Developing A Security Model for Enterprise Networks (SMEN)

Aiman A. Abu Samra[1], Khaled W. Alnaji[2]

[1] *Aiman A. Abu Samra Department of Computer Engineering Faculty of Engineering Islamic University of Gaza, Gaza Strip, Palestine,*

[2] *Khaled W. Al Naji Department of Computer & Industrial Professions University College of Applied Sciences, Gaza Strip, Palestine, kalnaji@ucas.edu.ps*

Abstract—Enterprise network (EN) supports thousands of users, and interconnects many networks. EN integrates different operating systems and hosts hundreds of servers that provide several services such as web applications, databases, E-mail, and others. Security threats represent a serious problem to EN. They try to damage enterprise confidentiality, integrity, and availability. Security provides protection against attacks, hacking, and data theft. In this paper, we propose a security model (SMEN) of EN. The proposed model provides security at different layers. It integrates both hardware and software security solutions. We perform a defense evaluation for the proposed model The results show that SMEN was able to detect and prevent all attacks and malwares that were induced by the framework Metasploit. Performance evaluation shows that applying proposed model has a little negative effect on bandwidth utilization and hence on network performance.

Index Terms—Enterprise network, security model, SNORT, OSSEC, intrusion detection/prevention.

I INTRODUCTION

Enterprise Network EN is composed of a distributed infrastructure that connects different users, devices and branches networks. It includes high performance computing servers, massive storage solutions, and speed network for both LAN and WAN[1]. Even enterprise network should meet a set of technical goals, it should also meet the business needs of the enterprise[2]. Enterprise network contains hundreds of network devices such as routers and switches. It integrates multiple technologies, protocols, software applications, and vendors. EN includes data center that hosts different services such as web, E-mail, DNS, FTP, and other services. EN includes Demilitarized Zone (DMZ) network[3], internal network, external network, and branches networks.It may also include other special networks such as management and monitoring networks. Some branches networks are connected to EN through WAN services such as VPN, Leased Line, and Frame Relay, while others may be connected using wireless technology such as Wi-Fi, WiMAX, and microwave. Enterprise network has several requirements like availability, scalability, security, and mobility. EN requires an updated security model that reflects changes in technology and services. So we have to build and maintain a robust network security for both end users and servers. This paper proposes a Security Model (SMEN) for enterprise network. In this paper, we recognize enterprise network as a real network that is in use until developing the proposed model. We use both hardware devices and open source tools such as SNORT, OSSEC, and Splunk to implement our model. Performing deep inspection of traffic that passes through EN, represents an important step in this work. We need to provide secure connection between branches networks and EN services. The SMEN model takes into account the defense in depth strategy by implementing security at more than one layer. Defense evaluation was done using Metasploit, while performance evaluations was done using FreeMeter.

II RELATED WORKS

There are number of security models that are designed for enterprise network. Some of them depend on firewall and routers, while others depend on intrusion detection/prevention system. Different factors are affected by security model design such as number of users, supported services, and others.

In [4], the proposed security model is implemented with connectivity fault management (CFM). CFM provides an end-to-end traffic carrier in the metro Ethernet domain.

CFM defines protocols and practices of Operations, Administration, and Maintenance for paths through 802.1 bridges and LANs. The proposed in [4] model provides an effective and reliable isolation of individual traffic flows and the associated LANs using CFM. But the paper did not provide real implementation of network security concepts,

Paper in [5] introduced a new concept, which is network business security. Using the proposed concept, the paper defines the object of information security in three parts, which are: data security, network system security, and net-

work business security. We think this research provides formal description of network business security model. But there is no practical implementation using either hardware or software. It is not sufficient to use only routers and firewall to provide network security for EN.

Authors in [6] proposed a network security model for the campus network. Internet access exposes Campus network to attacks and intrusions. It becomes so important to provide a secure campus network that has ability to defense against intrusions and attacks. But paper in [6] did not provide a security solution for branches networks, the proposed models have not a clear implementation of intrusion detection/prevention systems. Research in [6] does not provide either defense evaluation or performance evaluation.

Author in [7] used routers and firewalls to design and implement a network security model for cooperative networks. He listed the network security vulnerabilities in routers and firewalls. He discussed prevention mechanism against different types of threats and attacks. The model used PacketShaper, which is a traffic management appliance, in order to monitor and control network traffic passing over wide-area networks. We think PacketShaper is not sufficient, as devices and tools are required to provide a security model for EN.

