*Information & Security: An International Journal*

V. Aleksandrova et al., v.39:3, 2018, 275-285 https://doi.org/10.11610/isij.3923

# INTERFACE SOLUTIONS FOR IMPROVING INFORMATION INTEROPERABILITY IN THE CONDITIONS OF HYBRID THREATS

Veselina ALEKSANDROVA, Miroslav KOCHANKOV,
Vanya TAGAREVA, Anna GUNCHEVA, and Violeta VASILEVA

**Abstract**: In this article the authors offer interface alternatives and solutions for the information exchange in the infrastructure of cyber domains. Information interoperability is seen as a guarantee for secure information transfer related to the development of capabilities to counter hybrid threats. This is achievable when NATO interoperability directives are strictly followed. Technical interface gateways are proposed which allow change of data character in a heterogeneous environment as well as information exchange gateways in an environment with various security domains in order to check and filter information.

**Keywords**: information interoperability, interface solutions, information exchange gateways.

Interoperability of information infrastructure is necessary for achieving information transfer between different elements of the deployed joint forces or in conducting multinational operations with allied forces. Operations will not be effective and may not be successful until interoperability between communications and information systems (CIS) is not achieved. It allows the commander to implement the process of command and control and makes possible to coordinate the activities of all elements of allied forces. Another important aspect of interoperability is achieving a balance between interoperability and security measures. This is realised by observing NATO directives in conducting multinational operations.

## Information Exchange Gateways

For achieving interoperability among NATO countries, the following methods are applied:

- Technical standards – formal agreements applied by the participating countries. They are applied in the planning and design of the system, the purchase of its elements (which should meet the requirements). Standards for technical and operational procedures are also followed.

- Operational and configurations procedures. These are rules which allow the technically capable for information exchange communication and information systems to be preconfigured, to apply mechanisms after an agreement and a filed request following established procedures.
- Gateways are communication or computer interfaces that solve the problems related to the technical and procedural interoperability.

There are two main types of gateways:

- Technical interface gateways which change the nature of data in order to materialise exchange of data between the CIS and various types of equipment;
- Information Exchange Gateways (IEG) in an environment with various security domains in order to check and filter information.

These gateways serve to connect the various security domains in order to check and filter information which can be exchanged among them. These Information Exchange Gateways are defined in NATO and are included in NATO Interoperability Directive. Their function is to maintain and facilitate information exchange between NATO systems and between NATO and the participating nations. Each Information Exchange Gateway consists of two modules for interaction in the zone Co-operative Zone Modules (CZM) interconnected by secure communications (see Figure 1).[1]

Each module contains such elements as Boundary Protection Devices (BPD), Message Transfer Agents (MTA), Directive Service Agents (DSA) and Intrusion Detection Systems (IDS). They are designed with the possibility to be upgraded in order to satisfy the information exchange requirements for a future period of time. Each IEG is used in the following three cases described by NATO:

- Case A provides for maintaining a connection between two NATO Secret (Automation Information System) AIS within a national headquarters.
- Case B supports the connection of NATO Secret AIS to member nation’s secret CCIS operating at the national Secret level inside a national headquarter.
- Case C is about maintaining a connection between a NATO Secret AIS with AIS to non-NATO nations Secret or NATO Unclassified systems.

The function of each module in the Co-operative Zone Modules (CZM) is related to the following.

A Boundary Protection Device (BPD) is a firewall ensuring protection which is outlined in the NATO handbook for providing “self-protection” of the device.

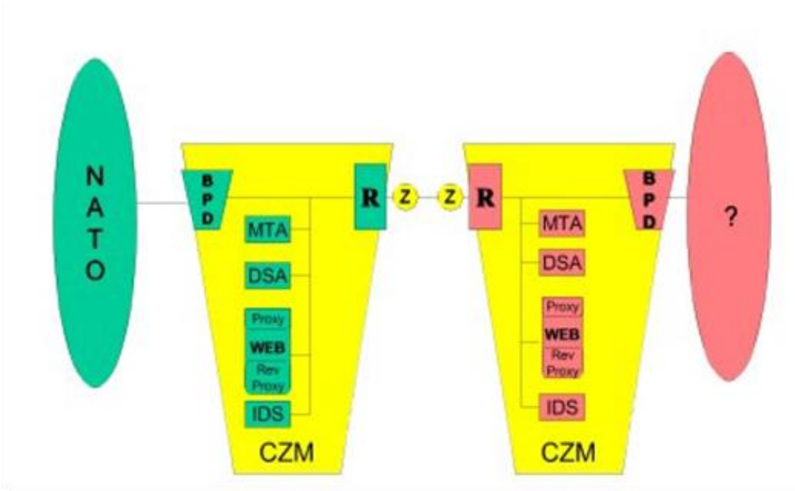

**Figure 1: Interface (Gateway) for information exchange among NATO users.**

A second Boundary Protection Device is a filtering router which controls and protects network routes, protocols and ports to other zones at level IP to IP.

