Security Alert Management System for Internet Data Center Based on ISO/IEC 27001 Ontology

Terry M. F. Tsang[1], Thomas M.W. Yeung[1], Dickson K.W. Chiu[1,2], *Senior Member, IEEE,*
Haiyang Hu[3,5], Yi Zhuang[4], Hua Hu[3]
[1]Department of Computer Science, Hong Kong Baptist University, Kowloon Tong, Hong Kong
[2]Dickson Computer Systems, 7 Victory Avenue, Homantin, Hong Kong
[3]Hangzhou Dianzi University, Hangzhou, China
[4]College of Computer Science and Information Engineering, Zhejiang Gongshang University, China
[5]State Key Laboratory for Novel Software Technology, Nanjing University, China
email: manfat@tsangle.com, thomasymw@yahoo.com.hk, dicksonchiu@ieee.org, {hhy, zhuang}@zjgsu.edu.cn, huhua@hdu.edu.cn

***Abstract* — Internet Data Centers (IDC) emerge as a major network service platform to converge Internet related services and applications to one location, managing servers, networks, together with valuable and sensitive data of many enterprises. Therefore, an appropriate security approach is essential. Intrusion Detection Systems (IDS) are often deployed in IDC as a security measure to detect real-time intrusions and alert system administrators to take proper handling actions. However, a large number of low-level alerts lacking of classification make their management difficult. To tackle this problem, we propose a Security Alert Management System (SAMS) in which alerts generated by each IDS undergo alert aggregation. By incorporating ISO/IEC 27001 requirements into the ontology, our system classifies and aggregates alerts from multiple sources, providing a consolidated view of security incidents which are compliant with the ISO/IEC 27001 standard. We further facilitate effective handling of security alerts with different urgency classifications via an Alert Management System (AMS).**

Keywords-Alert Management System, Security Alerts, Alert Aggregation, Security Ontology

I. INTRODUCTION

In this Internet era, Internet Data Centers (IDC) have emerged as a major network service platform to converge Internet services to one location and offers more efficient datacenter services to enterprises. An IDC manages servers and networks together with valuable and sensitive data of many enterprises. Therefore, an appropriate security approach is essential.

For IDC security, Intrusion Detection Systems (IDS) plays a key role for monitoring network and host activities. Detecting real-time, ongoing intrusions, and alerting system administrators for urgent responses may stop the intrusions and minimize possible damages.

However, therein lies the problem of numerous poor-quality alerts, including isolated alerts and alert flooding with high false positives or false negative rates. This inevitably hinders effective security response processes. In the context of IDC, IDS are distributed in a large amount of artifacts, including various software components of servers and switches. The situation becomes more intricate with a higher chance of delay as security information need to be consolidated for risk evaluation, causing some alerts inaccurate or stale. Worse still, only a few of the enormous amounts of alerts generated by most IDS correspond to real incidents. The remainders are false positives (i.e., alerts on non-intrusive actions), repeated alerts for the same incident, or alerts arising from erroneous activities or configurations.

Another problem is the lack of classification framework to correlate the alerts with proper response processes. The key advantage of classifying the alerts is that the number of alerts generated by different IDS can be reduced and prioritized, thus providing a global view of security incidents. Ideally, the classification framework should be widely recognized in the industry and is certified against international standards. In particular, operators with their IDC compliant with international standards, such as the ISO/IEC 27001, are more likely to increase their equity.

In this paper, we propose an SAMS with the use of alert aggregation and demonstrate how the ISO/IEC 27001 can be integrated to help maintain compliance. We focus on investigating the handling of security alerts with an Alert Management System (AMS) module. Our overall goal is to manage the alerts in order to allocate the right amount of resources at the right place and time to handle security incidents effectively. While most researches concentrate on intruder detection, few have investigated how detected incidents can be *handled* effectively in a timely manner. This is the main contribution of our SAMS.

The rest of the paper is organized as follows. Section 2 reviews background and related work. Section 3 describes our SAMS architecture and Section 4 explains how alerts are handled with our SAMS. Section 5 concludes our paper with our future work directions.

