A Security Engineering Process for Systems of Systems using Security Patterns

Jose Fran. Ruiz and Carsten Rudolph
Fraunhofer SIT
Darmstadt, Germany
{jose.ruiz.rodriguez;carsten}@sit.fraunhofer.de

Antonio Maña, Marcos Arjona
University of Malaga
Malaga, Spain
{amg;marcos}@lcc.uma.es

***Abstract*— The creation of secure systems of systems is a complex process. A large variety of security expertise and knowledge specific for application domains is required. This is even more important if systems of systems span different application domains. Then, security threats specific to different application-domains need to be considered. One example is integrated systems for industrial production processes that interface office domains with supply chain management systems as well as a production environment. Such integrated systems of systems can perform very efficient and economic processes. However, due to the many and different domain-specific security requirements and threats security engineering needs to support requirements specification and architecture design very early in the development process in order to ensure resilience and safety of the complete system. Working with different domains implies that properties and its functionalities are specific and the engineering process used for modeling and designing the complete system has to be able to work in this context, covering all the possibilities and allowing the use of trusted solutions that are compatible with the ones of different domains.**

We present in this paper a security engineering process for creating secure systems of systems that cover the necessities presented above by using a series of security artifacts that contain the domain-specific security information (in terms of security properties) and provide security solutions in the form of security patterns. These patterns contain the definition of the software/hardware elements used for providing the required solution and the information of related patterns for different domains, which provides a very helpful functionality for creating a system of systems.

Keywords—security engineering process; engineering systems of systems; Model-based systems engineering; Research in systems engineering;

I. INTRODUCTION

The creation of secure systems of systems is a complex process. A large variety of security expertise and knowledge specific for application domains is required. This is even more important if systems of systems span different application domains. Then, security threats specific to different application-domains need to be considered. One example is integrated systems for industrial production processes that interface office domains with supply chain management systems as well as the actual production environment. Such integrated systems of systems can perform very efficient and economic processes. However, due to the many and different domain-specific security requirements and threats security engineering needs to support requirements specification and architecture design very early in the development process in order to ensure resilience and safety of the complete system. Working with different domains implies that properties and its functionalities are domain-specific and the engineering process used for modeling and designing the complete system has to be able to work in this context, covering all the possibilities and allowing the use of trusted solutions that are compatible with the ones of different domains. Besides, the process has to offer tools that can work with multiple domains and helps the engineer in the search, selection, use and analysis of the security solutions. In addition, in order to facilitate the work, the description of applicable solutions should be computer-oriented and provide ways to identify how they will interact with other solutions and with different systems of other domains.

The SecFutur security engineering process is able to work in that context. It allows system engineers to use security domain knowledge artifacts that provide information about the security properties (and its characteristics such as assumptions, threats, attributes, etc.) of a specific domain and its solutions by means of a new type of security patterns called Computer-Oriented Security Patterns (COSPs). These security properties are used to fulfill the security requirements of the systems in the modeling phase, allowing the integration of security naturally in the system thanks to the information and knowledge the security properties contain. The knowledge artifacts are created by domain security experts that use their expertise in that field for creating security properties and link them to security patterns for providing the solution. The COSPs contain information of the different implementations that fulfill the solution, their functionality (by using UML diagrams), examples of use, etc. It is done in a way that can be semi-automatically processed by a tool, importing the models and integrating them into the system model diagram, showing information about the elements of the solution, etc. We have created a tool for MagicDraw called SecFutur Process Tool that provides support for the creation and use of the security knowledge artifacts and COSPs in the process.

In order to demonstrate the process we are going to use as example an integrated industrial production system that is composed of different subsystems (being each of them defined

978-1-4799-2086-0/14/$31.00 ©2014 IEEE

in a specific domain). They cover the demand of products, the availability and ordering of material, the automatic manufacture configuration of the products and its delivery, billing, accounting and other functionalities. Being the system a multi-domain one we have to use security solutions that can work in a correct, safe and secure way with elements of different domains. The security patterns [5] we propose for using as solution contain information of its functionality by means of UML diagrams, related security solutions and tests for checking their correct functionality in the system where they are used.

Following we describe in Section 2 a brief description of the state of the art of the security engineering of systems of systems and the lessons we learned from them. Section 3 defines our approach, describing the objectives, artifacts and engineering process. Finally, Section 4 presents the conclusions and future work of the approach.

