doi: 10.17234/INFUTURE.2015.31 Original scientific paper

Wireless Network Security recommendations Using the Application for Security Evaluation

Aleksandar Skendžić
Polytechnic "Nikola Tesla" Gospić
Bana Ivana Karlovića 16, Gospić, Croatia
askendzic@velegs-nikolatesla.hr

Božidar Kovačić
Department of Informatics, University of Rijeka
Radmile Matejčić 2, Rijeka, Croatia
bkovacic@inf.uniri.hr

Edvard Tijan
Faculty of Maritime Studies, University of Rijeka
Studentska ul. 2, Rijeka, Croatia
etijan@pfri.hr

Summary

The proposed system of security recommendations of wireless local area network allows applications to achieve higher levels of security. In order to build a security model, it is crucial to pre-evaluate the parameters that affect the security of the wireless network. When evaluating the parameters, expert literature along with practical experience of network administrators has been used. The results of evaluation parameters are included in the constructed security model of the proposed application. The proposed model contributes to a simpler problem solving of wireless network security through the evaluation of safety parameters. In addition, the proposed system gives recommendations regarding security at two levels, together with an appropriate security evaluation. The chosen safety parameters were evaluated using a questionnaire among CARNet system engineers in educational institutions. The results obtained may help to efficiently prevent wireless network security breaches.

Keywords: open source e-bus system, wireless network security, evaluation

Introduction

Configuring security is one of the main problems of wireless networks. It can be hypothesized that the security of wireless networks is lower than security of wire networks [1].

Security is a key element in wireless communication because the communication occurs via an unreliable media (air) [2]. Safety of networks, services and

transactions is essential for the creation of trust in various forms of personal communication. A threat in network environment is defined as a circumstance, condition or event that can harm the network and computing resources in the form of destruction, disclosure, modification of data, denial of service, fraud and abuse [6]. In order to protect the wireless network communication channel, numerous algorithms [8], certificates and protective mechanisms have been defined and used for the protection of wireless local area network (WLAN). They are an integral part of the security policy of institutions or organizations, and are carried out to a certain degree.

In the development of the proposed security model, the protective measures to be employed rely on the use of wireless networks security mechanisms in order to reduce the risk of security breaches. The choice of mechanisms for protection of wireless networks, with regard to the purpose of the local network, can result in optimal security solution that can be applied. If the effectiveness of wireless network security is confirmed by expert evaluation, the risk is reduced, and security is not compromised. If safeguards are not effective, security could be directly compromised. Although the security level cannot reach 100%, it is necessary to attempt all the necessary means of increasing the security level. Consequently, a higher security level requires greater financial investments, which implies a higher cost of planning and setting up the active wireless network equipment. In determining the concept of wireless network security, special attention should be given to the following segments:

- protection of an institution's information system,
- protection of personal data (on networked computers),
- restricted user access (user levels and user rights),
- use of standard encryption algorithms,
- use of compatible active network equipment,
- ease of network access,
- existence and enforcement of security policies [10].

The rest of this paper is structured as follows: Chapter 2 gives a description of the security system; Chapter 3 presents the methodology and tools used to develop the system for wireless network security evaluation; Chapter 4 describes the development and structure of the system; Chapter 5 and 6 offers security parameters evaluation and the interpretation of security evaluation values; finally, we conclude the paper (Chapter 7) and list references.

Security System

At the beginning, it was necessary to restrict the parameters that are an integral part of the overall security system. In the first phase of the study, the parameters that affect the security of the network were analyzed. Expert literature has been used for the purpose of determining and specifying the security parameters. Based on that, a questionnaire was devised and filled in by network adminis-

trators from state educational institutions (CARNet[1] members). These parameters were evaluated by network administrators based of the existing wireless network system in their home institutions.
Defining the level of security implies the creation of security system based on the optimal selection of parameters that influence it. The effective functionality of the system is associated with identifying the actions that interconnect all the elements of the security system. Regarding the security management process, the often applied methodology is known as Plan-Do-Check-Act (PDCA) [5]. The methodology is also known as the Deming cycle. Deming cycle of improvement always starts by analyzing the current situation, followed by deducing the problem.

