Journal of Computer Sciences

Original Research Paper

Enterprise Architecture Security Assessment Framework (EASAF)

Bandar Mzel Alshammari

Department of Information Technology,
School of Computer and Information Sciences, Aljouf University, Saudi Arabia

Article history
Received: 26-07-2017
Revised: 21-08-2017
Accepted: 04-10-2017

Email: bmshammeri@ju.edu.sa

Abstract: Many existing studies have shown that the causes of most of system attacks are not related to coding vulnerabilities that apply to individual systems, issues related to the run-time environment, or the technology in place. In fact, they are caused by issues associated with how systems within organizations are structured. Therefore, it is necessary to examine security with regard to all components that influence the organization's systems, including data, processes and even employees. The most promising approach to achieving this goal is Enterprise Architecture (EA). The main goal of this project is to develop a framework based on the concepts of well-established EA frameworks such as TOGAF and Zachman and their compositional layers (e.g., application, information and process). This framework will be combined with a data flow analysis of the principles that trace the potential information flow between high- and low-security enterprise components. Therefore, this paper studies various enterprise architecture frameworks and shows how to develop an enterprise architecture framework that considers the organization's information security from the perspective of information flow. This framework will have various layers, each with a set of security metrics that quantify the organization's relative security based on the specifications of that layer. The defined framework will be capable of defining Enterprise Architecture security-related principles and metrics. These principles and metrics will eventually be used to define how to develop secure enterprise systems based on the enterprise architecture with regard to security-critical information flow within any given organization. The defined framework will also be capable of providing guidance for information security architects by recognizing certain parts of the organization that are less secure than others.

Keywords: Enterprise Architecture, Security Design Principles, Security Metrics, Architecture Principles

Introduction

Organizations consist of various assets that require some form of protection or security. Some of these assets need to be protected from being disclosed to unauthorized parties. Other assets must be secured from modification by unauthorized parties. With regard to enterprise systems, it is necessary to identify the type of security that is required by a particular asset and studying the organization's systems architecture is essential for this purpose.

With the increasing demand for developing high-quality and more reliable systems, the process of developing trustworthy and secure enterprise architecture is a challenging one. Enterprise Architecture (EA) is an approach that aims to manage complex systems within the organization and to collaborate in the most effective way (TOG, 2011). The field of Enterprise Architecture mainly focuses on addressing two issues. One is to overcome the problem of complex systems to reduce their complexities, which can greatly decrease the overall cost of system deployment and maintenance (TOG, 2011). The other issue is to increase the alignment between the enterprise business and its enterprise systems (TOG, 2011). Therefore, EA can be defined as an architecture that clearly shows how the enterprise technologies, business processes and information systems are interrelated (TOG, 2011). In other words, EA defines how the systems can be used to meet the enterprise's needs in a more collaborative way. Several EA methodologies have been defined in the literature. However, the most common ones are the Zachman framework, The Open Group Architecture Framework (TOGAF) and the Federal Enterprise Architecture (TOG, 2011).

Several studies have focused on enterprise security and defined several approaches for addressing this issue. One of these studies is the work of Abreu *et al.* (1995) that aims to provide a security assessment for an enterprise based on its architecture. The goal of this work is to ensure that a given security objective for an enterprise is fulfilled (Abreu *et al*., 1995). Further works in this area include Jurjens (2005), the OCTAVE approach (Alberts and Dorofee, 2002) and the CORAS approach (Aagedal *et al*., 2002). However, none of these approaches considers security from an early stage of enterprise architecture development. Moreover, they depend on predefined security vulnerabilities to provide a security assessment of an enterprise based on its architecture.

It can be seen that EA frameworks can play a major role in enhancing the business of any organization. However, they need to provide an approach that assesses security from the point of view of information flow. None of existing EA methodologies (such as TOGAF and Zachman) gives a complete solution that considers assessing security of a given enterprise as part of the methodology. Therefore, this paper aims to develop an assessment framework that consists of a set of security metrics based on well-established enterprise architecture frameworks such as TOGAF and Zachman and their compositional layers (e.g., application, information and process). This assessment framework will be combined with data flow analysis principles that trace the potential information flow between various high- and low-security enterprise components. In particular, the main objective of this paper is to define a set of quantifiable "security metrics" that allow system security architects to quickly and easily assess the overall security of a given enterprise based on specific artifacts such as enterprise application interactions diagrams. These metrics can also be used to identify sound steps for improving the security of existing enterprise architectures.

The objective here is to define a technique for evaluating the level of security of a given enterprise based on its architecture. Since a non-trivial architecture does not consist of a single layer but instead is a composite of several layers, security metrics that measure the compositional properties of specific enterprise architecture layers must be developed. These compositional properties are based on traditional quality measures such as data accessibility, coupling and coherence. Defining these metrics allows enterprise security architects to assess the security of their enterprises at an early stage.

Related Work

This section reviews current research related to the area of the security assessment of organizations with respect to their Enterprise Architecture. In particular, it surveys well-established enterprise architecture frameworks, relevant security design principles and security metrics.

Enterprise Architecture Frameworks

As a result of the increasing demand for managing complex enterprise systems and using these systems to collaborate in the most effective way, the term "enterprise architecture" has emerged. In recent years, information technology has changed business, but in many cases, that change is not aligned with the business strategy of an organization (Covington *et al*., 2009). This has influenced organizations in a negative way and wasted many resources (Covington *et al*., 2009). Enterprise Architecture provides the structure and control required to align an enterprise's business operations and information technologies to support its business goals and strategies (Sun and Xu, 2012).

One of these EAs is Oracle Enterprise Architecture Framework (OEAF). Its main purpose is to be able to work in collaboration with Oracle's customers in developing strategic road maps that enable the alignment between business and information technology (Covington *et al*., 2009). The Oracle EA framework is known to be a hybrid of other existing enterprise architecture frameworks and it is mainly influenced by TOGAF, FEA and Gartner (Sun and Xu, 2012).

Another Example of EAs is Federal Enterprise Architecture Framework (FEAF). This framework was released in May 2012 as part of the US federal CIO policy for increasing the practice of enterprise architecture in the US federal government (EOPUS, 2012). It defines several principles for using enterprise architecture to help the federal entities within the US government make the best use of EA by eliminating duplications and increasing shared resources (EOPUS, 2012).

The Ministry of Defense Architecture Framework (MoDAF) is another EA framework (UKMD, 2012). It was defined originally by the United Kingdom Ministry of Defense to structure the integration of systems within the ministry. It was later modified to help acquire the needed information on business resources and processes to accomplish the anticipated strategy of the organization (UKMD, 2012). Currently, there are several organizations that have adopted the MoDAF in their work, including BAE systems, the Thales group, EADS and Avolution (2009).