II. State of the Art

The creation of System of Systems (SoS) is a task very different from a single system. The differences between them are the number of systems to be developed. SoS can have different domains and, the most important characteristic, while system engineering focuses only in the creation of the system right SoS engineering concentrates in creating the right systems and their interaction in order to satisfy the system requirements.

Due to this characteristics a security engineering process for SoS should provide joint work with different domains, security integrated in the system since the beginning of the modelling, support system engineers in the architecture elements and solutions of the system, provide information about the functionality of a system and its interaction with other systems, etc. For analysing different SoS examples and some of the current approaches to system engineering of SoS we checked the guide written by a M. Jamshidi [1]. It provided us with a good introduction to the constraints and problems of working with SoS and some solutions used for its creation. Following we present some SoS engineering processes that aim to cover all those gaps and that we have used as basis for our approach.

J. Dahmann et al. present a model of system engineering for SoS [2] that provides a process for analysing and creating a SoS model. It does not provide a specific process but explains the steps that should be mandatory in order to correctly create a SoS.

Baldwin et al. present a process of systems engineering for SoS [3] using as basis the U.S. Department of Defense published guidance on systems engineering of SoS. The process uses a wave model that covers all the characteristics of the systems and translates the SoS core elements, interrelationships, artefacts and information of a system to a model representation that represents better the systems and improves the creation of the SoS.

Another interesting work for SoS is the one provided by D. Luzeaux et al. for engineering of complex systems and systems of systems [4]. In this work the authors present case studies (from emergency situations to crisis management) and processes for analysing and creating a SoS, bearing in mind its critical functionality and the interdependency between the systems.

Although the previous works were very useful they only provided abstract processes and information about how to analyse and use the information of a SoS. Besides, they do not cover the artefacts used for the systems as solutions and security is usually treated as an extra functionality. Our proposed approach provides a process and knowledge artefacts for specific domains that can help system engineers in the creation of the SoS while integrating security naturally in the architecture.

III. Security Engineering Process

A. Introduction

The Security Engineering Process (SEP) provides processes, artefacts and tools for the creation of secure systems and Systems of Systems by using domain-specific security knowledge solutions. It was developed in the SecFutur EU Project [6] and is also used in others European and national projects such as the CUMULUS EU Project [7]. The SEP provides the security solutions into a modelling framework that can be easily integrated with existing processes. This property was tested by working with companies in the SecFutur project that used it together with their own processes. The modelling framework uses artefacts for: a) defining the structure that represents the security knowledge of any domain; b) gathering the security knowledge of a specific domain; c) providing security solutions and d) the implementation of the solutions.

The SEP main focus is to help developers and engineers in creating security-enhanced systems and systems of systems by using security aspects and elements created by security domain experts. The SEP can model systems of any number of domains using security knowledge artefacts. The system engineer can import DSMs of various domains and apply their solutions to the system model. The SEP main characteristics are:

- Provide support for users when working with systems and SoS. The SEP provides artefacts and a tool (the SPT, developed for the MagicDraw framework) that is used by all the different roles of the process for creating or using the artifacts. Knowledge security experts use it for creating security knowledge artefacts (Domain Security Metamodels), solutions experts create Computer-Oriented Security Patterns and import Security Building Blocks for implementing the solutions and system engineers apply the security knowledge artefacts to their system model.
- Facilitate and provide sound development of secure systems and SoS. System engineers use the SEP to check, import and integrate security solutions in their system models even without having security knowledge. The solutions provided by the SEP are composed of Computer-Oriented Security Patterns and SBBs that describe the implementation functionality, the components (software and/or hardware), etc. From the point of view of the system engineer she only needs to imports a security

solution in her system model and the SPT integrates automatically the solution, characteristics of the security property, tests and other information of the solutions.

- Increase the security and quality of any type of system developed by the SEP. It can be used with any type of system the user needs. It allows the use of various domain-specific solutions so system engineers can model systems of systems in an easy way.

B. *Artifacts Description*

The artifacts of the security framework have specific goals and functionalities. The metamodels are used for the modeling of the system and the COSPs and SBBs for the solutions of the security properties. Figure 1 shows the artifacts and their relation. Following we describe the artifacts individually and then explain the relations between them. Due to the length limit of the paper we only describe them briefly.