Choosing a Tool for Building a System for Wireless Network Security Evaluation

The system for security evaluation is implemented as an application for wireless network security evaluation. The application enables users action at two levels:

- Network administrator (expert) level of action,
- Examinee level of action (application user).

Figure 1 provides an overview of procedures which define the level of user action. These procedures are available to the user through authentication procedure of the system. Additionally, users are able to use certain procedures that do not require authorization.

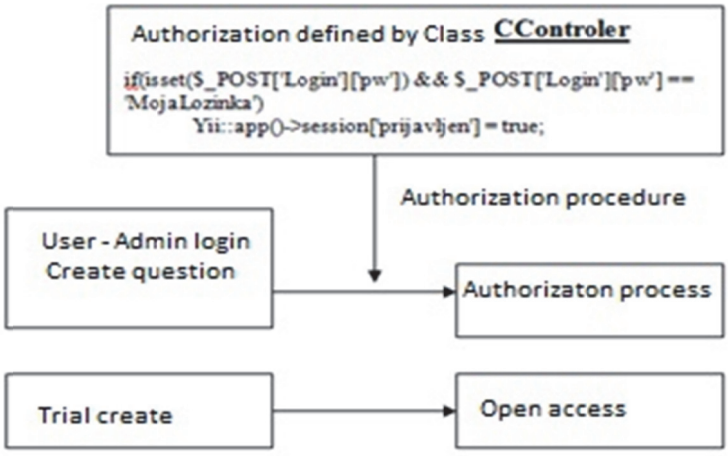


Figure 1. Defined user authorization procedure (source: authors)

The level of action of the network administrator (expert) through the interface provides the ability to create questions and multiple answers. Questions are

[1] Croatian Academic and Research Network (CARNet)

measured by weight grades and higher weight rating implies a greater impact of the given parameter on the overall security of wireless networks. The logging module enables a user to log in and create questions by selecting *Log in*. This module also allows user testing using the created questions. The questions create a structured tree with subordinate and super ordinate relations. By selecting the *Create Questions* option , the user has to fill in the required input fields: the number of the subordinate question, question description and the number of the super ordinate question. The button *Create* creates a question, and has the following required fields: question number and description. A tree structured in this way provides an overview of super ordinate and subordinate relations between questions and provides the option to edit questions and create multiple responses. The button *Create response* gives the opportunity to define all the answers to a question. Weight value is added to the answers based on user evaluation.

The level of action by the respondents relies on the possibility of evaluating wireless network security in the login module of the application. By selecting the *Create Test* option, user fills in a questionnaire which contains previously entered parameters by the administrator. The user selects each parameter and provides an answer from the list of possible answers. In the end, the result is checked through the recommendation module. By comparing the weight value of each parameter, recommendations are given to the user in order to achieve higher security levels. The level of action by the user is achieved by logging into the system via the administrator password. Users wishing to check network security select the option for creating a test.

For the construction of the system, PHP (server side) and Javascript (client side) have been used, driven by MySQL database management system. Development tool YII [9] was used as the framework. The use of scripting languages in the dynamic generation of web sites contains two main elements: (1) server with a programming platform and (2) database with the associated database management system and script language.

Development and Structure of the System for Wireless Network Security Evaluation

The application for wireless network security evaluation is based on the schema shown in Figure 2. Such a model may result from the transformations of the Entity-Relation (ER) data model [3]. The method of constructing an ER model is well known. The model was constructed according to Chen notation and uses key inheritance, while the weak entity type was determined according to the MIRIS[2] notation [4].

[2] Metodologija za Razvoj Informacijskog Sustava (MIRIS) – Methodology for Information System development.

