Designing Secure Information and Communication Infrastructure of Faculty of Transport and Traffic Sciences

Dragan Peraković – the main author
University of Zagreb
Faculty of Transport and Traffic Sciences
Zagreb, Croatia
dragan.perakovic@fpz.hr

Ivan Cvitić
Vrbica, Croatia
ivan.cvitic@vk.t-com.hr

Vladimir Remenar
University of Zagreb
Faculty of Transport and Traffic Sciences
Zagreb, Croatia
vladimir.remenar@fpz.hr

Abstract—**With the development of information and communication systems various methods and tools to attack them are being developed. Initially the attacks where performed for individual proof and the desire to learn, but the rise in popularity of Internet and the value of information that this medium transmit target attacks become financial benefit or even war activities.**
The purpose of this study is to determine the current state of information and communication systems of the Faculty of Transport and Traffic Sciences, define its security vulnerabilities or weaknesses, and based on its findings recommended solutions that will improve the level of safety and reliability of the system by applying the known methods and means of protection.

Keywords- Information security, Network security, Security management

I. INTRODUCTION

Safety and security of information and communication system includes a very wide range of observation and research, and to make it possible to deal with this topic is extremely important to define the basic concepts that security and protection of information and communication system includes. First of all it is necessary to define the concept of an information communication system which consists of two terms, an information system that includes the elements necessary for the collection, storage and processing of data, and a communication system that includes the elements required for data transmission. Practically speaking, the coexistence of the two systems is a necessity and is therefore used a unique name. According to [1], it can be observed and defined from two perspectives, technical and functional. From a technical perspective information and communication system consists of end devices, active and passive network equipment and data and information are stored, processed and transmitted as part of the system, while defining the information communication system from a functional perspective implies its role and activities and requirements compared to the organizational system.

This paper presents view of current state of information and communication infrastructure of the Faculty of Transport and Traffic Engineering which is divided into three segments. The first segment explains accommodation of Faculty servers, their network communications within the Faculty (internal) and communication with the servers via the public network (external). The second segment included a review of network devices and their disadvantages from the perspective of safety and security of Faculty information systems. third segment comprises the current state of network and user access control and recommendations for their improvement

II. SERVER INFRASTRACTURE OF FACULTY OF TRANSPORT AND TRAFFIC SCIENCES

A. Current state of server infrastructure

The center of the information infrastructure of the Faculty of Transport and Traffic Sciences are servers located in two physical locations, Vukelićeva and ZUK Borongaj, as shown in table 1.

TABLE I. FACULTY SERVER INFRASTRUCTURE

LOCATION	SERVERS	OPEN PORTS	
		Internal communication	External communication
Vukelićeva (failover cluster – FPZHC)	FPZDC01	all	/
	FPZDC02		
	FPZDC03		
	FPZEXCHANGE01	all	80 (HTTP), 443 (HTTPS)
	FPZSP01	all	80 (HTTP), 443 (HTTPS)
	FPZSQL01	all	/
	FPZSQL02	all	/
	FPZVPN	all	1701, 1723, gre47, UDP500, UDP4500

	FPZWEB01	all	80 (HTTP), 443 (HTTPS)
	FPZWEB02	all	80 (HTTP), 443 (HTTPS)
	FPZMySQL01	all	/
	FPZSC01	all	80 (HTTP), 443 (HTTPS), 8530, 8531, 5723
	FPZUR01	all	/
ZUK Borongaj (failover cluster – FPZVC)	FPZDC04	all	/
	FPZDC05		
	FPZSC02	all	/
	FPZLIC01	all	/
	FPZCOPY01	all	/
	FPZTFS01	all	/

