Requirements of Information Assurance

Ontology-Based Framework of Security Management for E-Payment Networks

Ahmed ARARA, El-Bahlul Fgee, and Mohammed Bargelail

***Abstract*— E**-payment networks security has become crucial because it touches all other areas of the e-banking domain, Processing the financial sensitive data whether it is in storage, processing or in transit requires consistent information assurance specification. This paper presents the information assurance requirements for e-payment networks based on ontology which provides common understanding and sharing of security requirements among all stake holders in the e-banking domain. Security management framework is proposed to include ontological concepts of security assurance such as e--payment networks threats, vulnerability, denial of service (DoS), and corruption of sensitive information. The security management framework is mainly based on security standards (ISO/IEC 27001 & 27oo2).

***Keywords*—**Information Security, e--payment security requirements, ontologies, security Management framework, Web Services Security, and web application

I. Introduction

INFORMATION sharing, rather than information processing is what characterizes information technology in the 21st century. However, sharing and exchanging information via networks have caused more threats and vulnerability of information resources and their use.

Managing information security is still problematic to security officers and the system administrators of an IT field due to incomplete requirements and lack of collaboration among all participants who are in need to share and exchange distributed information resources.

The IEEE Standard 729 [2] defines requirements as: A condition or capability needed by a user to solve a problem or achieve an objective. A condition or capability that must be met or possessed by a system to satisfy a contract, standard, specification, or other formally imposed document. Information assurance term used in this paper covers information security and information availability.

Our approach is to capture security requirements based on ontologies. Ontologies are used to build a framework that furnishes the information assurance and permits the achievement of security objectives such as integrity, availability, confidentiality…etc. The security requirements includes three types:- (i) functional requirements that determines what the system must perform in secure manner, (ii) non-functional requirements that describes properties the system must possess, and (ii) derived requirements which is implicit and derived from the functional and non-functional requirements [4].

Ontologies aim to support knowledge sharing and reuse in explicitly and mutually manner [10]. The ontology is formally specified in OWL, and defines e--payment vocabulary in terms of classes, properties and instances. The ontology shall contain the description of important sources of information (Information systems and databases) that can be exploited for the development of Security Management Framework for e--payment networks (SMF4e--paymentN). The SMF4e--payment is a semantic model capable of achieving the following objectives:-

- Expressing the security requirements of e--payment network machines in terms of ontological concepts.
- Capturing domain knowledge that is relevant with information security taking into account the Management of information security standards in the field.
- Providing the basis for developing security management tools.

SMF4e--payment framework is proposed to support security officers to control, manage, and supervise security demands and security requirements change in a collaborative distributed environment.

The paper is organized as it follows: section 2 will discuss the related work. Section 3 tackles the problem of security requirements. Section 4 introduces the framework and briefly describes the main components of SMF4e--payment. Section 5 discusses the main ontology aspects of information assurances. Section 6 will conclude the paper

II. Related Work

Ontologies have been applied in the information security domain to reduce the complexity of modern information systems.

Ontologies are also overwhelmingly used in the specific security sub-domains such as network security [6], access control [7, 8] and pervasive computing [8].

Semantic Web [9] is an extension of the Web where meanings (semantics) are brought to web pages. However, the security of information becomes very crucial when the semantic Web is used to disperse, communicate, and manage information systems. It should be noted that ontologies expressed in OWL [9] which is the main component that provides common understanding and sharing. Other

Ahmed ARARA is with University of Tripoli Faculty of Eng. Tripoli, Libya. Email: ahmedarara3@gmail.com

El-Bahlul Fgee is with High Institute of Vocational Studies, Gharian Yafren. Email fgeeee@dal.ca

Mohammed Bargelail is with National Academy of Graduate Studies-IT department.

Semantic Web components like XML and RDF should be also secure.

In security management frameworks, there are security architecture models namely: The ISO/IEC 27001&27002, SABSA (Sherwood Applied Business Security Architecture, FEAF (Federal Enterprise Architecture Framework) and NIST 800-53 [6,7,8]. Such standard models are used to implement security management tools.

