Secure IP Network Model

Ł. Apiecionek[1], **M. Romantowski**[2]

[1]*Kazimierz Wielki University, Bydgoszcz, Institute of Technology*
Jana Karola Chodkiewicza 30, 85-064 Bydgoszcz, Poland
E-mail: lapiecionek@ukw.edu.pl

[2] *Warsaw School of Economics*
Niepodległości 162, 02-554 Warszawa, Polska
E-mail: mromantowski@wp.pl

Received: 14 March 2013; revised: 13 September 2013; accepted: 16 September 2013; published online: 16 October 2013

Abstract: Although network security is a common concern in almost every network, it appears that no general model for building safe networks has been proposed. The existing models lack a comprehensive approach to the challenges that need to be faced by a modern, publicly accessible IT system. Such approach requires basing on modern access techniques and security mechanisms combination. The authors of this article conducted an examination of the existing IP-related technologies and developed a general secure network model. In this article a general-purpose layered network model is proposed. The presentation is preceded with a summary of the mentioned research. Additionally, the article contains an evaluation summary of two different military systems that have been created basing on the proposed model. The test has been formally executed during CWIX (Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise) organized by NATO.

Key words: network security, IP network

I. INTRODUCTION

Nowadays, computer networks are deployed at a number of organizations, including state institutions and enterprises. This is due to the significant influence that the information exchange has on many fields of human activity, including national security issues where constant communication is essential. Military trends, especially related to mission command, are focused on improving situation awareness. The aim of the NATO NEC [1] (The North Atlantic Treaty Organization Network Enabled Capability) concept is to create and deploy multinational network-centric systems capable of permanent communication and instant data processing, which will improve the collaboration and enhance the efficiency and effectiveness of the Alliance.

Internet protocols are data transmission protocols that meet the requirements of a network-centric system. Aside from providing efficient communication, the system is required to ensure information processing security. However, recent professional literature lacks a coherent securenetwork architecture model that combines suitable technologies. Due to the fact that the existing approaches do not provide a sufficient security level, the authors decided to present a general secure network architecture. This is a new approach that combines the existing mechanisms into a uniform model. This article considers the problem of building a general purpose secure IP network.

The second section of this article describes the requirements that should be met by IP networks, including network architecture, remote access and commonly deployed mechanisms and solutions. The third part presents the developed model, including ISO/OSI architecture model, hardware and software components and test results of model deployment. The architecture description contains ISO/OSI layers reference, hardware components with a proposed operating scheme. Finally, the architecture evaluation results are presented. The last part of this article covers a summary and conclusions.

II. CURRENT KNOWLEDGE

II. 1. IP network architecture

Securing access to the network itself and its resources is a key factor in designing a network of any kind. It is a common practice to place the substantial components in demilitarized zones (DMZ) of IP networks [2]. These zones are protected by firewalls that provide sophisticated packet filtering and blocking based on their source IP addresses, protocols and port numbers. This kind of device usually goes hand in hand with the Intrusion Prevention System. IPS uses configured packet transmission behavior patterns in order to detect and block suspicious network traffic. Secure internal network resources access as well as data flow control are provided by proxy servers that operate as access gateways for the protected network. Every request made by an external user is transferred through the proxy that transmits packets into the internal network. Remote access to the internal network in a system that is based on multiple physically distributed peers is frequently provided by Virtual Private Networks (VPN). This kind of network connection setup is based on several steps. In the first place, user authentication is performed. After that, encryption keys are negotiated. Only after a successful key negotiation does the external user gain access to the internal private network with the use of encrypted communication. Common encryption protocols are IPSec and SSL.

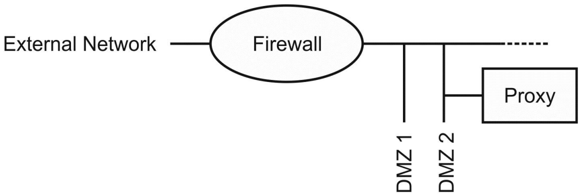

Fig. 1. Common IP network architecture

The existing networks are evaluated using various methodologies against conditions that may expose the given organization to different threats (such as an information leak) [3]. This is a foundation of network security quality assessment. However, such process of examination is time-consuming and it depends on a situation and system application. The commonly used solutions are often susceptible to intruder's actions and do not guarantee a sufficient security level. Therefore, elaboration of a new approach is required in order to achieve enhanced security.

