EFFECTS+ - Systems & Networks Cluster

Technical Workshop on Models

Draft Agenda

Location: Breakout Rooms VU University Amsterdam
Chairman: Roland Rieke

Date	Time	Description
04-Jul-2011	14:45 - 17:00	Part 1: Presentations 1-11 10-15 minutes per presentation
05-Jul-2011	09:35 - 09:50 09:50 - 10:40	Part 2: Presentation 12, 1 slide per participant w.r.t. next objectives, other opportunities for collaboration; Cluster forming discussions
05-Jul-2011	11:00 - 12:30	Part 3: Wrap up of cluster workshops and cluster discussions around next objectives, other opportunities for collaboration; 1 slide per participant giving an overview of the presentation

Part1 and Part2 are parallel cluster breakout sessions

- "Systems & Networks - Technical Workshop on Models" parallel to
- "Services and Cloud Technical Workshop on Software Assurance & Trust"

Part3 is a joint agenda for both clusters.

Programme:
http://www.eventelephant.com/EffectsplusClusteringEventAmsterdam/programme.htm

Registration:
http://www.eventelephant.com/ee/bookings/tickets/index.htm?siteurl=EffectsplusClusteringEventAmsterdam

Presentations

No	Project	Presenter	Title
1	EFFECTS+ MASSIF	Roland Rieke	Objectives of the EFFECTS+ Systems & Networks Cluster Workshop on Models
2	MASSIF	Igor Kotenko	Analytical attack modeling and security evaluation in MASSIF
3	VIKING	Teodor Sommestad	Enterprise Architecture Models for Security Analysis
4	VIKING	Mats B-O Larsson	Virtual City Simulator (ViCiSi)
5	DEMONS	Sathya Rao	BlockMon: A framework for Distributed Network Monitoring and Real-Time Data Intensive Analysis
6	ASSERT4SOA	Domenico Presenza	Ontologies in ASSERT4SOA
7	NESSoS SecureChange	Fabio Massacci, Federica Paci, Stephane Paul	Managing Security and Changes throughout the whole System Engineering Process
8	PoSecCo	Antonio Lioy	PoSecCo models
9	WSAN4CIP TAMPRES	Peter Steffen	Assessment models to Improve the Usability of Security in Wireless Sensor Networks
10	VIS-SENSE	James Davey	Multi-Dimensional Clustering for the Purposes of Root-Cause Analysis
11	ENDORSE	Mark McLaughlin	Introducing the ENDORSE Privacy Rules Definition Language
12	CoMiFin	Roberto Baldoni, Giorgia Lodi	Collaborative Security for Protection of Financial Critical Infrastructures: The Semantic Room abstraction model

1 Objectives of the Systems & Networks Cluster Workshop on Models

Presentation: Roland Rieke, project EFFECTS+/MASSIF

The vision of the Future Internet, where multiple services are transparently and seamlessly mixed, already created a paradigm which promises to largely enrich our ability to create new applications and businesses within this new environment. But this paradigm also enables new possibilities for threats and scales up the risks of financial and also physical impact. In many cases, the information itself will be the essential product which deserves to be protected, in the Internet of Things however, real and virtual cyber-physical resources deserve our attention.

Various projects in the ICT Framework Programme are currently using "Models" of different kinds in order to assess upcoming security and privacy challenges as well as mitigation strategies w.r.t. their possible impact.

The Effectsplus FP7 funded Coordination & Support Action, within the activity of Systems and Networks cluster, organises this workshop, which aims to provide a forum for discussing the different approaches of projects in this area.

At the end of the workshop, we expect to have a better understanding of possible areas of collaboration among projects. Specifically, we are interested to find out, which concrete models are publicly available and re-usable in related projects, the gaps between existing approaches and promising areas for future research.

2 Analytical attack modeling and security evaluation in MASSIF

Presentation: Igor Kotenko, project MASSIF

The talk suggests the common approach, architecture and main models for analytical attack modeling and security evaluation investigated in the EU FP7 MASSIF Project. The approach is based on processing current alerts, modeling of malefactor's behavior, generating possible attack subgraphs, calculating different security metrics and providing comprehensive risk analysis procedures.