In [5], an ontology-based framework for representing, storing, and reusing security requirements is presented. This framework is expressed in a formal representation of the requirements.

To the best of our knowledge, all existing researches do not consider the information assurance issue that includes information security, information availability, and risk assessment. In fact, we propose a security framework that covers the information assurance starting by risk analysis and ending to access control policies and mechanism that permit the management of collaborative, distributed environment.

III. E-PAYMENT SECURITY ASSURANCE REQUIREMENTS

Generally speaking, security requirements should include all types and levels of protection necessary for equipment, facilities, information resources and applications to meet security policies. Specifically, security requirements are identified by risk analysis. That is: "the systematic use of information to identify assets to estimate the risk." [4]. Risk analysis, assessment and management do comply with enterprise common business goals such as ensuring business continuity, minimize business damage and to maximize return on investment (ROI). Any security management framework requirements specification is considered to be complete if it includes the main components: security services, information states, and security countermeasures (See figure 1).

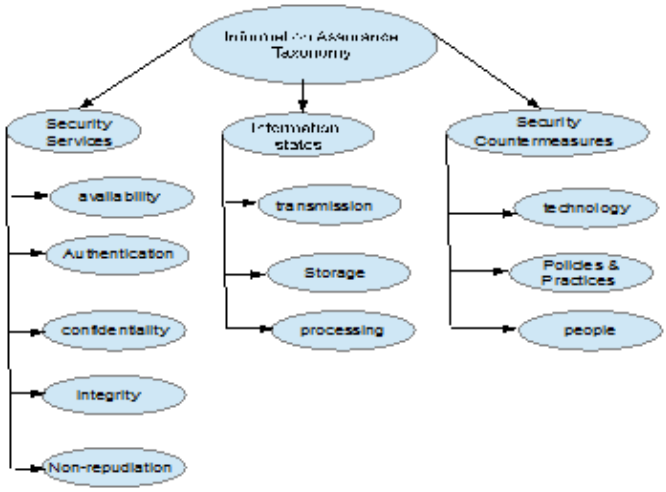

Fig. 1 information assurance taxonomy

Trustful e-payment system is no different with respect to such enterprise information security requirements. To develop a framework of e-payment management system, we need to consider the management aspect as well as the ontological concepts and their relationships as it follows:-

A. The security architecture or the security management model that shall be adopted for developing the tool (SMF4e—payment) is based on the existing security architecture models namely: ISO/IEC 27001 & 27002 [4], SABSA ([9], and NIST 800-53 [6]. The security management model should include the main elements of information assurance and security: security services, information states, and security countermeasures (see figure 1). In this research, our focus will be on capturing the information security requirements and expectations based on ontology. The Information Security Management model (ISMS) is described in Part 2 (ISO 27001) will be heart of the proposed framework (SMF4e--payment). This ISMS model is based on the life cycle of:- PLAN-DO-CHECK-ACT (see figure 2 below).

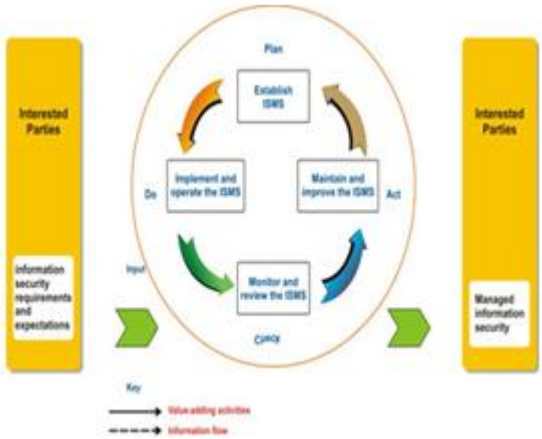

Fig. 2 Information Security Management System(ISMS) (Quoted from [4])