II. 2. IT system requirements

A modern IT system is required to be both secure and accessible remotely from any point of the IP network. These two requirements are hard to fully reconcile. The remote access obliges the owner of the system to protect it against unauthorized access.

Another aspect that makes the security requirements even more complex is related to the latest cooperation schemes such as Cloud Computing. Regardless of a technology that the cloud is built with, the issue of remote user data access always ensues.

The network structure depends significantly on the type of data that is stored and processed in the network. It is clear that the information sensitivity level influences essentially every aspect of an IT system, including hardware and software components.

A further issue is the determination of remote user authorization rules. Depending on the system type and purpose, this may range from granting each authenticated user the access to every available resource to strictly limiting the access to all assets.

It should be mentioned that in some cases both data processing sensitivity and authorization rules have to meet certain law requirements.

In summary, the flawless secure system architecture should be capable of:

- storing and processing data of different types,
- providing remote data access for the authorized user from the outside of the protected system.

For requirements stated as above, two key factors, such as remote and local access scheme as well as protection means that have to be applied, should be determined. The second factor ought to be validated against its sufficiency in an expected deployment scenario.

The designed network usually delivers certain basic services for the end user. This includes the Domain Name System (DNS) service with an internal name resolution server, a web (WWW) server for sharing data, and a mail server.

The placement of the internal network DNS server together with the mail and web servers has its pros and cons. Such solution remains fully operational for the internal users, even after the whole system is disconnected from the external (possibly public) network. On the other hand, providing such services (especially DNS and web) carries the risk of breaking in, as it requires enabling certain communication in order to maintain public network interoperability [4].

II. 3. Current tools and procedures

As it has been stated before, the system can be accessed both from the inside and outside of the IP network. This requires providing dependable authorization and authentication mechanisms and ensuring information integrity, nonrepudiation and confidentiality. The aim of the authentication is the user credibility confirmation, performed before granting any access rights to internal resources. Authorization is a process that grants access to system resources to the users by an application or system owner. Integrity guarantees that the data is not malformed in any way when stored, processed or transmitted. Non-repudiation means that the sender acquires a proof of delivery, whereas the receiver has sender credibility confirmation and none of them can deny that the information has been transmitted. Confidence restricts the access to certain data to a limited group of users.

In order to provide the above described elements, a number of tools was deployed. The first and most essential element is the creation of an individual password protected account for each user. The password has to meet a strict policy that determines password length and other requirements, such as including numerals and special characters.

A resource access policy determines user rights within the system. The policy may be built basing on at least a few technologies:

- Active Directory database combined with theMicrosoft Windows domain,
- XACML (eXtensible Access Control Markup Language) standard,
- Public Key Infrastructure (PKI).

The public key infrastructure is created using the Authorization Center (CA) that determines a general certification policy. In the structure of a single CA for particular appliances there may exist any number of dependent CA and users. Such structure constructs an authentication hierarchy, which in turn determines a certificate chain that leads from the users to the trusted Core CA. The certificates signed by CA are used to authenticate and authorize the users.

The PKI may be combined with an IPSec (Internet Protocol Security) protocol which has been designed as a set of protocols used for creating secure connections and encryption keys exchange between multiple devices.

The protocols that are a part of the IPSec architecture are used to secure IP packet transmission through the network. A separate protocol – Internet Key Exchange (IKE) has been developed to provide the authentication on transmission parties.

The IKE protocol determines a cryptographic authentication and key negotiation methods along with packet formats and states of the Internet Security Association and Key Management Protocol (ISAKMP).

It is common to use ISAKMP and IKE terms interchangeably. The IKE is capable of authenticating communication parties using one of the following methods:

- a static password known to both parties (Pre-Shared Key)
- RSA signs,
- X.509 certificates.