TABLE II. FACULTY SERVER INFRASTRUCTURE

LOCATION	SERVERS	OPEN PORTS	
		INTERNAL COMMUNICATION	EXTERNAL COMMUNICATION
Vukelićeva (failover cluster– FPZHC)	FPZDC01	DNS (TCP/UDP 53), Kerberos (UDP 88), AD (TCP/UDP389) DC->DC/Client (UDP/TCP 135), LDAP (UDP 389), GC (TCP 3268, 3269)	/
	FPZDC02		
	FPZDC03		
	FPZEXCHANGE01	LDAP (TCP 389, 379, 390), LDAP/SSL (TCP 636), LDAP->GC (TCP3268), HTTP (TCP 80), HTTPS (TCP 443)	80 (HTTP), 443 (HTTPS)
	FPZSP01	DNS (TCP/UDP 53), Kerberos (UDP 88), LDAP (TCP/UDP 389), SQL (TCP 1433, UDP 1434)	80 (HTTP), 443 (HTTPS)
	FPZSQL01	SQL->SP01/WEB01 (TCP 1433)	/
	FPZSQL02	SQL->SC01/WEB01 (TCP 1433)	/
	FPZVPN	1701 (L2TP), 1723 (PPTP), gre47, UDP500, UDP4500	1701 (L2TP), 1723 (PPTP), gre47, UDP500, UDP4500
	FPZWEB01	HTTP (TCP 80), HTTPS (TCP 443), FTPS (TCP/UDP 989),FTP (TCP/UDP 20)	80 (HTTP), 443 (HTTPS)
	FPZWEB02	SMB->DC02 (TCP 445)	80 (HTTP), 443 (HTTPS)
	FPZMySQL01	TCP/UDP 3306	/
	FPZSC01	SQL02 (TCP 1433), operation manager (TCP 5724), AD (TCP 389)	80 (HTTP), 443 (HTTPS), 8530
	FPZUR01	SMB (TCP 445) -> 192.168.92.0/24 (deanery)	/
ZUK Borongaj (failover cluster – FPZVC)	FPZDC04	DNS (TCP/UDP 53), Kerberos (UDP 88), AD (TCP/UDP389) DC->DC/Client (UDP/TCP 135), LDAP (UDP 389), GC (TCP 3268, 3269), SMB (TCP 445)-> 192.168.203.0/24 (PC lab)	/
	FPZDC05		
	FPZSC02	SMB (TCP 445) -> 192.168.95.0/24 (servers)	/
	FPZLIC01	Server administrator (TCP 80, 8090), (TCP 2080, 56192, 27000-27009)	/
	FPZCOPY01	SMB (TCP 445) -> 192.168.202.0/24 (lecturers computers)	/
	FPZTFS01	HTTP/HTTPS (TCP 80, 443), SQL02 (TCP 1433)	/

Server infrastructure vulnerability is mostly manifested through communication ports allowed in the internal (server-to-server and client-server) communication with other segments of the local network. To reduce the risk of exploitation of vulnerabilities, within the local network, it is necessary to disable the communication ports that are not needed for communication.

B. Faculty server infrastructure security improvement

To achieve higher level of security it is necessary to implement minimum authority concept, both, at the user level and also at the device level to reduce the vulnerability of the system and thereby achieve a satisfactory level of safety of information and communication system of the Faculty.

III. NETWORK INFRASRTUCTURE OF FACULTY OF TRANSPORT AND TRAFFIC SCIENCES

A. Current state of layer 2 switches

Within the Faculty network, layer 2 switches are used as access switches for connecting end devices to the network. Though simple to use in terms of adjustments and maintenance and have very little impact on performance and network speed, layer 2 switches have specific vulnerabilities to different methods of attack some of which will be described below.

The first vulnerability is CAM (Content-Addressable Memory) table overflow. CAM tables contain MAC addresses associated to the physical communications port switch. As the CAM table memory is limited, an attacker can overflow it with a large number of invalid MAC addresses, after which the switch starts to behave like a hub where network packets are forwarded to all physical ports, as in [2].