Intrusion Detection Systems (IDS) is for detecting an unauthorized access to the system and other shortages regarding security. It is designed to recognize potential threats for the system. An IDS supervises the traffic between the zones in both directions, intercepts incidents and trials for manipulation against proxy servers and security components.

Proxy servers redirect the traffic from / to the source / destination through BPD.

Message exchange service is based on the X-400 protocol, where each zone contains Message Transfer Agents (MTA). There are two X-400 connectors for linking with the local Message Transfer Agents – MTA and with the relevant connected zone.

### *Case C – Exchange of Information and Files Between a High Security Level and a Low Security Level Domains*

The main elements for messages and files exchange between domains with high and low security level are indicated below.

Node Protection Service (NPS) – This is a service for node protection; it is a boundary element in the Safe Information Exchange Gateway (SIEG) architecture. Its main task is intercepting an unauthorized access to the network. Interception systems and anti-intrusion systems are used.

Another element of SIEG architecture are the protocol proxies. Each of them is designed for strictly defined protocols: Hyper Text Transfer Protocol (HTTP), File Transfer Protocol (FTP) which convert dataflow in HTTP/SOAP (Simple Object Access Protocol) containing security labels. Some of the conveyed messages may contain security labels and for those who do not have special mechanism in the SIEG architecture is provided for labelling. A label can be received from the used protocol or by the Security Label Repository (SLR). Label meta data of security labels determine the minimum level of security where data can be transferred. The SIEG administrator can add labels on user request.

The security attributes are: owner, security classifications, category.

Classification determines labels and takes values: TOP SECRET, SECRET, RESTRICTED, CONFIDENTIAL, and UNCLASSIFIED.

The XML guard, which is a component in the SIEG architecture, is responsible for the execution of security policies in data exchange. This is the only element which physically connects both domains.

Extensible Messaging and Presence protocol (XMPP) is an open protocol for real-time communications. It provides message exchange, voice and video communication, interaction, combining content. The specification for that protocol are RFC 3920, RFC 3921[0].

Exchange of information and files between a high security level with a low level security domain is presented in Figure 2.**Error! Reference source not found.** When a user of high level security domain sends a message to a server in a low level security domain, the data flow will be as follows:

- User from high level security domain sends a message to XMPP server found in a low security level domain, the first element of SIEG is NPS. XMPP message must be sent to an IP address of the NPS node.
- The NPS node receives data, recognize XMPP traffic based on TCP port and protocol, and sends it to the XMPP proxy in the high-level security domain.
- The XMPP proxy converts a XMPP message in a unified format HTTP/SOAP formatted message and sends it to the XML guard. XMPP maintains labelling and for this reason it is not necessary for the proxy to put labels, it has already been labelled.
- The XML guard interprets the HTTP/SOAP message, checks the security label and the guard information. When the security label is valid and the security policies permit this type of data transfer out of the high-level security

domain, the message is sent to the XMPP proxy of the low-level security domain. Otherwise, the XML guard rejects the message.

- The XMPP proxy of the low-level security domain converts the message received from the HTTP/SOAP in the original XMPP protocol flow and sends it to the NPS on its side.
- The NPS checks if the received data could pass through the SIEG according to the IP packages filtering rules.

The XMPP message leaves the SIEG and can be reached by XMPP client of the low-level security domain.

Such type of solution gives the opportunity for message control by using protocols which have the advantages of XMPP. This protocol, used in combination with the SIEG, allows a set of scenarios to be created for information exchange between military and non-military structures such as police, emergency centres and government organizations. It is assumed that user applications apply appropriate technologies for message labelling, which the XML guard will recognize as valid and at the same time coming from a reliable source.

