Modeling the Linkage between Systems Interoperability and Security Engineering

Elena Irina Neaga
Systems Engineering Division
Department of Electronic and Electrical Engineering
Loughborough University
Loughborough, LE11 3TU, UK
e.i.neaga@lboro.ac.uk

Michael J de C. Henshaw
Systems Engineering Division
Department of Electronic and Electrical Engineering
Loughborough University
Loughborough, LE11 3TU, UK
m.j.d.henshaw@lboro.ac.uk

Abstract - *Industry, finance, and other business activities are increasingly reliant on computer networks and systems, which demand effective interoperability of systems. But this also demands effective systems security, which poses a major challenge to the socio-technical interactions enabled by interoperable tools. This paper addresses modeling of the linkages between interoperability and security in the model design stage of systems development. It considers current interoperability frameworks and the manner in which they may be combined with security standards and desirable characteristics to create trusted, robust systems that are central to the operation of network enabled large scale applications. An holistic approach for interoperability and security is presented based on systems requirements modeling and model based architecting principles.*

Keywords: interoperability, security, model driven architecting, SABSA^{R}, systems security engineering, interoperable secure systems

1 Introduction

Modern society depends on effective interoperability between systems but, at the same time, increased interoperability may lead to greater risks to systems security. The objective of this paper is to link interoperability frameworks to information protection approaches and systems security engineering using modeling approaches such as requirement elicitation and modeling, and model driven architecting principles. This paper describes the context and challenges associated with system of systems interoperability and security engineering, and explains the approaches and initial results derived within a new research programme, iGRC (Integrated Governance, Risk and Compliance, http://www.igrc.co.uk).

The interoperability frameworks considered are: ATHENA-IP (Advanced Technologies for interoperability of Heterogeneous Enterprise Networks and their Applications Integrated Project) [1], EIF (European Interoperability Framework) [2], INTEROP-VLAB (The International Virtual Laboratory for Enterprise Interoperability) [3], and SCOPE (Systems, Capabilities, Operations, Programs, and Enterprises) of NCOIC (Network Centric Operations Industrial Consortium) [4].

Interoperability is a key concern for network enabled complex systems and "systems of systems" which has facilitated advancement of highly collaborative environments such as virtual organizations and extended enterprises together with their supply chains. Several important aspects of enterprise interoperability have been the focus of European IST programmes and initiatives such as EIF, INTEROP-VLAB and ATHENA - IP. But without sufficient security guarantees, organizations will not be willing to share information and collaborate using interoperable software tools. Thus, holistic approaches to interoperability and security are needed and should be directed to the development of tools for supporting security engineering and broader information security risk management programmes. These approaches should consider organizational and human factors, such as personal responsibilities (policies and best practice for system security) from the earliest stage of the analysis.

The requirements view of a model is very important because it drives the system modeling (e.g. the definition of use-case diagrams in UML), and subsequently the development of the system. Usually, designers specify system models along with their requirements and use tools to automatically generate system architectures from the models including complete, configured access control infrastructures.

2 "Real-World" Interoperable Secure Systems

Despite a huge amount of literature on interoperability research and applications, e.g. [6],[7],[8], the development and implementation of interoperable systems in industrial and business contexts are at an early stage. There are still

978-1-4244-8196-5/10/$26.00 ©2010 IEEE
DOI 10.1109/SOSE.2010.453

several issues that will require novel solutions. Some of these issues are explained below:

1. The use of standards and architectural frameworks does not always guarantee achievement of desired levels of interoperability;
2. Non-technical issues, such as culture, human communication, and interaction alongside computer and human-domain specific knowledge, are proven to be barriers to achieving interoperability [5];
3. There is a need for analysis and evaluation of interoperability itself;
4. Rapid development of technology may decrease the degree of systems interoperability if the interoperability requirements are not fully considered at the design stage.

An important area of concern is that the interoperability frameworks do not sufficiently address information protection, trust and security. These issues are crucial for assuring trusted electronic business relationships and virtual/online collaboration as well as network enablement in supply chains and defence. A number of gaps have been identified in software engineering methods applied to the design and development of secure systems [9], [10], and whilst recent ontology driven systems development has a positive impact on interoperability, its openness increases systems vulnerabilities to security.