Layer 2 switches are also vulnerable on the VLAN hopping attack type in which an attacker who is in a VLAN, is trying to send network packets to the VLAN in which he do not belong (Double Tagging) or it tries to present to the network as a switch to gained the ability to communicate with other VLAN's (Switch Spoofing), as in [2].

B. Layer 2 switches security improvement

It is possible to avoid CAM table overflow using the security configuration of the physical communication port on the layer 2 switch. Thus limiting the number of MAC addresses per port that each switch can store which will result in blocking the MAC address or even blocking the physical port to which the device is connected if attacker attempts to enter more addresses in the CAM table than it was previously defined. There is also the possibility of defining certain MAC addresses that are allowed per single port, but this solution makes administrators difficulty maintaining the switch in case of constant change devices that are connected to the switch, as in [2].

Vulnerability to VLAN hopping attack method avoids with the modification of VLAN configuration. It is necessary to exclude the possibility of DTP (Dynamic Trunk Protocol), which is necessary for the performing of Switch Spoofing

attack method, it's important to use dedicated VLAN IDs for Trunk ports on the switch and disable unused physical ports and bundle them into an unused VLAN, as in [2].

C. Current state of layer 3 switches

Layer 3 switches are very similar to routers, and support the same protocols for routing. Packet routing is functionality that enables network communication between different subnets or VLANs. Within the Faculty network layer 3 switches are used in the distribution and the core level for communication between different VLANs and subnets. Layer 3, like layer 2 switches, contain specific vulnerabilities and security holes. One of these vulnerabilities are contained in the RIP (Routing Information Protocol) protocol that enables layer 3 switches to exchange information of routes within the network. An attacker can send RIP packet containing false information about the shortest path in the network. In this way, the routing of network traffic is performed by an attacker who has the ability to analyze network packets or perform MITM attack method, as in [3] [10].

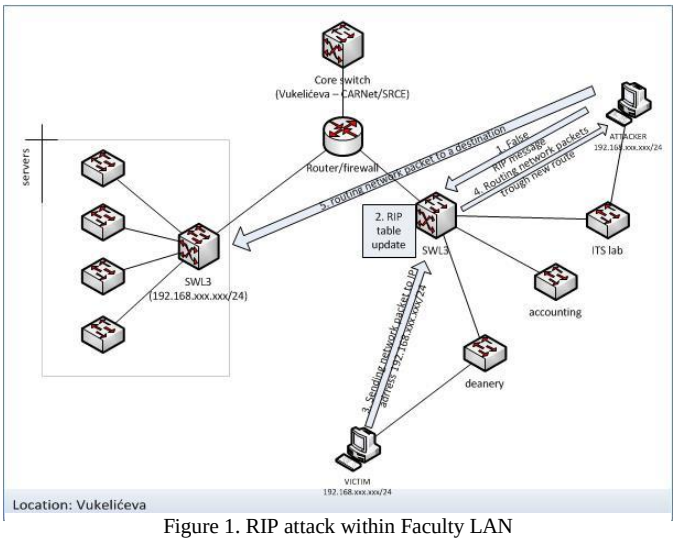

Figure 1. RIP attack within Faculty LAN

D. Layer 3 switches security improvement

RIP attack is avoiding using the RIPv2 protocol that contains a cryptographic algorithm MD5 (Message-Digest 5) authentication messages that are exchanged between the layer 3 switch. MD5 value is sent with a message that contains routing information. On receiving MD5 value key that is not transmitted through communication channel is checked. Every switch in the network possesses the key and thus validates the integrity of the received message. Performing RIP attack with RIPv2 protocol embedded within the layer 3 switch is shown in figure 2. Besides RIPv2 protocol is possible to apply OSPF (Open Shortest Path First) protocol, which also contains the cryptographic algorithms for authentication of exchanged routing messages, as in [3].