III Enterprise Network Model ENM

Here we introduce the topology of ENM and explain each component. We also discover functions of these components and their effects on ENM. Figure 1 shows the topology of our ENM.

Enterprise network includes several network devices such as layer 2 switches and layer 3 switches. They are used as access devices, distributed devices, and core devices. On the other hand, router is used for WAN services connection. Other devices such as firewalls are used to filter passing inbound and outbound. Intrusion prevention system is used to detect and prevent potential attacks according to predefined signatures. We also introduced different connections such as Frame Relay, Leased Line, and VPN. While Frame relay provides shared bandwidth, Leased Line providesdedicatedbandwidth for connected network. VPN presents a secure, cheap solution for connecting branches networks to enterprise networks. HTTP/HTTPS are the most used protocols in enterprise networks. We introduce DMZ network, which includes public services that allow public user (via Internet) to access them [3]. DMZ network hosts web server, E-mail server, DNS server, FTP server, Web-based application, and others.

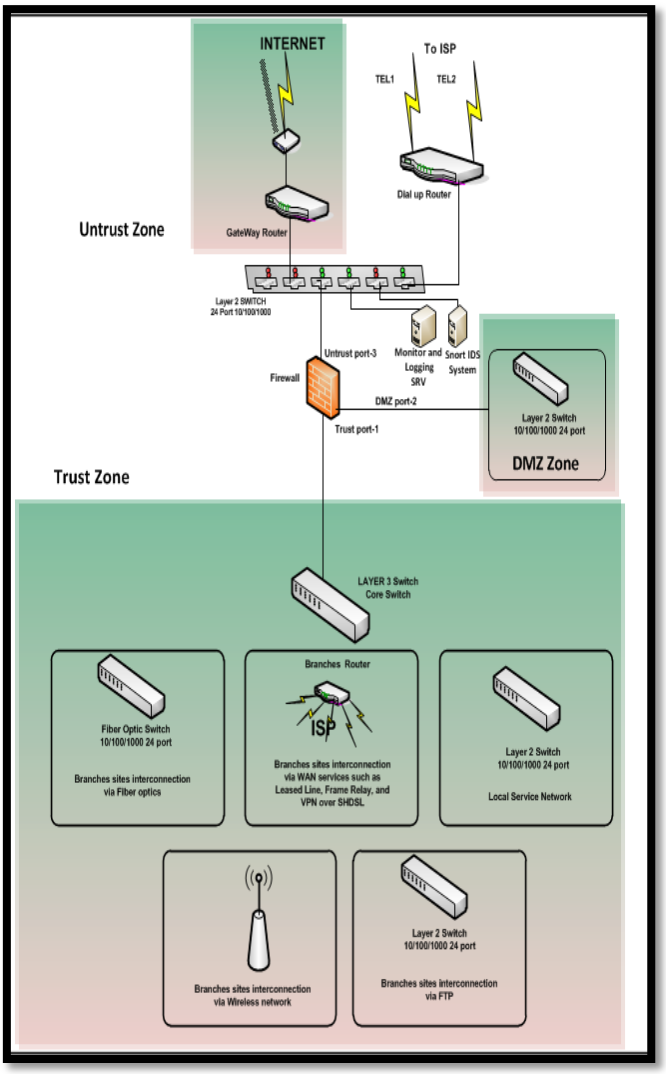

Figure 1:ENM Topology

IV Security Model for ENM

Our proposed model, Security Model (SMEN) for ENM, includes nine modules, see Figure 2

In SMEN model, we provide efficient and secure enterprise network. We use hardware firewall, which includes network intrusion protection system NIPS module. We prefer to place NIPS module inside firewall for the following reasons:

- Reducing budget, one appliance rather than two appliances (firewall and NIPS).
- Reduce false positive alarms that are generated, where no intrusion or attacks.
- Simplifying determination of attacks using real IP addresses and to avoid IP with NAT option.
- Providing intrusion prevention for DMZ network and Internal network.

In addition to NIPS module, the model use SNORT NIDS for monitoring and analysis traffic from/to DMZ and Inter-

nal networks. We intend to get deep inspection of traffic that pass through DMZ and internal networks. We run SNORT NIDS in active response mode in order to prevent potential intrusions and attacks.

