2012 IEEE International Conference on Green Computing and Communications, Conference on Internet of Things, and Conference on Cyber, Physical and Social Computing

The Ontological Approach for SIEM Data Repository Implementation

Igor Kotenko, Olga Polubelova and Igor Saenko
Laboratory of Computer Security Problems
St.Petersburg Institute for Informatics and Automation (SPIIRAS)
39, 14th Liniya, Saint-Petersburg, Russia
{ivkote, ovp, ibsaen}@comsec.spb.ru

***Abstract*—The technology of Security Information and Event Management (SIEM) becomes one of the most important research applications in the area of computer network security, including distributed networks of internet enabled objects (as in the Internet of Things). The overall functionality of SIEM systems depends largely on the quality of solutions implemented at the data storage level, which is purposed for the representation of heterogeneous security events, their storage in the data repository and the extraction of relevant data for the analytical modules of SIEM systems. An ontological approach at present becomes more applicable for realizing these tasks in various spheres of information security. The paper discusses the possibilities of applying the ontological approach for implementation of the data repository of SIEM systems for distributed networks of Internet enabled objects. Based on the analysis of existing SIEM systems and standards, the choice of ontological approach is done, an example of the ontological data model of vulnerabilities is presented, a hybrid architecture of the ontological repository is proposed and the issues of developing and testing the repository for attack modelling and secure evaluation tasks are discussed.**

Keywords-ontology; security information and event management; data model; data representation; logical inference; repository

I. INTRODUCTION

The technology of *Security Information and Events Management* (SIEM) becomes at present one of the most important research ways in the area of computer network security. The essence of this technology is to provide an ordered collection of security logs records (*security events*) from a variety of sources, their long- and short-term storage in a centralized data repository in a common format for modeling and analysis to detect and predict attacks and developing countermeasures. Data analysis in SIEM systems is based, as rule, on the methods of event correlation, data mining, logical reasoning and data visualization.

The usage of SIEM systems has particular importance for a large variety of information infrastructures such as *distributed networks of Internet enabled objects* (the Internet of things). The examples of such networks, which were analyzed in our work, are the distributed computer network of transnational corporation, the infrastructure of mobile money transfer service and critical infrastructures, such as dams and power plants, where embedded devices and sensors are connected with data centers and servers by the Internet or mobile networks [1]. Existing well-known SIEM systems have multiple constraints of their usage in above networks and infrastructures. The most significant their limitations are low scalability, restrictions on functions imposed the trust infrastructure, the inability of an agreed interpretation of the incidents and events at various levels, and the impossibility to provide high reliability and fault tolerance in distributed environments to capture event data.

To avoid the above shortcomings and ensure the effective application of SIEM technology for distributed networks of Internet things, the development of forward-looking SIEM systems is required. In other words, we need the development of new generation SIEM systems, which remove functional infrastructure restrictions and have the ability to correlate events in cross-domain manner, high reliability and durability of event data, and high scalability.

The data repository is the main component of new generation SEIM systems, which is purposed for the representation of heterogeneous security events in uniform internal format, their storage in accordance with the previously developed data model and supporting the extraction of relevant data for SIEM analytical modules. The overall functionality of the SIEM system depends largely on the quality of the solutions adopted in the repository implementation. An ability of the new generation SIEM systems to meet these requirements when they operate in distributed networks depends on the approach that is used for *data repository implementation.*

In our opinion, the *ontological approach* is one of the most appropriate for this goal. This approach involves the use of a formalized description of the subject area based on description logics, known as *ontology* [2].

Ontological approach now is increasingly used in many technical areas, including in the field of information security. We assume that this approach is also promising for the development of new generation SIEM systems. A confirmation of the fairness of this idea, the analysis of possible solutions and the demonstration of the data repository implementation is the main goals of the paper.

The rest of the paper is organized as follow. In *Section II* we present the review of related work in the field of applying the ontology approach for information security. In *Section III* we analyze existing SIEM systems and standards. In *Section IV* we select the ontological approach for our goals. *Section V* describes our proposals for ontological data model. In *Section VI* we discuss the results of implementation of the ontological repository. *Section VII* concludes our results.

978-0-7695-4865-4/12 $26.00 © 2012 IEEE
DOI 10.1109/GreenCom.2012.125

II. Related Work

The analysis of works on applying the ontologies for network security helped us to select the following basic directions that can be used for the generation SIEM systems: verification of security policies, intrusion detection, vulnerability analysis, security monitoring and forensics.

