Standardization of all Information Security Management Systems

Afshin Rezakhani
Department of Computer Engineering
Ayatollah Boroujerdi University
Boroujerd, Iran

AbdolMajid Hajebi
Department of Computer Engineering
Ayatollah Boroujerdi University
Boroujerd, Iran

Nasibe Mohammadi
Department of Computer Engineering
Ayatollah Boroujerdi University
Boroujerd, Iran

ABSTRACT
Information security relates to the protection of Information Technology assets against the risks of loss, misuse, disclosure or damage. Information security management system (ISMS) is controls that organizations need to implement to ensure that it is sensibly managing these risks. In the other hands, all IDSs/IPSs do many efforts to control networks attacks. In this article we propose creating standard platform for all information security management systems. Also we suggest placing standard knowledgebase in the new added section in ISMSs to create standard security implementation. With this, all information security management systems will be more powerful and decreasing/increasing new plans in organizations will be done easier.

Keywords
Information Technology; ISMSs; IDS/IPS.

1. INTRODUCTION
Information Security refers to the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption. Wikipedia says, "Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.1 The terms information security, computer security and information assurance are frequently used interchangeably. These fields are interrelated and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them. These differences lie primarily in the approach to the subject, the methodologies used, and the areas of concentration. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms [1].

2. MANAGING SECURITY IN ORGANIZATIONS
There are few standards are recommended in organizations to use for better and secure than. In this section, we review information security management systems/subsystems that are used in organizations to improve their security.

2.1 ITIL security management
The ITIL security management process describes the structured fitting of security in the management organization. ITIL security management is based on the ISO 27001 standard. According to ISO.ORG ISO/IEC 27001:2005 covers all types of organizations (e.g. commercial enterprises, government agencies, not-for profit organizations). ISO/IEC 27001:2005 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof. ISO/IEC 27001:2005 is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties. A basic concept of security management is the information security. The primary goal of information security is to guarantee safety of information. When protecting information it is the value of the information that has to be protected. These values are stipulated by the confidentiality, integrity and availability. Inferred aspects are privacy, anonymity and verifiability. The goal of the Security Management is split up in two parts:

1. The realization of the security requirements defined in the service level agreement (SLA) and other external requirements which are specified in underpinning contracts, legislation and possible internal or external imposed policies.

2. The realization of a basic level of security. This is necessary to guarantee the continuity of the management organization. This is also necessary in order to reach a simplified service-level management for the information security, as it happens to be easier to manage a limited number of SLAs as it is to manage a large number of SLAs.

The input of the security management process is formed by the SLAs with the specified security requirements, legislation documents (if applicable) and other (external) underpinning contracts. These requirements can also act as key performance indicators (KPIs) which can be used for the process management and for the justification of the results of the security management process. The output gives justification information to the realization of the SLAs and a report with deviations from the requirements. The security management process has relations with almost all other ITIL-processes. However, in this particular section the most obvious relations will be the relations to the service level management process, the incident management process and the Change Management process [2, 3, 4].

2.2 ISMS
ISMS includes a series processes for systematically establishing, documenting and continuous managing procedures to improve the safety and reliability of the assets of an enterprise, and for realizing information confidentiality,

integrity and availability which are the goals of information security, and includes the continuous enhancement of information security.

The ISMS certification is a system in which a third party certification agency objectively and independently assesses whether ISMS conforms to a certain certification criteria and to certifying that it meets those standards. In Korea, Article 47 Certification of Information Security Management System in the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. provides the legal basis. It stipulates that the Korea Internet & Security Agency under the Korea Communications Commission will certify the system by evaluating whether the comprehensive management system, including the technical and physical security measures, satisfy the certification criteria [5].