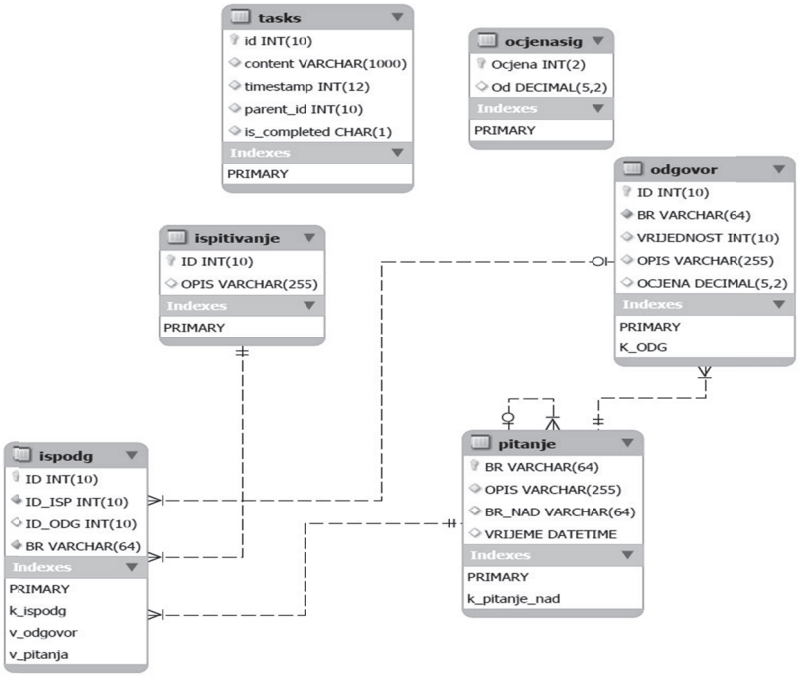


Figure 2. E-R diagram (schema) of the *ispitmreza.sql* database obtained via MySQL Workbench application (source: authors)

Access rules have been defined for every controller, which are executed only if user is logged into the system. For example, *IspitivanjeControler* enables acces to all users without the need for authentication. *IspitivanjeControler* controls the acces to the *Ispitivanje* module.

Evaluating the Selected Wireless Network Security Parameters

Questionnaire was consisted of 19 questions which are oriented on default wireless network security parameters [19]. Questionnaire was distributed through Google docs form in the period of May 2014 – July 2014 to a CARNet system engineers (59 respondents). Every engineer gave an answer and score to the each security parameter. Key questions were based from installed WiFi [18] network in organisation, security policies to evaluation of each security parameter which is shown in Table 1. Collected questionnaire data is used for application development.

The developed system gives recommendations based on the evaluation of security parameters which were defined using expert literature and network administrators (CARNet system engineers). The limitation of the system is the way parameters are evaluated, which relies on the weight value of each parameter. In

cases where two security parameters cannot be evaluated differently, the evaluation system will offer both logical solutions. Table 1 offers an overview of security parameters being evaluated. According to the calculated averages of the questionnaire results in which CARNet system engineers evaluated security parameters, the weight factors have been calculated, as shown in Table 1.

Table 1: Awarded weight factors (ponders) of security parameters based on research results

No.	Parameter	Weight factors (research)	Weight factors (%)	Parameter/ average
1.	Encryption	0.15	15.00%	4.03
2.	Network hardware model (type)	0.08	8.00%	3.74
3.	WIFI coverage	0.18	18.00%	4.15
4.	Firewall	0.21	21.00%	4.24
5.	Number of WIFI users	0.09	9.00%	3.77
6.	Defined security policy	0.13	13.00%	3.93
7.	Services	0.1	10.00%	3.81
8.	VPN	0.02	2.00%	3.41
9.	RADIUS + LDAP directory	0.04	4.00%	3.66
	Total	1	100 %	

As seen in Table 1, the weight factor 0.15 has been assigned to the encryption parameter (WEP[3], WPA[4], WPA2) [7], because it is considered that the encryption directly affects the security of wireless networks, i.e., wireless networks of an open type are extremely vulnerable to security threats and the use of encryption is strongly recommended in order to achieve a satisfactory level of security [12].