The greatest popularity is the use of ontologies for verification of security policies, especially in the area of access control. Cruz et al. [3] propose an ontology forming the formal basis to model the dynamic aspects of role-based access control. The information infrastructure of the Olympic Games is used as the scenario to assess the proposed approach. This use case is well suited to test the SIEM capabilities. Therefore, the positive results from this work certify our ideas.

Da Silva et al. [4] present a security ontology that is used to extract knowledge from natural texts. This ontology consists of a dictionary for natural language domain and a special kind of ontology descriptions, which describe the structure of the logical equations of texts.

Kolovski et al. [5] and Rochaeli et al. [6] propose an ontological approach to engineering the security policies, using the ontological "services-actors-resources" model and the paradigm of ontological templates respectively. These works showed the preference of the ontological approach in comparison with other ones, in particular, with an approach based on propositional logic.

Fitzgerald et al. [7] propose an ontological approach for configuring the firewall management policy for Linux Netfilter. The results demonstrate that this approach is a reliable, convenient and automated.

Rochaeli et al. [8] propose an ontological approach to construct the knowledge representation system for computers and their vulnerabilities modelling. Concepts and roles are described to represent the dependencies between the computer model and the communication mechanisms that have known vulnerabilities.

Schatz et al. [9] show that ontology is an effective tool for domain-specific event-based knowledge, which in the case of unification with the language rules is sufficient to apply the standard methods of correlation in the automated forensics. This is the case of cross-domain correlation. The proposed approach integrates the ontology of standardized components that can simulate particular domains. The approach is applied to the scenarios including the enterprise resource transactions and computer security events.

Kenaza et al. [10] suggests the use of an ontology to provide contextual security event monitoring and intrusion detection. The ontology is used on data preprocessing phase to convert a set of warnings into a set of formatted data.

Thus, the review of work in applying the ontologies for network security shows a set of successful cases. For this reason, we consider that the ontology based approach may also be acceptable and promising for security event presentation and storage in SIEM systems.

The main contribution of our paper is applying the ontological approach for implementation of the data repository of SIEM systems.

III. Existing SIEM Systems and Standards

We investigated the most interesting solutions in data representation and storage in *existing well-known SIEM systems*. For these goals we have chosen OSSIM AlienVault, Cisco AccelOps, QRadar, Prelude, ArcSight Logger, IBM Tivoli SIEM, and Novell Sentinel Log Manager. These systems are on the top in [11]. The results of this analysis lead to the following conclusions.

First, all developers of SIEM systems discussed above use relational databases. They use such DBMS as MySQL, PostgreSQL, and SQLlite. Some of them declare that they can use XML databases.

Then, the analysis of advanced SEIM systems allowed us to conclude that the main SIEM components, which are sources and consumers of data stored in the repository, are:

- event filtering, aggregation, abstraction and correlation;
- reasoning and visualization;
- decision support reaction and counter measures;
- attack modeling and security evaluation.

Information and event management standards provide the most common rules to represent the security events and incidents. As more comprehensive we investigated the following standards: SCAP [12], Common Base Event [13] and Common Information Model [14].

One of the most comprehensive standards is the SCAP protocol, which consists of a number of standards that describe:

- features of software and hardware configuration (Common Platform Enumeration - CPE);
- software and hardware configuration which adversely affects the security (Common Configuration Enumeration – CCE);
- vulnerabilities of these products (Common Vulnerabilities and Exposures – CVE);
- effects of configurations and security vulnerabilities (Common Vulnerabilities Scoring System – CVSS).

SCAP enables to compile a list of system platforms and applications, set their configuration, adversely affecting security, specify the list of vulnerabilities to assess the adverse effects of configurations and security vulnerabilities, identify the most critical vulnerabilities.

The Common Base Event (CBE) is used to represent the event models; it is supported in IBM products.

The Common Information Model (CIM) covers the widest possible scope among the listed methods. At the moment it is actively growing, and contains a detailed description of the network infrastructure, events, incidents, and many other concepts.

IV. Choice of the Ontological Approach

In all known and widespread SIEM systems the relational approach is used for data storage development.

However, the relational approach has various constraints on expression of relations between entities.