2.3 ISM3

The Information Security Management Maturity Model (ISM3 or ISM-cubed) extends ISO9001 quality management principles to information security management (ISM) systems. Rather than focusing on controls, it focuses on the common processes of information security, which are shared to some extent by all organizations. Under ISM3, the common processes of information security are formally described, given performance targets and metrics, and used to build a quality assured process framework. Performance targets are unique to each implementation and depend upon business requirements and resources available. Altogether, the performance targets for security become the Information Security Policy. The emphasis on the practical and the measurable is what makes ISM3 unusual, and the approach ensures that ISM systems adapt without re-engineering in the face of changes to technology and risk. Implementations of ISM3 are compatible with ISO27001 (Information Security Management Systems – Requirements), which establishes control objectives for each process. Implementations use management responsibilities framework akin to the IT Governance Institute's CobIT framework model [15], which describes best practice in the parent field of IT service management. ITIL users can employ ISM3 process orientation to strengthen ITIL security process seamlessly. Using ISM3 style metrics, objectives and targets it is possible to create measurable Service Level Agreements for outsourced security processes [16].

3. SECURITY MANAGEMENT STANDARDS

In this section the standards used in information security management units are investigated.

3.1 ISO/IEC 27001:2005

ISO/IEC 27001:2005 (formerly BS 7799-2:2002) is a standard setting out the requirements for an Information Security Management System. It helps identify, manage and minimize the range of threats to which information is regularly subjected. The standard is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties including an organization Customers. It is suitable for several different types of organizational use, including the following:

- Formulation of security requirements and objectives;
- To ensure that security risks are cost effectively managed;
- To ensure compliance with laws and regulations;
- As a process framework for the implementation and management of controls to ensure that the specific security objectives of an organization are met;
- Identification and clarification of existing information security management processes;
- To be used by management to determine the status of information security management activities;
- To be used by internal and external auditors to determine the degree of compliance with the policies, directives and standards adopted by an organization;
- To provide relevant information about information security policies, directives, standards and procedures to trading partners;
- To provide relevant information about information security to customers.

An organization using ISO/IEC 27001:2005 as the basis for its ISMS can become registered by BSI, thus demonstrating to stakeholders that the ISMS meets the requirements of the standard [6].

3.2 ISO/IEC 27002:2005

The ISO/IEC 27002 Code of Practice for Information Security Management establishes guidelines and general principles for organizations to initiate, implement, maintain, and improve information security management. The objectives outlined provide general guidance on the commonly accepted goals of information security management. ISO/IEC 27002 contains best practices of control objectives and controls in the following areas of information security management:

- Security policy;
- Organization of information security;
- Asset management;
- Human resources security;
- Physical and environmental security;
- Communications and operations management;
- Access control;
- Information systems acquisition, development and maintenance;
- Information security incident management;
- Business continuity management;
- Compliance [6].

3.3 NIST 800-26

NIST 800-26 is a popular control standard that many organizations base their security practices. NIST is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration. NIST's Computer Security Division has developed several standards to improve information systems security that have been widely adopted by both Federal agencies as well as commercial organizations. Rsam's NIST template is based on SP 800-26 Security Self-Assessment Guide for Information Technology Systems, SP 800-53 Recommended Security Controls for Federal Information Systems and other related documents. Each assessment area in Rsam is carefully mapped to NIST standards & guidelines, allowing clients to easily conduct an assessment against NIST. The purpose of this NIST 800-

53/26 is to provide guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government. The guidelines apply to all components of an information system that process, store, or transmit federal information [16].

4. PROPOSED APPROACH

According to above text, the security threads are managing in organizations and they divert their mind to work in secured platform. There are few standards which designed to create this platform. But they are several problems:

- Standards are consistently increase by the time.
- There is not any standard Intrusion Detection System in them in the world.
- Organizations have several type of IDS/IPS and some of their IDS/IPS is older.
- Organizations are not able to use from the capabilities and experiences of other organizations.

We propose the solutions of above problems are placed in the ISMS/ITIL Security management processes (and all other security management systems), to improve their powers in managing any intrusion and attacks behavior.We explain our suggested approach in the next sections in A to F.