The Core Security Metamodel (CSM) details the structure of the knowledge of a domain. It is defined as a language that describes the rules and grammar for creating domain-specific knowledge models. These models are the Domain Security Metamodels (DSMs). They describe the characteristics of the security properties of a domain along with information such as the assumptions, the threats, the elements of the domain, etc. This information helps the process when working with SoS, as the interaction of the elements of the different domains can be analysed in the model along with its functionality.

The solutions of the security properties come in the form of Computer-Oriented Security Patterns (COSPs) [5]. They are a new type of security patterns that computers can analyse and work with, on the contrary of the current format of security patterns that are human oriented. COSPs provide information about the security solutions together with its functionality, benefits, requirements, etc. They also include related or mandatory COSPs for working with specific domains, which helps the engineer when working with SoS.

The Security Building Blocks (SBBs) provide the implementation using software and/or hardware elements. In contrast to a security pattern, a SBB does not describe a complex integrated security solution. SBBs should be seen as encapsulated components that are domain-independent and can interact with external components in order to provide a clearly defined security service. They are individual blocks so they can be used in composition for creating many different security solutions. This allows the reusability of these artifacts.

The structure presented in Figure 1 shows the relations of the artifacts. The CSM is the basis for the creation of DSMs. Each DSM uses the language of the CSM for creating domain-specific security properties. The DSMs are stored in a repository where later will be accessed by system engineers for fulfilling the security requirements of the SoS.

The solutions of the security properties come in the form of COSPs. They provide different ways to implement the solution, having each of these solutions information about the functionality, related patterns, etc. The solutions come in the form of SBBs. They provide the functionality for the system by using software and/or hardware elements.

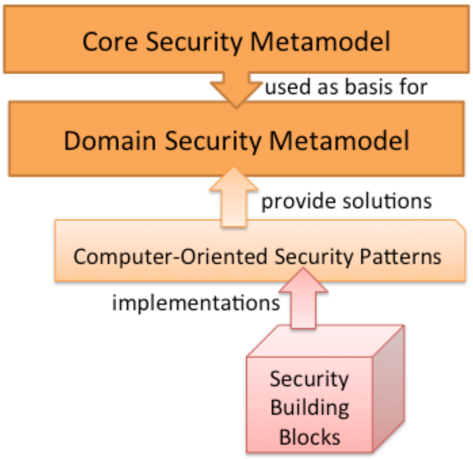

Figure 1. SEP Framework

C. *SEP Creation Process using a System of Systems Scenario*

Following we describe the creation of a SoS using the SEP. As with the security artefacts, due to the length limit of the paper we describe the process briefly.

The SoS system we are going to use as example is shown in Figure 2. The System of Systems is an integrated office/production architecture. It takes personalized orders and processes them automatically via a highly configurable production line (e.g. using 3D printers). The SoS can check the availability of elements and order new ones if necessary to an external provider. The interaction of the different systems of the SoS is large and direct. The intercommunication channels are displayed also in Figure 2. The order functionality is numbered so the reader can see better how the system works. We are going to describe first the SoS scenario and then how we use the SEP in the creation of this system.

A. *SoS Architecture*

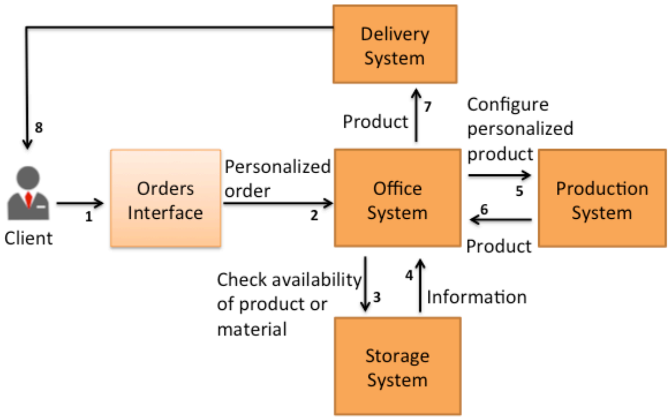

Figure 2. SoS Architecture

The SoS is composed of many subsystems. They are the Office System, the Storage System, the Production System and the Delivery System. The Orders Interface takes orders from the clients. This interface offers different options that can satisfy the needs of the clients. The order is sent to the Office System. It processes the order and sends its information to the

Storage System. This system checks if it has the necessary materials for creating the order or if they have to be requested to an external storage entity. Following it sends the information back to the Office System and this one sends it to the Production System, where the order is created. Finally the order information (e.g. package number) is sent back to the Office System and it sends it to the Delivery System. This system processes the created product and delivers it to the client using the information she introduced in the personalized order information.