E. Current state of Faculty perimeter security

Perimeter protection of the LAN (Local Area Network) of the Faculty of Transport and Traffic Engineering conducted

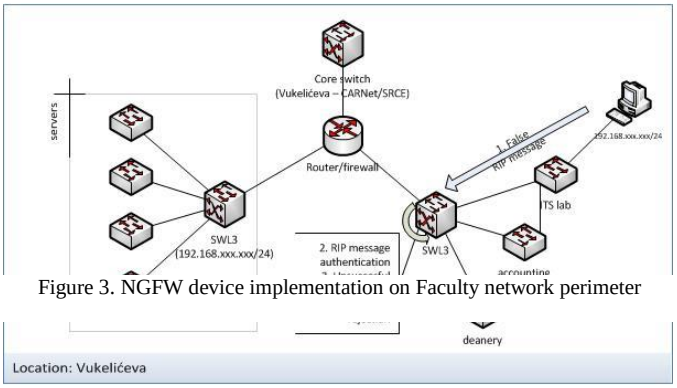

Figure 3. NGFW device implementation on Faculty network perimeter

exclusively through the function of packet filtering and NAT (Network Address Translation) functionality built in the border routers. Nowadays more and more applications are based on web, some of which are inevitable for a perfunctory task of system users. For this reason, restrict access to specific web sites is not possible, the only solution is blocking communication ports 80 and 443 which is unacceptable.

F. Faculty perimeter security improvement

Avoidance and reduction of vulnerability of the border router seeks to protect the entire local network of the Faculty from malicious immediate impact outside the perimeter of the network. In order to conduct adequate LAN protection from various sophisticated threats it is necessary to apply the devices and methods to perform analysis of network traffic to a greater number of parameters then the classic router firewall with packet filtering function that is embedded in the router. One of the devices that are capable to provide a higher level of network perimeter security is NGFW (Next Generation Firewall). Implementation of NGFW devices on the Faculty network perimeter, shown in figure 3, would greatly contribute to stronger control of network traffic that is coming from the public network to the local and vice versa because it contains first generation firewall, application and user awareness functionality, IPS and IDS capability, and many other options, as in [4].

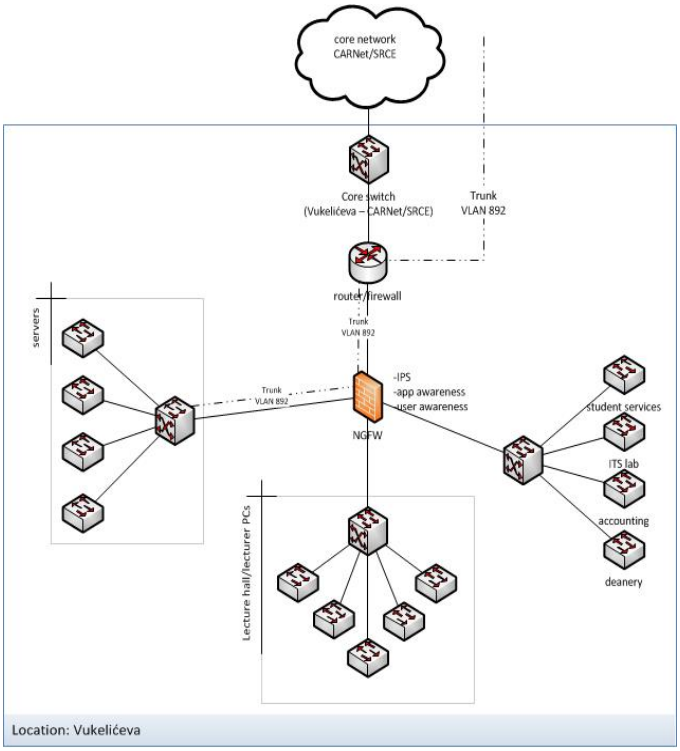

Figure 2. RIPv2 protocol embedded within the layer 3 switch

G. EoIP tunneling between Faculty dislocated objects

EoIP (Ethernet over Internet Protocol) is MikroTik's protocol that is used to create Ethernet tunnel between two separate routers on top of IP networks (Internet). In this way it is possible to link two dislocated LANs via a WAN into one, the apparent local network so it can be defined as a special form of VPN. EoIP is considered a "reverse" technology because standard IP packets transmitted over the Ethernet protocol.