4.1 Standardization All of Security Management Standards

Current problem in organizations, are having different methods in their security management systems. They are using different standards to implementing them. For example one organization may use ITIL Security management cycles, while other organization may use ISMS to accomplish its security managing. We propose all organizations require have information security managing with certain standards.

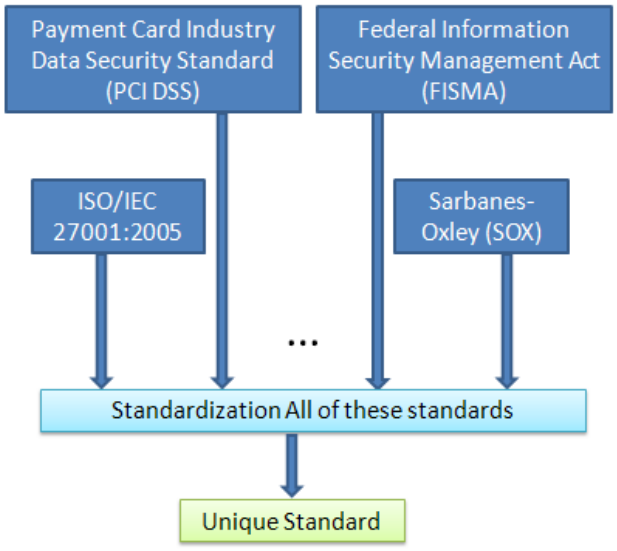

Figure.1 create unique standard to managing security

All organizations must effort to propel current standards to unique standard that be agreement among all of them. Because the new threats are done with accurate managing, organization must have unique standards methods in information security management process to confrontation with threats as well. Of course, all organizations must agree in this standard to avoid in using different standards. With this, coordinating and managing in next changes in organizations faster than is done.

4.2 Creating Standard Platform in All IDSS/IPSS

Another problem seems is lack the standard platform in intrusion detection /prevention systems. We consider all intrusion detection/prevention systems in our previous article and proposed to create standard semantic relation between them to improve their power in detect/prevent internal and external attacks [8].

Standardization between IDSs/IPSs causes all of them able to detect and prevent anomalies integrated. The semantic web comprises the standards and tools of XML, XML Schema, RDF, RDF Schema and OWL that are organized in the Semantic Web Stack. The ontology section has an important role to convert any concept in networks into a standard forms. It was explained by Jeffrey Undercoffer et al paper copiously [17]. We propose to use semantic web form for converting detected attacks to RDF schema in order to creating standard platform between them.

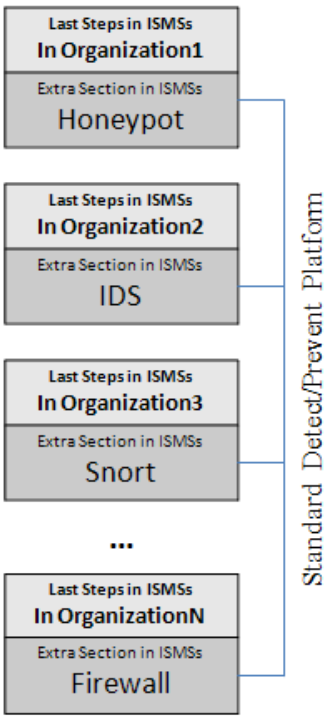

Figure2. Creating Standard Platform between All IDSs/IPSs

This work, leads to collaboration platform intrusion detection/prevention systems and causes all be able to use from other experiences of IDSs/IPSs. We proposed this idea in other paper precisely [13]. The form of semantic web that is created when an attack is detected is showing in below figure.

```
<Intrusion: rdf:about="Attacks"
Intrusion:IP_Address="An IP Address">

<Intrusion:resulting_in rdf:resource=
" 0.2 , 0.1 , 0.7 , 0.6 , 0.8 , 0.7 , 0.51 "/>
</Intrusion>
```

Figure 3. The Semantic Web Form of a detected Attack

4.3 Create a Dynamic Section in ISMSs

Because the threats such as internal intruders or external intruders maybe enter injury compensation in organization, we propose place a separate and independent section in all ISMSs. This dynamic section parallel works with other phases in ISMSs and its work is independent from their phases. This added section monitors the network traffics continuously and detects anomalies.