The US Ministry of Defense Architecture Framework (DoDAF) is another framework that was initially developed to be applicable for defense systems by the US Department of Defense (USMD, 2010). It originated from the previously developed architectural framework of command, control, communication, computers and intelligence, surveillance and reconnaissance known as C4ISR (Alghamdi, 2009). It organizes architectures based on four views: The overall view, operational view, system view and technical view (USMD, 2010).

Gartner is a recent EA framework that believes EA should always be a top-down discipline and hence when consolidating an EA, business should come first, then information and technology (Sessions, 2007). One of the key strategies in Gartner is to develop future state architecture before the current one is documented. This step is followed by other outcomes, including gap analysis and an actionable road map. Most of the effort in Gartner is spent on strategizing, communicating, leading and governing, while architecting receives little attention (Sessions, 2007).

The Queensland Government Enterprise Architecture (QGEA) framework has been developed by the CIO at the Queensland government (QGCIO, 2009). It consists of a number of policies and documents that provide guidance for Queensland government entities in improving the compatibility and reducing the cost of its IT systems (QGCIO, 2009). Therefore, the QGEA framework's main goal is to be able to organize the enterprise resources (i.e., services, processes, information, applications and technology infrastructure) (QGCIO, 2009).

John Zachman defines his EA framework as a "logical structure for classifying and organizing the descriptive representations of an Enterprise that are significant to the management of the Enterprise, as well as to the development of the Enterprise's systems" (Zachman, 1987). It can be seen from the above definition that the Zachman framework provides a logical structure for organizing the enterprise's design artifacts, which can help the enterprise's managers in the decision-making process (Zachman, 1987).

The Open Group Architecture Framework (TOGAF) originated from the US DOD framework and its main purpose is to provide organizations with a methodology that allows them to improve their business efficiency (TOG, 2011). This improvement can be achieved by utilizing resources in an efficient and effective way to have a greater impact on the business return on investment. TOGAF not only provides simple implementation and usability but also provides excellent alignment between IT and business (TOG, 2011).

In summary, it can be said that all existing enterprise architecture frameworks share the same objective, which is to create an enterprise architecture that maximizes the alignment of IT and business. This objective will eventually lead to reducing system complexity and sharing resources within the organization. However, TOGAF seems to identify a clear process of development for any organization. However, none of these EA frameworks provides an assessment approach that enables EA architect measures security of a given organization based on its EA artifacts.

Relevant Security Design Principles

The works of Saltzer and Schroeder (1975; Bishop, 2003; McGraw, 2006) have defined several design principles that should be followed to develop more secure systems. These principles aim to provide guidance for system architects and developers to increase the assurance of system quality and hence increase system security. Below, a number of such security design principles are reviewed.

One principle is called Secure the Weakest Link which aims to intensively secure the weakest parts of the system because hackers are always looking for parts of the system that seem to be simple to break (McGraw, 2006; Viega and McGraw, 2002). Another principle is called Economy of Mechanism which its main objective is to make security mechanisms as simple as possible without weakening them (Bishop, 2003). Reduce the Size of the Attack Surface is another common principle that aims to make programs more secure (Howard, 2004). Its main aim is to reduce the number of components that can be reached from outside the system (Howard, 2004).

Least Privilege principle main advantages consist of minimizing interactions between privileged components in a given system and hence minimizing loss in case of a successful attack (Saltzer and Schroeder, 1975). Another common principle that is similar to this one is called the Principle of Least Authority (POLA) (Spiessens, 2007).

Defense in Depth principle is derived from the security principle "*Defense in Depth*", which requires backing up one layer of security in a given system with another one (Dowd *et al*., 2006).

Security Metrics

Security, unlike other software quality attributes such as performance, reusability and reliability, has received relatively little attention (Bansiya and Davis, 2002). Many system developers tend to assess the security level of a given program based on the identification of pre-existing vulnerabilities (Chess and West, 2007; Viega *et al*., 2000a; 2000b; OWASP, 2010; Landwehr *et al*., 1994). The technique used by Maruyama (2007) and Howard and LeBlanc (2002) provides an approach for assessing the level of security of a given program based on its code. These approaches classify code as either secure or not secure. However, such approaches do not evaluate which parts of the code are more secure than others and hence it is necessary to define a metric-based software security model (McGraw, 2006) to assess the level of security of a given program. Recent work by Alshammari *et al*. (2013; 2009; 2010; 2012) has focused on measuring the overall security of a given object-oriented program with regard to its potential information flow. This approach has defined a number of information security metrics derivable from a program's design artifacts (e.g., class diagrams) and code instructions based on the program's design properties, such as coupling, cohesion, inheritance and design size. However, this approach is only applied to the design of a program and does not quantify the overall security of enterprise systems.

It has been shown that most security metrics assess program security at either a very high level (i.e., the system architecture), the design level (i.e., based on the system's design artifacts), or a low level (i.e., with respect to program's code). However, the most efficient approach for quantifying the overall information security of a given enterprise is to measure it with respect to its Enterprise Architecture (EA). This approach needs to consider data flow analysis principles between all components of the enterprise in order to trace the potential information flow between high- and low-security variables. This research aims to develop an assessment framework that consists of a number of security metrics that are capable of measuring the overall security of a given organization based on its enterprise architecture. This paper defines a novel evaluation technique for easily measuring the relative security of an organization with respect to its security- critical information flow. Achieving this goal will provide us with a technique suitable for evaluating the security level of any organization at various layers of its enterprise architecture, such as information, application and technology.

Enterprise Architecture Security Assessment Framework (EASAF) Overview

The main goal of this project is to define a framework that consists of a set of security principles, security-related artifacts and security metrics. This framework can be used to assess and recognize the relevant security characteristics of a given organization based on its Enterprise Architecture. Achieving this goal will allow enterprise information security architects to easily evaluate the security of the enterprise various components and identify principles for improving the security of existing components. Much existing work has addressed security as a separate concern when developing the architecture for a certain organization. In many cases, security is not addressed until the enterprise architecture is in its final stages or even after it has been developed. This practice has raised many security issues within enterprises and their security protection.

TOGAF 9 (TOG, 2011) is one of the few frameworks that address security when developing an EA. It aims to provide a methodology for security practitioners to follow when developing the security architecture for a given enterprise. Security architectures have a number of characteristics that need to be considered by security architects. These characteristics include defining a security methodology, composing views and viewpoints and addressing information flow within the architecture systems (TOG, 2011). Even though TOGAF considers security separately, it states that security must be addressed throughout all phases of the enterprise architecture. Therefore, it has provided security architects with a methodology for this purpose that can present guidance with a step-by-step process for developing secure enterprise architectures. This methodology consists of a number of policies and principles that must be addressed in every phase of the Architecture Development Method (ADM) (TOG, 2011). They are related to the general security properties: Authentication, authorization, audit, assurance, availability, asset protection, administration and risk management (TOG, 2011). At each phase of the ADM, there are a number of inputs from the previous domain and, of course, outputs for the next domain. For instance, the inputs of the business architecture include disaster recovery and business continuity plans, while its outputs include a threat analysis matrix (TOG, 2011). These outputs aim to consider all the policies and principles that must be considered by security practitioners to create a secure architecture. However, none of these outputs is concerned with assessing the security of every domain of the enterprise architecture. Therefore, this project aims to address this point by providing a set of metrics that measure the security of every domain in the enterprise architecture.