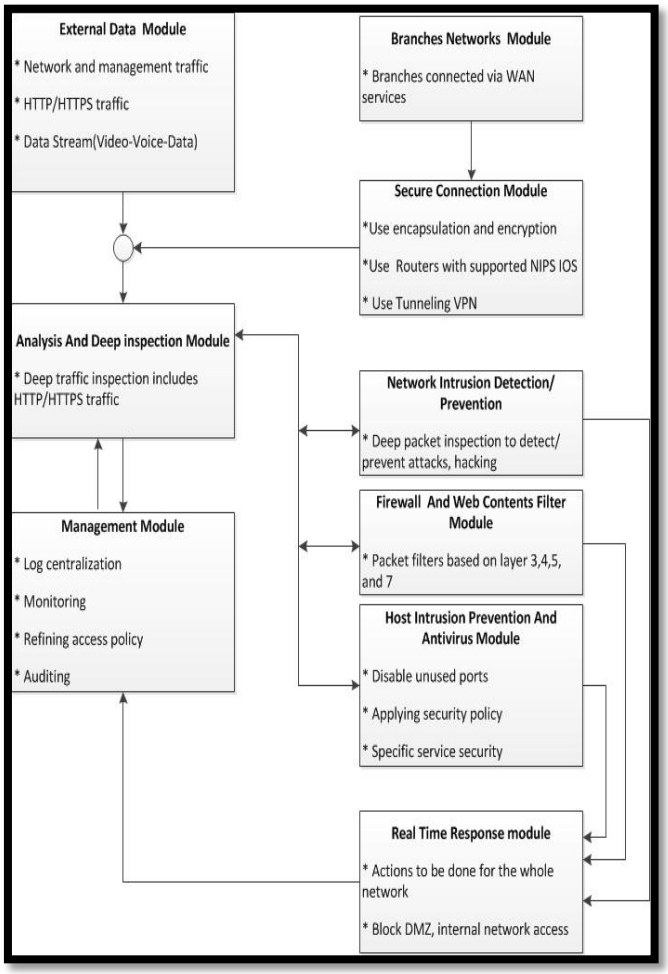

Figure 2:Modules of the proposed security model

Figure 3 shows the proposed SMEN model of enterprise network, it shows the placement of NIPS and NIDS in EN. We implement two SNORT NIDS to monitor real time traffic for DMZ and internal Network. The first SNORT NIDS is connected to both DMZ layer2 switch and to the management network. The second SNORT NIDS is connected to Internal layer 3 switch and to the management network.

It is necessary to provide security for branches networks, this will require NIPS for each branch due to management needs and cost requirements. We prefer to use NIPS module inside router at each branch network to reduce cost and management requirements. Monitoring and management of routers are done remotely from EN management network.

As NIDS and NIPS are not sufficient, the proposed model provides Host Intrusion Prevention System (HIPS) for individual hosts to provide security at servers and hosts level. We use HIPS to protect servers, which host services of enterprise network. HIPS will protect our servers from zero-day attacks. HIPS uses anomaly detection, which provides ability to stop unknown attacks.