As rule, the relational model in SIEM is often overloaded. This can lead to the conclusion that querying the data takes a long time. This is due to the lack of

flexibility and expressiveness of the SQL query language used in relational databases.

The next relational data modeling challenge is the need to update the data schema, when strong changes of the subject area occur. For relational database systems, saving large amounts of data, this task requires a lot of overhead.

The example of vulnerability description represented by CVE standard is shown in Fig. 1. It means that the vulnerability occurs when the host has application "microsoft ie" and one of the following operation systems: "microsoft vista sp2" or "microsoft vista sp2 x64" or "microsoft server 2008 sp2 x86" or "microsoft server 2008 sp2 x64" or "microsoft 7 x86" or "microsoft 7 sp1 x86" or "microsoft 7 x64" or "microsoft 7 sp1 x64" or "microsoft server 2008 r2 x64".

```
<vuln:vulnerable-configuration id="http://nvd.nist.gov/">
  <cpe-lang:logical-test negate="false" operator="AND">
      <cpe-lang:logical-test negate="false" operator="OR">
          <cpe-lang:fact-ref name="cpe:/a:microsoft:ie:9"/>
      </cpe-lang:logical-test>
      <cpe-lang:logical-test negate="false" operator="OR">
          <cpe-lang:fact-ref name="cpe:/o:microsoft:windows_vista::sp2"/>
          <cpe-lang:fact-ref name="cpe:/o:microsoft:windows_vista::sp2:x64"/>
          <cpe-lang:fact-ref name="cpe:/o:microsoft:windows_server_2008::sp2:x86"/>
          <cpe-lang:fact-ref name="cpe:/o:microsoft:windows_server_2008::sp2:x64"/>
          <cpe-lang:fact-ref name="cpe:/o:microsoft:windows_7:::x86"/>
          <cpe-lang:fact-ref name="cpe:/o:microsoft:windows_7::sp1:x86"/>
          <cpe-lang:fact-ref name="cpe:/o:microsoft:windows_7:::x64"/>
          <cpe-lang:fact-ref name="cpe:/o:microsoft:windows_7::sp1:x64"/>
          <cpe-lang:fact-ref name="cpe:/o:microsoft:windows_server_2008:r2::x64"/>
          <cpe-lang:fact-ref
      name="cpe:/o:microsoft:windows_server_2008:r2:sp1:x64"/>
      </cpe-lang:logical-test>
  </cpe-lang:logical-test>
</vuln:vulnerable-configuration>
```

Figure 1. Description of vulnerability by CVE (example).

In the relational data model (SQL data bases), the entire product list, describing the vulnerability, along with logical operators is stored as a row in a table (Fig. 2).

16	OR(cpe:/o:hp:apollo_domain_os:sr10.2,cpe:/o:hp:apollo_domain_os:sr10.3:beta)
17	OR(cpe:/o:sun:sunos:4.1,cpe:/o:sun:sunos:4.1.1)
18	OR(cpe:/o:sun:sunos:4.0.3,cpe:/o:sun:sunos:4.1,cpe:/o:sun:sunos:4.1.1)
19	OR(cpe:/o:sun:sunos:4.0.3,cpe:/o:sun:sunos:4.0.3c)
20	OR(cpe:/o:digital:ultrix:4.0,cpe:/o:digital:ultrix:4.1)
21	OR(cpe:/a:next:next:2.1)
22	OR(cpe:/o:att:svr4:4.0)
23	OR(cpe:/o:digital:ultrix:4.2)
24	OR(cpe:/a:ncsa:telnet)

Figure 2. Description of vulnerability by SQL (example).

This representation form does not allow specifying a parameterized query with the names of the products, versions, etc. for the analysis of vulnerabilities and processing them in the program. Such process takes a very long time. An alternative solution on data representation in information processing systems with complex data structures (such as SIEM systems) is an *ontological approach*, which makes much easier the expressions of complex relationships between entities. When using this approach, the concepts and relationships can be formulated on the base of description logics, where the terms of the dictionary are the names of unary and binary predicates (concepts and relations). Such predicates are used to express the relations between concepts and to limit their intended interpretation. Hence, the *ontology* is a knowledge base that describes the facts that are always true as part of a community based on the generally accepted meaning of the dictionary. In the simplest case, the ontology describes only a hierarchy of concepts and relationships.