Figure4. Add a Dynamic Section in ISMSs Process

This dynamic added section is used to implement our proposed approach. We suggest more attention (more than other phase in information security management process) should be given to attackers and their activities, such as change/remove files or each other hurt. This dynamic section helps to place standard roles (anomalies or signatures [7]) for detecting/prevent any intrusion. These roles can be standard roles that were obtained from previous section.

4.4 Create Collaborative Platform between ISMSs

If experience in any organization, transfer to other organizations, the ability of them be increased and they can control threats better than. For this idea we place several coordinators in countries with most attacks such as China and USA [9, 18]. Coordinator can be several servers which sniff networks and convert newest attack behaviors to a standard form and send it to added section of ISMSs that exist in organizations. These servers have modern and intelligent algorithm [10] and able to detect newest attacks well.

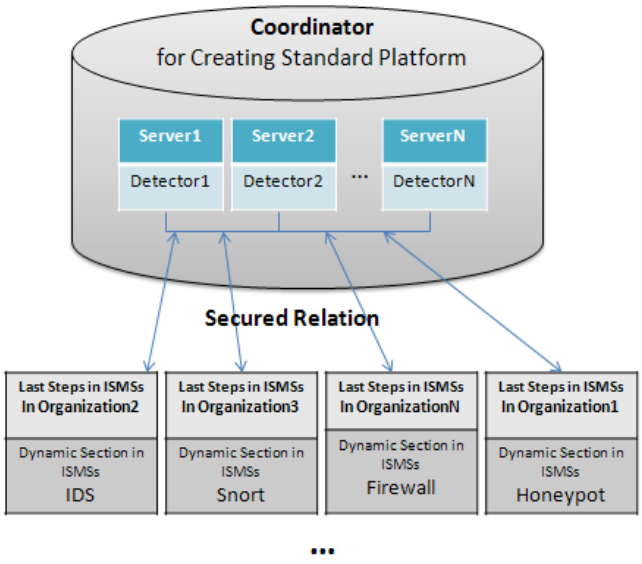

Figure5. Creating Collaboration between All ISMSs

These servers relate together in secured environment to ensure the integrity, availability and confidentiality of them well done [11, 12].

5. RELATION BETWEEN SERVERS

Another point in this study is the methods that are used in the relation between servers. We propose use Cloud/Grid model to creating relation between servers [13]. Also their security is important. It was proposed a communication model that integrates both Grid system and Mobile Agent to perform parallel computations with secured communication in a complete heterogeneous and distributed environment. This framework is platform independent [14].

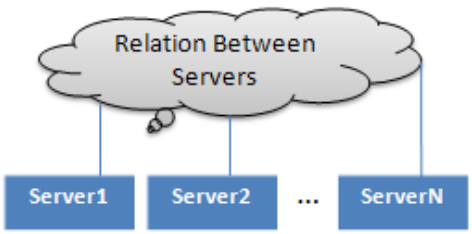

Figure6. Cloud/Grid Model to Creating Relation between servers

6. EVALUATION ENTERED TRAFFIC

We considered the rate of identical attacks that happened in another paper and showed the traffic between coordinators did not create many extra overhead in the networks and would be balanced. The attacks would be identical and it was not necessary to send them to other ISMSs (dynamic section) [13]. This result is showing in figure6.