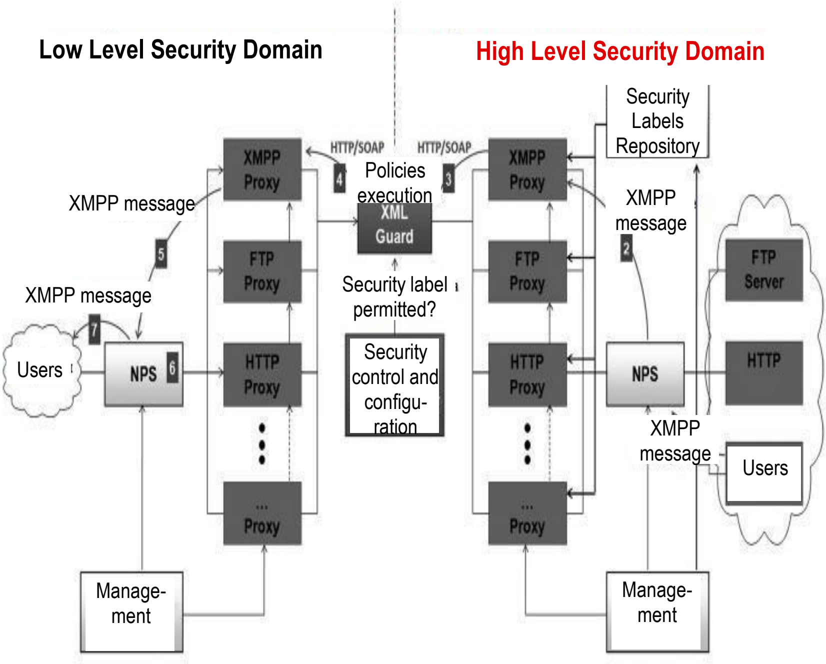

**Figure 2: Exchange of information and files between a high-level security with a low-level security domain.**

### *A Document Exchange Portal Interface Solution*

A scenario of document exchange from low-level security domain that tries to get access to documents from the WEB portal of a high-level security domain is presented on Figure 3.

When a low security level domain user tries to access the document from high level security domain WEB portal, the data flow is as follows:

1. A user from the low-level security domain is connected to a proper IP address and a port number of NPS node of the low security level domain;
2. The node recognizes the protocol based on the TCP\IP port and the protocol information and transfers the connection to the WEB proxy of the low security level domain;
3. The low-level security domain WEB proxy processes the GET message into a HTTP/SOAP message and sends it to the XML guard;
4. The XML guard checks HTTP/SOAP message security labels and security policies configuration;
5. If the security label is appropriate, the message is sent to the WEB proxy of the high security level domain.
6. The high-level security domain WEB proxy converts the message in its original type and sends it through the NPS to the WEB portal from which a user wants to download a document;
7. The documents are sent through the NPS to the WEB proxy of the high security level domain;
8. The proxy server checks if all documents have the necessary security labels and, if they do not have the security label, query is issued to the SLR for all documents which have to be transferred but do not have relevant security labels;
9. After receiving the necessary security labels, the proxy converts the message into a HTTP/SOAP message and sends it to the XML guard;
10. The XML guard checks the security labels of the HTTP/SOAP message and checks the security policies configuration;
11. If the security labels are appropriate, the message is sent to the WEB proxy of the low security level domain;
12. The low-level security domain WEB proxy converts the HTTP/SOAP message in its original type and sends it through the NPS to the user;
13. NPS checks if the received data can pass through SIEG according to the rules of filtering IP packets;

