Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 3 (2011) 537–543

Procedia Computer Science

www.elsevier.com/locate/procedia

WCIT 2010

Enterprise information security, a review of architectures and frameworks from interoperability perspective

Marzieh Shariati[a], Faezeh Bahmani[a], Fereidoon Shams[a]

[a] *Department of Electrical & Computer Engineering,Shahid Beheshti University, Tehran, Iran*

Abstract

With the growth of ICT opportunities, the enterprises have realized the significance of interoperability as a competitive advantage. Thus, many enterprises have adopted the main strategy of rapidly changing their structures to support interoperability. On the other hand, interoperability is incompatible with information security.

The Enterprise Information Security Architecture (EISA) offers a framework upon which business security requirements, the risks and the threats are analyzed and a portfolio of the best integrated enterprise security solutions is put together. Frameworks and models introduced in the past six years have examined different aspects of EISA.

We realized the diversity of the mentioned approaches and in this paper, first, we develop two facets according to which these approaches are categorized. These facets are abstraction level (holistic vs. partial) and architectural viewpoint (managerial vs. technical). As interoperability is the primary focus of our study and it is a broad concept, we restrict our discussion to holistic frameworks and models. In this regard, we survey the prominent holistic approaches namely Gartner, SABSA, RISE frameworks, AGM-based model and intelligent Service-Oriented EISA.

In the next step, we compare the mentioned frameworks from technical, organizational and semantic interoperability aspects. We conclude that none of the frameworks, not even those which are holistic, practical and greatly elaborated, have explored interoperability clearly.

We assert that the competitive advantages offered by interoperability, justify the costs needed for implementing the incompatible concepts of interoperability and security along with each other. In addition, we suggest that the requirements which are common to both interoperability and security should be extracted and the significance of interoperability to EISA should be apprehended

Selection and/or peer-review under responsibility of the Guest Editor.

Keywords: Enterprise Information Security Architecture (EISA); Enterprise Architecture (EA); Enterprise Information Security (EIS); Enterprise Security Management (ESM); Information Security Management (ISM); Interoperability; Architecture Framework

1. Introduction

Recently, the enterprises have come to think of interoperability as a competitive advantage[1], [2]. Many enterprises have adopted the main strategy of rapidly changing their structures to support interoperability. On the other hand, the quality attributes of interoperability and information security are incompatible. Therefore, enterprise information security has been adversely affected by the mentioned change.

The Enterprise Information Security Architecture (EISA) introduces a framework which is based on enterprise architecture (EA) [3]. The identification, analysis and prioritization of business security requirements, the risks and the threats and the choice of a portfolio of the best integrated enterprise security solutions are done based on the mentioned framework. In the past six years, many frameworks and models were introduced which consider different aspects of EISA.

The aim of the next section is to examine EISA frameworks and models from both the abstraction level (holistic vs. partial) and architectural viewpoint (managerial vs. technical) facets. Next, since abstraction level is more significant we limit our discussion to surveying EISA approaches from only this aspect.

Through our analysis, we found out that partial methods could be mainly divided into the categories of:

- security policies and configurations management
- security of enterprise services
- security role management and access control
- security assessment and requirements engineering.

However, because of the reasons mentioned later, the main focus of this paper is on holistic frameworks. The most important holistic frameworks including Gartner, SABSA, RISE frameworks, AGM-based model and intelligent Service-Oriented EISA are explicated.

doi:10.1016/j.procs.2010.12.089

The most eminent framework is Gartner which was the first one to define the term EISA in [4]. Gartner considers the compatibility of EISA with EA program and insists on the collaboration between these two [3]. The next prominent framework is SABSA [5] and [6]. It has made the most outstanding attempt in the field of holistic EISA. It is a layered architecture, accompanied by an implementation methodology. RISE [7] is another important framework. It is a threat-based and risk-managing method which has been introduced for information security management across enterprise. AGM-Based SOAE Security Governance model [8] was generated by using two important information security standards, namely ISO/IEC 17799 and SOGP in Agile Governance Model. Intelligent Service-Oriented EISA [9] is a layered intelligent service-oriented architecture for the systematic and intelligent management of EISA activities. In addition, ISO27002 has been used to choose information security services and carry out risk management.

Interoperability is the primary focus of the next section. Out of five aspects of interoperability we chose three most relevant ones. These three are technical, organizational and semantic aspects. As interoperability is a broad concept, we confine our discussion to holistic frameworks and models. In this regard, we evaluate these approaches from the mentioned interoperability aspects.

Finally, the outcome of the comparison is presented in the last section.