Key elements of suggested architectural solutions for attack modeling and security evaluation are using security repository (including system configuration, malefactor models, vulnerabilities, attacks, scores, countermeasures, etc.), effective attack tree generation techniques, taking into account as known as well as new attacks based on zero-day vulnerabilities, stochastic analytical modeling, combined use of attack graphs and service dependency graphs, calculation metrics of attack and security countermeasures (including attack impact, response efficiency, response collateral damages, attack potentiality, attacker skill level, etc.), interactive decision support to select the solutions on security measures/tools by defining their preferences regarding different types of requirements (risks, costs, benefits) and setting trade-offs between several high-level security objectives.

This talk considers shortly the analysis of state-of-the-art in attack modeling, main functional requirements and essence of the approach to analytical attack modeling, main models as well as generalized architecture of Attack Modeling and Security Evaluation Component (AMSEC) suggested to be developed and implemented in MASSIF project.

3 Enterprise Architecture Models for Security Analysis

Presentation: Teodor Sommestad, project VIKING

Enterprise architecture is an approach to management of information systems, including control systems, that relies on models of the systems and their environment. This section briefly outlines the structure of the work carried out by the VIKING project on the topic of cyber security analysis and modeling. It combines attack- and defense graphs with Bayesian statistics and enterprise architecture modeling.

Attack graphs are a notation used to depict ways that a system can be attacked. It shows the attack steps involved in attacks (nodes) and the dependencies that exists between them (arcs). Defense graphs extend this notation by including security measures in the graph to represent the attack steps they influence. Both of these notations can be used to create models over systems and to assess the system's security, e.g. by assessing if a particular attack is possible, given that the graph is parameterized.

The VIKING project has produced a tool where defense graphs are produced programmatically from a model of an information system or control system and its environment. A user of this tool produces architectural drawings of their enterprise (e.g. including network zones, machines, services, security processes executed) and the based on this the tool generates a defense graph that represent this specific enterprise's situation. Based on logical relationships and quantitative data collected from literature and domain experts the user can also calculate approximate values for the probability that an attempted attacks would succeed against the system.

The workshop in Amsterdam will present the work done in VIKING on Enterprise Architecture Modeling and how we believe the research work can extended to practical tools to evaluate existing and new control system for security and to do "what-if" studies on different control system configurations.

4 Virtual City Simulator (ViCiSi)

Presentation: Mats B-O Larsson, project VIKING

One of the main objectives of the Viking project is to assess the cost to the society coming from power outages. In order to do this a virtual society simulator has been developed. The virtual society is created by the Viking City Simulator, ViCiSi. In short ViCiSi is creating a virtual society, with all necessary functions, and it is based on parameters from the EU database Eurostat. ViCiSi can be parameterized to any country in EU country plus Switzerland and Norway.

In summary ViCiSi is:

- A virtual society with all necessary infra-structure built on blocks, apartments, streets, etc.
- With companies, public and private service operations producing welfare
- With people living in the city consuming welfare.
- Includes a distribution electrical grid with all common voltage levels to give realistic load curves
- Calculates the activity in the society at all moments, in terms of Business Activity
- Calculates cost for power outages as lost GDP
- Can scale to all EU countries

In the workshop in Amsterdam we will present the ViCiSi. We will show how it is designed, how it can used to calculate societal costs at power outages, how we present the results and how ViCiSi will be integrated into the VIKING Test bed.

5 BlockMon: a framework for Distributed Network Monitoring and Real-Time Data Intensive Analysis

Presentation: S. Rao, project DEMONS

DEMONS project will address the 'decentralised, cooperative and privacy preserving monitoring for trustworthiness'. The monitoring scenario of the system architecture targets both intra-domain and inter-domain aspects.

Intra-domain monitoring, primary requirements here being scalability, resilience and innetwork distribution of monitoring tasks; performance effectiveness in terms of detection and mitigation reaction time; and authorized and controlled access to monitoring data in accordance to domain-specific operational workflow processes and policies;

Inter-domain monitoring, core requirement here being the tight control of inter-domain cooperation in terms of which monitoring data is exchanged and under which conditions, which protocols should be used for guaranteeing inter-domain inter-operability, and how to exploit and support advanced cryptographic data protection technologies for improving inter-domain cooperation ability and permitting secure joint analysis and computation over monitoring information provided by the multiple involved domains.

The presentation will address the BlockMon Monitoring Overlay (BMO) monitoring infrastructure chosen as the basis of the DEMONS' Measurement Layer and Coordination Layer for what concerns the intra-domain monitoring scenario. The internet Exchange Point (IXP) will coordinate across inter-domains.