The changes in the ontological data model require much less effort than in the relational model. Therefore, it is particularly relevant in areas where it is needed to store different types of information that can be quickly changed. On our opinion, these areas, of course, include the security issues of distributed networks of Internet enabled objects.

It should be also noted that when designing SIEM systems for the Internet of things, the data model must be most common and at the same time not overloaded one, which will be adapted and specified for each area of application in the process of implementation.

Therefore, the use of ontologies is a necessary approach that enables to create a general model that can be flexibly and quickly applied for all necessary concepts in new generation SIEM systems. Loose coupling of domain ontologies makes it easy to add, delete and support individual ontologies. In addition, the components of the ontologies may be dynamically combined during a performance to meet specific application requirements.

Mathematics underlying the ontological approach allows building more accurate queries and thus reducing the time spent by the analytical modules of new generation SIEM systems to select information from the storage for a subsequent analysis. This advantage is particularly important in the field of distributed network security, because here there is a need to carry out in-depth and heterogeneous analysis information.

As it was mentioned above, the application of the ontological approach involves the use of description logics for logical reasoning. Therefore, we considered systems and approaches for logical reasoning, based on other kinds of logics. They include Event Calculus based on the first-order logic and Model checking based on the linear temporal logic.

Event Calculus is a first-order language with fluents, events and time points as sorts [15]. A fluent is a time-varying property of the world. Event Calculus verification consists in system behavior modeling. Fluents and events are related through a domain-depended axiomatic.

Model checking methods are based on passing through states of a system [16]. System states are determined by the values of variables and concurrent processes executing state change. The Model checking system considers all possible sequences of steps for specified processes and signals about potential incorrect states.

Considered above mechanisms of logical reasoning can be used in new generation SIEM systems, but it seems that for data modeling the description logic is better and it is another reason for choice of the ontological approach.

V. ONTOLOGICAL DATA MODEL

As an example of an ontological data model the Attack Modeling and Security Evaluation Component (AMSEC), a component of new generation SIEM system, was chosen [17]. AMSEC generates a graph of attacks using the network model and the probabilities of vulnerabilities (defined as weights). Further, on the basis of the constructed graph, the AMSEC evaluates the common level of protection for the network, identifies weaknesses and assesses possible countermeasures aimed at increasing the level of security of the network. The AMSEC also allows calculating the likely characteristics of the malefactor, predicting possible avenues for attack and possible actions by the malefactor, which preceded the main attack.

The SCAP protocol has been chosen as the framework developed for the AMSEC data model.

The fragment of the ontology, describing concepts, vulnerabilities, attacks, software/hardware manufacturers and other concepts, is shown in Fig. 3.

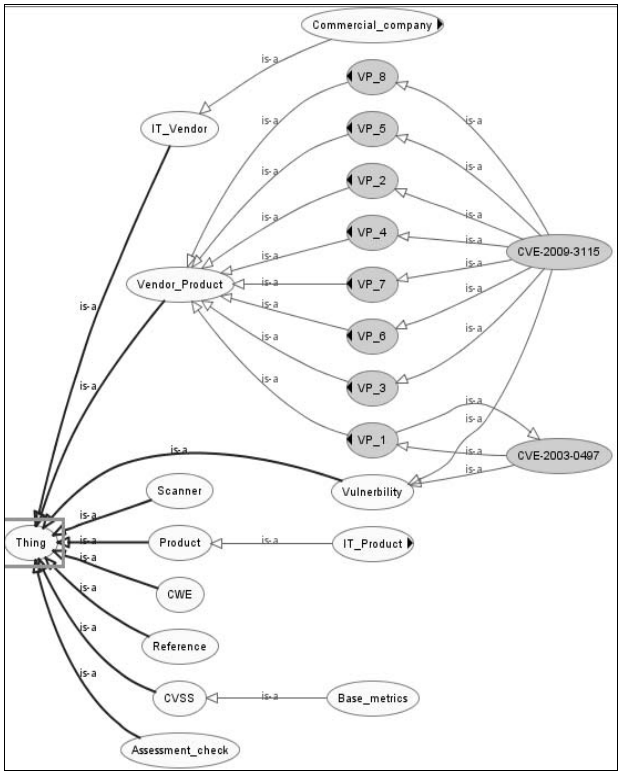

Figure 3. Ontological model for vulnerability representation.