2. EISA Related Frameworks and Models

Many efforts have been made to introduce architecture frameworks or reference models for enterprise information security. The difference in the scopes and aims of these approaches as well as the lack of reviews and discussions makes it difficult to analyze and appraise these approaches.

The mentioned problem urged us to categorize these models and frameworks. We developed two facets for this categorization. These facets are abstraction level (holistic vs. partial) and architectural viewpoint (managerial vs. technical). As stated before, architectural viewpoint (managerial vs. technical) is beyond the scope of this paper. Accordingly, we examined the available methods from only abstraction level (holistic VS. partial) aspect.

1.1. Holistic vs. Partial approaches

In the past, information security was regarded as an insignificant and peripheral issue; the threats posed low risks to the information of the enterprise. Thus, the integration of partial security solutions seemed sufficient for handling the mentioned threats and establishing information security across the enterprise. The enterprises' increasing use of ICT brought about widespread side effects and new issues for which there were no solution in the integration of partial approaches. Resolving these new issues was certainly a stimulus to the development of approaches with top-down perspectives which study the issues from a higher level of abstraction. In addition to the mentioned stimulus, three factors further precipitated the development of holistic approaches:

1- Separation of strategic planning initiatives and security solutions decisions and activities which resulted in incompatibility in applying partial security solutions.
2- Functionality overlap between partial security solutions which led to the reduction of performance
3- Incomplete coverage of information security in the enterprise.

Enterprise information security is expected to conform to new requirements and respond to new threats and hazards. This emphasizes the need for recursive solutions which consist of sequenced phases. No partial approaches support the dimension of time. However, a few holistic approaches support this dimension.

Later in this section, we take a brief look at partial approaches and do an in-depth analysis of the most important holistic approaches.

1.1.1. Partial Approaches

In this section, we try to review recent partial enterprise information security approaches. Since there is a great variety in these methods, we decided to classify them. We recognized that partial methods could be mainly divided into categories of :

- security policies and configurations management
- security of enterprise services
- security role management and access control
- security assessment and requirements engineering

. The majority of these partial approaches fit into at least one of the mentioned categories. The methods left out of this classification are either outside the scope of this paper or are too specific and could not be classified. Later in this section we will give a general overview of each of the mentioned categories.

A. Security policies and configurations management

"Information Security policies are generally high-level, technology neutral, concern risks, set directions and procedures, and define penalties and countermeasures if the policy is transgressed"[10].

"Policy-Maker" is one method of managing security policies. This method introduces a toolkit for the security policy management of heterogeneous networks[11]. Another method presented in [12] aims at developing a means of policy mediation in multi-organization collaboration environment. In addition, [13], [14]and [10] have tried to establish architectures or frameworks for security policy.

B. Security of enterprise services

The increasing use of service-oriented architectures has both benefited and harmed the security of enterprise information. On the one hand, service-orientation facilitates the automation of service collaborations and the increase of collaborations leads to the exposure of enterprise information. On the other hand, it paves the way for the easy collaboration of security services. In this regard, [15]examines the security challenges of service-oriented architecture in enterprises (SOEA).The security of web services is one of the most important applications of enterprise services security. [16] and [17] have offered solutions specific to this issue. In addition, [18] method is very comprehensive in establishing security in open grids.

C. Security role management and access control

Role management and access control were among the first enterprise-specific security solutions.
The most prominent solutions presented so far are:
DAC (Discretionary Access Control) [Harrisson M.A, Ruzzo], [Lampson B.W.], MAC (Mandatory Access Control) [Bell D.E., LaPadula] and RBAC (Role Based Access Control) [Nyamchama].
Moreover, a method called ERBAC (Enterprise RBAC) has been recently introduced [Axel Kern].
Two more architectural approaches, one role-based in [S. Megaache] and one agent-based in [Boulanger] are presented for access control and role management.

D. Security assessment and requirements engineering

Much work such as those [19] , [20], [21] and [22] has been done in the field of security and risk evaluation. Assessment of the current situation of enterprise information security, evaluation of information assets and risk assessment are the purposes of most of these methods.
The work of [23] and [24] is the most notable in the area of requirements engineering and those by [25] , [26] are the most eminent ones in the area of risk and threats detection.

1.1.2. Holistic Approaches

A. Gartner EISA Program [4] and [3]

Garter defined the term EISA for the first time in [4] and presented the recommended framework and architecture for ESIA. Gartner's approach was inspired by enterprise architecture frameworks. Gartner defined three levels of abstraction (conceptual, logical and implantation) and three view points (business, information and technical) for EISA framework .Furthermore, Gartner considers the compatibility of EISA with EA program and insists on the collaboration between these two. Nevertheless, he has not offered a specific methodology for implementing EISA and has only given a general description of the structure and framework of EISA.