Advantage EoIP tunneling versus traditional VPN is that the VPN forwards only those packets that are pre-configured to its configuration, and it also has to know all the protocols used in the network. Unlike VPN, EoIP network interface can be defined at the routers that are on the perimeter of two local networks. When network traffic reaches the network interface of the router, EoIP encapsulates Ethernet frames within IP packets over 47 GRE (Generic Route Encapsulation) protocol after which forwards them to the Ethernet interface over EoIP tunnel to another router as if they were physically connected, as in [5].

EoIP has no mechanisms for authentication or encryption of data transmitted over the network for which it is necessary to define and secure tunnel between the routers that are connect. It is possible to use some of the safe tunneling protocols such as IPsec or PPTP, as in [5].

Since the local network of the Faculty is dislocated, establishing EoIP tunnel between these locations would significantly facilitate mutual communication. Primarily

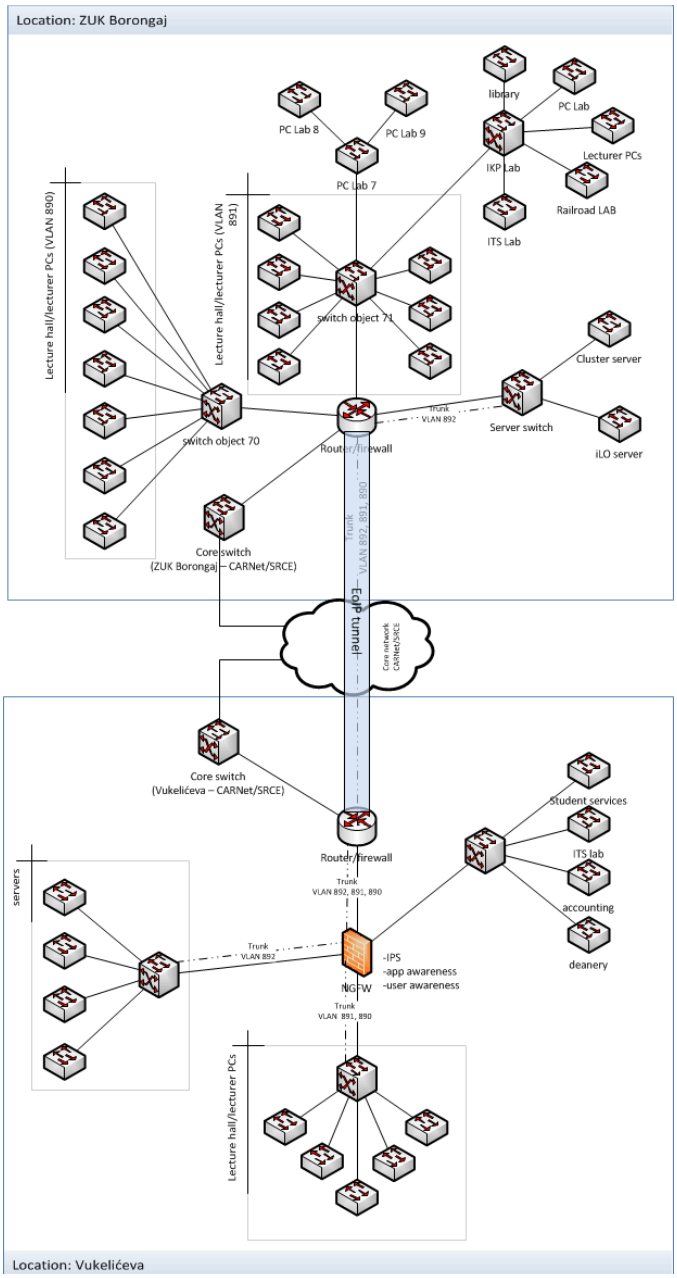

Figure 4. EoIP tunnel between two Faculty LANs

because in both locations (Vukelićeva and ZUK Borongaj) are the ultimate devices that can be logically connected to the same logical group. Currently this is done only for the server infrastructure through VLAN 892 that is enabled by CarNET / SRCE institutions. Establishing EoIP tunnel would expand the possibility of grouping computers through existing VLAN groups 890 and 891, within which there are teachers and computers in school halls and computers in the PC labs can be seen from Figure 4. Besides logical grouping, EoIP would facilitate the overall network communication, and sharing of network resources between two physically separate networks.

IV. FACULTY USER AND NETWORK ACCESS CONTROL

A. Current state of user and network access control

Faculty user access control also contains certain security vulnerabilities and defects that significantly increase the likelihood of the realization of different types of security threats. User access control is defined and implemented through a GPO (Group Policy Object) service for all users and computers connected to the Faculty local network. The rules are defined within AD DS on a virtual server (FPZDCD01, FPZDCD02, FPZDCD03, FPZDCD04, and FPZDCD05). When users perform identification and authentication, the server can perform data verification after which the user is authorized, and awarded his rights under the defined group which, users and computers that access it belongs.

One of the vulnerabilities of defined rules is the ability to access the command prompt with groups of computers that are in the PC labs. Via the command line user has the option of obtaining a variety of information that can be used in further breach of security of Faculty information system.

Additional vulnerability is insufficient use of strong passwords when connecting to the domain of the Faculty as well as the absence of user passwords periodic change. The said vulnerability allows a malicious user to easily decrypt the passwords using brute-force attack methods.