B. Domain ontology of information assurance of e-payment security management system is derived based on complete security requirements. As a matter of fact, ontology development should support the completeness and consistency of the information assurance requirements in cases when some concepts and/or relationships are missed or ignored during the system requirements analysis. The following section elaborates on the domain ontology of information assurance in the scope of e-payment systems

IV. ONTOLOGY OF INFORMATION ASSURANCE FOR E-PAYMENT SECURITY MANAGEMENT SYSTEM

The e-payment domain is such a complex transaction system. To manage the information assurance and security, we strongly believe that ISMS model should serve as a kernel for the framework proposed in our research. Moreover, we feel that the domain ontology should be considered to allow for shared common understanding among all stakeholders such as banks, customers, financial institutions, and ITC staff. Ontology domain consists of sub-domains that are mutually disjoint. The sub-domains (security services sub-domain and security policies sub-domain) are given priorities

and must be part of our framework.

The ontology (shown in figure 3) is represented in OWL and it will be implemented by protege editor to represent the knowledge base part of the model. The OWL classes (represented in Oval shape) and the relationships (directed arrows).

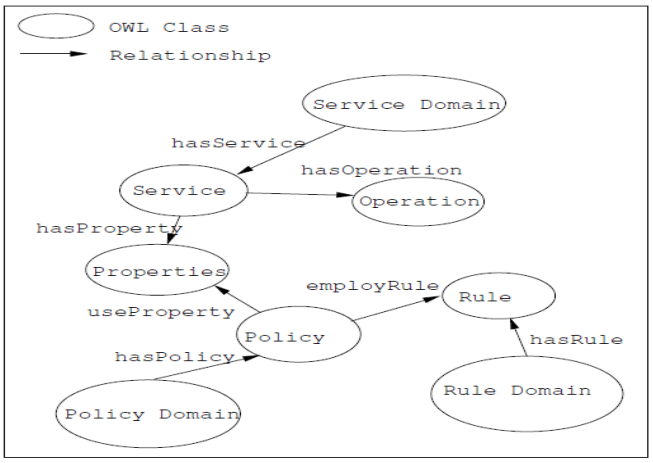

Fig. 3 Light ontology of service sub-domain and policy domain (Quoted from [11])

V. The Framework: SMF4e—payment

A. The SMF4e—payment stands for Security Management Framework For e-payment system. It is a model based on ontology to provide a base-line of technical and operational requirements of information assurance. It is used as a tool to store and manage the diversified information assurance entities. The following objectives are intended from the SMF4e—payment framework:-

1. Promote effective management and governance of information assurance and security by providing a machine processable taxonomy of information security entities or ontological concepts and their relationships (see figure 1).
2. Enrich the security services and objectives by well defining semantically all terms of concepts and relationships in OWL ontology language.
3. To reason via a reasoning engine about the information assurance entities such as security countermeasures

B. SMF4e—payment Architecture

The framework SMF4e—payment is a 3-tier architecture. Clients make their inquiries to the middle-tier by requesting the service provider (a Web server, or Security server or both). The service provider will response to the type of request by either answering the client or by going up one tier namely the information assurance security tier (IAS-tier). The IAS is kept as an independent level in which an IAS processor can by accessed by security managers, and ITC managers according to their privileges and their access rights.