In order to provide remote access to the IP network, it has to be connected to the external system which is presently the Internet network. This connection may additionally be protected by the elements that provide information flow control such as:

- diodes,
- information exchange gateways.

A diode is a one directional network component that isolates connected networks. It prevents from sending the data outside the protected network. In practice, this results in blocking most communication protocols, which means that external network users would be able neither to download nor to upload data to the internal system.

An information exchange gateway has been created and widely described by NATO [5] as a concept of connecting computer systems that operate on different confidentiality levels. The gateway is a bidirectional component capable of:

- securing the internal network from external attacks,
- providing fully controlled information flow basing on a security label that internally stored data is described with.

Strict implementation rules of an exchange gateway have not been imposed by the NATO. This indicates that various development approaches are possible, as long as they fulfill the information exchange protocol requirements [6, 7].

Servers which store data are recommended to be placed in a particular demilitarized zone. The number of zones is not limited by any restriction other than deployed routers capabilities. As a result, depending on information sensitivity, servers may be grouped in multiple zones.

Firewall is a border element that can operate either standalone or as an exchange gateway component [8]. This kind of device may operate as:

- a stateful device,
- a packet filter enabled device,
- a proxy (an application level firewall).

The proxy operates as a data transmission intermediary, as connections are terminated at the proxy server which subsequently passes the queries to the actual server. This process conceals the information about the actual connecting user. Currently, apart from firewalls, anomaly and attack attempt detection systems – Intrusion Prevention System (IPS) – are in use. These systems are capable of determining suspicious traffic and block it with firewall assistance basing on well known attack mechanisms and comparing data transmission with certain signatures. It should be pointed out that in some cases harmless connections are labeled as suspicious and therefore terminated. This obstructs legitimate users accessing the network resources. Still, an IPS and firewall integration is currently one of the most common approaches applied on the network edge.

Concealing information about the internal network (including the IP address space) is a good practice. Either Network Address Translation (NAT) or Port Address Translation (PAT) may be used for such purpose.

III. PRESENTATION OF A SECURE ARCHITECTURE MODEL

III. 1. A layered model

A secure network model, like many other security models [9], may be presented relating to the ISO/OSI layered model. The presented model places the elements in three different layers.

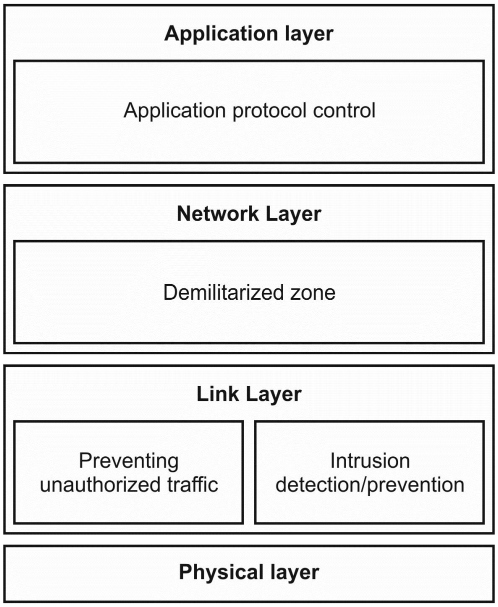
Application layer
Application protocol control
Network Layer
Demilitarized zone
Link Layer
Preventing unauthorized traffic
Intrusion detection/prevention
Physical layer

Fig. 2. Layered model for a secure network

Prohibited transmission protocols blocking, anomaly detection and break in attempts detection should be ensured in the data link layer. On the network layer level, working users should be appropriately separated from sensitive and public servers. The application layer should control the application transmitted data and its sensitivity.