The four architecture layers described in TOGAF (TOG, 2011), business, information, application and technology, are also considered when defining the framework developed by this project. However, this framework differs from TOGAF in that it specifies five layers by splitting the business layer in TOGAF to include two layers: Employee and process. The reason for this practice is the importance of these two entities to any organization's security. It is believed that considering employees and processes as part of one layer (the business layer, as in TOGAF (TOG, 2011)) has a negative impact when developing a secure architecture for any organization. This practice can lead security architects give these two entities little attention when they are considered to be part of the business layer. Therefore, they need to be considered separately since they make a major contribution to the security of organizations. Figure 1 shows the five architectures that must be addressed separately by the EASAF.

The framework defined here, EASAF, consists of three elements. One is the Security Architecture Development Method (SADM), which consists of the major steps of the framework, as shown in Fig. 2. SADM can be represented as an iterative process for implementing the framework within a specific organization. The second element of the framework is the framework content model, which shows all the layers of the framework. It also gives detailed information on the related principles, inputs and outputs for every layer of the EA with relation to security, as shown in Fig. 3. The third element of this framework is a list of security metrics for assessing the security of every layer of the enterprise architecture. To define security metrics for a specific architecture, the architecture principles for every layer have to be studied. This element aims to define the principles that have the most impact on security in terms of their relation to specific security design principles. At the end, various security metrics are defined, each of which is related to a specific architecture layer and is responsible for measuring a particular architecture principle. The process that needs to be followed to define these metrics is shown in Fig. 4.

Security Architecture Development Method (SADM)

The TOGAF architecture development method is a repeatable process for the development of the enterprise architecture framework. This project defines a method that is responsible for developing the enterprise architecture security assessment framework. It is an iterative process that enables enterprise architects to develop, assess and maintain the security assessment framework, as shown in Fig. 2. It consists of seven phases; each is assigned a specific task that contributes towards developing the enterprise architecture security assessment framework. Each phase has a number of inputs and produces outputs as a result of processing the inputs. These seven phases are illustrated below in greater detail, including their responsibilities, inputs and outputs.

Phase One: Define Relevant Security Design Principles

The main task of this phase is to define the security design principles with which the organization is most concerned. If not defined by the architecture vision, these principles can usually be captured by analyzing the organization's business strategy and security policies. The output of this phase is a list of security design principles two which the organization needs to adhere in order to secure its assets. These security principles will be used later to develop the security metrics that quantify the organization's relevant security.

Phase One Inputs

- Enterprise Architecture Vision
- Enterprise Security Policies

Phase One Output

- Relevant Security Design Principles

Phase Two: Define Security-Related Enterprise Architecture Principles

Enterprise Architecture principles play a major role in deploying the organization's business strategy. Once properly defined, they have a major impact on achieving the organization's vision. In terms of information security, the enterprise architecture principles that have an impact on security must be identified, assessed and maintained to achieve a more secure architecture. Therefore, the main objective of this phase is to define those security-related enterprise architecture principles that establish the guidelines for achieving a secure organization.

Phase Two Input

- Enterprise Architecture Security Design Principles

Phase Two Output

- List of Security-Related Enterprise Architecture Principles

Phase Three: Define Employee Security Architecture

The objective of this phase is to describe the development process of the employee security architecture. It shows how this architecture is developed with regard to the architecture principles that are applicable at this stage. The outcome must adhere to the security design principles that should be applied at this architecture. Therefore, the inputs of this phase area list of security design principles and a list of architecture principles that need to be followed. The outcome is a list of security metrics that assess the security level of this phase.

Phase Three Inputs

- Employee-Related Enterprise Architecture Security Design Principles
- Employee-Related Enterprise Architecture Principles

Phase Three Output

- Employee-Based Architecture Security Metrics

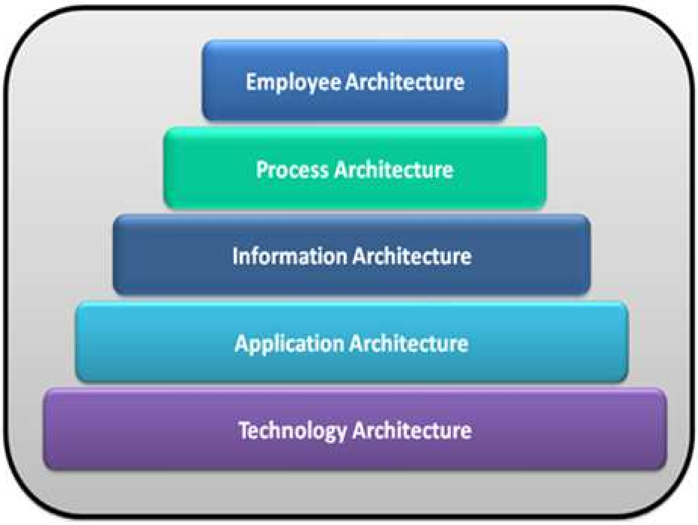


Fig. 1. EASAF architecture layers

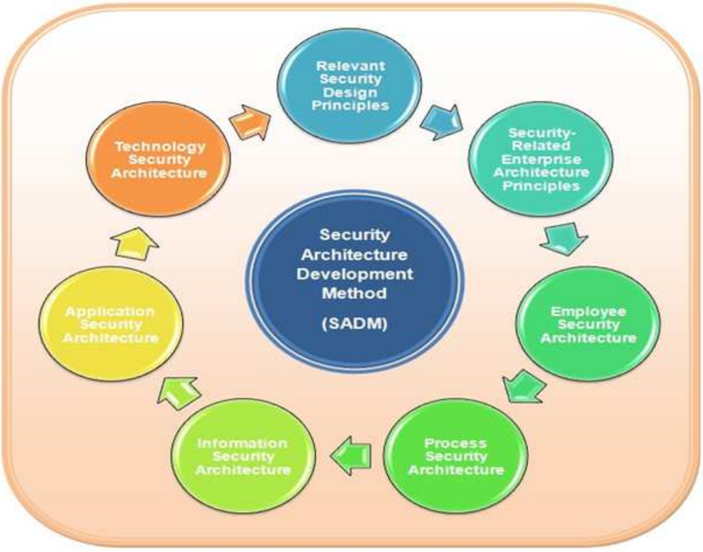

Relevant Security Design Principles
Security-Related Enterprise Architecture Principles
Employee Security Architecture
Process Security Architecture
Information Security Architecture
Application Security Architecture
Technology Security Architecture
Security Architecture Development Method (SADM)

Fig. 2. Security Architecture Development Method (SADM)

Phase Four: Define Process Security Architecture

This phase aims to define the development process of the process security architecture. It has to consider the applicable security design principles that must be adhered to in order to achieve a secure architecture with regard to the enterprise processes. It also takes into account related security enterprise architecture principles. The outcome of this phase consists of security metrics for the process architecture.