6 Ontologies in ASSERT4SOA

Presentation: Domenico Presenza, project ASSERT4SOA

The presentation intend to deal with the use of ontologies in the context of the ASSERT4SOA Project.

ASSERT4SOA Project aims to produce novel techniques and tools for expressing, assessing and certifying security properties for service-oriented applications, composed of distributed software services that may dynamically be selected, assembled and replaced, and running within complex and continuously evolving software ecosystems.

ASSERT4SOA Advanced Security Certificates (a.k.a. ASSERTs) are machine readable documents stating that a given Web Service has a given Security Property.

An ASSERT also contains a model of the service and a "proof" that can be used by the requesters of that Web Service to re-check the asserted Security Property. Based on the type of provided proof, three different types of ASSERT will be considered: evidence-based ASSERT (a.k.a. ASSERT-E), ontology-based ASSERT (a.k.a. ASSERT-O) and model-based ASSERT (a.k.a. ASSERT-M)

The use of OWL-DL Ontologies within ASSERT4SOA is twofold: (1) to investigate the use of an ontology-based approach to describe security properties of services (2) to enable the interoperability and comparison of the other kinds of ASSERTs.

The envisaged ASSERT4SOA Ontology will contain the description of both general concepts and ASSERT specific ones. The instances of all types of ASSERTs will refer the terms defined in the ASSERT4SOA Ontology.

Within the ASSERT4SOA Ontology concepts are represented as OWL-DL classes thus allowing to express decision problems about ASSERTS (e.g. mapping between different kind of ASSERTs) as Description Logic inference problems (e.g. Class Expression Subsumption).

7 Managing Security and Changes at Model Level throughout the whole System Engineering Process

Presentation: Federica Paci, project NESSoS/SecureChange

Security engineering is not a goal per see. Security applies to a system or software, whether large IT or embedded system, which must itself be engineered. Security engineering must therefore comply with the constraints and pace of the mainstream system / software engineering processes, methods and tools. Assuming a model driven approach to the mainstream system / software engineering, we explain how to support evolution while maintaining security at all levels of the system / software development process, from requirements engineering down to deployment and configuration.

A system / software lifecycle typically has seven phases: (i) specification, (ii) design, (iii) realisation or acquisition, (iv) integration and verification, (v) validation and deployment, (vi) operation and maintenance, and (vii) disposal. In some cases, a system / software may occupy several of these phases at the same time. Security engineering can be conducted regardless of the system / software lifecycle phase; however the pursued goals may significantly differ (see Figure 1).

During the specification phase, the main goal of security engineering is to influence the definition of the system / software requirements, and thus gain early assurance that the proposed architectural solution is sound with respect to security concerns. This step encompasses customer security need elicitation and early risk assessment. This early approach contrasts sharply with current-day practices in which risks are only analysed when requirements have been elicited, and sometimes even later, when the main system design is frozen or developed. With standard approaches: (i) safeguards may be very expensive to implement; (ii) some elicited requirements may reveal themselves as too risky to be fulfilled; (iii) some requirements may be error-prone; (iv) locally designed safeguards to cope after hand with risky requirements may obstruct the fulfilment of other requirements.

. . . [1]

[1] For the full abstract see appendix.

8 PoSecCo Models

Presentation: Antonio Lioy, project PoSecCo

PoSecCo aims at addressing some of the main service provider challenges for the viability of Future Internet (FI) applications, that will see dynamic compositions of services providing a broad diversity of functions, starting with business functionality down to infrastructure services. In fact, in a FI scenario, service providers will need to achieve, maintain and prove compliance with security requirements stemming from internal needs, third-party demands and international regulations, and to cost-efficiently manage policies and security configuration in operating conditions.

PoSecCo overcomes this by establishing a traceable and sustainable link between high-level requirements and low-level configuration settings through decision support systems. To achieve this goal a consistent effort is being put into system and network modelling, whose main purpose is to create a set of meta-models and a security ontology that will be presented at the Network and System Workshop.

First of all, reaching the PoSecCo objectives requires the modelling of FI services, a challenge that PoSecCo is addressing through a refinement loop between the Service Provider partners, providing the requirements ensuring the practical usage, and academia ensuring the self- coherence, extensibility and the possibility to be formally used.

The result is the functional system meta-model, including a business and an IT layer. Moreover, since services will be actually implemented on existing (physical or virtual) networked systems, the functional system meta-model includes an infrastructural layer that refers to a landscape meta-model.

