XXI IMEKO World Congress "Measurement in Research and Industry"
August 30 – September 4, 2015, Prague, Czech Republic

ENTERPRISE ARCHITECTURE ANALYSIS FOR SECURITY ISSUE DIAGNOSTICS IN DISTRIBUTED SYSTEMS

Justinas Janulevičius [1], *Lauryna Šiaudinytė* [2]

[1] Vilnius Gediminas Technical University, Vilnius, Lithuania, justinas.janulevicius@vgtu.lt
[2] Vilnius Gediminas Technical University, Vilnius, Lithuania, lauryna.siaudinyte@vgtu.lt

Abstract – Distributed systems offer great benefits, such as resource balancing and scalability as well as being the foundation for new generation of services, enabling enterprises to outsource a great portion of their infrastructure, necessary for daily operations. However, usage of distributed systems, especially if using them as a service from a third party provider, brings concerns of security to the focus. Typically, well established enterprises run their internal infrastructure, therefore diagnosing new issues that are brought along with the new technology is a challenge. However, having the model of the existing enterprise architecture and using analysis models enables diagnostics of security issues and provides information, essential to ensure proper operation. This paper presents an attempt to map and design the required components to be able to perform security issue diagnostics in distributed systems by Enterprise Architecture (EA) analysis.

Keywords: distributed systems, enterprise architecture, security.

INTRODUCTION

Distributed systems is an emerging field of computing, bringing numerous new features into use. Using of such distributed resources is beneficial from many perspectives beginning with meeting the enterprise needs as well as enabling high-scale research projects for organizations that do not specifically have the infrastructure, required to run them.

However, the complexity of a modern enterprise or research facility infrastructure and its' influence on the overall performance level is such a complex structure that defining the influence of any component requires a systematic approach. Therefore, a methodology for structured modeling and analysis of the Enterprise Architecture (EA) has been introduced [1]. Using the concept of enterprise architecture modeling enables the analysis of the performance architecture as well as diagnosing the malfunctioning components [2], including security issues. Moreover, the enterprise architecture is supported by various sophisticated tools and software products that simplify the modeling as well as provide automation for diagnosing the problematic areas. Description of such architecture is defined by conceptual models visualized as diagrams [3]. Although EA is a broader subject, covering aspects from performance (PRM), business (BRM) to data (DRM), application (ARM), and infrastructure (IRM) reference models [4], this study covers to the latter (ARM and IRM) as presented in Table 1.

Table 1. Covered areas of the EA

ARM	• System; • Application Component; • Interface.
IRM	• Platform; • Network; • Facility.

Distributed network security issues are related to the categories, presented in Table 1.

1. RELATED WORKS

Portions of EA have modeling languages that meet the requirements of the field. Architectural modeling languages is the key component for the design of the EA, as it enables the modeling process itself. Information system architecture, presented as diagrams is one of the EA fields. There are numerous modeling languages that serve for this purpose. They include SysML [5], BPMN [6] and the extensions to use them for certain domain, such as industrial control system security analysis [7]. Some of the modeling languages, like CORAS [8] have extensions to perform the analysis according to international standards.

However, the sophistication of such tools does not cover the reasoning at the required level by suffering of being vague or subjective therefore leaving the diagnostic part partially uncovered. As a solution, a modeling language covering the security aspects of the EA that includes expertise of the field expressed as probabilities – the CySeMoL [9] – is used for this research. It offers a sophisticated tool developed on [10].

2. ENTERPRISE ARCHITECTURE MODELING

Based on the area, covered by the model, proper modeling is carried out in a way that every aspect is covered by it. Based on [11], on the technical level this study deals with the concepts of Technology layer, that include interfaces, communication paths, services, networks, software products and devices. Combinations of these concepts and the relations between them can represent the information infrastructure as a complete view. The meta-model of the Technology layer is presented in Fig. 1.

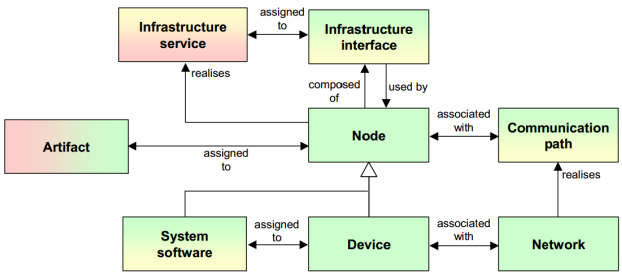

Fig. 1. Meta-model of Technology layer of enterprise architecture [11]

The Technology layer is the lowest layer that serves as a foundation for application and business layers, therefore the security issues of this layer are critical for the whole system.