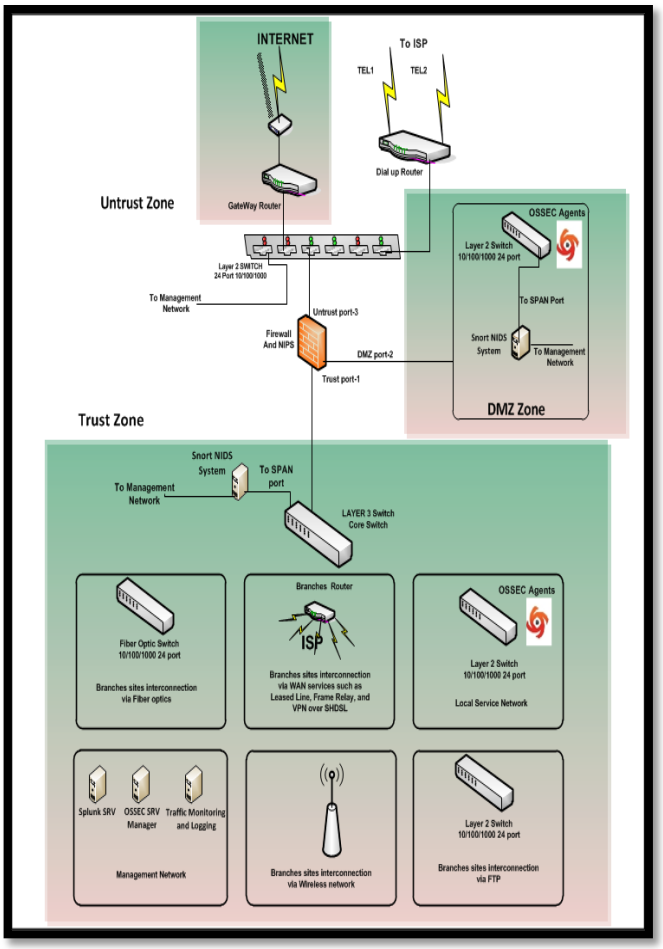

Figure 3:The proposed security model of enterprise network

As shown in Figure 3, we implement OSSEC on each server of our enterprise network, also we have OSSEC server as central management sever for monitoring and analysis real time traffic received from servers (OSSEC agents). OSSEC manger is configured in active response in order to stop malicious activity.

Traffic analysis is considered as the starting point for designing a security model of ENM. We use "NetFlow analyzer professional plus" and MRTG as a traffic analysis tools to perform network traffic analysis. Traffic analysis was done during a work week - five eight-hour days. EN has Internet bandwidth of 150 Mbps, which is provided by a local Internet ServiceProvider ISP. The maximum inbound traffic of Internet usage is about 27.2Mbps (27.2%), while the maximum outbound traffic is about 105.3 Mbps (70.2%). The average inbound traffic of Internet usage is about 20 Mbps (13.33%), where the average outbound traffic is about 85.5

Mbps (57%). We observe that Internet usage is nearly the same for most work days in the week.
EN interconnects its branches via WAN services through bandwidth of 90 Mbps. The maximum inbound traffic used by branches networks is about 11.6 Mbps (12.88%), while the maximum outbound traffic is about 69.7 Mbps (77.44%). The average inbound traffic used by branches networks is about 10.291 Mbps (11.43%), while the average outbound traffic is about60Mbps (66.66%). Also we observe that the traffic used by branches networks is nearly the same for most work days of the week. The percentage of traffic usage byHTTP applications/protocols occupy the most percentage of the total traffic, it is about 93% of the traffic. HTTPS application/protocol is considered to be the second one to consume traffic with about 4% of the total traffic. HTTP applications/protocols occupy the most percentage of the total traffic from branches network to public network (Internet) and/or DMZ network, it is about 64% of the traffic. Users in the branches networks use HTTP protocol to reach public network such as Internet. HTTPS application/protocol is considered to be the second one to consume traffic with about 33% of the total traffic. We observe that HTTPS traffic is fairly large. Other applications/protocols (as we stated previously) consume less than 1% of the total traffic. HTTP applications/protocols occupy the most percentage of the total traffic from one branch network to public network (Internet) and/or DMZ network, it is about 74% of the traffic. HTTPS applications/protocols are considered to be the second one to consume traffic with about 5% of the total traffic. Domain services occupy about 2% of the total traffic, they are used by domain controller for domain management. We have 2% of traffic consumed by Oracle applications, it uses ncube-lm-licenser manager- at port 1521. Custom applications which are programmed and developed by programmers of enterprise network consume less than 1% of the total traffic.
According to our previous traffic analysis of our enterprise network, we observed that most traffic is represented by HTTP/HTTPS applications/protocols. Intrusion Detection and Prevention Systems(IDPS) can inspect layer 7 applications/protocols like HTTP, FTP, and SMTP. Once IDPS detects intrusion, it will apply corresponding actions that we previously defined. Even IDPS provides additional security layer to our enterprise network, it cannot be used alone. We will use firewall beside IDPS system to provide defense in depth strategy for our enterprise network. NIDS never replaces firewall device, encryption, and other authentication methods.

V Implementation and Evaluation

A Implementation

To implement and evaluate performance of proposed SMEN model, we used number of devices and tools. Table 1 describes the devices and tools used.