Also the policy is represented at three different layers of abstraction, the business, the IT and the landscape configuration layers, therefore the design of three policy meta-models is in progress.

The PoSecCo security ontology is being developed to vertically connect all the abstraction layers and horizontally connecting each abstraction layer with the corresponding policy-meta model, and to enrich the knowledge of the systems using the expressive power that ontologies can guarantee.

9 Assessment models to Improve the Usability of Security in Wireless Sensor Networks

Presentation: Peter Steffen, project WSAN4CIP/TAMPRES

Wireless Sensor Networks play a major role in the Future Internet. They deliver data that may influence important decisions in further process steps. To improve the security and reliability as they are required for such networks, many protocols, algorithms, and services have been proposed in recent years. The complexity of the approaches is often significantly and the trade-offs are hardly understood by even by experts. This is a particular issue in projects such as WSAN4CIP (wireless sensor networks for critical infrastructure protection) where eventually domain experts apply networks in critical environments.

As solution we propose a model-based approach that maps requirements and system properties on exchangeable security models, expressed in a flexible meta-model-language. The initial requirements are understood by users, and the system properties are assessed based on properties of the individual components, which can be stored in pre-configured repositories. The exchangeable security models allow to focus on specific security aspects such as vulnerabilities, attacks, or resistances.

As example the models shall evaluate the effects of tamper resistant sensor nodes, as they are investigated in the TAMPRES project. Naturally, the existence or non-existence of such tamper resistance in the network alters the security properties of the entire network and its application significantly. This has to be respected by the models.

The model approach as well as the implications for the projects WSAN4CIP and TAMPRES are addressed in the presentation.

10 Multi-Dimensional Clustering for the Purposes of Root-Cause Analysis

Presentation: James Davey, project VIS-SENSE

One of the goals of the VIS-SENSE project is to generate an overview of the malware and spam landscapes in the Internet. A major part of this process is root-cause analysis, which is the search for and identification of coordinated criminal campaigns. Through a better understanding of how these campaigns evolve over time, security experts should be able to improve the protection of their networks.

When analysing the behaviour of spam or malware, a very large number of alerts are collected every day. What constitutes an alert is defined by the data collection infrastructure used to collect information for the purposes of analyses. The alerts are the starting point for our root-cause analysis.

The next phase in the analysis process involves the generation of events, based on the alerts. These events are essentially groups of alerts, together with some additional annotations. The groups and annotations are derived with the help of rule-based or experience-based models.

Events are the first level of aggregation in the root-cause analysis. While this aggregation does increase understanding of the threat landscape, it is not condensed enough to provide an overview. To attain an overview, a further aggregation step is undertaken. In this step, each feature of the events is first considered individually. Based on the data type of the feature, similarity measures are chosen and, if necessary, parameterised. The feature-based similarities can be used to cluster events on a feature-by-feature basis. These clusters provide clues for the specification of a multi-dimensional similarity measure. With the help of this measure, multi-dimensional clustering is possible. Visualizing the results of multi-dimensional clustering reveals a much more insightful overview of the original malware and spam alerts.

Many models exist for the feature-by-feature as well as for the multi-dimensional similarity measures. The choice of models and their parameterization has direct implications for the results of the multi-dimensional clustering step. An overview of these models will be presented, as well as a description of techniques for the support of iterative visualisation and adjustment of parameters. Through the targeted use of visualization in the analysis process VIS-SENSE will assist the analyst in the generation of useful overviews of the threat landscape.

11 Introducing the ENDORSE Privacy Rules Definition Language

Presentation: Mark McLaughlin, project ENDORSE

One of the core outputs of the ENDORSE project will be a Privacy Rules Definition Language (PRDL). This language will allow organisations to codify their data protection and privacy operating policies regarding sensitive user data. PRDL will be used for internal compliance and transparency with regard to external parties. The ENDORSE system will use PRDL rules to ensure that personal data are processed legally and appropriately within the organisation in terms of access control and meeting obligations for data handling over the lifetime of the data. ENDORSE is taking a model driven architecture (MDA) approach to building the ENDORSE platform. As such, the definition of PRDL is also crucial for generating many of the platform software components. An early draft of the PRDL metamodel will be presented.