III. 2. An architecture model

While considering a general layered model, it should be pointed out that there are different hardware solutions which after appropriate configuration may execute their tasks successfully. In the data link layer a firewall may be deployed. It enables only known and admitted protocol transmission, while blocking other network traffic. It is a limited trust principle appliance which is expected to accept only the portion of the network traffic which is known to be rather secure. It should be mentioned that modern firewalls and IPS devices are usually capable of providing complex and sophisticated protection mechanisms. However, deploying other layer protections is highly advisable. For the purpose of this article's clarity, the main role of a firewall in the presented model is simplified to data layer protection. On the network layer level, the system may be divided into a number of demilitarized zones, while at the application layer the isolation is reached by deploying proxy services. In this scenario the proxy operates with reverse configuration, which is a new approach to this network application service. Instead of concealing internal network users from the external network, it hides the internal network servers (and their addresses) from the users that work outside the protected network. An ordinary proxy is used as an intermediary that provides access to the external resources for the internal network users. This allows less external bandwidth consumption and internal user IP address coverage. The other way round, a reverse proxy described in the presented model is an intermediary service that makes a certain application server accessible from the external network. From the external user's point of view, a proxy service acts as the original server, while the server itself is directly unreachable. On the other hand, from the application server's point of view, that kind of proxy acts as an ordinal client, as it transfers external network traffic.

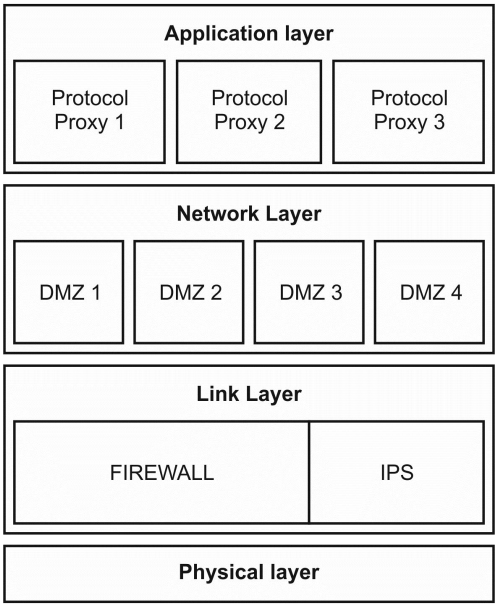

Fig. 3. Architecture model for a secure network

When all above described components are deployed at the same time, a complete routing separation between selected demilitarized zones is achieved, which has not been practiced before. This provides *significantly higher* information loss prevention, especially for cases caused by unauthorized users' operations (i.e. hackers), which could lead to obtaining direct access to the data server.

Most of the existing network security solutions are based on a particular filtering behavior by the firewall device. The presented approach eliminates the IP routing between protected domains and a public network entirely. The actual communication is accomplished with the use of proxy servers.

III. 3. A network equipment model

The proposed secure network architecture model appliance, including insulated demilitarized zones, is presented in Fig. 4.

The presented model appliance contains an internal DNS server and a CA (Certificate Authority). The DATA and

WWW servers have been included in order to show the data servers. The proxy server acts as a traffic control executor.

As it has been stated before, the system allows the external network user to connect remotely. It is obvious that this assumption implies that the system needs to be connected to an external network. The stored data protection requires to:

- divide the users into groups, based on an information subset which they require to have access to,
- determine an access policy that specifies the user groups permitted to download and upload particular data.

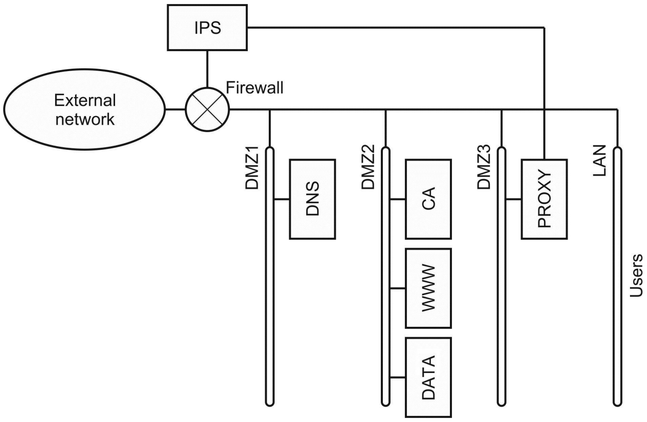

Fig. 4. A secure IP network model

DMZ isolation

In order to preserve continuous operation, an internal DNS server needs to be deployed. IP addresses ought to be assigned dynamically to computer MAC addresses and an EAP user authentication mechanism should be enabled. This allows the network security administrator to identify every computer and ensures that its user has entered a correct access password.