The main structural component in this layer is node, which is considered as a computational resource that enables deployment of executable artefacts. A device is a node with physical presence. Interface is a point of access, where node functionality can be accessed by other nodes and application components. Network in this case is a physical communication medium. System software is an environment for components and objects to operate on [12]. A specific modeling language covering all the required concepts and providing analysis – CySeMoL [9] that runs on the Enterprise Architecture Analysis Tool [10] is used in this study.

2.1 Modeling in CySeMoL

Cyber Security Modeling Language (CySeMoL) is an expertise meta-model based realization for the assessment of information security of enterprise architectures. It covers the technical layer of enterprise architecture as well as parts of application layer. CySeMoL performs as attack-graph tool so the accuracy depends on the level of detail provided by the model.

The CySeMoL model concepts are represented as classes with two types of attributes – `defense` and `attack step`. These attributes are specific depending on the concept. This model has predefined constrains for object pairing, and the relations between them, thus disabling illegal connections as well as providing various types of relations for the same architecture depending on the situation. An `Attacker` object is connected to the infrastructure to a desired component to assess the possibility of misusage through the specific object. This also leads to the ability to have different target goals. The attacker can also have connections to multiple objects simultaneously [13].

2.2 Specifics of Distributed System Modeling

A distributed system is a complex architecture, therefore the representation of such architecture as a model has its' own specifics. This kind of architecture can be represented as a three-layered stack, where the bottom layer covers the physical infrastructure, the middle layer defines the platform and the top layer serves as application level from the technical point of view.

Modeling in CySeMoL according to [13] is carried out with the predefined meta-concepts and the relations between them. In this case `SoftwareProduct` is a primary version of any software that runs the hardware excluding patches and updates. It is followed by `OperatingSystem` which is the same as `SoftwareProduct`, except the patching issues are resolved. The relation between the two objects is set to "*Operates*". Connecting `OperatingSystem` to `ApplicationServer` denotes that the server operates the machine. `ApplicationServer` relation to `SoftwareProduct` specifies the server type. `ApplicationServer` connection to `WebApplication` specifies that the type of this server is a web server. `Datastore` denotes that the server stores data. Connecting the server to `NetworkZone` defines an interface to the network.

3. SECURITY ASPECTS FOR DISTRIBUTED SYSTEMS

To formalize the features of a distributed device control systems, International Electrotechnical Commission has released a specification [14]. It offers a systematic approach for the design of distributed industrial process measurement and control systems (IPMCS) as well as specifies reference models and covers the life cycle of a control system [15]. The reference Distributed Control Systems Model is presented in Fig. 2.

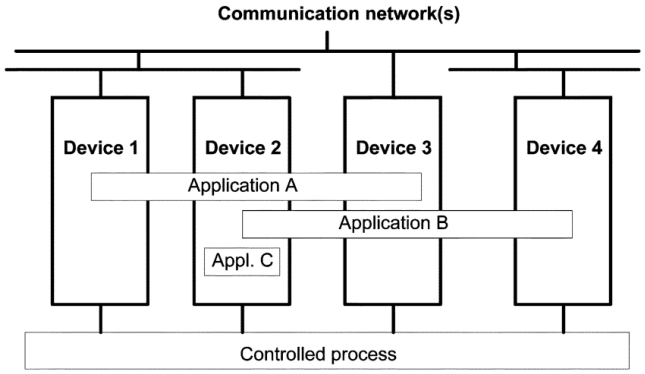

Fig. 2. Distributed Control Systems Model [14]

From the model, provided in Fig. 2 it is visible that applications can run on various machines simultaneously, sharing different roles and communicating via communication networks by a controlled process.

The security challenges that such system is facing are identification, entity authentication, data authentication, authorization, integrity, confidentiality, non-repudiation and execution safety. This model, proposed in [15] introduces a secure device control gateway that consists of:

- Security Agent – checks the authenticity and integrity of incoming dataflow;
- XML-Binder Agent – generates supported schedulable tasks;
- Admission Agent – checks task compliance with admission policy;
- Queue Agent – queues successfully admitted tasks;

This gateway is illustrated in Fig. 3.

Modeling of a distributed control system in an enterprise architecture modeling language based on the presented methodology would be beneficial for a complex, multi-perspective analysis of such system.