TABLE 1
Control Rule Base for MPPT Fuzzy

Device Name	Specification	Operating System	Installed Tools
PC1-OSSEC	- CPU: Core i5, 1.8 GHz - RAM: 6GB	Windows 7 OS 64bit	- FreeMeter - OSSEC Agent
P2-No-OSSEC			- FreeMeter
PC3-Metasploit		CentOS 6.3	Metasploit PRO 4.7
SRV-SNORT-DMZ	- Dell PowerEdge 2950 Server - CPU: Intel Xeon 5300 Sequence: Dual Independent 1066MHz; - RAM: 32GB	CentOS 6.3	SNORT 2.9.5.5
SRV-SNORT-Internal			
SRV-OSSEC	- Dell OptiPlex 755 - CPU: Core i5, 1.8 GHz - RAM: 6GB	CentOS 6.3	OSSEC-hids-2.7.1
SRV-SPLUNK			Splunk-6.0
Firewall	FortiGate-3140B firewall with NIPS	FortiGate	FortiGate-3140B

In SMEN proposed model, we used a hardware firewall with integrated IPS module, it is FortiGate-3140B firewall. FortiGate-3140B provides up to 58 Gigabits per second (Gbps) firewall throughput, it includes integrated IPS, application control, user-based policies, and endpoint policy enforcement.
We used SNORT to perform a real time traffic analysis and packet logging on enterprise network. SNORT provides multiple function, it can do protocol analysis, content searching, and content matching [8].
We used OSSEC as HIPS in our proposed model. We prefer OSSEC as HIPS for many reasons, it has the ability to inspect encrypted protocols such as HTTPS traffic. OSSEC is a powerful correlation and analysis engine, it integrates log analysis and does file integrity checking [9]. Moreover, we

can use OSSEC to monitor Windows registry, detect Rootkit using host-based anomaly detection and provide centralized policy enforcement.

In SMEN proposed model, we used OSSEC server with iptables service (Linux firewall) to implement and build host-based intrusion prevention system. In this case OSSEC will act as HIDS, when OSSEC HIPS detects intrusion we will place the IP address into the iptables for a period of time to prevent its access to network. When no more scan activity is present the iptables will drop the IP address from the table.

Open source tools were used in implementing SMEN model of enterprise network. Splunk is an open source free tool that can be integrated with both SNORT NIDS and OSSEC HIPS. When integrated with SNORT, Splunk provides field extractions for SNORT alert logs, dashboards, graphs, event types, tags, correlates real-time data, and reports [10]. We can also integrate Splunk with OSSEC for better correlation of alerts generated by OSSEC. Splunk generates reports for future analysis and management, it displays logs in a graphic format.

B Evaluation

In this section, we evaluate both the defense and performance of proposed SMEN model. For defense evaluation, we used Metasploit tool as penetrating test tool, while bandwidth utilization wasusedfor performance evaluation.

We used Metasploit framework to induce malicious codes and attacks to enterprise network. Metasploit launches 688 different attacks in order to exploit security vulnerability of enterprise network [11]. SMEN model successfullydetects all of these attacks, we havethe recent update signatures for both firewall and SNORT NIDS.

We use personal computerwithout OSSEC (PC2-No-OSSEC) to evaluate bandwidth utilization before applying proposed SMEN model, PC2-No-OSSECis connected directly to Internet service. It bypasses firewall and SNORT NIDS, it has no OSSEC agent.

Figure 4 shows the graph of bandwidth utilization of PC2, Y-axis represents time in seconds, while X-axis represents bandwidth in Megabits (Mb). We can observe that PC2 consumes bandwidth in different ways along time, but generally it consumes little bandwidth. There is no heavy consuming of bandwidth.

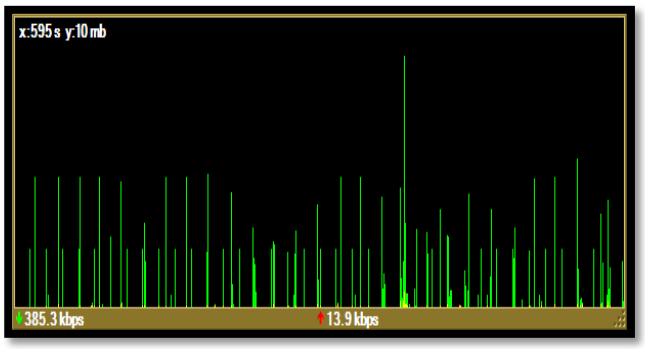

Figure 4: Bandwidth utilization before applying proposed model

A graph of bandwidth utilization after implementing proposed SMEN model is represented in figure 5, a quit few additional amount of bandwidth is consumed. It is almost unnoticeable that OSSEC agent has effects on network bandwidth when compared with Figure 4. Firewall still has more effects on network performance, we have to remember that firewall contains IPS module. OSSEC affects CPU and RAM utilization rather than bandwidth utilization and hence network performance.