The DNS server with other required servers are recommended to be placed in one of isolated zones (DMZ1). Granting potential access to any of these servers does not result in accessing other zones. Sensitive data servers are deployed at a separate zone (DMZ2) that can be accessed only by internal users.

The access to remote data servers is provided by a proxy server deployed in another zone (DMZ3). The proxy server transfers the external user's queries to the data servers in the protected zone (DMZ2). This ensures that the entire external domain communication is transmitted through the proxy server and the DMZ2 zone access is completely restricted to a potential attacker. Access restriction is simultaneously ensured by:

- firewall rules,
- network routing rules, as the DMZ2 zone's IP network is entirely concealed from the external users, while the address space broadcasting is unavailable.

A new role of proxy

Proxy servers can be deployed for any data exchange protocol. This provides complete control over the capability of the transmitted data [7]. It seems that applying a single proxy server may lead to a communication bottleneck, taking into consideration the increasing user's expectations concerning the transmission bandwidth. Therefore, it is recommended to deploy the proxy servers on multiple computers by maintaining either a separate physical machine for particular protocols or even a cluster of proxy servers. In the first case, the traffic may be routed to a proxy server basing on firewall rules. The second case requires a more complex infrastructure. Detailed explanation of clustering technologies is beyond the scope of this article.

Despite the fact that every application layer protocol requires a dedicated proxy service, its implementation in most cases should not be difficult. Actually, there is a number of proxy server solutions for many communication protocols (for example for HTTP service operating on Linux).

An edge protection

As it has been stated before, a firewall device is deployed on the network edge. Its task is to obstruct any direct communication to internal systems and enable access to particular services, such as DNS and proxy servers. The firewall is combined with an anomaly and attack attempt detection system (IPS) that blocks packet traffic by means of firewall assistance in case a network problem is detected. The IPS module is required to operate with proxy servers placed in demilitarized zone DMZ3. Packet traffic and proxy actions ought to deliver some valuable hints concerning the network state and possible threats to the IPS module. Basing on these additional data, the IPS module decides whether to block dangerous traffic. The IP address space of the internal system is concealed by the NAT mechanism, while the DMZ2 zone is not available from the external network at all, which is achieved by an appropriate IP network routing configuration.

Mobile user access

Remote user access is provided by IPSec tunnels, deployed with an authentication based on an X.509 certificate authentication generated in an internal network zone and a user name and strong password consistent with the secure password policy. The CA server that makes the certificates accessible is placed in a secure DMZ2 zone.

TTL control

Appropriate setting of the IP packet header TTL (Time To Live) field is a valuable mechanism that secures data transmission based on the IP protocol. The field value is decreased in the packet each time it passes a router. A forced setting of the packet field's value at a proxy server limits the number of router devices that the packet may pass. However, transmission over an IPSec tunnel bypasses the router packet hops. When the IPSec tunnel is used, the TTL value does not affect the communication in any way. In case of a data takeover attempt without such tunnel, the TTL field value blocks transmitting the packet by the routers in the network. Therefore, the TTL control is an additional data protection method against unauthorized access.

III. 4. Test results

Current implementation

The proposed secure network model and its derivative versions were possible to be seen in action at the Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise (CWIX) in Bydgoszcz in 2012. The solutions that use gateways, IPS and proxy servers were included:

- Dutch IGB,
- Polish: Information Exchange Gateway JASMINE [6] and Save Information Exchange Gateway (SIEG) [7].

The solutions are capable of providing successful control over the access to the internal network, including information flow control for HTTP (WWW), FTP, SMTP/POP3 and XMPP protocols.

From the point of view of the supported protocol range, the most advanced solution is SIEG which deploys two separate proxy servers and a central XML Guard service that controls the entire traffic. The SIEG was funded by Polish Ministry of Science and Higher Education. The authors of this article were the co-creators of this solution. SIEG architecture is presented in Fig. 5. NPS, which stands for Node Protection System, is a subsystem that contains a firewall and an IPS.