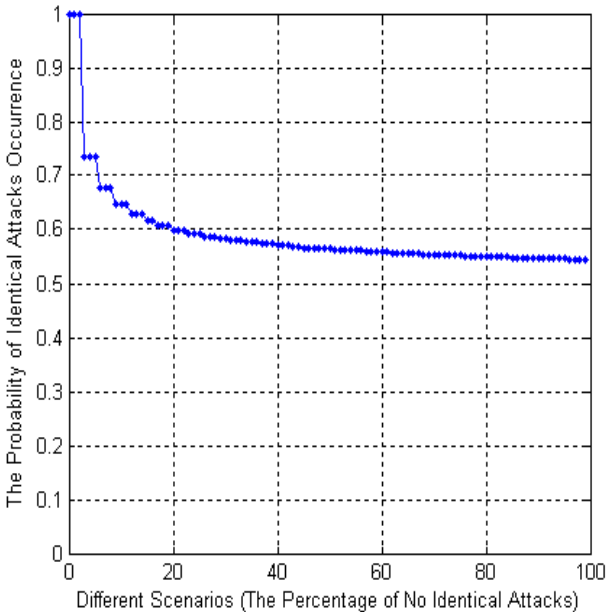

Figure7. Considering the probability of Identical Attacks

7. CONCLUSION

In this research we studied information security management systems such as ISMS and ITIL Security management. We considered that the current activities in this scope would be varied in future. Thus, we proposed create a unique standard between all of them. Also we suggested place standard intrusion detection/prevention system in added section of information security management processes. With this, all information security management systems will be more powerful and decreasing/increasing new plans in organizations will be done easier.

8. REFERENCES

[1] The Definition of Information Security on Wikipedia, last visited in December 2010.

[2] Bon van, J. (2004). IT-Service management: een introductie op basis van ITIL. Van Haren Publishing

[3] Cazemier, Jacques A.; Overbeek, Paul L.; Peters, Louk M. (2000). Security Management, Stationery Office.

[4] Tse, D. (2005). Security in Modern Business: security assessment model for information security Practices. Hong Kong: University of Hong Kong.

[5] A Study of Effect of Information Security Management System [ISMS] Certification on Organization Performance, IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.3, March 2010.

[6] http://www.iso.org/iso/, last visited in December 2010.

[7] S. Axelsson, "Intrusion Detection Systems: A Taxonomy and Survey," Technical Report No 99-15, Dept. of Computer Engineering, Chalmers University of Technology, Sweden, March 2000.

[8] Leila Rikhtechi, Afshin Rezakhani Roozbahani, "Creating a Standard Platform for All Intrusion Detection/Prevention Systems", ICCMS, 2010.

[9] URL:http://www.networkworld.com/news/2008/090908-japan-attacktraffic.html, last visited in December 2009.

[10] Shun, J. Malki, H.A., "Network Intrusion Detection System Using Neural Networks", ICNC 08, Jinan , November 2008.

[11] S.A.Onashoga, Adebayo D.Akinde and A. S.Sodiya, "A Strategic Review of Existing Mobile Agent-Based Intrusion Detection Systems" Department of Computer Science, University of Agriculture,Abeokuta, Nigeria, Volume 6, 2009.

[12] Cryptography and Network Security: Principles and Practice By William Stallings, 2010.

[13] Afshin Rezakhani Roozbahani, L.Rikhtechi and N.mohammadi, "Converting Network Attacks to Standard Semantic Web Form in Cloud Computing Infrastructure", International Journal of Computer Applications (0975 – 8887) Volume 3 – No.4, June 2010

[14] K.MuthuManickam, "A Security Model for Mobile Agent in Grid Environment", International Journal of Computer Applications (0975 – 8887) Volume 2 – No.2, May 2010.

[15] COBIT control management Rsam: Automated COBIT governance platform.

[16] http://www.ism3.com/page9.phps, last visited in December 2010.

[17] S.A.Onashoga, Adebayo D.Akinde and A. S.Sodiya, "A Strategic Review of Existing Mobile Agent-Based Intrusion Detection Systems" Department of Computer Science, University of Agriculture,Abeokuta, Nigeria, Volume 6, 2009.

[18] Kaspersky Security Bulletin 2009. Statistics, 2009.