II. BACKGROUND AND RELATED WORK

The Internet and related applications are assiduously expanding and have become an indispensable part of mod-

978-0-7695-4227-0/10 $26.00 © 2010 IEEE
DOI 10.1109/ICEBE.2010.78

ern life. Statistics show that the growth rate of the world Internet population reached an astonishing 362.3% in the last 10 years [1]. It provides support for daily communications and collaborations among the general public, such as shopping, banking, and even working. As these activities involve the transaction of a large amount of valuable and sensitive data, cybercriminals are eagerly exploiting the vulnerabilities of unsecured system to make high-profit and low-cost crimes possible. The targets of these crimes are often information and intellectual property important to business continuity.

IDC business was developed in 2000, a year known for its high-speed Internet boom [13]. Although IDCs have evolved for many years, it still suffers from many weaknesses and vulnerabilities. Recently, there was a phishing attack on Microsoft's famous Hotmail service, exposing the email logins and passwords of more than 10,000 users online [12]. Another common security incident is credit card information leakage. The consequences of these incidents can be serious and often damage the reputation of client companies. Thus, the demand for IDC security rises rather than diminishes.

If IDCs do not take proper precautions in systems security, the consequences could be much more costly. In fact, security is no longer considered as a costly responsibility that generates no additional business for organizations [2]. On the contrary, the management is obliged to assure business partners and customers a certain level of reliability and trust with an appropriate IT security approach, especially one that complies with international standards.

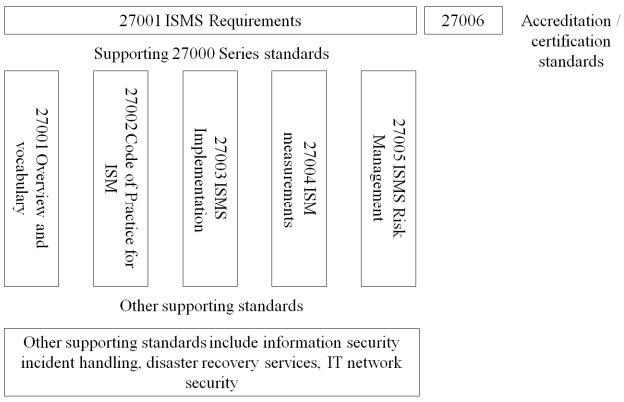

Figure 1. The ISO/IEC 2700x family of standards

There are several certification initiatives that specialize in the security of specific business aspects. Building on the British standard BS7799 [3] and the ISO/IEC 17799 [4], the ISO/IEC 2700x family of standards [5] provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving security management practices [10]. The series of evolving and subsequent standards includes: ISO/IEC 27003, an Information Security Management System (ISMS) implementation guide; ISO/IEC 27004, a standard for information security measurement and metrics; ISO/IEC 27005, a standard for risk management; and ISO/IEC 27006, a guide to the certification process. Figure 1 illustrates the ISO/IEC 2700x family of standards [6].

There are a number of researches related to IDS done since Anderson's Report [12] in 1980 to advance the effectiveness of IDS. Most of them aim to overcome the disadvantage of poor quality alerts by correlating and evaluating alerts based on certain ontology. For example, Yu et al. [13] propose an architecture which consists of collaborative alert aggregation, knowledge-based alert evaluation, and alert correlation. Tang et al. [14] describe a complementary approach which focuses on alert analysis and evaluation, based on event correlation and a truth maintenance system built upon artificial intelligence techniques.

Utilizing relationships among alerts is a common way to extract "valid" alerts from raw IDS alerts. This filter view of alert correlation has been taken by Cuppens et al. [7] and Ning et al. [8], to name a few. Approaches based on this filter view can remove (or filter out) large percentage of false positives. However, they work directly on the alerts and do not distinguish between alerts and intruders' actions in the aggregation process, nor do they relate handling actions.