Information security is different from IT systems security. For many years the focus has been mainly on IT security (e.g. cryptographic analysis) and usually the implementation of security tools has been done by IT departments and computer experts. During the early 90s key aspects started to change and the first draft of an information security management standard BS 7799 was produced. It focused on security related to the synergies of people, processes, and information as well as IT systems. Since then, early security management standards have been transformed into international standards published by ISO/IEC. These standards are being used by enterprises and organizations, and there are currently several initiatives holistically capturing security issues related to people, organization and technology. However application of standards does not guarantee solving the broad spectrum of systems security problems.

This paper explores existing solutions and proposes ideas to bridge the gaps. The main contribution is the identification of the requirements for a design model of secure interoperable systems**.** Such systems would maintain an acceptable level of interoperability without compromising information protection and systems security requirements as defined in standard ISO/IEC 13335. The paper also contributes to the advancement of integrating systems, software, and security engineering by conceptually linking interoperability approaches and security engineering, which has been defined in relation to software engineering [9] and Enterprise Security Architecture [11].

3 Integrating Interoperability and Security Models

3.1 Model-Driven Approach

Model-Driven (Software and Systems) Engineering (MDE) is a promising approach [12] that:

1. deals with models as an important artefact during software development;
2. envisages the problem and the solution domain at different levels of abstractions and;
3. defines methodologies for each level of abstraction and provides techniques to lower the level of abstraction by defining relationships between the participating models.

The development of models using model driven approaches is already used in software and systems engineering [12]. The construction of models during requirements analysis and system design can improve the quality of the resulting systems by providing a foundation for early analysis [10]. The models also provide support for systems specifications for the later development phases and, when the models are sufficiently formal, they can provide a basis for implementation.

Model Driven Architecture [13], [14] is a concept and approach to specifying and developing applications where systems are represented as models and transformation functions are used to map between models as well as to automatically generate executable code. MDA used the following hierarchy of models [13], [14]:

- Computation Independent Model (CIM) dedicated to the representation of domain and system requirements in the environment in which the system will operate;
- Platform Independent Model (PIM) dedicated to modeling of the systems functionality, but without a definition of any platform for implementation;
- Platform Specific Model (PSM) which is a modified PIM through the transformation into a platform dependent model.

MDA is applied to modeling interoperable systems and a major result of ATHENA IP is a set of models and tools called PIM4SOA (PIM for Service Oriented Architecture). MDA is also used for model driven systems security engineering solutions by providing a framework in which security concepts are modeled using UML and Domain Specific Languages at the PIM abstraction level

and are merged with other requirement models that could include interoperability requirements. These secure enhanced PIMs are transformed to different open standard specifications (PSM) which in turn configure the component based reference architecture. However a risk of using MDA is that it is not possible to adeuqately capture the layers of complexity at the implementation level.

3.2 Levels

The European Interoperability Framework (EIF) identifies three levels of interoperability [2]:

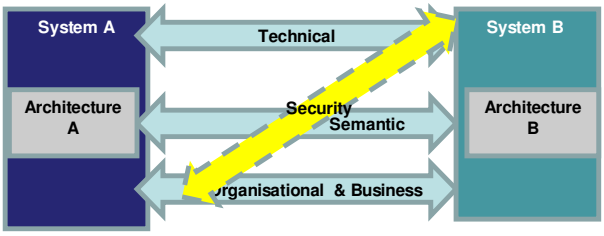

Figure 1. Levels of Interoperability including Security

Organizational interoperability (i.e., business unit, process and people interactions across organization borders) is focused on the definition of business goals, modeling business processes and organizational collaboration issues. It addresses the requirements of the user community by making services and systems available, easily identifiable, accessible and user-oriented. In the context of IT, definition of this level corresponds with the *business interoperability* definition by Legner and Wende (2006) [7]: 'the organisational and operational ability of an enterprise to co-operate with its business partners and to efficiently establish, conduct and develop IT-supported business relationships with the objective to create value'.

Semantic interoperability (i.e., information and service sharing) is concerned with ensuring that the same meaning of exchanged information is obtainable in the same way by any other computer system and/or human agent that were not initially designed for this purpose.

Technical interoperability (i.e., data and message exchange) covers the technical aspects of connecting (computer) systems and services through interfaces, protocols etc. applying software engineering techniques. It includes key aspects such as open interfaces, interconnection services, data integration and middleware, as well as data presentation and exchange, accessibility and security services as defined by the standard IEC TC65/290/DC.

