATION OF POSSIBLE SECURITY LEVELS



Source: Hadjina (2009).

Conclusion

Because of the use of radio waves, a wireless LAN will not be secure unless we take special precautions. Wireless security is the prevention of unauthorized access or damage to computers using wireless networks. The most common types of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP is a notoriously weak security standard. The password it uses can often be cracked in a few minutes with a basic laptop computer and widely available software tools. WEP has weaknesses, making it inadequate for protecting networks containing information valuable to others. The problem is that 802.11 does not support the dynamic exchange of WEP keys, leaving the same key in use for weeks, months, and years. Cracking methods have become much more sophisticated and innovative with wireless. Cracking has also become much easier and more accessible with easy-to-use Windows or Linux-based tools being made available on the web at no charge. There is no ready designed system to prevent from fraudulent usage of wireless communication or to protect data and functions with wirelessly communicating computers and other entities. However there is a system of qualifying the taken measures as a whole according to a common understanding what shall be seen as state of the art. The system of qualifying is an international consensus as specified in ISO/IEC 15408. For a higher level of wireless network security is necessary to adopt appropriate and effective security policy.

References

Barman, S. (2002). *Writing Information Security Policies.* New Riders Publishing.

Čerić, V., Varga, M. & Birolla, H. (1998). *Poslovno računarstvo*. Zagreb: Znak.

Hadjina, N. (2009). *Zaštita i sigurnost informacijskih sustava (nastavni materijali).* Zagreb: FER.

Peltier, R. & Thomas, B. (2004). *Information Security Policies and Procedures*. Auerbach Publications.

Radojević, B. (2011). Problematika provođenja sigurnosne politike u visokoškolskim ustanovama u RH. U Zborniku *MIPRO 2011* (195‒209). Opatija: MIPRO.

Sigurnosna akreditacija. (n.d). Retrieved April 8, 2013, from http://www.zsis.hr/site/SigurnostISa/Sigurnosnaakreditacija/tabid/90/Default.aspx

Sigurnosna politika ustanove. (n.d). Retrieved April 6, 2013, from http://www.cert.hr/sites/default/.../sigurnosna_politika_ustanove.pdf

Weidenbaum, M. (2004). Outsourcing: Pros and Cons. *America: History and Life, 19(1),* 23-37.

Zakon o informacijskoj sigurnosti. Narodne novine. Retrieved February 22, 2013, from http://narodne novine.nn.hr/clanci/sluzveni/298919.html