The model (type) of network equipment has been assigned a weight value of 0.08. On the network equipment market, various manufacturers offer diverse active network equipment. Active network equipment with greater capabilities can affect the security of the wireless network. Wireless network signal coverage has been assigned a weight value of 0.18. If there is a need for greater availability of wireless network signal, inside or outside the building, network security is decreased because the network covers a larger area that is accessible to more people and is more vulnerable to security breaches [13]. Firewall usage has been assigned a weight value of 0.21. LAN or wireless network firewall is extremely important because it filters the network traffic from the sender to the receiver and vice versa.

[3] Wired Equivalent Privacy (WEP)

[4] Wi-Fi Protected Access (WPA)

The number of wireless network users is proportional to the wireless network signal spatial coverage, and has been assigned a weight value of 0.09. Greater wireless network coverage generally implies more users and lower security level, and vice versa [14]. The definition and the existence of security policies in the organization have been assigned a weight value of 0.13. Encryption, firewall and security policy are key elements in both LAN and wireless network security within the organization. The security policy defines the planning and describes the goals or procedures of security. The network services have been assigned a weight value of 0.1. Educational institutions basically use e-mail services, Web services and file transfer services (FTP[5]).
The minimal weight value of 0.02 refers to the use of virtual private networks (VPN[6]). Such WLAN setup is neither standardized nor mandatory, but contributes to increasing the overall network security. The weight value of 0.04 refers to using the RADIUS protocol and LDAP directory service that are well represented in higher education institutions. Through LDAP + RADIUS, user accounts are assigned certain rights regarding the use of network resources (access to services and applications), which contributes to network (and overall) security. According to the survey, the calculated weights indicate a high correlation (strong association defined within ± 0.70 to ± 0.90) with the results of the study r = 0.78 (Table 1). Two parameters (VPN, RADIUS[7] + LDAP[8]) have low weight values (2% and 4%) and are almost negligible in the final evaluation, because they show low influence on the final result.

The Range of Values of Security Grades

The grades for assessing wireless network security are shown as values between 1 and 5, where 5 represents the highest level of security (Table 2). The range of values of security grades as well as the percentage of each evaluated parameter within the overall wireless network security is given in Table 2.

Table 2: The range of values of security grades

Security grade (level)	Grade (MIN)	Average grade (AVG)	Grade (MAX)		
1	0	20	29		
2	20	40	49		
3	50	60	69		
4	70	80	89	Correlation (r)	
5	90	100	99	Ponders - research	0,779604014

Source: Authors

[5] File Transfer Protocol (FTP)
[6] Virtual Private Network (VPN)
[7] Remote Authentication Dial-In User Service (RADIUS)
[8] Lightweight Directory Access Protocol (LDAP)

System engineers have evaluated the parameters that are used in the proposed model of evaluation. A random sample of examinees was used (N=59), all of whom are employees (system engineers) of the CARNet member institutions. The questionnaire consisted of ten questions. Each examinee needed to evaluate wireless network security parameters individually.

Questionnaire items consisted of statements, and by evaluating each of them, average values for individual statements and parameters which influence wireless network security were obtained. In order to evaluate preparatory tasks, a five-point Liker scale was used (1 = security parameter not important, 2 = important to a small degree, 3 = security parameter is important, 4 = security parameter is very important, 5 = security parameter is crucial). Average values of security parameter grades were used as the basis for establishing the level of wireless network safety in institutions. The main assumption is that if the average grade value of a particular wireless network security parameter is lesser than 2 (<2), it does not represent a satisfactory level within the overall wireless network security, as it directly lessens wireless network security. On the other hand, the average grade value of each parameter which contributes to wireless network security larger than 2, represents a satisfactory security level, but offers a different level of security. Security levels based on each parameter grade and the percentage of parameter grade value in the overall security are given in Table 3.