Figure 1 depicts these main levels of interoperability. In addition the security level is suggested and it covers the description of the security that can be incorporated into the design of an interoperable secure system. This level includes security concepts, services and procedures. The security level can be split into the following components:

1. Physical software systems security based on applying computer cryptography and safety or software criticality implementation;
2. Human / personnel security based on the procedure, regulations, methodologies that make an organisation/enterprise/ system safe
3. Cyber / Networking level that is mainly concerned with controling cyber attacks and vulnerabilities and reducing their effects.

3.3 Interoperability Requirements

Requirements elicitation and modeling are detailed processes with highly developed methods and procedures as part of requirements engineering and management. The application of the principles of requirements engineering is not an objective of this paper and we provide only a few ideas on interoperability and security requirements supporting the approach. From a systems engineering perspective, the requirements for interoperability should be positioned alongside those for maintainability, reliability, safety and supportability [15]. These requirements can be described at a high- level as follows:

a) network enabled systems must be able to effectively and efficiently interoperate if needed
b) (newly) designed systems must be able to interoperate effectively and efficiently and time sensitively when deployed anywhere within legacy dominated Systems of Systems environments;
c) human driven socio-technical systems must be able to interoperate at different levels;
d) robustness to external and unexpected events must be considered.

3.4 Using SABSA^{R} and Model Driven Security

Figure 2 shows a modeling framework for designing interoperable secure systems that combine model driven security, requirements modeling and enterprise security architecting as will be explained in the sections that follow.

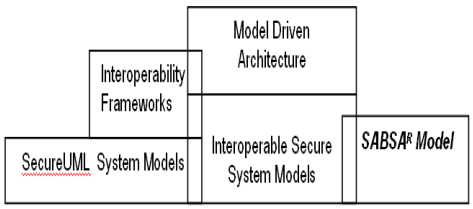

Figure 2. Modeling Interoperable Secure Systems

Additional investigations and experimental work are required at the intersection of existing modeling approaches and this could be directed to meta-modeling techniques for systems of systems security engineering.

3.4.1 SABSA^{R}: Enterprise Security Architecture

Generally the main role of architecting is to effectively manage complexity and, therefore, approaches for the management of complexity has also included system security and certification aspects. SABSA (Sherwood Applied Business Security Architecture) is a framework and methodology for Enterprise Security Architecture and Service Management used by numerous organisations [11]. This framework is used globally to meet a wide variety of Enterprise needs, including Risk Management, Information Assurance, Governance, and Continuity Management. It ensures that the needs of the enterprise are met completely and that security services are designed, delivered and supported as an integral part of the business and IT / software systems management infrastructure. The model follows the Zachman architecting principles [16].

3.4.2 Model Driven Security

INCOSE Working group on Systems Security Engineering has defined Model Driven Security as "An element of system engineering that applies scientific and engineering principles to identify security vulnerabilities and minimize or contain risks associated with these vulnerabilities" [17]. Therefore it is a discipline that uses a systems engineering approach and methods to produce a comprehensive spectrum of protection mechanisms for a system or program at the following levels: physical, information, software systems, communications, personnel, and operations. According to ISO/IEC 13335 security standard "system security consists of defining, achieving, and maintaining the following properties: confidentiality, integrity, availability, non-repudiation, accountability, authenticity, and reliability" [18]. The systems engineering approaches include model based systems engineering, and Basin et al. (2005) have demonstrated that the Model Driven Architecture (MDA) can be specialized to the Model Driven Security approach using RBAC (Role Based Access Control); this is a mechanism used for modeling the access control for designed models [10]. The concept of role-based permissions is included in the principles of access control, which defines limits of using only the IT resources they need to perform their tasks. The types of access control are as follows [10]:

- Discretionary: access to information is controlled by the owner.
- Mandatory: Imposes security conditions and restrictions for all users of IT systems.
- Role based: access to information and its resources is based on the user's role.

Model Driven Security Architecture is defined as:

- an extension of MDA through modeling the security requirements in PIM (Platform Independent Model)
- applying SecureUML: A UML-Based Modeling Language for Model Driven Security.

3.5 Security Requirements

System security weaknesses originate in the incomplete or conflicting nature of security requirements. A comprehensive analysis of software systems security is described in Software Security Assurance State-of-the-Art Report (SOAR) by Goertzel et al. (2007) [19]. Software assurance is "the ability to provide to software acquirers and users the justifiable confidence that software will consistently exhibit its required properties. Among these properties, *security* is what enables the software to exhibit those properties even when the software comes under attack" (Goerzel et al., 2007: xvii) [19]. The considered properties are correctness, predictable operation, usability, interoperability, performance, dependability, and safety. The security requirements can be classified as follows:

Functional Security Requirements which are security functions and services that need to be achieved by the system under consideration. Examples could be authentication, authorization, backup, server-clustering, etc. This requirement artefact can be derived from best practices, policies, and regulations.