12 Collaborative Security for Protection of Financial Critical Infrastructures: The Semantic Room abstraction model

Presentation: Roberto Baldoni, project CoMiFin

The growing adoption of Internet in the financial ecosystem has exposed financial institutions to a variety of security related risks, such as increasingly sophisticated cyber attacks aiming at capturing high value and sensitive information, or disrupting service operation for various purposes. To date, single financial institutions have faced individually these attacks using tools that re-enforce their defence perimeter (e.g. intrusion detection systems, firewalls). However, today's attacks are more sophisticated making this kind of defences inadequate. Attacks are typically distributed in space and time meaning that they can be coordinated on a large scale basis and often consist of a preparation phase spanning over days or weeks, involving multiple preparatory steps aiming at identifying vulnerabilities (e.g., open ports). In order to detect these attacks a larger view of what is happening in the Internet is required, which could be obtained by sharing and combining the information available at several financial sites. This information must be processed and correlated "on-the-fly" in order to anticipate threats and frauds, and mitigate their possible damages. Even though this sharing can result in a great advantage for financial institutions, it should be carried out only on a clear contractual base and in a trusted and secure environment capable of meeting privacy and confidentiality requirements of financial institutions.

In this context, the CoMiFin project, ended last April 2011, developed an open source middleware system for monitoring the Financial Critical Infrastructure domain. The system is currently a research prototype and has been demonstrated in several occasions even to financial stakeholders such as SWIFT board members and a number of Italian banks. It facilitates the sharing and processing of critical operational data among interested parties (e.g., financial institutions, telco providers, power grid operators), and is utilized for timely activating local protection mechanisms. In doing so, the CoMiFin project introduced a novel abstraction model named Semantic Room (SR).

... [2]

[2]For the full abstract see appendix.

Appendix

CoMiFin project: short abstract

The growing adoption of Internet in the financial ecosystem has exposed financial institutions to a variety of security related risks, such as increasingly sophisticated cyber attacks aiming at capturing high value and sensitive information, or disrupting service operation for various purposes. To date, single financial institutions have faced individually these attacks using tools that re-enforce their defence perimeter (e.g. intrusion detection systems, firewalls). However, today's attacks are more sophisticated making this kind of defences inadequate. Attacks are typically distributed in space and time meaning that they can be coordinated on a large scale basis and often consist of a preparation phase spanning over days or weeks, involving multiple preparatory steps aiming at identifying vulnerabilities (e.g., open ports). In order to detect these attacks a larger view of what is happening in the Internet is required, which could be obtained by sharing and combining the information available at several financial sites. This information must be processed and correlated "on-the-fly" in order to anticipate threats and frauds, and mitigate their possible damages. Even though this sharing can result in a great advantage for financial institutions, it should be carried out only on a clear contractual base and in a trusted and secure environment capable of meeting privacy and confidentiality requirements of financial institutions.

In this context, the CoMiFin project, ended last April 2011, developed an open source middleware system for monitoring the Financial Critical Infrastructure domain. The system is currently a research prototype and has been demonstrated in several occasions even to financial stakeholders such as SWIFT board members and a number of Italian banks. It facilitates the sharing and processing of critical operational data among interested parties (e.g., financial institutions, telco providers, power grid operators), and is utilized for timely activating local protection mechanisms. In doing so, the CoMiFin project introduced a *novel abstraction model* named *Semantic Room (SR)*.

A Semantic Room is a private and trusted collaborative cloud through which financial institutions can federate for the sake of distributed data aggregation and near real time data correlation and dissemination, necessary to effectively monitor distributed IT infrastructures and timely detect various types of frauds and threats. Note that the SR model is highly flexibly to accommodate (i) the detection of different threat scenarios in different business contexts; (ii) the use of different software technologies for data processing and sharing, and (iii) different functional and non-functional requirements to be met.

A software component named SR gateway has been developed so as to allow financial institutions to interface local network management systems: through this component raw data can be pre-processed and fed into the SR for collaborative processing and sharing, following specific contractual clauses included in Semantic Room *contracts*. The results of the collaborative processing can be then sent back to the internal network monitoring systems, which define the countermeasure policies a financial domain can adopt as response to what has been detected by the Semantic Room.