The IEG JASMINE solution also provides a number of common military specific protocols control capability.

Test description

The test scenario of the described internal domain security solutions contained the evaluation of:

- capability of correct information exchange with an external system,
- the level of system security.

The tested protocols included:

- HTTP,
- SMTP/POP3,
- XMPP.

The tests were performed in a multinational environment with a number of military network systems delivered by various countries (Germany, Canada, Poland, Finland) and NATO.

All tests proved that the SIEG system is capable of establishing a remote connection from an external system with proper data transmission, preserving a desirable protocol compliance level. Confidential (sensitive) data is never transmitted to an external network. At the same time, the blocking process does not affect the communication channel operation. The external user obtains a message compliant with the particular protocol, which informs him that the security policy execution has made accessing the requested resource impossible.

It is noteworthy that the communication process revealed no significant transmission delays, even though they have been expected. Actually, the differences in either sending

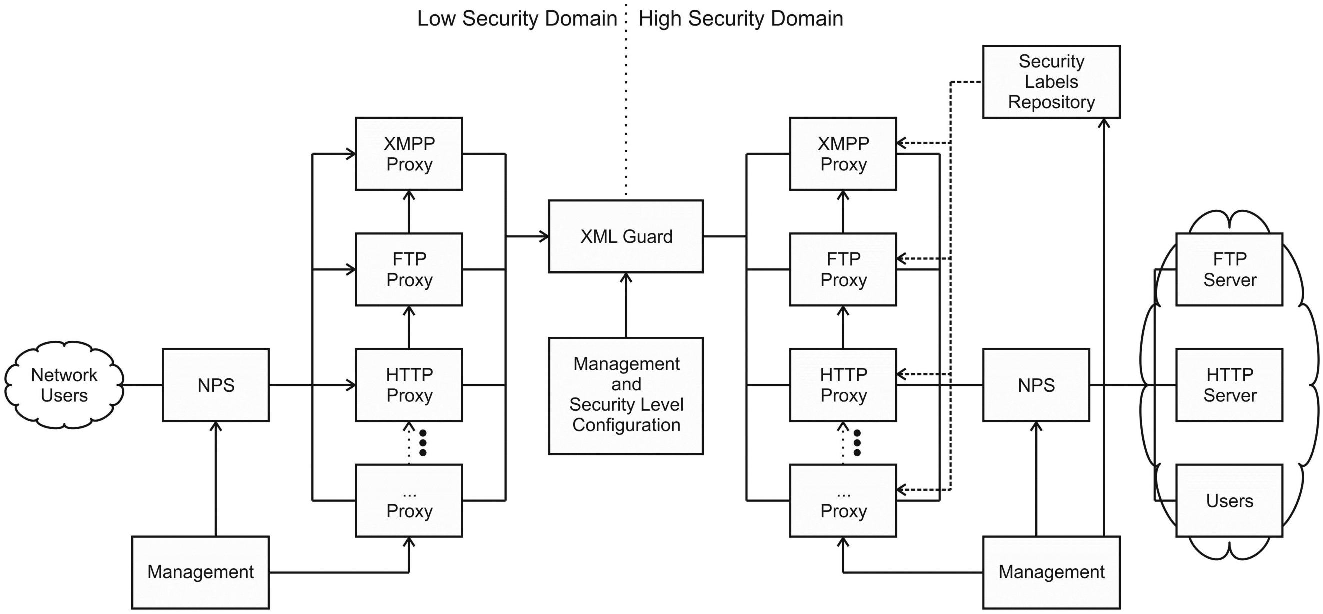

Fig. 5. SIEG architecture [7]

and delivering email messages or browsing web pages are imperceptible.

The system security level has been evaluated by performing an open port and IP addresses scan as well as potential gaps investigation. No threats have been found in the described system. This confirms the possibility of deploying the presented secure network model in military areas, as it fulfills their elevated security requirements.