Table 3: The range of security grade values

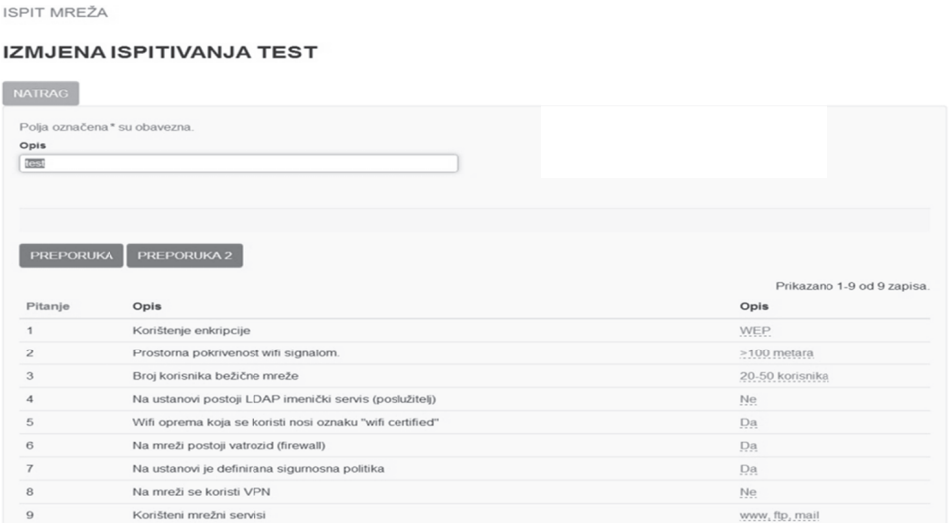
Parameter	Grade (INPUT)	Result	Grade (INPUT)	Result	Grade (INPUT)
1.	1	3.00%	2	6.00%	3
2.	1	1.60%	2	3.20%	3
3.	1	3.60%	2	7.20%	3
4.	1	4.20%	2	8.40%	3
5.	1	1.80%	2	3.60%	3
6.	1	2.60%	2	5.20%	3
7.	1	2.00%	2	4.00%	3
8.	1	0.40%	2	0.80%	3
9.	1	0.80%	2	1.60%	3
Parameter No.	Overall percentage	20.00%		40.00%	
See table 1!	Security level	1		2	

Parameter	Result	Grade (INPUT)	Result	Grade (INPUT)	Result
1.	9.00%	4	12.00%	5	15.00%
2.	4.80%	4	6.40%	5	8.00%
3.	10.80%	4	14.40%	5	18.00%
4.	12.60%	4	16.80%	5	21.00%
5.	5.40%	4	7.20%	5	9.00%
6.	7.80%	4	10.40%	5	13.00%
7.	6.00%	4	8.00%	5	10.00%
8.	1.20%	4	1.60%	5	2.00%
9.	2.40%	4	3.20%	5	4.00%
Parameter No.	60.00%		80.00%		100.00%
See Table 1!	3		4		5

Source: Authors

Network administrators have given the highest grades to parameters relating to encryption and firewall usage (see Table 1). The lowest grade was given to VPN, which can be explained by the fact that VPN is not often found in educational institutions, or is not employed by the current sample of examinees. Authors recommend further research.

Figure 4 illustrates the security level given the value 2 (32% overall), based on the parameter value input. After making a choice, recommendations are given at two levels: level 1 recommendation (named "Preporuka") compares evaluated parameters in case of two choices being made, while level 2 recommendation (named "Preporuka 2") compares evaluated parameters in case of three or more choices being made (Figure 3).


ISPIT MREŽA

IZMJENA ISPITIVANJA TEST

NATRAG

Polja označena * su obavezna.