Phase Four Inputs

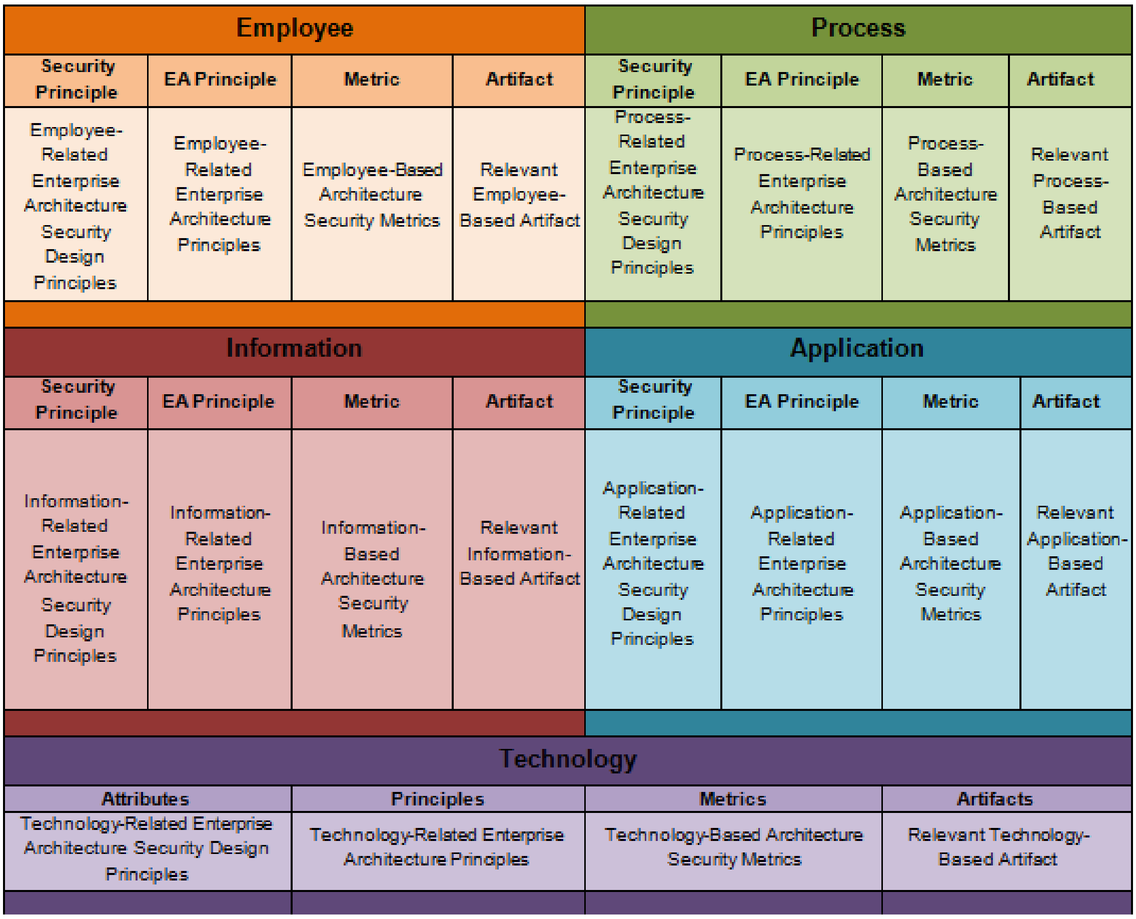
- Process-Related Enterprise Architecture Security Design Principles
- Process-Related Enterprise Architecture Principles

Phase Four Output

- Process-Based Architecture Security Metrics

Phase Five: Define Information Security Architecture

The objective of this phase is to show the process of developing the information security architecture and its outcome consists of security metrics. They assess the relevant security level of an enterprise with regard to its information architecture layer. To achieve this objective, associated enterprise architecture principles are taken into account. These metrics also need to adhere to the security principles that the architecture has stated to be necessary.



Employee				Process			
Security Principle	EA Principle	Metric	Artifact	Security Principle	EA Principle	Metric	Artifact
Employee-Related Enterprise Architecture Security Design Principles	Employee-Related Enterprise Architecture Principles	Employee-Based Architecture Security Metrics	Relevant Employee-Based Artifact	Process-Related Enterprise Architecture Security Design Principles	Process-Related Enterprise Architecture Principles	Process-Based Architecture Security Metrics	Relevant Process-Based Artifact

Information				Application			
Security Principle	EA Principle	Metric	Artifact	Security Principle	EA Principle	Metric	Artifact
Information-Related Enterprise Architecture Security Design Principles	Information-Related Enterprise Architecture Principles	Information-Based Architecture Security Metrics	Relevant Information-Based Artifact	Application-Related Enterprise Architecture Security Design Principles	Application-Related Enterprise Architecture Principles	Application-Based Architecture Security Metrics	Relevant Application-Based Artifact

Technology			
Attributes	Principles	Metrics	Artifacts
Technology-Related Enterprise Architecture Security Design Principles	Technology-Related Enterprise Architecture Principles	Technology-Based Architecture Security Metrics	Relevant Technology-Based Artifact

Fig. 3. EASAF meta-model

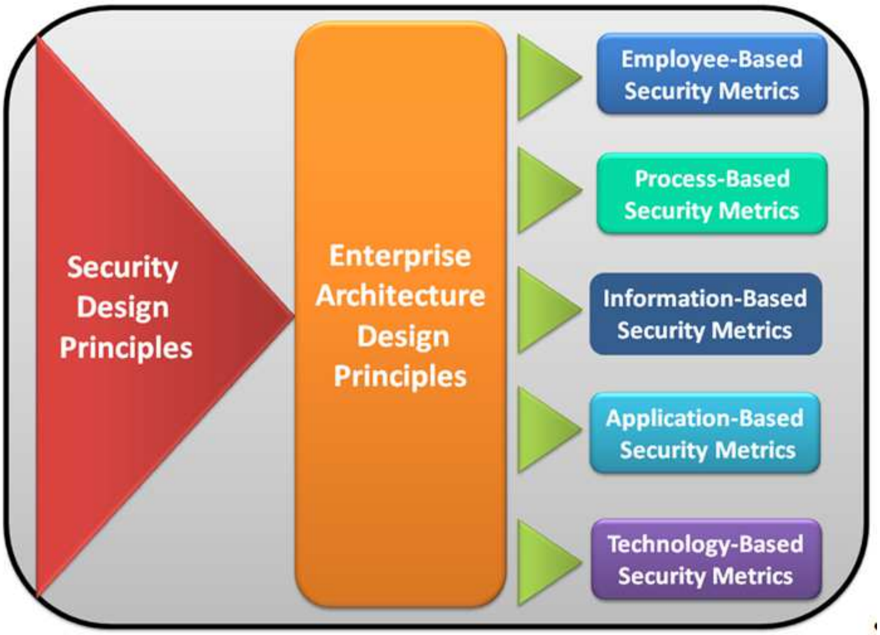

Security Design Principles
Enterprise Architecture Design Principles
Employee-Based Security Metrics
Process-Based Security Metrics
Information-Based Security Metrics
Application-Based Security Metrics
Technology-Based Security Metrics