B. SABSA layered architecture and methodology [5] and [6]

SABSA has made the most outstanding attempt in the field of Holistic EISA. It is a six-layered architecture which consists of the horizontal layers of contextual, conceptual, logical, physical, component and the vertical layer of security service management [5]. The developers of SABSA claim that one of the features of SABA is its usage of best practices and its compliance with enterprise information security standards (ITIL v.3 and TOGAF). This framework has been fully elaborated in [6]. Compared to Gartner framework which is abstract and theoretical, SABSA is more practical and comes with a methodology. In addition, the development and risk management processes and life cycle of SABSA are well-documented.
SABSA has its own specific method for carrying out requirement engineering. The developers claim that this method can establish a proper relation between business strategies and designing technical solutions.
The heart of SABSA methodology is its Business Attributes Profile. This profile is a taxonomy of business requirements and the required guidelines. SABSA is one of the few methods which take the requirements of time dimension into account and has offered its framework and methodology in a special way so that it can guarantee the security of the enterprise information through a continuous process.

C. *RISE methodology [7]*

This threat-based and risk-managing method has been introduced for "Across Enterprise" information security management. The developers of this method have tried to enhance enterprise architecture. They have achieved this by incorporating security and privacy features into business processes.
RISE emphasizes the processes and lifecycles which should be implemented and uses standards such as [27] in compiling its framework.
Although this methodology is very comprehensive from the processes point of view, the downside is that it is not based on one specific framework.

D. AGM-Based SOAE Security Governance model [8]

This model was generated by applying two important information security standards, namely ISO/IEC 17799 and SOGP to Agile Governance Model.

The purpose of this model is to suggest a Governance Model for security requirements management in the context of service-oriented enterprise architecture (Service-Oriented Enterprise Architecture).

Using AGM offers more clarity in terms of both role definition and requirements management of security components in serviced-oriented architecture.

This model is composed of four organizational decision making levels namely “strategic”, “tactical, operational and real-time and the two views of "Design, Planning and Support" and "Development and Execution".

E. Intelligent Service-Oriented EISA [9]

Intelligent Service-Oriented EISA is a model for the systematic and automated management of EISA activities .In this model, both the selection of information security services and the implementation of risk management are based on ISO27002.

This model has five layers including Security Database Layer, Security Application Layer, Integration and Intelligent Layer and Information Security Portal Layer. Integration and Intelligent Layer is the most important layer of this model and it is where data, processes and applications are integrated so that they can meet the rapid changes in business processes. This layer is where inter-application and inter-process communications are carried out and the four models of BPM, Business Intelligence, Rule Engine and PDCA Adapter are designed to facilitate these communications.

3. Comparison of frameworks from interoperability perspective

According to [28], the five facets of interoperable ecosystem are as follows:

- Technical Interoperability: This facet of interoperability usually emphasizes applications which are either designed interoperable off the shelf or could be made interoperable by using translators or converters.
- Organizational Interoperability: This facet of interoperability focuses on business processes and user-based adoption issues. It aims at promoting productivity within organizations.
- Semantic interoperability: This facet of interoperability makes sure that all systems and users “speak the same language” and understand each other.
- Legal/public policy interoperability: This facet of interoperability concentrates on laws and public policies affecting interoperability among government entities and organizations, such as accessibility, privacy, security, etc.
- Effect of different political, economic, cultural and social paradigms.

The last two facets are beyond the scope of our discussion. Thus, in this section the most prominent holistic EISA frameworks, introduced in the Introduction Section, have been evaluated and compared in terms of the first three facets.

A. Gartner framework

The Gartner framework introduced in [3] is very abstract and little information is available on it. However, the following facts could be extracted from the available documents ([3], [4]).

The technical interoperability analysis of the Gartner framework is impossible since this framework has a theoretical essence. No evidence could be found even on the implementation layer of this architecture indicating whether this architecture is technically interoperable or not.

Organizational interoperability implicitly exists in the conceptual and logical layers of Gartner framework. The reason is that the development of Gartner EISA was based on Gartner EA and is compatible with it.

As for semantic interoperability, it could be noted that Gartner supports it. The reason is that one of the primary aims of the developers of this framework was to establish a common" language" for information security within the organization .They achieved this common language by firstly forming a portfolio of primary security services in their methodology and then setting this service framework as the cornerstone of other models, infrastructures, architectures and security components and processes.