Opis

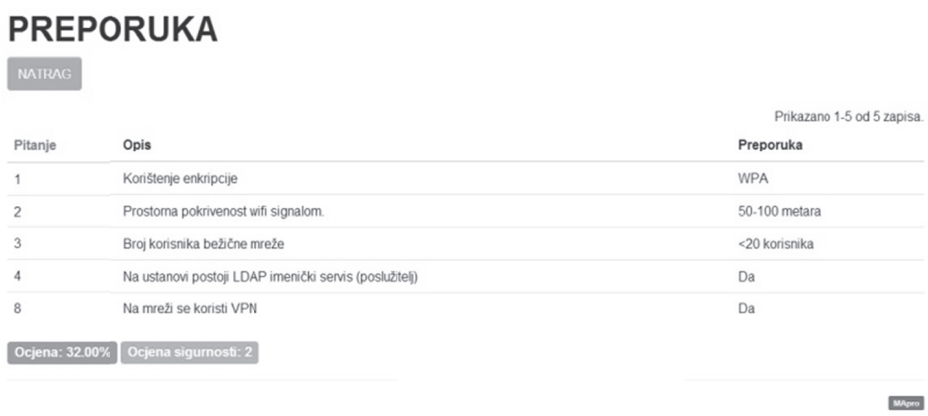
test

PREPORUKA PREPORUKA 2

Prikazano 1-9 od 9 zapisa.

Pitanje	Opis	Opis
1	Korištenje enkripcije	WEP
2	Prostorna pokrivenost wifi signalom.	>100 metara
3	Broj korisnika bežične mreže	20-50 korisnika
4	Na ustanovi postoji LDAP imenički servis (poslužitelj)	Ne
5	Wifi oprema koja se koristi nosi oznaku "wifi certified"	Da
6	Na mreži postoji vatrozid (firewall)	Da
7	Na ustanovi je definirana sigurnosna politika	Da
8	Na mreži se koristi VPN	Ne
9	Korišteni mrežni servisi	www, ftp, mail

Figure 3: Data input within the *Ispitivanje* module for wireless network security check


PREPORUKA

NATRAG

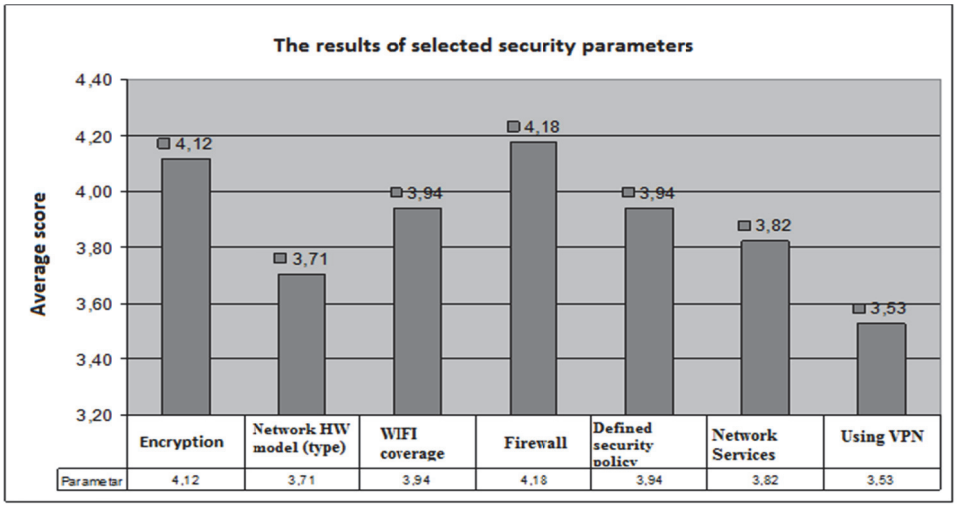
Prikazano 1-5 od 5 zapisa.

Pitanje	Opis	Preporuka
1	Korištenje enkripcije	WPA
2	Prostorna pokrivenost wifi signalom.	50-100 metara
3	Broj korisnika bežične mreže	<20 korisnika
4	Na ustanovi postoji LDAP imenički servis (poslužitelj)	Da
8	Na mreži se koristi VPN	Da

Ocjena: 32.00% Ocjena sigurnosti: 2

Figure 4: An example of wireless network security recommendation ("Preporuka" - Level 1) with the overall security grade ("Ocjena") (32%) and the corresponding security level (2) ("Ocjena sigurnosti"). At the end of the research and parameter evaluation, the examinees (network administrators) have evaluated the selected security parameters.