The concrete CoMiFin outcomes can be summarized as follows:

- It has identified vulnerabilities of interconnected and interdependent financial infrastructures and defined local policies of a financial domain for monitoring them. For studying interdependencies between the financial, power grid, and telco infrastructures, it has leveraged the research carried out in other FP6 projects such as IRRIIS, CRUTIAL and GRIDS specially targeted to those environments.
- It has identified and detailed a set of use cases of interest for financial end-users and that involved different players. These use cases included in publicly available deliverables allowed CoMiFin to identify a set of relevant information and its format to be exchanged among entities and to design the necessary building blocks to be integrated with local network management systems.
- It has designed a middleware architecture capable of supporting the construction and instantiation of Semantic Rooms. The middleware is constructed out of principal building blocks deployed on the top of Internet that meet non-functional requirements such as responsiveness and predictability by design, as prescribed by Semantic Room contracts.
- It has developed innovative techniques for threat information dissemination and infrastructure self-protection plans.
- It has developed fast online monitoring. In particular, CoMiFin designed, implemented and evaluated new algorithms for cyber attack detection (i.e.,, inter-domain stealthy port scans, Man-in-the-Middle, botnet-driven HTTP session hijacking) using different event processing technologies;

namely, complex event processing engines (e.g., Esper), MapReduce-based distributed event processing systems to be used outside and within local financial domains.

- It has defined metrics to assess its threat monitoring capabilities. A *monitoring system* has been developed for such purpose that periodically collects metrics of interest (e.g., number of messages exchanged in the Semantic Room) and detects whether specific SR contract violations occur. This is realized in cooperation with *a trust management system* that permits to evaluate and monitor the trust levels of SR participants. Trust evaluation is based on past behavior and the reputation of each participant through direct experience, recommendation, referral, and roles. The trust may influence the processing carried out within a SR: depending on the trust level of the information injected by specific SR participants, the processing algorithms are able to adapt and assign priorities to the events they analyze.

Futher details of the project can be found at the Comifin web site http://www.comifin.eu/

Managing Security and Changes at Model Level throughout the whole System Engineering Process

Fabio Massacci[2], Federica Paci[2], Stephane Paul[1]

Thales[1]
Palaiseau, France
stephane.paul@thalesgroup.com

DISI[2]
University of Trento
Povo, Trento
{Massacci, federica.paci}@unitn.it

Security engineering is not a goal per see. Security applies to a system or software, whether large IT or embedded system, which must itself be engineered. Security engineering must therefore comply with the constraints and pace of the mainstream system / software engineering processes, methods and tools. Assuming a model driven approach to the mainstream system / software engineering, we explain how to support evolution while maintaining security at all levels of the system / software development process, from requirements engineering down to deployment and configuration.

A system / software lifecycle typically has seven phases: (i) specification, (ii) design, (iii) realisation or acquisition, (iv) integration and verification, (v) validation and deployment, (vi) operation and maintenance, and (vii) disposal. In some cases, a system / software may occupy several of these phases at the same time. Security engineering can be conducted regardless of the system / software lifecycle phase; however the pursued goals may significantly differ (see Figure 1).

During the specification phase, the main goal of security engineering is to influence the definition of the system / software requirements, and thus gain early assurance that the proposed architectural solution is sound with respect to security concerns. This step encompasses customer security need elicitation and early risk assessment. This early approach contrasts sharply with current-day practices in which risks are only analysed when requirements have been elicited, and sometimes even later, when the main system design is frozen or developed. With standard approaches: (i) safeguards may be very expensive to implement; (ii) some elicited requirements may reveal themselves as too risky to be fulfilled; (iii) some requirements may be error-prone; (iv) locally designed safeguards to cope after hand with risky requirements may obstruct the fulfilment of other requirements.

During the design phase, the system / software design slowly freezes. As time goes by, any major change in design has a more and more significant cost impact. The main goal of security engineering at this stage is thus to propose cost-efficient countermeasures for the identified security risks, with minimal impact on the architectural solution. Proven security design patterns may be used. Security risk assessment is performed in parallel, defining security objectives until residual risks are tolerable or acceptable.

During the realisation or acquisition phase, the system / software is implemented or acquired; the main goal of security engineering at this development stage is thus to implement or acquired the countermeasures. In some cases, when the proposed security controls are elementary or available off-the-shelf, this implementation / acquisition may be carried out as part of the mainstream engineering process. When SOA technology is the targeted platform, the project advocates security-as-a-service.

During the integration & verification phase, the main goal of security engineering is to integrate and test the countermeasures. As for realisation or acquisition, the integration of the security countermeasures may be carried out as part of the mainstream engineering process; however testing (i.e. system discovery, vulnerability scan and assessment, security assessment, penetration testing, security audit and review) represents a security-specific task, aiming at proving that the information system protects data and maintains functionality as intended.