B. SABSA framework

Traditionally, security solutions are chosen or designed based on technical aspects. Thus, the compatibility and interoperability of these solutions are not guaranteed. This is one of the issues which SABSA developers complain about. SABSA developers believe that having long-term cost analysis and business goals supportive strategies are essential to the development of security solutions [5].

SABSA supports technical operability due to the fact that SABSA business attributes profile has defined interoperability as a subset of operational attributes.

It could be stated that SABSA explicitly supports organizational interoperability for two reasons. Firstly, SABSA adopts a Business-Driven method for EISA development. This method describes a structured inter-relationship between technical and procedural solutions. Secondly, SABSA defines "interoperability both internally and externally" as one of the eight business requirements in its decision criteria.

SABSA supports semantic interoperability implicitly. The reason is that SABSA framework places application programs, people, processes and assets close to each other as the columns of the framework.

C. RISE framework

RISE severely disapproves of costly methods which address security solutions from a bottom-up perspective. It has attempted to offer a holistic approach for integrating security requirements into business process management.

This method does not go into technical details so it excludes technical interoperability.

RISE supports organizational interoperability because it was designed to promote security in enterprise architecture frameworks. This framework does not address organizational interoperability directly and supports it implicitly.

No information is available regarding the semantic interoperability of this model.

D. AGM-Based Model

This model is a combination of theoretical models and standards. It has offered a macro-level governance structure based on the considerations of information security management standards and frameworks and SOA principles.

The above explanations and the available documents lead us to infer that obviously this model does not support technical interoperability.

This model supports organizational and semantic interoperability implicitly because of the following facts:

- The long-term objectives of this model.
- The introduction of "communications and operation management" in the real-time layer of this model.
- The information security roles and responsibilities view of this model.

E. Intelligent SOA-based EISA

Although this model has a holistic approach, it has a technical outlook on the issue. This model explicitly resolves the problem of "inter-process" and "inter-application" communications in its "Integration and Intelligent Layer". This model has made use of BPM model to manage and configure S2S, H2S, H2H and S2H communications.

Thus it could be concluded that this model explicitly supports the three interoperability aspects of technical, organizational and semantic.

F. Comparison and Results

Table 1 illustrates the summary of the evaluation of the reviewed frameworks and models:

Intelligent SOA-based EISA has a technical outlook on the issue and has attempted to resolve interoperability with a technical approach. Except for this framework, no other frameworks, even the ones which are holistic, practical and greatly elaborated, have explored all facets of interoperability clearly.

We believe that the competitive advantages offered by interoperability, justify the costs needed for implementing the incompatible concepts of interoperability and security. In addition, we suggest that the requirements which are common to both interoperability and security should be extracted and more attention should be paid to the status of interoperability in EISA.

Table 1. The comparison of prominent EISA frameworks from interoperability perspective

	Frameworks				
Interoperability Aspects	Gartner	SABSA	RISE	AGM-based Model	Intelligent SOA-based EISA
Technical	UK	ES	NI	NI	ES
Organizational	IS	ES	IS	IS	ES
Semantic	ES	IS	UK	IS	ES

IS=Implicit Support, ES= Explicit Support, NI= Not Included, UK= Unknown

4. Conclusion

This paper, tried to show that the inherent incompatibility of two quality attributes of interoperability and information security makes it difficult to apply these two concepts simultaneously and this causes many problems. Next, it divided EISA approaches to the main categories of partial and holistic and elaborated on each category. Then, it examined the EISA approaches of Gartner, SABSA, RISE frameworks, AGM-based model and intelligent Service-Oriented EISA from interoperability perspective. This survey examined the technical, organizational and semantic aspects of interoperability. The result was that the role of information security in interoperability was often neglected. It seems that much practical research should be done so that the two incompatible quality attributes of security and interoperability could be implemented along with each other.

Acknowledgements

Authors would like to acknowledge the support provided by Education and Research Institure for ICT(ERICT), Iran.