Graph 1: Network administrator satisfaction with the selected parameters included in the system model (average values)



Source: Authors

As shown in Graph 1, network administrators have given the highest grades to encryption algorithms (average value 4.12) and firewall usage (average value 4.18) if compared to other selected parameters which influence wireless network security. The lowest grade (3.53) was given to the use of VPN, which can be explained by the fact that VPN is not often employed in educational institutions or is not used by the sample of examinees included in this research [15]. Overall score of network administrator satisfaction with selected parameters was 3.59. Authors recommend further research.

Conclusion

In order to define the specifications for the security model, an analysis of all the key aspects of security settings of active wireless network equipment was undertaken. Using a questionnaire, data was collected from administrators (system engineers) at educational institutions regarding security of the wireless network they administrate, security criteria and the structure and evaluation of these criteria. The collected data was analysed statistically. The collected data was used to set the criteria for assessing threats, and weight factors for each criteria. Data analysis has yielded properties important for the set research goals. Statistical analysis was used as the basis for developing application for security evaluation. In addition, the evaluation of the model was conducted. It was concluded that the proposed application enables recommendations of security measures which enhance the level of security. In the process of security planning, it is very important to choose network equipment by an established manufacturer.

On today's market, different equipment is available, but when making a choice, certain qualities should be taken into consideration, namely, the possibility of maximum adaptability of network equipment. If case a network device got lost, there should be a procedure for reporting it. Moreover, it is important to define a procedure in case of intrusion, i.e., in case of a security breach. In addition to developing the system for evaluating the security of wireless local area networks , this work is also sample research of wireless networks security in educational institutions in Croatia.

This research represents a contribution to the theoretical and practical considering the areas of security of wireless local area networks and provides exceptional importance on recruiting value of each parameter active safety wireless network equipment for the purpose of determining the level of required security protection. Security tests regarding wireless network vulnerability should be conducted periodically, and it is necessary to evaluate security risks [16]. Everything mentioned above should be incorporated into the security policy. In order to enhance the model of evaluation, the authors recommend further research.

References

[1] A. S. Tanenbaum, D. J. Wetherall, Computer networks, 5th ed. SAD: Prentice Hall, 2011.
[2] H. Hamidović, WLAN - Bežične lokalne računalne mreže. Zagreb: Info press, 2009.
[3] C. J. Date, An introduction to database systems, 6th edition. Reading MA: Addison Wesley, 1995.
[4] M. Pavlić, Razvoj informacijskih sustava, Znak, Zagreb, 1996.
[5] M. Piškor, V. Kondić, Đ. Mađerić, "Proces implementacije lean-a u malim organizacijama". Tehnički glasnik, Vol. 5 No. 1, 2011.
[6] G. Gledec, M. Mikuc, M. Kos, Sigurnost u privatnim komunikacijskim mrežama. Zagreb: FER, 2008.
[7] http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2009-06-267.pdf (12.2.2013.)
[8] http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-12-001_0.pdf (12.2.2013.)
[9] http://www.yiiframework.com/about/ (06.02.2015)
[10] Radojević, B. Problematika provođenja sigurnosne politike u visokoškolskim ustanovama u RH. Opatija: MIPRO, 2011.
[11] Skendžić, A. Sigurnost infrastrukturnog načina rada bežične mreže standarda IEEE 802.11. Zbornik Veleučilišta u Rijeci, Vol. 2 (2014), No. 1.
[12] Prodanović, R., Simić, D. A Survey of Wireless Security. Journal of Computing and Information Technology - CIT 15, 2007, 3, 237–255.
[13] http://blogs.aerohive.com/blog/the-wireless-lan-training-blog/wifi-back-to-basics-24-ghz-channel-planning. (08.02.2015)
[14] http://wireless-spot.blogspot.com/2009/11/ad-hoc-and-infrastructure-modes.html (02.10.2015)
[15] http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-02-05.pdf (09.10.2015)
[16] http://www.cis.hr/sigurosni-alati/ispitivanje-sigurnosti-bezicnih-mreza.html 01.10.2015)
[17] https://docs.google.com/forms/d/1G4kpM52yhh5z2U3oon92iEyRy0dQeSi2jdFr6_mzWs/viewform (05.6.2014.)
[18] http://www.wi-fi.org/ (01.10.2015)