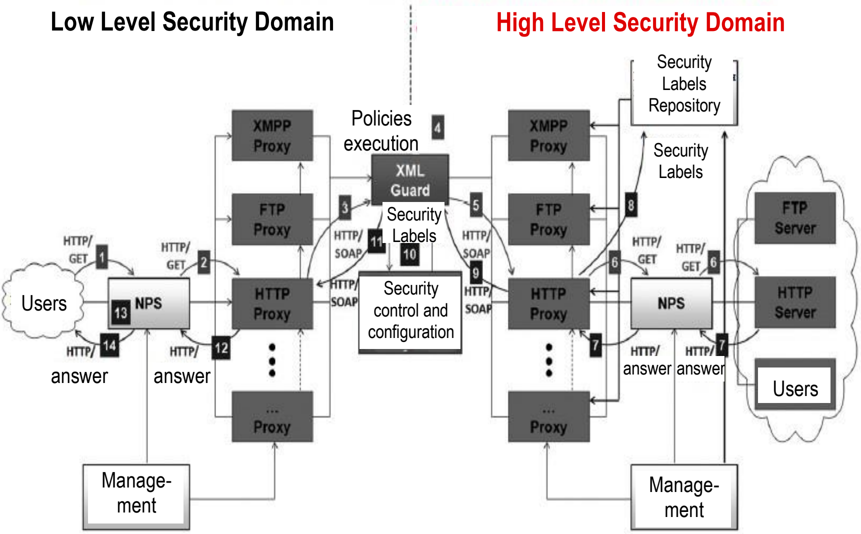

**Figure 3: Documents exchange portal. Documents exchange from low-level security domain to documents in the WEB portal located in the high security level domain.**

14. The document leaves SIEG and reaches the user in the low security level domain.

## *Development of Technologies for Information Exchange*

The tested and approved gateways configuration for information exchange from Allied Systems Interoperability Testbed (ASIT) is regarded as basic. Further development in the following technological spheres is envisaged:

- Adding functional services;
- Adding security services by tightening security measures and gateway development in cases two and three;
- Development of basic services.

Adding functional services is a requirement which is dependent on the development in the following fields: spreading of existing interfaces from and to NATO nations and coalition partners; deployment of new alliance systems; operational requirements resulting in the necessity of new functional services. For example, application of the new system for messages exchange (NATO Messaging Services – NMS) poses a requirement for additional services for a transfer through the zone for maintaining the system for military messages and to NATO infrastructure with a public key access.

The same applies to the video transfer in real time, videoconference services, distributed databases, and web services.

### Nexor Information Exchange Gateway

The architecture of Information Exchange Gateways according to the Nexor white book “NATO Information Exchange Gateways, Reference Architecture” consists of the following main elements: [3]

- proxy servers supporting different types protocols;
- firewalls, routers and switches;
- intrusion detection system (IDS);
- management system; and
- protection systems.

Information exchange in Nexor IEG is made possible through the use of proxies which allow data transfer for specific protocols through the gateway.

*Nexor Mailer (Email Proxy Server)* – provides exchange of e-mail and uses SMTP or X.400 protocols. Nexor Mailer is a proved agent for email exchange, which is used in government and defence systems worldwide. It is designed as a modular architecture that serves a base for security, reliability and scalability. Messages are exchanged through single channels which are required and initiated and, in the same time, the channels can increase automatically for ensuring the necessary load. This architecture for single messages ensures an independent storage of each processed message from the other messages. This approach is based on the stability of the operational system; it does not rely on databases which can be victims of intrusion victim, which that can in turn affect all other messages.

Nexor Mailer maintains many technologies for guarantying secure messages exchange including:

- Authentication – supports X.400 and SMTP protocols;
- Security labels – supports security labels transfer between different formats including “first level of text” (FLOT);
- Content check – supports the verification of the header and the main body of the message for the given key words;
- Viruses check – supports virus scanners;
- SPAM recognition – supports authorization policies, using lists of authorized and blocked addresses, checking also external anti-spam like Realtime Blackhole List (RBL).

*Nexor Mailer management system* – supports SNMP for distant supervision and has graphical user interface for remote supervision and control of the information flow. Nexor Mailer supports detailed log file which can be used against intrusion.

*Nexor Centurion* (server for standard messages exchange) provides formalized messages exchange and uses X. 400 protocol. If necessary, additional security could be provided by using S/MIME v3 according to STANAG 4406 (NATO Standard for Military Messaging) and other related standards. NATO Messaging System – NMS provides standard message exchange.

### *Applications for Information Security*

These applications check the data and, after they prove to be suitable, are admitted into the internal domain.

The Security system (Nexor Sentinel Mail Guard) does admit exit of management messages outside the internal domain, while checking the entering messages for the presence of attached malware. Nexor Sentinel is used in NATO, when email security functionalities are provided. It supports X.400 и SMTP protocols, both in protected and non-protected scenarios.

### *Filters*

Nexor Sentinel can be used with different filters that can be configured to ensure messages access into the domain and exit of the domain.