In the presented model, the relationships between software and hardware components, which generate vulnerability, are specified using the description logic. Connections between the concepts are represented, mainly, by the subclasses, rather than through the properties of the objects. Thus, the logical reference here is confined to the task of classification, which increases the processing speed.

An example of the most basic vulnerability affecting only one software product (Cache database version 5 of the Intersystem Company) is shown in Fig. 4.

Figure 4. An example of ontological vulnerability representation.

The ontological vulnerability data model for the AMSEC allows uploading from the database much smaller amount of data and eliminates the need of software processing, shifting the analysis task to the logical reference system.

VI. ONTOLOGICAL REPOSITORY IMPLEMENTATION

The common ontological data storage, or the *repository*, provides a cross-layer integration of different components of the new generation SIEM system.

According to the research and development in data repositories area [18–20], we formulate the following basic functional requirements for the repository:

- Data storage;
- Storage of metadata;
- Possibility of correcting metadata;
- Data management at different levels of detail;
- Concurrent access to data, based on privileges;
- Support of data integrity and consistency;
- Support of multiversion management.

As a base for the implementation of the repository that satisfies the above requirements we choose Service-Oriented Architecture (SOA), which is implemented as a set of web services for data access in the repository. The advantages of this architecture are the flexibility and loose coupling of components, which provide high scalability and extensibility of the system.

SOA is a concept of the distributed information environment that joins together the various software modules and applications based on well-defined interfaces and contracts between them. The main principle of SOA is that the elements of business processes and elements of the information infrastructure, underlying them, are considered as components that are combined and repeatedly used as "building blocks" for the implementation of corporate processes. Fig. 5 shows the general architecture of the repository, based on SOA, and its interaction with the other components of the SIEM system (*CRUD* designates basic operations *Create*, *Read*, *Update*, and *Delete*).

In accordance with principles of SOA, the ontological data store architecture can be divided into three basic layers: *Storage*, *Presentation*, and *Service Implementation*.

The *storage layer* includes various kinds of storages, such as the relation storage, the triplet storage and the XML storage.

The *presentation layer* covers everything that is related to the user interaction with the SIEM system.

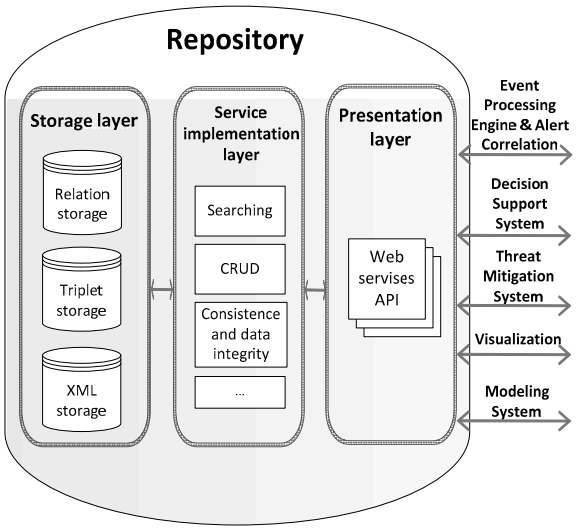

Figure 5. Common ontological repository architecture.

The main features of presentation layer are the mapping of information and the interpretation of the SIEM system user input commands with their conversion into the corresponding operations in the context of the domain (business logic) and the data source. This layer provides the mapping data, the event processing, the user interface, the service requests HTTP, the support functions and the command line API batch execution.

The *service implementation layer* is an additional layer between the presentation layer and the data access layer. The service layer allows abstracting the interaction between one or more business objects, workflows and services through an intermediate interface API.

Our proposals for implementation of the repository are, firstly, the recommendations on the choice of the data base management systems (DBMS).

In order to choose DBMS for repository, we investigated a set of relational databases, XML-based data bases, and triplet stores. A *triple store* is a purpose-built database for the storage and retrieval of RDF metadata [21]. A *triple* is a short formal statement in the form of "subject-predicate-object". Of course, traditional and popular relational DBMS (such as MySQL and PostgreSQL) together with XML-based DBMS can be used, but for the realization of an advanced ontology-based SIEM, which includes possibilities of developed logical reasoning, the triplet stores are preferable.