There are a number of alert aggregation languages that have been proposed [9], but most are not grounded on any standard taxonomy. Their classification schemes are ad-hoc and localized. As such, we propose the use of ontology. Gruber [10] defines ontology as a specification of a conceptualization to represent the knowledge of a domain in a declarative formal way, including entities, classes, relations, functions, or other objects. With common ontology, exchange of inter-IDC information is possible to further prevent and combat intruders in the future.

While most researches concentrate on intruder detection, few have investigated how detected incidents can be *handled* effectively in a timely manner. This is the main contribution of our SAMS.

III. SAMS ARCHITECTURE

Figure 2 shows the overall SAMS architecture based on our previous AMS core, implemented on the J2EE and Oracle platforms [15]. Our SAMS collects alerts from various IDS in the IDC via the Intrusion Detection Message Exchange Format (IDMEF) encoder, which transform them into a unified format as discussed in the next section. Such alerts are then fed into the incoming alert monitor for aggregation based on an ontology compliant to ISO/IEC 27001.

When incidents are detected and security management actions are required, the scheduler generates alerts with

the necessary specification to the AMS. This approach separates the complex logic of communications management from the scheduler and normal processes, which follows the models we proposed [18]. Any subsequent processing that depends on the response or the result of external services has to wait till it finishes (as signaled by the AMS); otherwise the handling process can continue. On the other hand, functions from existing internal modules of the security management application logics can be triggered by the Process Execution Module of the AMS through the scheduler to carry out timely appropriate actions in response to incoming security alerts. In addition, the application logic supports an administrative Web front-end for the IDC staff.

To extend the accessibility for users on different platforms, eXtended Markup Language Stylesheet Language (XSL) technology is employed. For example, different Hypertext Markup Language (HTML) outputs are generated for Web browsers on desktop PCs and PDAs respectively, while WAP Markup Language (WML) outputs are generated for mobile phones. We can then build an *alert response form* through WAP on a mobile phone and a PDA browser respectively [16].

The AMS module consists of two major parts (see Figure 2). The *Incoming Alert Monitor* is responsible for receiving alerts and enacting the corresponding services (processes). In addition, the *Process and Alert Definition* module supports a tool, with which administrators may pre-define the tasks and their associated alerts according to the AMS model. For example, an outage alert through the local power grid monitor or one from a neighboring power grid can trigger immediate programmed responses, because they are reliable sources with substantial information. However, when a citizen reports an undetected outage, an investigation process is triggered instead. That means, the alert triggers the appropriate handler in the scheduler application logic through the *Process Execution* module. Such handler workflows can then generates outgoing alerts to administrators and other organizations (e.g., partner IDCs).

The *Outgoing Alert Monitor* subsystem is responsible for sending the alerts to the corresponding service providers (persons, programs, or organizations) and monitoring their responses. Human service providers (e.g., IDC staff) can be communicated with SMS, email, and instant messaging (IM) such as ICQ [17] through Extensible Messaging and Presence Protocol (XMPP) open-source libraries. In this way, a service provider supporting only manual interactions may still participate in data and process integration through an *alert response form*, through which the required response can be entered and send to the requestor.

The *Outgoing Alert Monitor* subsystem consists of three modules: the *Urgencies Strategy Definition*, the *Role Matching*, and the *Service Provider Monitoring* modules. The *Urgencies Strategy Definition* module enables the administrators to specify the policies that will be followed if the alert is not acknowledged within the deadline (e.g., send the alert to another IDC staff). The *Role Matching* module is responsible for identifying the service providers to which the alert will be forwarded (e.g., select a suitable staff member "intelligently"). The *Service Provider Monitoring* module is responsible for applying the strategies defined at the urgencies strategy definition by executing the actions specified by the administrators. Its functions include sending alert messages, receiving response, maintaining alert status, and logging information. For every response message received, the *Service Provider Monitoring* module updates the status information of the associated alert, and tags the alert as "taken care of". If the alert message has been sent to several service providers