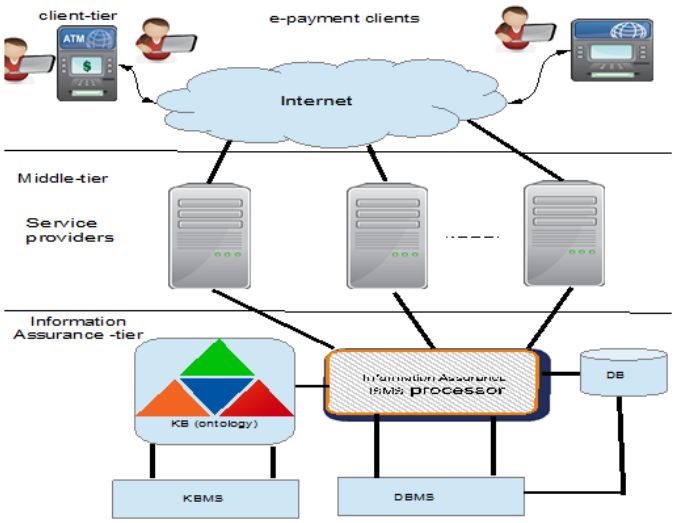

Fig. 4 SMF4e-payment system Architecture

VI. Conclusion and Future Work

In the paper, we have shown the requirement of a framework of Information assurance that deals with interconnected systems. As a result of the vast spread of the Web and ICT, inter-connectivity has increased and consequently information is exposed to a growing number and a wider variety of threats and vulnerabilities. The use of domain ontology to represent knowledge of information assurance is considered to be a challenge but it provides us with secure organization, communication and re-usability. The ontology-based framework model to represent the information assurance model contributes to common understanding and removal of ambiguities by providing the semantics of e-payment systems and consequently the common shared understanding.

The framework is intended to be implemented as a security tool for the Sirafa enterprise which is responsible for all e-payments transactions performed by the Libyan central bank as well as other national banks.

References

[1] The ATM Forum Technical Committee, 'ATM Security Specification 1.0', ATM-SEC-0100.001, February 1999.

[2] IEEE Std 610 Glossary OF SOFTWARE ENGINEERING TERMINOLOGY Standard

[3] Krishan Tuli and Kaur,Gurpreet,"ATM SAFETY & SECURITY", International Journal of Advanced Research in IT and Engineering Vol. 2 No.2, February 2013: ISSN 2278-6244 www.garph.co.uk

[4] ISO27002 (2005): ISO/IEC 17799-27002 Code of Practice for Information Security Management.

[5] Joaquín Lasheras et al, "Modelling Reusable Security Requirements based on an Ontology Framework", Journal of Research and Practice in Information Technology, Vol. 41, No. 2, May 2009.

[6] A. Simmonds, P. Sandlands and L. Van Ekert , " An ontology for network security attacks.", in Proceeding of Asian Applied Computing conference (AACC), Ser. Lecture Notes in Commerce Science, Vol. 3285. Kathmandu, Nepal: Springer Berli, October 2004, pp 317-323.

[7] H. Li, X. Zhang, H Wu, Y. Qu, " Design and application of rule-based access control policiess."in Proceeding of Semantic Web and policy workshop, Galway, Irland, November 2005, pp 34-41.

[8] A. Tonninelli, J.M. Bradsha, L. Kagal, and R. Montanari, " Rule-based and ontology based policies: toward a hyprid approach to control agents I

pervasive environment." In Proceedings of the semantic Web and workshop, Galway, Irland, November 2005, pp 42-54.
[9] T. Berners Lee, J. handler and O. Lassila, " The Semantic Web.", Scientific American May 2001, http:// www.sciam .com/ article.cfm?article ID=00048144-10d2-Ic70-84A9809EC 588EF21.
[10] GRUBER, T. (1995), "Towards principles for the design of ontologies used for knowledge sharing.", International Journal of Human-Computer Studies, 43(5/6): 907-928. http://dx.doi.org/10.1006/ijhc.1995.1081
[11] Dong Huang et al. "A Knowledge-based Security Policy Management Framework for Business Process", Technical paper, Siemens AG, Corporate Technology Otto-Hahn-Ring 6 81739 Munich, Germany.dong.huang.ext@siemens.com
[12] D. Huang, Y. Yang, and J. Calmet. "Modeling web services policy with corporate knowledge.", In Proc. of 2006 IEEE In-ternational Conference on e-Business Engineering, Shanghai,China, October 2006.
[13] http://csrc.nist.gov/publications/fips/inde x.html
[14] http://www.praxiom.com/iso-17799-intro.htm
[15] http://www.webstore.ansi.org/
[16] http://csrc.nist.gov/publications/nistpubs/.