The storage of triplets can be divided into two basic groups: implemented as standalone solutions (AllegroGraph, BigOWLIM and PelletDb), and parts of complex enterprise semantic system stores (Virtuoso, OpenAnzo and Semantics.Server) [22]. The analysis shows that the best solution is the Virtuoso by the OpenLink Software Company [23]. It is a very powerful Enterprise-product, which has a free version and combines the support of all three types of storages that implements all necessary languages and protocols for data access and also supports a variety of necessary drivers.

For these reasons as the best practical solution for the ontological data storage we proposed to combine the storage of triplets, the relational databases and the XML databases. This provides a balance in the flexibility of data manipulation, the effective use of metadata and the acceptable processing speed.

The implementation of the Web services was made in Java. All Web services are implemented as stateless, i.e. services do not share among themselves any variables and objects. This allows running the request from the client in a single thread on the application server. Thus, a single service can handle multiple threads of the same instances of classes.

The repository was tested according the scheme shown in Fig. 8. The scheme demonstrates the integration of the ontological repository with the AMSEC.

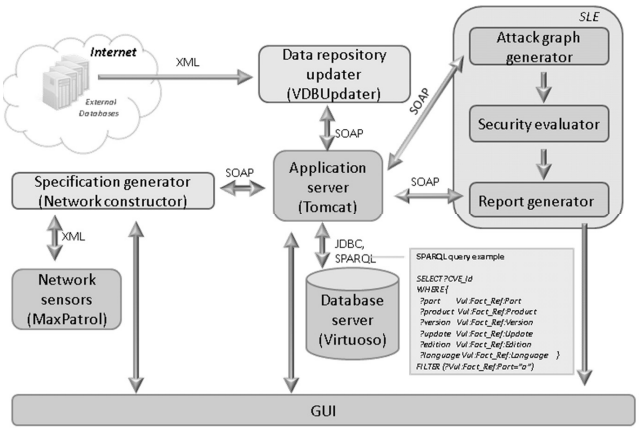

Figure 6. Integration of the repository and the AMSEC

The *data repository updater* downloads the open databases of vulnerabilities, attacks, configuration, weaknesses, platforms, and countermeasures from the external environment.

The *specification generator* converts the information about network events, configuration and security policy, from other SIEM components or from users, into an internal representation.

The *attack graph generator* builds attack graphs (or trees) by modeling sequences of malefactor's attack actions in the analyzed computer network using information about the available attack actions of different types, the services dependencies, the network configuration and the used security policy.

The *security evaluator* generates combined objects of the attack graphs (routes, threats) and service dependencies, calculates the metrics of combined objects on basis of the security metrics of elementary objects, evaluates the common security level, compares obtained results with requirements, finds "weak" places, generates recommendations on strengthening the security level.

The *reports generator* shows vulnerabilities detected by the AMSEC, represents "weak" places, generates

recommendations on strengthening the security level and depicts other relevant security information.

The attack graph generator, the security evaluator and the reports generator are included in the *Security Evaluator* component.

The repository components, as shown in Fig. 6, are the *Application server* (service implementation layer), the *Database server* (storage layer), and the *GUI* (presentation layer).

The *Simple Object Access Protocol* (SOAP) is a protocol to exchange structured messages in a distributed computing environment.

VII. CONCLUSION

In the paper we considered the task of applying the ontological approach for data representation and storage in new generation SIEM systems. We developed the ontological repository and integrated it with the Attack Modeling and Security Evaluation Component of the SIEM system.

For these purposes, we proposed the following innovations (these are the main contributions of the paper).

First, for data representation and modeling we proposed and applied the ontological approach that provides the necessary flexibility to the internal data representation in the repository and the possibility of using logical inference for more accurate and high-quality queering.

Secondly, we proposed a hybrid approach to the ontological repository implementation, which integrates the use of the relational databases, the XML databases and the stores of triplets.

Finally, the ontological repository architecture was suggested and implemented, which was tested with the data used in the Attack Modeling and Security Evaluation Component of the SIEM system.

Further research is planned to expand the vulnerability ontology, as well as to add different services that provide security, including modeling and analysis of security, verification of security policies, etc. In addition, we plan to explore the issues of logical inference based on the ontological repository, as well as the development of mechanisms for data visualization.

ACKNOWLEDGMENT

This research is being supported by grants of the Russian Foundation of Basic Research (projects #10-01-00826 and #11-07-00435), the Program of fundamental research of the Department for Nanotechnologies and Informational Technologies of the Russian Academy of Sciences, the State contract #11.519.11.4008 and by the EU as part of the SecFutur and MASSIF projects.