Fig. 4. EASAF security metric development process

Phase Five Inputs

- Information-Related Enterprise Architecture Security Design Principles
- Information-Related Enterprise Architecture Principles

Phase Five Output

- Information-based Architecture Security Metrics

Phase Six: Define Application Security Architecture

The development process of the application security architecture is the main objective of this phase. Therefore, it examines the enterprise architecture principles to identify the ones that have an impact on the organization's security. These principles have to be assessed with regard to the security design principles that are defined for the application layer. The outcome is a list of security metrics that measure the security of the application architecture layer.

Phase Six Inputs

- Application-Related Enterprise Architecture Security Design Principles
- Application-Related Enterprise Architecture Principles

Phase Six Output

- Application-Based Architecture Security Metrics

Phase Seven: Define Technology Security Architecture

The main task of this phase is to show how to develop the technology security architecture. Security-related enterprise architecture principles are analyzed with regard to the identified security design principles. The result of this analysis is a list of security metrics that aim to assess the security level of an organization with regard to its technology architecture layer.

Phase Seven Inputs

- Technology-Related Enterprise Architecture Security Design Principles
- Technology-Related Enterprise Architecture Principles

Phase Seven Output

- Technology-Based Architecture Security Metrics

Adapting the SADM

The SADM is a flexible architecture development method designed in a way that makes its integration with an enterprise architecture framework an easy task. For example, if an organization is adapting the TOGAF, the SADM can be deployed in parallel with every phase of the architecture development method. Even if the organization has developed its architecture using another framework, deploying the SADM is not a challenge since it can be executed by itself after studying the organization's business strategy. This is a necessary step that aims to identify the organization's business nature and its stakeholders. This identification enables security architects to determine the security design principles that the organization is required to follow for security. This step is followed by identifying the main principles of the architecture that are of interest due to their impact on the security of the organization.

EASAF Results

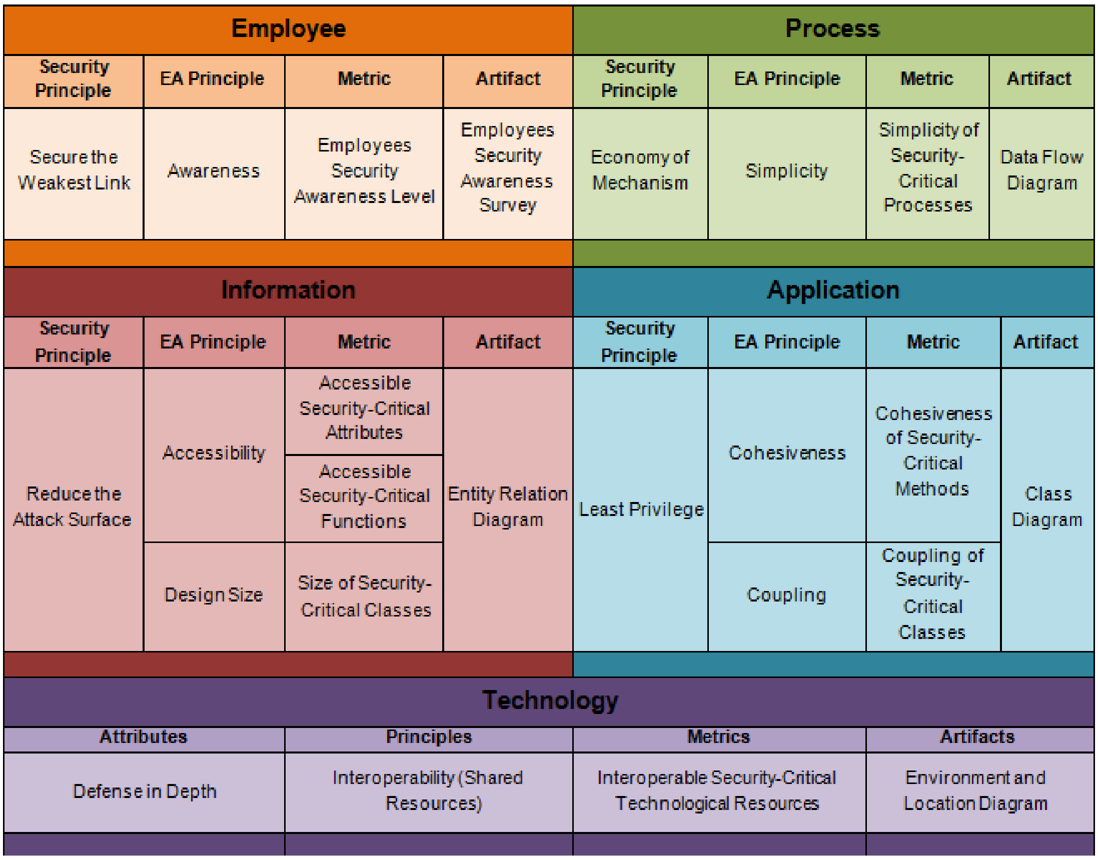
This section illustrates how to define security-related enterprise architecture principles from the educational sector perspective. The architecture principles for educational enterprises have been described in the literature review. Here, these principles are studied in more detail to define which ones have major effects on security. This section also shows how to define security metrics based on the security principles defined for every layer of the EASAF.

Security-Related Enterprise Architecture Principles

As shown previously, the enterprise architecture principles vary among different architectures. The differences primarily depend on the business nature, vision and strategy of the organization. This section defines the enterprise architecture principles that have an impact on the organization's information security based on its enterprise architecture. Therefore, a number of security-related principles are defined for each of the enterprise architecture framework layers. However, the focus here is on enterprise architecture principles related to educational organizations. Therefore, these principles will differ if other types of organizations are studied. The principles for each layer are shown in the framework model in Fig. 5.