Non-Functional Security Requirements which are security related architectural requirements, such as robustness, high integrity and scalability. This type of requirement is typically derived from architectural principles and best practices including standardisation.

Secure Development Requirements which describe required activities during system development which assure that the outcome is not subject to vulnerabilities. Examples could be data classification, coding guidelines or test methodology.

Mead (2007) has analysed the process for the identification of security requirements using a method called "security quality requirements engineering" (Square) that has been developed within the CERT programme at Carnegie Mellon University's Software Engineering Institutes [20]. The main issues regarding the identification of security requirements are as follows:

a. Although they are planned to be identified during the systems life cycle they tend to be general mechanisms such as password protection, firewalls and virus detection tools.

b. They are developed independently of the rest of the requirements engineering and hence are not integrated into the main stream activities.

c. Therefore, specific system protection mechanisms are neglected and implementation is not feasible.

d. Some times the security requirements are considered negative requirements such as "the system shall not allow successful attacks" (Mead, 2007:46) [20]

e. The security requirements are still not seen as a benefit for the systems due to increase costs.

4 Gaps Identification and Analysis

Generally, integration of system design models consisting of interoperable models and security models has not been achieved. Currently the need to maintain a critical balance between openness and embedded security requirements from the modeling stage has not yet received much consideration. Although security requirements and threats are often considered during the early development phases (requirements analysis), and security mechanisms are later employed in the final development phases (system integration and test), there is a gap in the middle. As a result, security is typically integrated into systems in an ad-hoc manner, which degrades the security and maintainability of the resulting systems. Despite the development of SecureUML the development of interoperable secure systems is not guaranteed, because the balance is towards achieving security neglecting interoperability.

The Security Enterprise Architecture Model SABSA^{R} [11] does not consider enterprise interoperability architectures, levels and layers and this model could not be mapped to the levels of interoperability of EIF as well as layers of NCOIC QoS [4]. Therefore, a more holistic approach to modeling interoperability and security requirements from the system design stage is required. It is also needed to progress the development of interoperable security strategies through standard harmonisation, mapping and/or the development of a top-level, new standard that can cover different systems characteristics, including interoperability and security.

5 Modeling and Contributions

The suggested integrated modeling approach is shown in figure 2 based on combining interoperability and security models and balancing the requirements that have been briefly presented in the previous sections; and described them through a model driven approach or an enterprise architecture. The requirements presented in the 3rd paragraph of section III could be modified as follows:

a. secure systems must be able to effectively and efficiently interoperate only with other secure systems;

b. (newly) designed secure systems must be able to interoperate effectively and efficiently when deployed in a secure environment, time sensitively;

c. human driven socio-technical systems, legal procedures and regulation as well as governance principles must be described (e.g. governance modeling using ontologies);

d. external, unexpected events and potential vulnerabilities and threats have to be considered and methods to dynamically model them have to be developed (e.g. iGRC programme);

e. harmonization and/or mapping of enterprise architectures, and secure interoperable architectures at different levels of abstraction have to be produced.

These general high level requirements can be particularised for secure enterprise systems that interoperate as follows. The following examples are based on Haley et al. (2007) [21]:
"The system shall provide Personnel Information only to a system of Human Resources"
"The system shall provide this information only during normal working hours"
"IT personnel should follow rules defined by data protection acts and nondisclosure agreements"
"Confidential information shall be provided with special approval and only to a member of the organisation"

6 Conclusion

A combined modeling approach for the linkage between systems interoperability and security has been discussed. The paper urges consistent and harmonious modeling of interoperability and security requirements at the system design stage, as well as using model based driven architecture. This will embed security and interoperability requirements in the design stage of a new system to achieve the following results:
a. Provision of security and interoperable systems solutions that are harmoniously integrated into enterprise architecture.
b. Security and interoperable capabilities in which requirements are adequately considered in systems engineering modeling and design activities.

Acknowledgment

This work is supported by the iGRC programme, and is funded by the UK Government's Technology Strategy Board and the South East England Development Agency (SEEDA) under the grant TP14/IIP/6/I/BJ029H. Sponsor

and financial support acknowledgment goes to the whole Consortium and especially to the leading organization Information Governance Limited.