Network access control has not been established within the Faculty network, although PKI (Public Key Infrastructure) exist and all computers and users have digital certificates. Thus compromised computer can access the network without checking by network devices and thus cause security distortion of the entire information system.

B. User and network access control improvement

User access control must be based on the concept of minimum authorization to minimize the risk of security threats [8] [9]. All employees and users of Faculty information system through access control must be authorized to access only those resources information system that they are necessary to perform the defined tasks. Providing administration rights to users must be avoided, or administrator privileges should be granted only to persons authorized to administer certain segments of the ICT infrastructure, as in [6]. Significant role in maintaining efficient security standards can be achieved with basic user training as an additional layer of security.

User access control to the Faculty information system is defined through AD role and Group Policy on the DC servers. Within Group Policy are defined group of users and groups of the network devices and the rights over information resources. Users' prior authorization must enter their user name and password assigned by the system administrator. Users need through GPO impose complexity password that must be respected when its changes, which includes a combination of large and small letters, special characters and numbers and length of the password of at least eight characters. In addition, it is necessary to define the password expiration period after which the users are forced to change it in order to access the system. In addition to user password control, administrator must allow access to defined user groups but only to those components of the operating system that the user needed for everyday work. For example, within the Windows operating system it is necessary to ban access to the control panel, command prompt, option run, access to system files, installing applications, etc.

Network access control (NAC) allows verification of each device before being permitted access to the information system. Devices that do not meet certain criteria defined by NAC (operating system that is not up to date, a software firewall is turned off, not having the latest antivirus updates) will be redirected to an isolated part of the network to correct the identified failures of the devices. The goal of NAC system is prevention from accessing the network to computers that have identified vulnerabilities. This prevents the security threats for the entire information system. NAC system can allow network access to computers that are not owned by Faculty without compromising security, as in [7].

Since PKI infrastructure already exists at the Faculty and all devices have digital certificates it is necessary only to implement HRA (Health Registration Authority) server. HRA issues a certificate confirming safety based on safety assessments performed by System Health Agent on the client computer. If carried out security assessment meets defined criteria HRA issued security certificate to a client on the basis that the client can access the local network. Otherwise, the client is redirected to the quarantine. The principle of the system is shown in Figure 5.