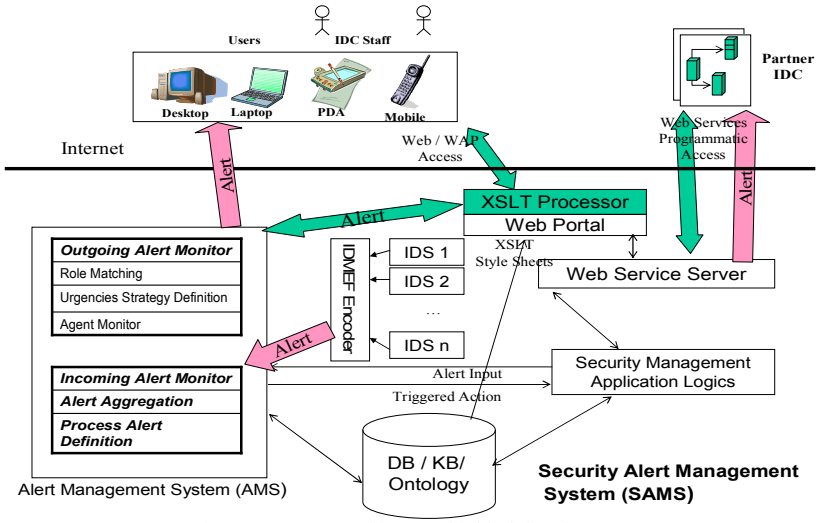

Figure 2. SAMS Architecture highlighting the AMS

(e.g., IDC supervisors and managers) for a very urgent request, those confirm the earliest are assigned to the task while the rest will receive cancellation messages instead. Then for every alert in the *active alert table* with its deadline expired, the module checks the *urgency strategy table*, executes the associated action, and updates the status information accordingly.

IV. Alert Mechanisms

A. Alert Generation

Distributed IDSs correspond to third party IDSs located at different artifacts of an IDC. In case of security incidents, they generate alerts. Therefore, the performance can directly affect the efficiency of the system. However, different IDSs may generate alerts in different formats. For better consistency, the alerts should be encoded in a standard format so that they can be processed effectively.

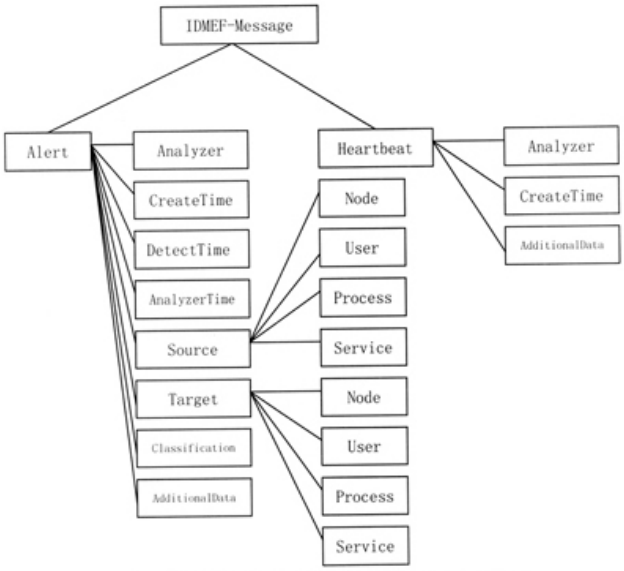

Figure 3. IDMEF data model

```
158.182.155.17 sshd[54738]: Failed password for Terry from 61.21.54.90 port 5498

Extract of an IDMEF message:
  classification.text=SSH Remote user login failed
  assessment.impact.severity=high
  Source.node.nameOrIp=61.21.54.90
  source.service.nameOrPort=5498
  target.node.nameOrIp=10.10.0.3
  target.service.nameOrPort=ssh
  target.user.nameOrId=john
```

Figure 4. Extract of an IDMEF alert message

The Intrusion Detection Message Exchange Format (IDMEF) [11] is a reporting language for describing the format of alerts produced by the security incident detection system. IDMEF is a specification provided by the Intrusion Detection Working Group (IDWG) for defining data formats and exchange procedures for sharing information in the context of security incident detection and response management systems that may need to interact with them. In order to make alerts compliant with the IDMEF, we have to translate raw alerts generated from various sources into a standardized format as shown in Figure 3. The attributes of the standardized alert contain alert type, analyzer time, attacker nodes, attack graph, consequence, name, priority, etc. For example, a user is trying to login a server remotely via SSH but fails. The IDS on that server then generates a corresponding alert depicting this incident. Figure 4 shows an extract of such an alert message.