During the validation / qualification phase, the main goal of security engineering is the security qualification of the system / software, which will potentially lead to certification. The qualification of a product gives evidence of the robustness of the security services of the product. It is based on: (i) the verification of the conformity of the product with the security characteristics specified in the target, on the basis of an evaluation realized by one or several laboratories approved by a certification authority (e.g. DCSSI in France); (ii) the approval, by the certification authority, of the relevance of the security target with respect to the planned use and the requested level of qualification. This qualification allows: a) to

separate the purely technical assessment of the system from a wider assessment of its ability to protect sensitive information in given conditions; b) to recognize that the same system (i.e.

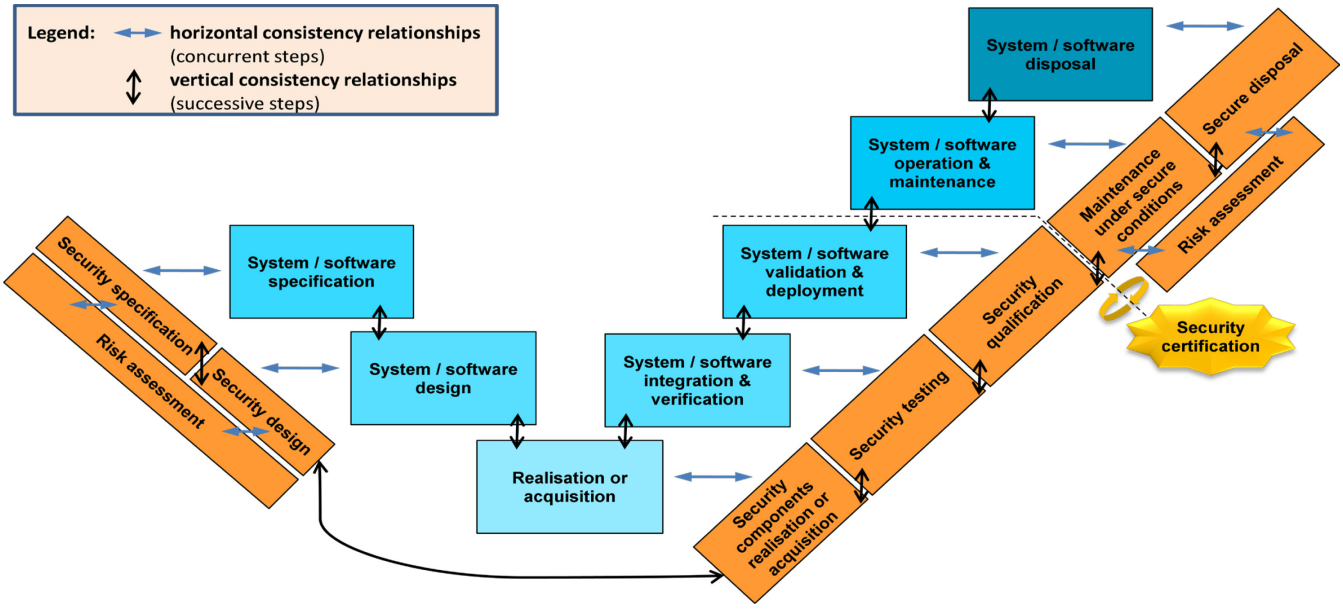

Figure 1. Mainstream and security system /software engineering processes

with a given robustness) can allow for the protection of information of different levels, and thus can obtain various levels of approval, according to the conditions of use.

During the operation & maintenance phase, the main goal of security engineering is to monitor the effectiveness of the countermeasures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system or enterprise. In case security is found to be flawed, the previous activities (e.g. risk assessment, security realisation or acquisition, security integration and testing, etc.) may be performed anew to ensure an acceptable level of risk.

We focus here on how the specification phase of the system/software engineering process can be orchestrated with risk assessment given a mapping between the concepts between the requirement domain and the risk assessment domain [1].

We illustrate the interactions between the *risk analyst,* the *requirement analyst* and the *system designer* how the activities performed by these stakeholders can be orchestrated. The key feature of the orchestrated process is the *separation of concern principle*. An important advantage of separation of concern is that in-depth expertise in the respective domains is not a prerequisite. The orchestrated process allows the separate domains to leverage on each other without the need of full integration. As a counterpart, consistency of concerns should be ensured. We assume that risk analyst and the requirement analyst, and the system designer share a minimal set of concepts which is the interface between their respective processes: each process is conducted separately and only when a change affects a concept of the interface, the change is propagated to the other domain.