Employee Architecture Security-Related Enterprise Architecture Principles

It has been shown that there are a number of enterprise architecture principles that are related to the business layer of the enterprise architecture framework. This section focuses on those principles that influence the security of the organization with regard to its employees. The reason for focusing on the employees of organizations as a separate entity from the business layer is the important role of employees in security. In fact, many security attacks on organizations are enabled by the lack of awareness of their employees. Thus, this project defines an assessment of a given organization based on its employees' level of security awareness.



Employee

Security Principle	EA Principle	Metric	Artifact
Secure the Weakest Link	Awareness	Employees Security Awareness Level	Employees Security Awareness Survey

Process

Security Principle	EA Principle	Metric	Artifact
Economy of Mechanism	Simplicity	Simplicity of Security-Critical Processes	Data Flow Diagram

Information

Security Principle	EA Principle	Metric	Artifact
Reduce the Attack Surface	Accessibility	Accessible Security-Critical Attributes	Entity Relation Diagram
		Accessible Security-Critical Functions	
	Design Size	Size of Security-Critical Classes	

Application

Security Principle	EA Principle	Metric	Artifact
Least Privilege	Cohesiveness	Cohesiveness of Security-Critical Methods	Class Diagram
	Coupling	Coupling of Security-Critical Classes	

Technology

Attributes	Principles	Metrics	Artifacts
Defense in Depth	Interoperability (Shared Resources)	Interoperable Security-Critical Technological Resources	Environment and Location Diagram

Fig. 5. Education EASAF meta-model

Process Architecture Security-Related Principles

Most of the previous studied enterprise architectures have given the organization process a large role when designing the EA of the organization. However, they all make it part of the Business layer. In this project, it has been determined that processes can have enormous impact on the organization when considering its security. Therefore, it has to be studied separately and therefore, there is a layer called Process. Most of the principles in the defined enterprise architecture frameworks specifically concentrate on making the process as simple as possible. Thus, simplicity is the main enterprise architecture principle for the process layer and a number of security metrics are developed to measure this principle.

Information Architecture Security-Related Principles

It has been shown previously that the information architecture layer can be related to a number of principles, including making data accessible and shared. In fact, these two principles are the commonly defined in most enterprise architecture frameworks. Therefore, these principles are the ones that need to be considered when defining a secure architecture in terms of the information layer. These two principles satisfy the security design principle of reducing the attack surface size.

Application Architecture Security-Related Principles

At the Application layer, there are a number of principles that many organizations aim to adapt in their enterprise architecture. These principles include ease of use, availability and user- friendliness. In fact, there are two main principles that most of the reviewed enterprise architectures identify as essential for any enterprise to consider when developing its architecture. The first is increasing the cohesiveness within the organization's applications, while the second is making the application architecture as loosely coupled as possible. Due to this importance, it is believed that these two principles will have the greatest impact on security. Thus, making enterprise applications secure with regard to these two principles will make the applications adhere to the security principle of least privilege. Such adherence will make the applications more secure in this regard, thus increasing the overall security of the enterprise architecture.

Technology Architecture Security-Related Principles

It has been shown that many organizations have various principles with regard to the technology architecture. Some of these principles are concerned with flexibility, scalability and making resources platform independent. These principles can be summarized in one principle, described as interoperability. All these principles have the same objective, which is to make technological resources available and able to be shared with other resources within the organization. The interoperability principle has a great effect on the security of the enterprise's technological resources. Thus, making the architecture secure with regard to this principle would adhere to the security design principle of defense in depth.

EASAF Security Metrics

This section defines the security metrics that are related to a specific layer of the EASAF. It has been shown that each layer is associated with a specific enterprise architecture design property and each metric aims to satisfy the requirements of the security design principle to which it is the most applicable. Here, five types of security metrics are defined, with descriptions of how each is extracted from specific artifacts in the enterprise architecture. The security metrics for each layer and their associated artifacts are shown in the framework model in Fig. 5.

Employee-Based Security Assessment

The layer of Employee Architecture is associated with the enterprise architecture principle of awareness. This means that the metric that quantifies how secure this layer must be defined in regard to this principle. It has been shown in many studies that employees are the weakest link in any organization in terms of information security (Edwards *et al*., 2016; Kotenko *et al*., 2011; Irani *et al*., 2011). Many security attacks are due to social engineering, which relies on a low level of employee awareness of safe security practices that need to be followed to prevent such attacks (Edwards *et al*., 2016; Kotenko *et al*., 2011; Irani *et al*., 2011). Therefore, the security metric for this layer has to be defined to meet the requirements of the security design principle of securing the weakest link. The metric associated with this layer is outlined below.

Employees' Security Awareness Level

To predict the level of security awareness of employees for any organization, a survey has to be developed. The survey must address the most important issues in terms of information security for any organization. More specifically, this survey has to concentrate on the aspects of security that any employee faces on a daily basis and measure the response to it. Ultimately, the result is calculated and interpreted to provide a meaningful result that shows the level of security awareness of the employees of a given organization. This survey can be given to employees who are asked to reply to it.

Process-Based Security Assessment

The role of business processes in the security of organizations has been investigated in a number of studies, including the work of Wangen and Snekkenes (2014) and the work of Taubenberger *et al*. (2013). These studies have shown that enterprises' business processes play a major role in the security of the organizations. They can introduce many security risks if they have not been designed properly. The best approach to reducing the risks associated with the organization's business process is to make the process as simple as possible, which satisfies the enterprise architecture principle of simplicity. Therefore, this metric quantifies the complexity of the business process in order to adhere to the EA principle of simplicity. Lowering the complexity of the processes of any system adheres to the specifications of the security design principle of Economy of Mechanism, hence making the system more secure in this regard.

Simplicity of Security-Critical Processes Metric

This metric will be capable of measuring the complexity of the business processes of a certain organization. The business processes on which this metric will focus are the ones that are automated, since they are the ones that produce the most security risks for the organization. To be capable of applying metrics of this layer to the enterprise architecture, a complete Data Flow Diagram must be supplied. This diagram will have to show the processes that rely on security-critical data.

Information-Based Security Assessment

The main aim of the metrics defined in this section is to identify how secure an enterprise is with regard to its information architecture layer. Therefore, this section defines three metrics to accomplish this goal. However, in order to be capable of measuring these metrics, an annotated Entity Relation Diagram for the enterprise must be defined. Annotations must specify security-critical attributes, functions and classes. Another solution is to propose another approach for capturing the information necessary for these metrics. The metrics are described below.

Accessible Security-Critical Attributes Metric

This metric aims to measure the accessibility of attributes that store security-critical data over attributes that do not. Therefore, it measures the ratio of accessible security-critical attributes that can be accessed from outside their class: In other words, the ratio of attributes that are not defined as private to security-critical attributes in the information architecture based on the entity relation diagram. This metric is defined with regard to the design property of data accessibility. The effect of this property on security has been shown by the works of Maruyama (2007; Alshammari *et al.* (2009). These studies have shown that making security-critical attributes less accessible from outside their classes renders these programs more secure. This approach will eventually satisfy the security principle of reducing the attack surface size.