References

[1] A.-J. Berre, B. Elvesæter, N. Figay, C. Guglielmina, S. G. Johnsen, D. Karlsen, "The ATHENA Interoperability Framework" Proc. 3rd International Conference on Interoperability for Enterprise Software and Applications Enterprise Interoperability II. Funchal, Portugal: Springer, 2007, pp. 569-580.

[2] IDABC, "European Interoperability Framework for Pan-European eGovernment Services, Version 1.0", IDABC,2004. http://europa.eu.int/idabc/en/document/3761

[3] http://interop-vlab.eu/

[4] NCOIC™ (Network-Centric Operations Industry Consortium™) "SCOPE (*Systems, Capabilities, Operations, Programs, and Enterprises)"* Model for Interoperability Assessment V1.0, 2008.

[5] Whitman, L. E and Panetto, H. "The missing link: Culture and language barriers to interoperability" *Annual Reviews in Control* vol. 30 pp. 233–241, 2006.

[6] Doumeingts G, and Chen D. "Interoperability of enterprise applications and software—an European IST thematic network project: IDEAS", Proceedings eChallenges Conference, October 2003, Bologna, Italy.

[7] Legner, C., & Wende, B. (2006) Towards an Excellence Framework for Business Interoperability in the Proceedings of 19th Bled eConference eValues, Bled, Slovenia, June 5 - 7, 2006, pp. 1-16.

[8] Legner, C., & Lebreton, B. "Business interoperability research: Present Achievements and upcoming challenges" in *Electronic Markets*, vol. 17 (3), pp. 176–186, 2007.

[9] Mouratidis, H. and Giorgini, P (eds.), *Integrating Security and Software Engineering – Advances and Future Visions*, Idea Group Publishing, 2007.

[10] Basin, D., Doser, J. and Lodderstedt , T. "Model Driven Security: from UML Models to Access Control Infrastructures", 2005.

[11] Sherwood, J., Clark, A, and Lynas, D. *Enterprise Security Architecture: A Business Driven Approach,* CMP Books, 2005.

[12] Schimidt, D.C. "Model –Driven Engineering, *IEEE Computer,* vol 39, 2, http://www.cs.wustl.edu/~schmidt/PDF/GEI.pdf.

[13] OMG (Object Management Group) MDA Guide, Version 1.0.1, omg/03-06-01, 2003.

[14] OMG (Object Management Group) Model Driven Architecture (MDA) Document 2001-07-01, 2001

[15] Blanchard, B.S. *System Engineering Management* 4th Edition by John Wiley & Sons Inc., 2008.

[16] http://www.zifa.org

[17] D.o. Defense (Editor) *Handbook for Systems Security Engineering Program Management Requirements*, Headquarters Air Force Systems Command, Office of the Chief of Security Police, 1995

[18] Houmb, S.H., Georg, G., Jurgens, J., France, R. "An Integrated Security Verification and Security Solution Design Trade-Off Analysis Approach", in *Integrating Security and Software Engineering – Advances and Future Visions* by Mouratidis, H. and Giorgini, P (eds.), Chapter IX, pp. 190- 219, Idea Group Publishing, 2007.

[19] Goertzel, K.M, Winograd, T., McKinley. K. M. Goertzel, T. Winograd, H. L. McKinley, H.L., Oh. L. and Colon, M., Software Security Assurance State-of-the-Art Report (SOAR), July 31, 2007.

[20] Mead, N.R. "Identifying Security Requirements Using the Security Quality Requirements Engineering method" in *Integrating Security and Software Engineering – Advances and Future Visions* by Mouratidis, H. and Giorgini, P (eds.), Chapter III, pp. 44-69, Idea Group Publishing, 2007.

[21] Haley, C.B., Laney, R., Moffett, J.D., Nuseibeh, B. "Arguing Satisfaction of Security Requirements" in *Integrating Security and Software Engineering – Advances and Future Visions* by Mouratidis, H. and Giorgini, P (eds.), Chapter II, pp. 16- 43, Idea Group Publishing, 2007.

[22] Holt, J. and Perry, S. *SysML for Systems Engineering*, IET Professional Applications of Computing Series 7, 2008

[23] Object Management Group, OMG Systems Modelling Language (OMG SysML™)" v1.1, /2008-11-01.