IV. CONCLUSIONS

The exact specification of secure network architecture is a difficult task. The continuous evolution of network technologies brings also new threats and attack techniques. However, it is possible to obstruct unauthorized resource access attempts by deploying appropriate protections. Obviously, the proposed network architecture is one of them. The presented concept of combining three layer network components is a fresh and comprehensive approach to network security. The innovation is based on the idea of deploying a proxy server for controlling remote user network resource access. Isolating the network by disabling the routing protocol between separate DMZ zones and a TTL field value manipulation allows to build a secure network system using common mechanisms. This reinforces the existing means in a struggle against hackers. The literature related to the existing network security hardly describes combining such isolation mechanisms as: proxy, isolating DMZs by disabling IP protocol routing between them and a TTL field value manipulation. This concept brings three ISO/OSI model layer settings together. It should be pointed out that the presented architecture requires specific proxy servers implementation for particular communication protocols.

Nevertheless, a human user is considered the weakest point in the security matters. It is a common issue that the user, in order to simplify his/her work expense (by setting a simple, weak password or in another way) introduces security risks to the computer systems. The proposed model takes this natural susceptibility into consideration and limits its possible effects by applying adequate architecture level restrictions.

References

[1] ISSC NATO Open Systems Working Group, Allied Data Publication 34(ADatP-34) NATO C3 *Technical Architecture* Volume 2. *Architectural Descriptions and Models.* Version 7.0, 15.XII.2005

[2] D. Minoli, *Security in an IPv6 Environment*, Auerbach Publications 2009, Print ISBN: 978-1-4200-9229-5, eBook ISBN: 978-1-4200-9230-1

[3] J.K. Tudor, *Information Security Architecture. An Integrated Approach to Security in the Organization*, Auerbach Publications 2001, Print ISBN: 978-0-8493-9988-6, eBook ISBN: 978-1-4200-3103-4

[4] S. McClure, Scambray J., Kurtz G., Hacking Exposed Fifth Edition: *Network Security Secrets & Solutions*, Osborne, California 2005, ISBN 0-07-226081-5

[5] Guidance document on the implementation of gateways for information exchange between NATO and external CIS communities" version 1.21 dated 16th February 2007, AC/322(SC/4)N(2007)0007, MULTI REF

[6] Ł. Apiecionek, M. Woźniak, M. Romantowski, W. Znaniecki, *Information assurance in coalition mission environment*, Military Communications and Information Systems Conference (MCC), Wrocław 27-29.09.2010

[7] Ł. Apiecionek, M. Romantowski, J. Śliwa, B. Jasiul, R. Goniacz, *Safe Exchange of Information for Civil-Military Operations.* MCC 2011: Military Communications and Information Systems Conference, Amsterdam, 17-18.10.2011. w: Military Communications and Information Technology: A Comprehensive Approach Enabler. Pod redakcją Marka Amanowicza. Warszawa: Redakcja Wydawnictw Wojskowej Akademii Technicznej, 2011. ISBN 978-83-62954-20-9, s. 39-50 (MK-312)

[8] Olson R., *Cyber Security Essentials*, Auerbach Publications, Pages 1-70, Print ISBN: 978-1-4398-5123-4, eBook ISBN: 978-1-4398-5126-5, DOI: 10.1201/b10485-2

[9] M. Chiang, A.R. Calderbank, *Layering as Optimization Decomposition: A Mathematical Theory of Network Architectures*, Proc. of the IEEE, vol. 95, pp. 255-312, January 2007

Ł. Apiecionek is presently an assistant professor at the Kazimierz Wielki University. He received his MSc Eng Degree in 2003 at the Academy of Technology and Agriculture and has been a holder of PhD degree gained at the Institute of Fundamental Technological Research Polish Academy of Science since 2011. His research interests focus on analysis, design, control and security of IT networks.

M. Romantowski completed his PhD studies at the Warsaw School of Economics in 2012. He graduated from Information Technology and Econometrics at the Poznan University of Economics and received an MSc in 2007. He has worked as a software developer, architect and coordinator in SME, banking and military industries. His research interest is business data exchange, interoperability, communication protocols and security.

DOI:10.12921/cmst.2013.19.4.209-216