As examples of requirement framework and risk framework we adopt SI* [2] and RA DSML [3] respectively.

SI* is a requirement framework which supports both early and late requirement analysis. SI* has several extensions, but in this paper we focus on the trust and risk extension proposed in [4].

RA DSML is the language and a tool developed to capture the security risk analysis concepts derived from the French EBIOS methodology [5]. As a tool, RA DSML realizes a Viewpoint of a system Architecture Model as defined in coming ISO 42010 standard [6].

Even though conducted separately, the requirement analysis, and the risk analysis processes can be orchestrated so that they can benefit from the respective results. In order to allow the orchestration between these processes, we need to identify a set of concepts that is the *interface* between them (see Table I).

We distinguish the interface concepts in *shared elements* and *mappable elements*. The shared elements are model elements that conceptually have the same semantic in the three domains. The mappable elements are elements from one domain that are

not shared by the other, but nevertheless can be mapped to elements of the other domain.

TABLE I. INTERFACE

	Conceptual Mapping		
Requirement	***Risk***	***Architecture***	***Type***
Business Object	Essential Element		Shared
Goal	Security Objective		Mapped
Security Goal	Security Requirement		Mapped
Process		Security Solution	Mapped

When a change affects a mappable or shared element in one domain such change is propagated to the other domain. The following table summarizes the conceptual mapping.

We illustrate the idea of the orchestrated process that involves the risk analyst, the requirement analyst and the system designer by using an example of evolution related to the ATM domain. Part of ATM system's evolution process is the introduction of a new decision support tool for air traffic controllers (ATCOs) called Arrival Manager (AMAN) in order to support higher traffic loads. The main goal of the AMAN is to help ATCOs to manage and better organize the air traffic flow in the approach phase. The introduction of the AMAN requires new operational procedures and functions and imposes new security properties to be satisfied.

The main steps of the orchestrated process when the AMAN is introduced are the following:

1) The requirement analyst and the risk analyst interact to identify an initial set of security objectives.

2) A change request is triggered for the requirement domain and the SI* model is produced by the requirement analyst.

3) The system designer analyzes the SI* model provided by the requirement analyst and then passes it to the risk analyst.

4) The risk analyst identifies the following new security objectives:
   - **O1** The system shall be computed automatically by an Arrival Manager system that covers the risk
     - **R1** Failure in the provisioning of correct or optimal arrival information due to ATCO mistakes.
   - **O2** The update of the system should be handled through a dedicated role of Sequence Manager that covers the risk **R1**.

   The above security objectives are refined into the following security requirements:
   - **RE1** The system should integrate an AMAN (refines security objective **O1**)
   - **RE2** The organization should integrate a SQM (refines security objective **O2**).

5) The changes into the RA DSML model trigger a change request for the requirement domain. The requirement analyst receives the new security objectives and requirements and updates the SI* model by adding two new actors, AMAN and the SQM have been added with their goals, process and resources.

6) The new processes Compute Arrival Sequence provided by AMAN and Monitor and Modify provided by SQM identified by the requirement analyst has to be propagated to the system designer and to the risk analyst.
   The risk analyst assesses the new processes proposed by the requirement analyst and defines new security solutions to match the processes. Then, the risk analyst passes the identified security solutions to the system designer for validation.

ACKNOWLEDGMENT

This work has been partly funded by EU project - Network of Excellence on Engineering Secure Future Internet Software (NESSoS) and by the EU-FP7-FET-IP-SecureChange project.

REFERENCES

1. Edith Félix, Olivier Delande, Fabio Massacci, Federica Paci, Managing Changes with Legacy Security Engineering Processes, IEEE International Conference on Intelligence and Security Informatics, Beijing, China, July 10-12, 2011.
2. P. Giorgini, F. Massacci, J. Mylopoulos, and N. Zannone, "Requirements engineering for trust management: model, methodology, and reasoning," International Journal of Information Security, vol. 5, no. 4, pp. 257–274, Oct. 2006.
3. V. Normand, E. Félix, "Toward model-based security engineering: developing a security analysis DSML", ECMDA-FA, 2009.
4. Y. Asnar, P. Giorgini, and J. Mylopoulos, "Goal-driven risk assessment in requirements engineering," Requirements Engineering, pp. 1–16, (to appear).
5. EBIOS. http://www.ssi.gouv.fr/en/confidence/ebiospresentation.html
6. ISO/IEC FCD 42010, Architecture description, draft.