B. Ontology Based Alert Aggregation

Alert aggregation is the major process in our central administration server. It aggregates formatted alerts across the distributed IDS with the knowledge of the ISO/IEC 27001 ontology. However, if the incoming alerts are not encoded in IDMEF, they will be passed to the encoding module before undergoing alert aggregation.

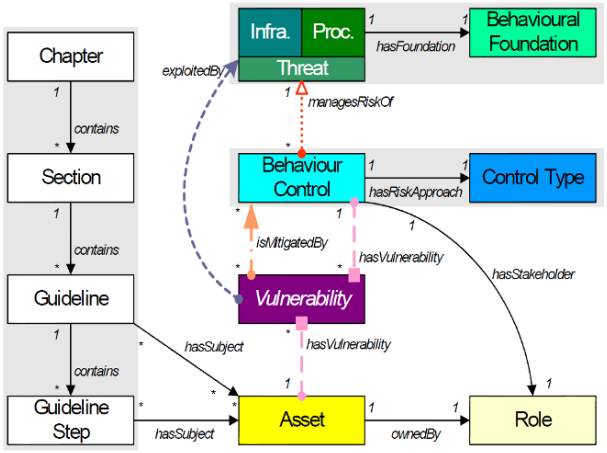

Figure 5. An overview of the ISO/IEC 27001 ontology

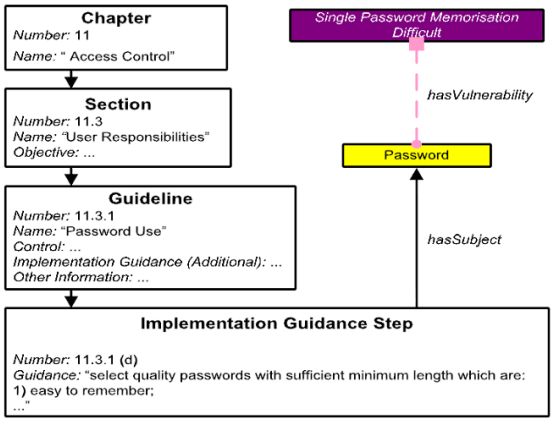

Figure 6. Application of the ontology

The content of the ISO/IEC 27001 standard is arranged in Chapters. Each Chapter refers to a general area of information security management, e.g., access control, and has a number of Sections which each address a specific area of the Chapter's subject matter. Each Section contains a number of Guidelines detailing specific procedural concerns, e.g., User Password Configuration. Each Guideline contains Implementation Guidance, which in some cases is broken down into discrete steps. Figure 5 shows an overview of the ontology accordingly.

During the alert aggregation process, an alert is subjected to the ontology and is aggregated according to their nature. Alerts that are similar in nature such as source, service, time are condensed. Figure 6 shows an alert undergoing the alert aggregation process.

C. *Alert Handling*

For security handling, the ISO/IEC 27001 standard also provides quantitative metrics are for the important issue of risk measurement. Risk of Exposure (RoE) is one of them which can be used to classify the security incidents. As shown in Table 1, the higher the RoE, the greater the chance or likelihood of a serious incident occurring [6].