The filters include:

- Labels check in order to guarantee that labels attached to the messages are appropriate for accepting. Different parts of the messages are checked including First Line of Text (FLOT), X. 400 P1 shell, STANAG 4406 P772 content and S/MIME v3 ESS. Nexor Sentinel also supports labels with different format – from unstructured text to binary ASN labels in X.411, SDN.801 and X.841 formats. According to the configured security policies, Nexor Sentinel will guarantee that there will be a label, that this label is valid and that in the message there is no other label which will dominate. It also guarantees that every Microsoft Office attached file has valid security labels.
- Signature check and encrypting which guarantee that each S/MIME or PCT signature and/or encrypting attached to the message are valid.
- A check that only valid attached files leave or enter the domain. The content of attached zip files is checked, too.
- A check for presence of keywords guarantees that there are no forbidden words which leave the domain with a given message.

- A check for presence of viruses and malware codes.

### *Management Subsystem*

That subsystem guarantees that Information Exchange Gateways components are managed in a secure and reliable way. Nexor Provost (Security Policy Management) contains Security Policy Information File (SPIF) which describes the security policies in the organization or in the domain. Nexor Provost has a graphical user interface and allows the administrator to create and distribute SPIF. The SPIF file has a digital signature as well and can be stored and sent through Lightweight Directory Access Protocol (LDAP). Nexor Mailer Monitor (Messaging Management) serves for monitoring and management of messages. The graphic interface allows the administrator to monitor the queues of many servers for message exchange through just one application. This allows the administrator to monitor the traffic of formatted and unformatted messages of the proxy as well as the security system. Mailer Monitor quickly indicates the status of the system and problematic areas. If necessary, it can hold the queues with queries and to eliminate suspicious messages.

## Conclusion

In conclusion, we have proposed here interface solutions for the exchange of information in the infrastructure of different cyber domains. The topic would be interesting because the offered technical interface gateways and their software implementation could successfully be used to improve the organization of information exchange among various security domains in the infrastructure of a heterogeneous environment and thus to improve interoperability in the conditions of hybrid threats.

## Bibliography

1. “NATO C3 Technical Architecture,” Allied Data Publication 34 (ADatP-34), Volume 2, Architectural Descriptions and Models, Version 6.0 (ISSC NATO Open Systems Working Group, 2004).
2. Łukasz Apiecionek and Michał Romantowski, “Secure IP Network Model, Computational Method,” *Science and Technology* 19, no. 4 (2013): 209-213.
3. Information Exchange Gateways: Reference Architecture, A Nexor White Paper (Nexor, 2009), https://nexor.com, accessed November 3, 2016.
4. “Extensible Messaging and Presence Protocol (XMPP): Core (RFC 3920),” (Jabber Software Foundation, October 2004).
5. “Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence (RFC 3921)” (Jabber Software Foundation, October 2004).

## About the Authors

Veselina ALEKSANDROVA, Ph.D., is an associate professor in the "Communications and Information Systems" department at the "G.S. Rakovski" National Defence College in Sofia. She holds a master degree in Computer Science from the Technical University of Sofia and Ph.D. degree from the "G. S. Rakovski" National Defence College. Her main research interests are in the field of information systems in security and defence, analyses, system design and integration, networking, and cybersecurity.

Miroslav KOCHANKOV is a major from the Bulgarian Armed Forces. He serves as a senior expert in the Land Forces Command. He holds a master degree in the professional field "Military Affairs" – "Organization and Contol of Military Operations at Operational Level," specialization "Communications and Information Systems" from the "G. S. Rakovski" National Defence College. He has field experience in implementing and maintaining communications and information systems for security and defence, interoperability and integration at multinational level.

Vanya TAGAREVA, Ph.D., holds a master degree in security and defence management from the "G. S. Rakovski" National Defence College, and a Ph.D. degree in the field of public communications and information sciences from the University of Library Studies and Information Technologies. Her research interests are in the field of interagency cooperation and organizational management.

Anna GUNCHEVA, Ph.D., is a tester and leader of the STANAG testing team of the Department of Distance Learning, Language Training and Qualification at the "G.S. Rakovski" National Defence College. She holds a Ph.D. degree from the same institution. Her main research interests are in the field of international cooperation regarding computer adaptive testing methodologies and implementation of advanced information technologies in the field of education and testing, as well as cybersecurity.

Violeta VASILEVA holds a master degree in Business Intelligence and Process Management from Berlin School of Economics and Law. She has been involved in working with German-based start-ups entrepreneurial hubs and corporations, supporting projects for innovation and digitalization. She has experience with business development activities, developing ideas and implementing strategies, both for businesses and NGOs. She also has experience in working for the EU Commission on projects and programs covering the Digital Single Market.