REFERENCES

[1] Miller D., Harris S., Harper A., VanDyke S., Blask C. Security information and event management (SIEM) implementation. McGraw-Hill Companies. 2011.

[2] Baader F., Horrocks I., Sattler U. Description Logics as Ontology Languages for the Semantic Web. Festschrift in honor of Jörg Siekmann, Lecture Notes in Artificial Intelligence (2003), pp. 228-248.

[3] Cruz I. F., Gjomemo R., Lin B., M. Orsini. A Constraint and Attribute Based Security Framework for Dynamic Role Assignment in Collaborative Environments. Proc. The 4th International Conference on Collaborative Computing: Networking, Applications and Worksharing. Orlando, FL, USA, November 13-16, 2008.

[4] Da Silva G. M. H., Rademaker A., Vasconcelos D. R., Amaral F. N., Bazílio C., Costa V. G., Haeusler E. H. Dealing with the Formal Analysis of Information Security Policies through Ontologies: A Case Study. 3rd Australasian Ontology Workshop (AOW-07), Gold Coast, Queensland, Australia. Conferences in Research and Practice in Information Technology, Vol. 85, 2007.

[5] Kolovski, V., Hendler, J., and Parsia B. Analyzing web access control policies. In WWW '07: Proceedings of the 16th international conference on World Wide Web. ACM, New York, NY, USA, 2007, pp. 677-686.

[6] Rochaeli T., Eckert C. RBAC Policy Engineering with Patterns. Proc. of the Semantic Web and Policy Workshop. Nov. 2005.

[7] Fitzgerald W. M., Foley S. N., O'Foghlu M. Confident Firewall Policy Configuration Management using Description Logic. Twelfth Nordic Workshop on Secure IT Systems, Short Paper, Reykjavik, Iceland, October 11-12, 2007.

[8] Rochaeli T., Eckert C. Attack Goal Generation Using Description Logic-based Knowledge Representation. Proceedings of the 2005 International Workshop on Description Logics (DL2005), Edinburgh, Scotland, UK, July 26-28, 2005.

[9] Schatz B., Mohay G., Clark A. Generalizing Event Forensics Across Multiple Domains. Proc. of 2nd Australian Computer Network & Information Forensics Conference (Forensics 2004), pages 136-144. Edith Cowan University, November 2004.

[10] Kenaza T., Yahi S., Benferhat S. From representing Contextual Intrusion Detection Information in Description Logics to Monitoring Target Events. Agence Nationale de la Recherche. Délivrable, 2006, No.10, 20 p.

[11] Nicolett M., Kavanagh K.M. Critical Capabilities for Security Information and Event Management. Gartner. 21 May 2012.

[12] SCAP, 2011. The Security Content Automation Protocol (SCAP). Website. http://scap.nist.gov.

[13] Ogle, D., Kreger, H., Salahshour, A., Cornpropst, J., Labadie, E., Chessell, M., Horn, B., Gerken, J., Schoech, J., Wamboldt, M., 2004. Canonical Situation Data Format: The Common Base Event V1.0.1. International Business Machines Corporation.

[14] CIM, 2011. Common Information Model (CIM), DMTF. Website. http://dmtf.org/standards/cim.

[15] Kowalski R., Sergot M. A logic-based calculus of events. New Generation Computing, 1986. V.4.

[16] Holzmann, G. The Spin Model Checker. IEEE Transactions on Software Engineering, 1997, Vol. 23, No. 5.

[17] Kotenko I., Chechulin A., Novikova E. Attack Modelling and Security Evaluation for Security Information and Event Management. SECRYPT 2012. International Conference on Security and Cryptography. Proceedings. Rome, Italy. 24-27 July 2012.

[18] Marco D. "Building and Managing the Meta Data Repository: A Full Lifecycle Guide". Wiley. 2000.

[19] Garcia-Molina H., Ullman J.D., Widom J.D. Database Systems: The Complete Book. 2001.

[20] Triple Store Evaluation Analysis Report. Revelytix, Inc. 2010.

[21] Barret R. XML Database Products: Native XML Databases, 2010. http://www.rpbourret.com/xml/ProdsNative.htm,.

[22] Storage And Inference Layer Solutions, 2009. http://alexidsa.blogspot.com/2009/12/sail.html

[23] Virtuoso. http://virtuoso.openlinksw.com