TABLE 1. RISK OF EXPOSURE (ROE)

		Threat			
	RoE	Low	Medium	High	Very High
Vulnerability	Low	1	2	3	4
	Medium	2	3	4	5
	High	3	4	5	6
	Very High	4	5	6	7

Since it is a quantitative measure, administrators can pre-define the urgency level of various security incidents with RoE, say, *normal*, *urgent*, very *urgent*, *critical*, and *very critical*. If the alert is corresponds to a security incident with high RoE, its urgency will be higher and should be processed more immediately. The integration of such metrics can help achieve the goal of "right amount of resources allocated to the right place at the right time to deal with the security incidents". Table 2 shows some typical example of alerts for an IDC, their urgency level, and handling. For an IDC, reliability alerts (such as abnormal server outage and slowness) should be handled with security alerts in a coherent manner to ensure holistic service security and quality.

According to urgency level of an alert, different notifying and monitoring actions can be carried out according to an urgency strategy table, such as Table 3. Further, we may a *urgency function* as follows in order to elevate the urgency of the alert, if the alert has not been properly handled:

$$U_{002}(t) = \begin{cases} \text{Urgent} & t \le \mathrm{T} \text{ (default)} \\ \text{Very Urgent} & \mathrm{T} < t \le \mathrm{T} + \mathrm{dt}_1 \\ \text{Critical} & \mathrm{T} + \mathrm{dt}_1 < t \le \mathrm{T} + \mathrm{dt}_1 + \mathrm{dt}_2 \\ \text{Very Critical} & \mathrm{T} + \mathrm{dt}_1 + \mathrm{dt}_2 < t \le \mathrm{T} + \mathrm{dt}_1 + \mathrm{dt}_2 + \mathrm{dt}_3 \end{cases}$$

This can seek attention among more staff members and possible alert a staff of a higher rank if necessary.

TABLE 2. EXAMPLE SECURITY ALERTS AND HANDLING

Alerts	*Urgency Level*	*Action*	*Handler*	*Alert Type(*)*	*Affected Object*
DoS Attack	Very Critical	Trigger affected site and isolate it	listracer, Manager	S, R	Network
Mass Admin login attempts	Critical	Trigger source IP and block it	Eventlog, Supervisor	S	Server
Mass User login attempts	Normal	Trigger source IP and block it	Log Tracer	S	Site/ Application
HTTP status 500 of site	Normal	Notify Clients	Alert Mailer	R	Site/ Application
Application pool terminated	Urgent	Restart Application Pool	Script, Admin.	R	Site/ Application
Failure of Service Telnet test	Very Urgent	Restart the corresponding service	Script, Sr Admin.	R	Site/ Application
Ping large response time or Timeout	Critical	Contact Data Center	Network Tracer, Sr Admin	R	Server
Slow response of performance test	Urgent	Check parameters of PA Monitor	PA Monitor, Sr Admin	R	Server
Disk out of space	Very Urgent	Add Space, Trigger large directory usage	PA Monitor, Sr Admin	R	Server
Frequent application pool recycling	Normal	Trigger sites with large memory usage, isolate it	Event log	R	Server
Backup error	Low	Log down the error and restart backup	Alert Mailer	R	Server
Virus Infection	Critical	Scan entire server and report	McAfee Anti-Virus, Supervisor	S	Server
Router/switch outage	Very Critical	Contact Data Center	Manager	R	Network
Firewall Alert	Critical	Trace Firewall Log	Manager	S	Network
CPU high usage	Urgent	Check high CPU usage processes	PA Monitor	R	Server
Memory high usage	Urgent	Check high Memory usage processes	PA Monitor	R	Server
Mass emails in queue	Urgent	Check spammers and email logs, isolate spams	SmarterMail Monitor	S, R	Server
Members' folder high usage	Normal	Send Alert to clients	PA Monitor, Alert Mailer	R	Site/ Application

(*) S = security, R = Reliability

TABLE 3. URGENCY STRATEGY TABLE

Urgency Level	*Action*
Normal	Default - notify the selected agent
Urgent	Submit a second alert to the same agent, notifying about the approaching deadline
Very Urgent	Redirect the alert to another agent that has the best response time
Critical	Send the alert to several agents and accept the results of the one that response first, notify an administrator
Very Critical	Role Substitution: send to all staff with a superset of roles

V. CONCLUSION

This paper proposes a Security Alert Management System (SAMS) with the use of ISO/IEC 27001 ontology in alert aggregation. We emphasize on the effective handling of alerts with the help of an Alert Management System (AMS) module, through which appropriate IDC staff can be effectively notified for handling security alerts in a timely manner. This helps reduce down time and possible damages, and therefore improves the overall service reliability and quality of an IDC. As handling activities and progresses are also recorded, performance evaluation and process improvement is also facilitated.