Accessible Security-Critical Functions Metric

Similar to the previous metric, this metric aims to measure the ratio of security-critical functions that are accessible from outside their class. Such functions interact with security-critical data, which are either their inputs or their outputs. The number of these functions is divided by the number of accessible functions in the entire EA diagram of the organization. This metric is also defined with respect to the design property of data accessibility. Another possible way of accessing data is through methods that have access to attributes. Accessing security-critical attributes through methods that interact with them can have the same security impact as the direct accessibility of security-critical attributes. Therefore, it is recommended to allow less accessibility to methods that interact with security-critical attributes to satisfy the security design principle of reducing the attack surface size (Alshammari *et al.*, 2009), which can increase program security.

Size of Security-Critical Classes Metric

Security-critical classes are ones that contain security-critical data or functions. Hence, this metric's objective is to measure the ratio of security-critical classes in a given enterprise architecture to the total number of classes in that architecture. This metric relates to is the size of the security-critical classes in the information layer of the enterprise architecture. Many studies have shown that it is desirable to have a small design size of security-critical components in the system in order to adhere to the security design principle of reducing the attack surface size (Chowdhury *et al.*, 2008; Alshammari *et al.*, 2010).

Application-Based Security Assessment

The metrics defined by this layer aim to quantify how secure the enterprise architecture of a given architecture is with respect to its Application layer. To be able to capture the information needed for these metrics, an annotated Class Diagram for the enterprise must be supplied. Annotations must specify the attributes, functions and classes that are security-critical. Those metrics are shown below.

Cohesiveness of Security-Critical Methods Metric

The objective of this metric is to define a security metric with regard to the enterprise architecture principle of cohesiveness. Thus, it measures the degree of interactions between security-critical attributes and methods in a given enterprise architecture. Cohesiveness is about privileges over security-critical attributes and the smaller the number of such interactions, the better is the adherence to the security design principle of least privilege (Alshammari *et al.*, 2009). In terms of security, it is recommended to decrease the cohesiveness of interactions between security-critical attributes and methods within their classes to achieve more secure programs (Alshammari *et al.*, 2009).

Coupling of Security-Critical Classes Metric

This metric aims to develop a security metric that takes into consideration the effect of the coupling in the enterprise architecture on the Application layer in a given enterprise architecture. With regard to information security, it has been shown that there is a high correlation between coupling and the insecurity of programs. The work of Liu and Traore (2006) has shown that successful attacks in many cases are caused by highly coupled objects. Furthermore, the studies of Alshammari *et al.* (2009; 2010) have shown that loosely coupled programs can decrease the potential flow of security-critical information, thus creating more secure programs. This approach satisfies the security design principle of least privilege (Saltzer and Schroeder, 1975; Bishop, 2003). This coupling metric aims to measure the occurrence of links between security-critical attributes and classes in a given application architecture.

Technology-Based Security Assessment

The main goal of this part is to develop a security metric that can quantify the security level of the technology architecture layer in the enterprise architecture.

In terms of security, any metric developed for this layer must be defined in terms of the enterprise architecture principle of interoperability. This requirement is due to the major impact of this principle on organization security. A number of researchers have studied the importance of interoperability to security.

Interoperability is one of the principles that any enterprise architecture should preferably address at the technology layer due to its impact on lowering the cost of resources. On the other hand, the security design principle of defense in depth must also be practiced at the technology layer. Therefore, the approach of defining a security metric with regard to interoperability that quantifies the security of the technology layer is the most appropriate one.

Interoperable Security-Critical Technological Resources

This metric quantifies the security of an enterprise architecture based on its shared resources that interact with security-critical data. Its goal is to minimize the number of shared resources in a given enterprise in order to achieve the requirements of the security design principle of defense in depth. Hence, the fewer shared resources there are in a given organization, the better the design adheres to the security principle of defense in depth, thus creating a more secure organization. To be capable of applying this metric to a given enterprise architecture, a detailed location and environment diagram must be provided. The diagram has to distinguish the shared resources with security-critical data from those that do not.

Conclusion and Future Work

The primary goal of this project is to define a framework that can easily be applied to quantify the security of any organization based on its enterprise architecture. This project has achieved this goal by developing a framework based on modifying one of the most common frameworks, TOGAF, to obtain the "Enterprise Architecture Security Assessment Framework". This new framework (EASAF) has restructured the layers defined in TOGAF according to their effect on information security. Instead of the four common layers in TOGAF, this frame defines five layers: Employees, processes, information, applications and technology.

The outcomes of the EASAF include a security architecture development framework with steps to apply the framework on any architecture. The second outcome is the framework meta-model, which illustrates all the architecture layers, their relevant security design principles and enterprise architecture design principles. It also contains the security metrics for each layer and the approach that can be used to apply these security metrics.

The EASAF concentrates on quantifying the potential flow of security-critical data within an organization. Each of the five architecture layers defined in this framework has a number of security metrics that measures the security of that layer. Each of these security metrics is developed in relation to a certain enterprise architecture principle that is considered to have a major effect on security. Furthermore, this metric has to consider the main security design principle of each layer. Therefore, there are eight security metrics defined according to five enterprise architecture principles to meet the security requirements of five security design principles.

When developing the EASAF and its associated security metrics, the simplicity of application of this framework was a major objective. Therefore, this framework can be applied at the design stage of any organization's enterprise architecture as long as the required design artifacts are supplied. This approach will make it easy to quantify security at an early stage of EA development, hence discovering security risks and fixing them at an early stage. These metrics will eventually be used to compare various versions of the same architecture and show which version is more secure.

Future extensions to this work include defining a set of transformation rules for developing and maintaining secure enterprise architectures. The main aim of such rules is to provide guidance for introducing modifications into a particular EA to enhance its security. These rules will be used to allow enterprise architects to change the existing structure of an enterprise while still preserving or even improving its current security level. Further work in this project will be to implement a software tool that enables enterprise architects to automatically assess the security of any enterprise based on its architecture. This tool will provide an easy aid for designing security-critical architectures by giving enterprise architects the ability to assess their architectures automatically with regard to these security metrics.

Acknowledgement

I wish to thank the anonymous reviewers for their helpful comments. The author gratefully acknowledges Aljouf University for funding this research through grant 35/344.

Ethics

The author confirms that there are no ethical issues may arise after the publication of this manuscript.

References

Aagedal, J.O., F. den Braber, T. Dimitrakos, B.A. Gran and D. Raptis *et al*., 2002. Model-based risk assessment to improve enterprise security. Proceedings of the 6th International Enterprise Distributed Object Computing Conference, Sep. 17-20, Lausanne, Switzerland, pp: 51-51.