B. *SEP Creation Process*

The creation of the SoS is composed of a series of phases. It is an iterative process because, as the SoS is composed of many subsystems, after applying one security solution to the system the system engineer has to check the interaction with the other existing systems or security solutions. For that objective the security knowledge artifacts contain information about the solutions and the related artifacts for other systems.

The first phase is the analysis of the SoS and the subsystems. The system engineer obtains the security requirements of the subsystems and the SoS (for the complete system). The analysis is very straightforward and should describe also the elements of the system that are involved in the requirements. Next comes the identification of the domains of the SoS. It is necessary for the search and selection of the DSMs that better fit the system.

Following, the system engineer accesses the DSM repository and, using the previous information, selects DSMs for fulfilling the requirements of the subsystems and SoS. The DSMs are imported to the modeling tool using the SPT. The next phase is the creation of the system model using UML. The creation of the system is done in a normal way, only taking attention to the security requirements identified previously. Once the system engineer has the system model scenario created and the DSMs of the different domains imported she starts fulfilling the identified security requirements.

The security properties are applied to the system using the SPT. They are applied to the elements or relations that have the security requirement. When applied the tool imports automatically the information of the security property such as the threats, assumptions, the possible solutions, etc. The system engineer selects then the solution that works better for her system, according to its characteristics, properties, etc. The solutions come in the form of COSPs, as we explained before. They contain information of the solutions that can help the system engineer in the selection of the one that better covers the necessities of the requirements or the system. Among others it includes diagrams showing its functionality and interaction with other elements of the system or external ones. That way the user can check if its functionality fits the one of the SoS and the required relation with other elements of the system. The selection of a COSP implies that the elements of the solution are imported to the system model. The tool asks the system engineer about the elements the solution needs (e.g. what element of the system model is the storage database) and create automatically the links between the solutions and the elements of the system. That way the system engineer can see how the system evolves and all the functionalities of the SoS are created and secured.

The application of security properties and selection of a solution are iterative processes, as each time the system engineer applies or selects one she has to check if she needs to model a required connection or create a new element that is used by other element of a different system. One of the biggest complexities of the creation of a SoS is the interaction between their systems. We cover that part by providing information of the solutions used in the system and how they interact with other elements.

Once all the security requirements of the SoS are fulfilled and all the interactions created the system engineer can use the tests of the solutions for checking its correct functionality and resilience.

IV. Conclusions

We present in this paper a Security Engineering Process for the creation of secure SoS. The process allows system engineers to integrate security in their systems naturally since the beginning of the modelling phase. It provides domain-specific security knowledge artefacts that can be used to fulfil the security requirements of the systems. These artefacts contain information about the interaction of the solutions with other elements of the system or external systems. That way the functionality and interactions between the systems can be achieved in an easy way. The security knowledge artefacts contain information about the possible threats, attacks, the assumptions of the security properties, tests for checking the correct functionality, etc. of that domain so the system engineer does not need a high level of expertise in security.

Acknowledgment

This work is partially supported by the E.U. through FP7 project SECFUTUR (IST-256668) and FP7 project CUMULUS (IST-318580).

References

[1] Jamshidi, M. "Introduction to Systems of Systems, in Systems of Systems Engineering: Innovations for the 21st Century", Wiley, 2009.

[2] Dahmann, J; Lane, J.A.; et al. "A Model of Systems Engineering in a System of Systems Context".6th Conference on Systems Engineering Research (CSER 2008), Redondo Beach, CA, 2008

[3] Baldwin, Kristen, Judith Dahmann, George Rebovich, Jo Ann Lane, and Ralph Lowry. "An Implementers' View of Systems Engineering for Systems of Systems". 2011 IEEE International Systems Conference, Montreal, Canada, April 2011

[4] Luzeaux, D.; Ruault, JR & Wippler, JL "Complex System and Systems of Systems Engineering", ISTE Ltd and John Wiley & Sons Inc, 2011

[5] Maña, A.; B. Fernandez, E.; Ruiz, J.F.; Rudolph, C.; "Towards Computer-Oriented Security Patterns"; PLOP 2013. To be published.

[6] SecFutur European Project. www.secfutur.eu

[7] Cumulus European Project. www.cumulus-project.eu/