Future work includes the integration of various risk measurement metrics, which is useful in prioritizing the alerts for proper allocation of security management resources. We are also interested in inter-IDC security alert exchange for better prevention of massive intrusion attacks over the Internet.

ACKNOWLEDGMENT

This paper is supported by the National Natural Science Foundation of China under Grant Nos. 60873022 and 60903053, the Open Fund provided by State Key Laboratory for Novel Software Technology of Nanjing University, and the Key Natural Science Foundation of Zhejiang Province of China under Grant No.Z1100822.

REFERENCES

[1] Internet World Stats, *World Internet Users and Population Stats*, http://www.internetworldstats.com/stats.htm, 2009.

[2] PriceWaterhouseCoopers, Information security breaches survey, http://www.dti.gov.uk/industries/information_security/, 2006.

[3] British Department of Trade and Industry (DTI). *BS7799-2:2002 Information security management systems - Specification with guidance for use*, 2002.

[4] International Organization for Standardization and International Electrotechnical Commission. *ISO/IEC 17799:2005, Information technology – code of practice for information security management*, 2005.

[5] International Organization for Standardization and International Electrotechnical Commission. *ISO/IEC 27001:2005, Information technology – security techniques – information security management systems – requirements*, 2005.

[6] Edward Humphreys, *Implementing the ISO/IEC 27001 Information Security Management System Standard*, Artech House, 2007.

[7] F. Cuppens, F. Autrel, A. Miege, S. Benferhat, *Correlation in an Intrusion Detection Framework*, 2002 IEEE Symposium on Security and Privacy, May 2002, pp. 202 – 215.

[8] P. Ning, D. S. Reeves, Y. Cui, *Correlating Alerts using Preconditions of Intrustions*, Technical Report, TR-2001-13, North Carolina State University, Department of Computer Science, December 2001.

[9] J. Undercoffer, A. Joshi, J. Pinkston, *Modeling Computer Attacks: An Ontology for Intrusion Detection*, Proceedings of the 6th International Symposium on Recent Advances in Intrusion Detection (RAID 2003), 113 – 115, 2003.

[10] Tom Gruber, *What is an Ontology?*, http://www-ksl.stanford.edu/kst/what-is-an-ontology.html, 1992.

[11] D. Curry, H. Debar, *Intrusion Detection Message Exchange Format: Extensible Markup Language (XML) Document Type Definition*, Jan 2003.

[12] Telegraph, *Microsoft Hotmail leak blamed on phishing attack*, http://www.telegraph.co.uk/technology/microsoft/6264539/Microsoft-Hotmail-leak-blamed-on-phishing-attack.html.

[13] N. H. Won. A Study on the Roles and Development Direction of IDC (Internet Data Center) Business in IT society. *Sejong University*, 2005.

[14] A. Tang, P. Ray, L. Lewis. Improvements in Security Alert Analysis with a Truth Maintenance System. Proceedings of the 41st Annual Hawaii international Conference on System Sciences, IEEE Computer Society, 2008.

[15] M. Wright and A. Reynolds. Oracle SOA Suite Developer's Guide. Packt Publishing, 2009.

[16] M. Firtman. Programming the Mobile Web. O'Reilly Media, 2010.

[17] P. Saint-Andre, K. Smith, and R. Troncon. XMPP: The Definitive Guide: Building Real-Time Applications with Jabber Technologies. O'Reilly Media, 2009.

[18] E. Kafeza, D.K.W. Chiu, S.C. Cheung, and M. Kafeza. Alerts in Mobile Healthcare Applications, IEEE Transactions on Information Technology in Biomedicine, 8(2):173-181, June 2004.