Abreu, F.B.E., M. Goulão and R. Esteves, 1995. Toward the design quality evaluation of object-oriented software systems. Proceedings of the 5th International Conference on Software Quality, (CSQ' 95), Austin Texas.

Alberts, C.J. and A. Dorofee, 2002. Managing Information Security Risks: The Octave Approach. 1st Edn., Addison-Wesley Professional, Boston, ISBN-10: 0321118863, pp: 471.

Alghamdi, A.S., 2009. Evaluating defense architecture frameworks for C4I system using analytic hierarchy process. J. Comput. Sci., 5: 1075-1081.

Alshammari, B., C. Fidge and D. Corney, 2012. An automated tool for assessing security-critical designs and programs. Proceedings of the National Workshop on Information Assurance Research, Apr. 18-18, IEEE Xploer Press, Riyadh, Saudi Arabia, pp: 1-10.

Alshammari, B., C.J. Fidge and D. Corney, 2009. Security metrics for object-oriented class designs. Proceedings of the Ninth International Conference on Quality Software (CQS' 09), Jeju, Korea, pp: 11-20.

Alshammari, B., C.J. Fidge and D. Corney, 2010. Security metrics for object-oriented designs. Proceedings of the Twenty-First Australian Software Engineering Conference IEEE Computer Society, Apr. 6-9, Auckland, California, USA, pp: 55-64.

Alshammari, B., C.J. Fidge and D. Corney, 2013. Security metrics for java bytecode programs. Proceedings of the Twenty-Fifth International Conference on Software Engineering and Knowledge Engineering, Jun. 27-29, Boston.

Bansiya, J. and C.G. Davis, 2002. A hierarchical model for object-oriented design quality assessment. IEEE Trans. Software Eng., 28: 4-17.

Bishop, M., 2003. Computer Security: Art and Science. 1st Edn., Addison- Wesley, Boston.

Chess, B. and J. West, 2007. Secure Programming With Static Analysis. 1st Edn., Addison-Wesley, Upper Saddle River, NJ.

Chowdhury, I., B. Chan and M. Zulkernine, 2008. Security metrics for source code structures. Proceedings of the Fourth International Workshop on Software Engineering for Secure Systems, (ESS' 08), Leipzig, Germany, pp: 57-64.

Covington, R., H. Jahangir, G. Wright, P. Silverstein and H. Dia *et al*., 2009. The oracle enterprise architecture framework. White Paper Oracle.

Dowd, M., J. McDonald and J. Schuh, 2006. The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities. 1st Edn., Addison Wesley Professional, Harlow, ISBN-10: 0321444426, pp: 1174.

Edwards, L., D. McAuley and L. Diver, 2016. From privacy impact assessment to social impact assessment. Proceedings of the IEEE Security and Privacy Workshops, SP Workshops, May 22-26, San Jose, pp: 53-57.

EOPUS, 2012. A common approach to federal enterprise architecture. Executive Office President United States.

Howard, M. and D. LeBlanc, 2002. Writing Secure Code. 1st Edn., Microsoft Press, Redmond, ISBN-10: 0735617228, pp: 768.

Howard, M., 2004. Attack surface: Mitigate security risks by minimizing the code you expose to untrusted users. Microsoft MSDN Magazine.

Irani, D., M. Balduzzi, D. Balzarotti, E. Kirda and C. Pu, 2011. Reverse social engineering attacks in online social networks. Proceedings of the 8th International Conference Detection of Intrusions and Malware and Vulnerability Assessment, Jul. 7-8, Amsterdam.

Jurjens, J., 2005. Secure Systems Development with UML. 1st Edn., Springer Science and Business Media, Berlin ISBN-10: 3540264949, pp: 316.

Kotenko, I.V., M. Stepashkin and E. Doynikova, 2011. Security analysis of information systems taking into account social engineering attacks. Proceedings of the 19th International Euromicro Conference on Parallel, Distributed and Network-based Processing, Feb. 9-11, Ayia Napa, Cyprus, pp: 611-618.

Landwehr, C.E., A.R. Bull, J.P. McDermott and W.S. Choi, 1994. A taxonomy of computer program security flaws. ACM Comput. Surv., 26: 211-254.

Liu, M.Y. and I. Traore, 2006. Empirical relation between coupling and attackability in software systems: A case study on DOS. Proceedings of the Workshop on Programming Languages and Analysis for Security, (LAS' 06), Ottawa, pp: 57-64.

Maruyama, K., 2007. Secure refactoring - improving the security level of existing code. Proceedings of the Second International Conference on Software and Data Technologies (ICSOFT' 07) Barcelona, Spain, pp: 222-229.

McGraw, G., 2006. Software Security: Building Security In. 1st Edn., Addison-Wesley Professional, Upper Saddle River, ISBN-10: 0321356705, pp: 408.

OWASP, 2010. The open web application security project.

QGCIO, 2009. Queensland government enterprise architecture framework 2.0 (QGEA) Queensland Government Chief Information Office.

Saltzer, J.H. and M.D. Schroeder, 1975. The protection of information in operating systems. Proc. IEEE, 63: 1278-1308.

Sessions, R., 2007. A comparison of the top four enterprise architecture methodologies.

Spiessens, A., 2007. Patterns of safe collaboration. PhD Thesis, University of Catholique de Louvain.

Sun, P.S.H. and S. Xu, 2012. Oracle enterprise architecture framework: Information architecture domain. White Paper, Oracle.

Taubenberger, S., J. Jürjens, Y. Yu and B. Nuseibeh, 2013. Resolving vulnerability identification errors using security requirements on business process models. Inf. Manag. Comput. Security, 21: 202-223.

TOG, 2011. TOGAF Version 9.1. Open Group.

UKMD, 2012. Mod architecture framework. UK Ministry Defence.

USMD, 2010. The DoDAF architecture framework. US Ministry Defence.

Viega, J. and G. McGraw, 2002. Building Secure Software: How to Avoid Security Problems the Right Way. 1st Edn., Addison-Wesley, Boston.

Viega, J., G. McGraw, T. Mutdoseh and E. Felten, 2000a. Statically scanning java code: Finding security vulnerabilities. Software, IEEE, 17: 68-77.

Viega, J., J. Bloch, Y. Kohno and G. McGraw, 2000b. Its4: A static vulnerability scanner for C and C++ code. Proceedings of the 16th Annual Conference Computer Security Applications, (CSA' 00), pp: 257-267.

Wangen, G. and E.A. Snekkenes, 2014. A comparison between business process management and information security management. Proceedings of the Federated Conference on Computer Science and Information Systems, Sept. 7-10, Warsaw, Poland, pp: 901-910.

Zachman, J.A., 1987. A framework for information systems architecture. IBM Syst. J., 26: 276-276.