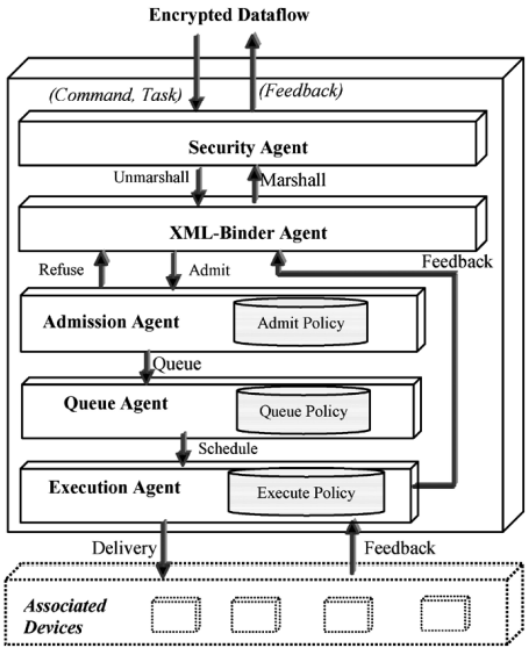

Fig. 3. Architecture of SDCG [15]

3.1 Modeling a Distributed System for Security Assessment

The Distributed Control Systems Model presented in Fig. 2 represented as an enterprise architecture technical layer model is presented in Fig. 4.

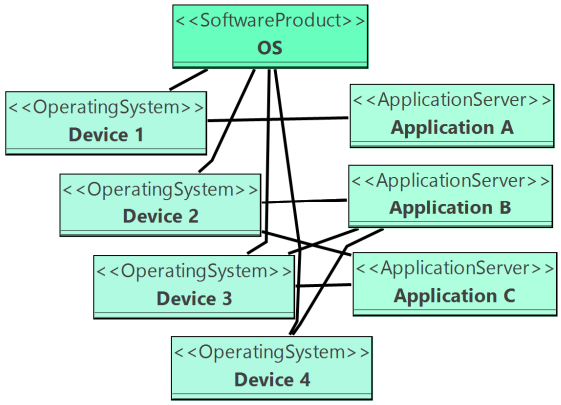

Fig. 4. Distributed Control Systems Model as EA technical layer model

From this model it is clear that conversion of the provided model to the EA technical layer model leaves the security issues coming from the inter-communication via networks uncovered. Therefore it is necessary to examine and implement the factors of impact of such phenomenon to the model.

3.2 Application of the Research for Cloud Computing

Cloud computing information security is a complex issue as it takes more components into account for the assessment. The choice of the delivery model defines the sharing of security areas managed by customer and vendor. This shows the importance of trust between the customer and vendor.

The cloud is designed as a four-layered architecture, consisting of infrastructure, application stack, application, and user layers.

Technical reports on cloud computing security assessment [16] provide information on this topic based on technical documentation, issued by trusted sources. One of the sources, the ENISA report on Cloud Computing [17] consists of known vulnerabilities, covering the most of the domain.

Architecture security is assessed using scenarios, called the attack vectors. They represent malicious activity possibilities may be executed have to be defined. The aggregation of these vectors provides a complete picture of probable attacks called the attack surface [18].

The attack surface of cloud computing expands the conventional computing attack surface due to the communication over public networks. Moreover, when using the public cloud model, the same infrastructure is shared among multiple users (or tenants) leaving a possibility of side-channel attacks of shared resources.

Gruschka and Jensen [19] proposed a model in which cloud computing scenario is built based on three classes of actors: users, services and providers. In this model, every cloud computing scenario interaction can be addressed to two entities, thus every attack vector here is detailed as a set of three-class bi-directional model interactions. Based on this concept, the reasoning, designed for client-server type of services only two surfaces.

Public cloud service providers manage most of the security aspects inside the cloud architecture, leaving the usage of the outsourced infrastructure based on trust. Level of trust and responsibility divided by the parties from technical aspects is managed setting up a contractual relationship between the customer and the provider. Service Level Agreement (SLA) is typically the realization of the subject. An international standard covering this domain [20] is being prepared, although guidelines for cloud service level agreement standardization [21] have already been published and fully cover the SLA aspect of cloud computing security. Based on the resource management architecture provided in [22], it plays the key role.

SLA enables the control of the security aspects as well as the overall quality of service. However there is no distinctive line between the two areas, as aspects of proper delivery of service fall for the security category as well (e.g. Availability is one of the main concepts of information security, however it is nested under the Quality of Service).