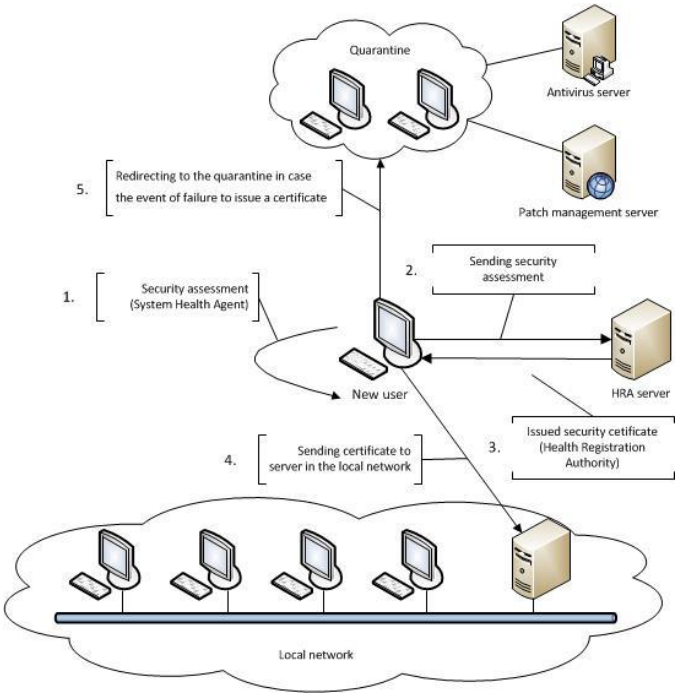

Figure 5. Logical scheme of NAC system

V. CONCLUSION

Information and communication systems, although they greatly contributed to the progress of business and communication in general, contain a large number of vulnerabilities that are found in all the elements that make up such a system. Since each vulnerability can be exploited for the purpose of unauthorized access to resources, information and communication system, which can lead to large financial losses of the organization, the loss of credibility or other unintended consequences, it is extreme attention to system security and the preservation of availability, integrity and confidentiality of information as the basic principles of security.

Complete security system is impossible to achieve because every method and means of protection has vulnerabilities that can be exploited in order to compromise security systems. For this reason it is necessary to apply a multi-layered security approach so potential attacker will be more difficult to gain unauthorized access to system resources.

Designing a secure information and communication infrastructure of the Faculty of Traffic Engineering, which is presented in this paper, is based on the present state of the system and its drawbacks. This paper presents recommendation for secure Faculty information and communication infrastructure, which is defined through the improvement of network and server infrastructure, internal communications, improve user access control and deployment of network access control.

REFERENCES

[1] D. Dragičević, "Kompjutorski kriminalitet i informacijski sustavi," Zagreb, Informator, 1999.

[2] Cisco, "Cisco IOS Software Configuration Guide," Cisco, 2012.

[3] R. Atkinson, 2007. "RIPv2 Cryptographic Authentication," Extreme Networks, 2012.

[4] AlgoSec, "The Practitioner's Guide to Deploying, Optimizing and Managing Next Generation Firewall," AlgoSec Inc., 2012.

[5] Mikrotik (2013, July, 11). EoIP general information, *Online document.* Available: http://www.mikrotik.com/testdocs/ros/3.0/vpn/eoip.php

[6] M. Ciampa, "Security+ Guaid to Network Security Fundamentals, 4th Edition," Boston, Course Tehnology, 2011.

[7] K.S. Furnel, P.J. Lopez, "Securing Information and Communications Systems," Artech House, 2008.

[8] P. Stavroulakis, M. Stamp; Handbook of Information and Communication Security, Springer, 2010, ISBN 978-3-642-04116-7

[9] T.R. Peltier; Information Security, Policies, Procedures and Standards, Auerbach, 2002, ISBN 0-8493-1137-3

[10] J.A. Vacca; Network and System Security, Syngress, 2010, ISBN 978-1-59749-535-6