References

1. Pathak, J., *Security of Organizations ' Information Systems (IS) and the Auditors : A Schematic Study*
2. Nachtigal, S., *E-business Information Systems Security Design Paradigm and Model*, in *Department of Mathematics*. 2009, Royal Holloway, University of London. p. 347.
3. Scholtz, T., *Structure and Content of an Enterprise Information Security Architecture*. 2006, Gartner Inc.
4. Kreizman, G. and B. Robertson, *Incorporating Security into the Enterprise Architecture Process*. 2006, Gartner, Inc.
5. Sherwood, J., A. Clark, and D. Lynas, *Enterprise security architecture whitepaper*. SABSA Limited, 2009.
6. Sherwood, J., A. Clark, and D. Lynas, *Enterprise Security Architecture: A Business-Driven Approach*. 2005: CMP Books.
7. Anderson, J.A. and V. Rachamadugu. *Managing Security and Privacy Integration across Enterprise Business Process and Infrastructure*. in *Services Computing, 2008. SCC '08. IEEE International Conference on*. 2008.
8. Korhonen, J.J., M. Yildiz, and J. Mykkanen. *Governance of Information Security Elements in Service-Oriented Enterprise Architecture*. in *Pervasive Systems, Algorithms, and Networks (ISPAN), 2009 10th International Symposium on*. 2009.
9. Jianguang, S. and C. Yan. *Intelligent Enterprise Information Security Architecture Based on Service Oriented Architecture*. in *Future Information Technology and Management Engineering, 2008. FITME '08. International Seminar on*. 2008.
10. Rees, J., B. Subhajyoti, and E. Spafford, *PFIRES: A Policy Framework for Information Security*. Communications of the ACM, 2003. **46**(7): p. 101-106.
11. Pilz, A. *"Policy-Maker": a toolkit for policy-based security management*. in *Network Operations and Management Symposium, 2004. NOMS 2004. IEEE/IFIP*. 2004.
12. Galiasso, P., et al. *Policy mediation for multi-enterprise environments*. in *Computer Security Applications, 2000. ACSAC '00. 16th Annual Conference*. 2000.
13. Alam, M. and M.U. Bokhari. *Information Security Policy Architecture*. in *Conference on Computational Intelligence and Multimedia Applications, 2007. International Conference on*. 2007.
14. Claycomb, W. and D. Shin. *Enabling mobility in enterprise security management*. in *Performance, Computing, and Communications Conference, 2006. IPCCC 2006. 25th IEEE International*. 2006.
15. Schumacher, M. and D. Witte, *Secure Enterprise SOA, Known and New Security Challenges*. Datenschutz und Datensicherheit, 2007. **31**: p. 652-655.
16. Gutiérrez, C., E. Fernández-Medina, and M. Piattini, *Web Services Enterprise Security Architecture : A Case Study*. ACM 1-59593-234-8/05/0011, 2005.
17. Nakamur, Y., S. Hada, and R. Neyama. *Towards the integration of Web services security on enterprise environments*. in *Applications and the Internet (SAINT) Workshops, 2002. Proceedings. 2002 Symposium on*. 2002.
18. Nagaratnam, N., P. Janson, and J. Dayka, *The Security Architecture for Open Grid Services*. 2002.
19. Aagedal, J.O., et al. *Model-based risk assessment to improve enterprise security*. in *Enterprise Distributed Object Computing Conference, 2002. EDOC '02. Proceedings. Sixth International*. 2002.
20. Buck, K., P. Das, and D. Hanf. *Applying ROI Analysis to Support SOA Information Security Investment Decisions*. in *Technologies for Homeland Security, 2008 IEEE Conference on*. 2008.
21. Johansson, E. and P. Johnson, *Assessment of Enterprise Information Security - An Architecture Theory Diagram Definition* in *CSER 2005*. 2005: Hoboken, NJ, USA.
22. Martin, C. and K.A. Abuosba. *Utilizing a Service Oriented Architecture for Information Security Evaluation and Quantification*. in *Business-Driven IT Management, 2007. BDIM '07. 2nd IEEE/IFIP International Workshop on*. 2007.
23. Stephenson, P., *S-TRAIS : A Method for Security Requirements Engineering Using a Standards-Based Network Security Reference Model.*
24. Menzel, M., I. Thomas, and C. Meinel. *Security Requirements Specification in Service-Oriented Business Process Management*. in *Availability, Reliability and Security, 2009. ARES '09. International Conference on*. 2009.
25. Hall, G., *Identifying and Managing Internal Security Threats in Enterprise Systems.* 2009.
26. Sengupta, A., C. Mazumdar, and A. Bagchi. *A formal methodology for detection of vulnerabilities in an enterprise information system*. in *Risks and Security of Internet and Systems (CRiSIS), 2009 Fourth International Conference on*. 2009.
27. NIST, *Standards for Security Categorization of Federal Information and Information Systems*, N.I.o.S.a. Technology, Editor. 2004, FIPS Publication.
28. Baird, S.A., *Government Role and the Interoperability Ecosystem.* Journal of Law and Policy for the Information Society, Vol. 5, No. 2, p. 219, Summer 2009.