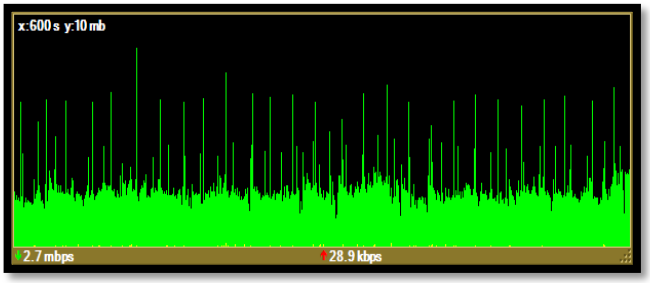

Figure 5: Bandwidth utilization after applyingproposed model

VI CONCLUSION

The proposed Security Model SMEN provides security at different layers. It integrates both hardware and software solutions. We performed a defense evaluation for the proposed SMEN model, the results show that SMEN was able to detect and prevent all attacks and malicious codes that were induced by Metasploit framework. Performance evaluation shows that applying proposed SMEN model has unnoticeable impact on the system's performance and little effects on bandwidth utilization and hence network performance

REFERENCES

[1] S. M. Nadaf, H. K. Rath, and A. Simha, "A novel approach for an enterprise network transformation and optimization," in India Conference (INDICON), 2012 Annual IEEE, 2012, pp. 317-322.

[2] M. Weinstein, "Planning enterprise networks to meet critical business needs," in Enterprise Networking Mini-Conference, 1997. ENM-97. In conjunction with the ICC-97., First IEEE, 1997, pp. 3-13.

[3] E. Dart, L. Rotman, B. Tierney, M. Hester, and J. Zurawski, "The science dmz: A network design pattern for

data-intensive science," in IEEE/ACM Annual SuperComputing Conference (SC13), Denver CO, USA, 2013.
[4] S. Singh, "EtherSec: An Enterprise Ether-network security model," in Networks, 2008. ICON 2008. 16th IEEE International Conference on, 2008, pp. 1-5.
[5] W. Kehe, Z. Tong, L. Wei, and M. Gang, "Security model based on network business security," in Computer Technology and Development, 2009. ICCTD'09. International Conference on, 2009, pp. 577-580.
[6] W. Zongjiang, "A new type of intelligent network security model of the campus study," in Computer Research and Development (ICCRD), 2011 3rd International Conference on, 2011, pp. 325-329.
[7] S. Alabady, "Design and Implementation of a Network Security Model for Cooperative Network," Int. Arab J. e-Technol., vol. 1, pp. 26-36, 2009.
[8] SNORT. (2016, october 1). SNORT | Network Intrusion and Detection System. Available: https://www.snort.org/
[9] OSSEC. (2016, october 1). Home --- OSSEC. Available: http://ossec.github.io/
[10] Splunk. (2016, october 1). Operations Intelligence, Log Management, Application Management, Enterprise Security and Compliance|Splunk. Available: https://www.splunk.com/
[11] Metasploit. (2016, october 1). Penetration Testing Software|metasploit. Available: https://www.metasploit.com/

Dr. Aiman A. Abu Samra is an associate professor at the Computer Engineering Department at the Islamic University of Gaza. He received his PhD degree from the National Technical University of Ukraine in 1996. His research interests include computer networks and mobile computing. Dr. Aiman is a member in the Review Committee of the International Arab Journal of Information Technology (IAJIT)

Eng. Khaled W. Alnaji is graduated from Isalmic University of Gaza (IUG-Gaza), Gaza Strip, Palestine (Bachelor of computer engineering) in 2006. He received the Master of computer engineering from IUG-Gaza, Gaza Strip, Palestine in 2014. He is curently an asscoicate teacher ate University College of applied Sciences (UCAS). His interests: computer networks and network security. E-mail: kalnaji@ucas.edu.ps