4. CONCLUSIONS

The enterprise architecture technical layer modeling use and benefits are presented in this paper, as well as the possibilities early diagnosis of weak links and risk assessment are analyzed. Moreover, security aspects of distributed systems are analyzed. A model, provided by [14] is implemented as enterprise architecture model. The need of extension of the enterprise architecture for network intercommunication security issue estimation is presented. A description of implementation of the research for cloud computing is presented and points out the need of trust management to control and prevent the threats coming from third party service suppliers. This leads to a need of regulatory basis to define the responsibilities over the distributed

components of the overall system.

REFERENCES

[1] S. A. Bernard, An Introduction to Enterprise Architecture, Bloomington: AuthorHouse, 2012.

[2] M. Pulkkinen, A. Naumenko and K. Luostarinen, "Managing information security in a business network of machinery maintenance services business – Enterprise architecture as a coordination tool," *Journal of Systems and Software,* vol. 80, no. 10, p. 1607–1620, 2007.

[3] International Organization for Standardization, ISO/IEC 42010:2007 Systems and software engineering - Recommended practice for architectural description of software-intensive systems, Geneva: International Organization for Standardization, 2007.

[4] US Office of Management and Budget, "Federal Enterprise Architecture Framework Version 2," US Office of Management and Budget, Washington, 2013.

[5] S. Friedenthal, A. Moore and R. Steiner, A Practical Guide to SysML, Waltham: Elsevier, 2014.

[6] M. Chinosi and A. Trombetta, "BPMN: An introduction to the standard," *Computer Standards & Interfaces,* vol. 34, pp. 124-134, 2012.

[7] L. Lemaire and J. Lapon, "A SysML Extension for Security Analysis of Industrial Control Systems," in *2nd International Symposium for ICS & SCADA Cyber Security Research 2014 (ICS-CSR 2014)*, St Pölten, 2014.

[8] K. Beckers, M. Heisel, B. Solhaug and K. Stølen, "ISMS-CORAS: A Structured Method for Establishing an ISO 27001 Compliant Information Security Management System," in *Engineering Secure Future Internet Services and Systems*, Heidelberg, Springer, 2014, pp. 315-344.

[9] T. Sommestad, M. Ekstedt and H. Holm, "The Cyber Security Modeling Language: A Tool for Assessing the Vulnerability of Enterprise System Architectures," *Systems Journal,* vol. 7, pp. 363-373, 2013.

[10] M. Buschle, P. Johnson and K. Shahzad, "The Enterprise Architecture Analysis Tool – Support for the Predictive, Probabilistic Architecture Modeling Framework," in *Nineteenth Americas Conference on Information Systems*, Chicago, 2013.

[11] H. Jonkers, M. Lankhorst, R. V. Buuren, M. Bosangue and L. V. D. Torre, "Concepts for Modeling Enterprise Architectures," *International Journal of Cooperative Information Systems,* vol. 13, pp. 257-287, 2004.

[12] The Open Group, ArchiMate 2.1 Specification, The Open Group, 2013.

[13] H. Holm, M. Ekstedt, T. Sommestad and M. Korman, "A Manual for the Cyber Security Modeling Language," Department of Industrial Information and Control Systems, Royal Institute of Technology, Stockholm, 2013.

[14] International Electrotechnical Commission, IEC/PAS 61499: Function blocks for industrial-process measurement and control systems, International Electrotechnical Commission, 2001.

[15] Y. Xu, R. Song, L. Korba, L. Wang, W. Shen and S. Lang, "Distributed Device Networks with Security Constraints," *IEEE Transactions on Industrial Informatics,* vol. 1, no. 4, pp. 217-225`, 2005.

[16] Context Information Security, Ltd., "Assessing Cloud Node Security," Context Information Security, Ltd., London, 2011.

[17] D. Catteddu and G. Hogben, "Cloud Computing: Benefits, Risks and Recommendations for Information Security," European Network and Information Security Agency, Heraklion, 2009.

[18] M. Howard, J. Pincus and J. M. Wing, "Measuring Relative Attack Surfaces," Carnegie-Mellon University, Pittsburgh, 2003.

[19] N. Gruschka and M. Jensen, "Attack Surfaces: A Taxonomy for Attacks on Cloud Services," in *IEEE 3rd International Conference on Cloud Computing*, 2010.

[20] "ISO/IEC CD 19086-1. Information technology Cloud computing: Service level agreement (SLA) framework and Technology Part 1: Overview and concepts," International Organization for Standardization, 2015.

[21] "Cloud Service Level Agreement Standardisation Guidelines," European Commission. The Cloud Select Industry Group. Subgroup on Service Level Agreements, Brussels, 2014.

[22] D. C. Marinescu, Cloud Computing - Theory and Practice, Amsterdam: Elsevier, 2013.