Welcome message from the Program Chairs

On the On behalf of the Organizing Committee, we would like to welcome you the International Workshop on the Interplay of Security, Safety and System/Software Architecture (ISSA 2018), held in Barcelona, th 7 th of September 2018, in conjunction with the 23 rd European Symposium on Research in Computer Security (ESORICS) 2018.

Several frameworks have been proposed to help the designers of software system applications. However, we currently lack methodological tool support to take into account the interplay between security and safety and the other architecture properties. The main focus of ISSA workshop is on the topic of making security and safety expert knowledge available to system and software engineering processes. Special emphasis will be devoted to promote discussion and interaction between researchers and practitioners focused on the particularly challenging task to efficiently integrate security and safety solutions within the restricted available design space for software systems. Furthermore, one important focus is on the potential benefits of the combination of model-driven engineering, formal methods with pattern-based representation of security and safety solutions. Some of the topics that we seek to include in the workshop are related to the development of concepts, modeling languages, evaluation and validation techniques, methods and tools to support the inclusion of security, safety and architecture issues into the software engineering process. We are inviting the submission of papers with high quality research contributions, work in progress, challenge problems, tool demonstrations, experimental and ongoing projects results.

Among the 10 initial submissions, 04 papers have been selected and organized in a session covering a wide spectrum of the subject of the Interplay of Security, Safety and System/Software Architecture. It is our wish that the workshop provides an appropriate and relaxed environment to discuss these new ideas and approaches. In order to facilitate it, each speaker will have 25 minutes for the presentation. The program is completed with a keynote talk given by By Gabriel Pedroza (CEA, France) on Challenging aspects for a consistent safety and security intertwining. Moreover, we will close the workshop with a working and a discussion session about: the Interplay of Security, Safety and System/Software Architecture, Why, What and How.

We would like to thank all the people that have made possible this event. First of all, thanks to the organizers of the ESORICS 2018 for accepting our proposal of celebrating this workshop; second, to the authors that submitted their articles; third, to the members of the Program Committee and other reviewers for their enormous effort during the review process, you put a lot of efforts in the discussion and the provide the great results.

September 2018 ***Brahim Hamid***

Barbara Gallina

Keynote Talk

Gabriel Pedroza

CEA (French Alternative Energies and Atomic Energy Commission), France

Title: Challenging aspects for a consistent safety and security intertwining

Abstract

In this talk, we conduct a non-exhaustive survey on high level aspects which are identified as relevant to consistently settle links between safety and security analyses in the engineering development cycle. In the literature, the referred intertwining often relies on models which are considered as analogous and, moreover, compatible, e.g., attack trees vs. fault trees, threat sources vs. failure causes, etc. Despite that, certain particularities are identified which may impede a seamless co-engineering process. This talk aims to highlight those particularities, address questions on models' limitations and provide some insights to solve them.

Bio

Gabriel Pedroza is a Research Engineer at the Laboratory of Systems Requirements and Conformity Engineering (LECS) of the CEA institute in France. He conducts research in the field of systems security, safety and privacy by exploring, using, defining and extending high level languages and methods to conduct systems modelling and multi-concern analysis. His work includes the development of techniques like modelling by reverse engineering, and language transformation towards formal frameworks in order to validate systems properties. He has participated in several projects like EVITA (FP7), SESAM-Grids (French R&D project), AMASS (ECSEL JU) and more recently PDP4E (H2020).

Friday, September 7, 2018

08:30 – 09:00

Registration

09:00 – 09:15

Room: TBA
Opening & Welcome

09:15 – 10:00

Invited Talk: Challenging aspects for a consistent safety and security intertwining
By Gabriel Pedroza, CEA, France

In this talk, we conduct a non-exhaustive survey on high level aspects which are identified as relevant to consistently settle links between safety and security analyses in the engineering development cycle. In the literature, the referred intertwining often relies on models which are considered as analogous and, moreover, compatible, e.g., attack trees vs. fault trees, threat sources vs. failure causes, etc. Despite that, certain particularities are identified which may impede a seamless co-engineering process. This talk aims to highlight those particularities, address questions on models' limitations and provide some insights to solve them.

10:00 – 10:30

Coffee Break

10:30 – 12:15

Session 1: Research Papers

Room: TBA
Chair: TBA (institution)

Understanding Common Automotive Security Issues and Their Implication, ***By Aljoscha Lautenbach, Magnus Almgren and Tomas Olovsson (Chalmers University of Technology, Sweden)***

With increased connectivity of safety-critical systems such as vehicles and industrial control systems, the mportance of secure software rises in lock-step. Even systems that are traditionally considered to be non safety-critical can become safety-critical if they are willfully manipulated. In this paper, we identify 8 important security issues of automotive software based on a conceptually simple yet interesting example. The issues encompass problems from the design phase 1 to the choice of concrete parameters for an API. We then investigate how these issues are perceived by automotive security experts through a survey.
The survey results indicate that the identified issues are indeed problematic in real industry use-cases. Based on the collected data, we draw conclusions which problems deserve further attention and how the problems can be addressed. In particular, we find that key distribution is a major issue. Finally, many of the identified issues can be addressed by improved documentation and access to security experts.

SAM: A Security Abstraction Model for Automotive Software Systems
By Markus Zoppelt and Ramin Tavakoli Kolagari (Nuremberg Institute of Technology, GERMANY)

Due to the emergence of (semi-)autonomous vehicles and networked technologies in the automotive domain, the development of secure and reliable vehicles plays an increasingly important role in the protection of road users. Safe and secure road transport is a major societal and political objective, which is substantiated by the

concrete goal of the European Commission to “move close to zero fatalities in road transport" 1 within the next three decades.
One historically often neglected aspect of this objective in automotive system development is security, i.e., freedom from maliciously implemented threats. In the automotive software industry, model-based engineering is the current state of the practice. Instead of integrating security into the entire system development process, it currently tends to be an afterthought. Because of the tight interdependencies and integration of components, the consequences of gaping security flaws are grave. The contribution of this paper is a secure modeling approach enabling the automotive engineer to analyze the software system in the context of industrial model-based engineering in an early phase. The security modeling language specification is presented as a proposed annex to the relevant industry standard EAST-ADL, and therefore offers a common modeling approach for architectural and security aspects. All security extensions are in line with this standard and its meta level, which is shared with AUTOSAR. The security modeling language specification is demonstrated in a small modeling example, along with a formal evaluation which applies the Grounded Theory method to a set of expert interviews, showing that it is comprehensive and embraces even
non-standardized pertinent research.

SysML model transformation for safety and security analysis

By Rabéa Ameur-Boulifa, Florian Lugou and Ludovic Apvrille (Université Paris-Saclay, France)

While the awareness toward the security and safety of embedded systems has recently improved due to various significant attacks, the issue of building a practical but accurate methodology for designing such safe and secure systems still remains unsolved. Where test coverage is dissatisfying, formal analysis grants much higher potential to discover security vulnerabilities during the design phase of a system. Yet, formal verification methods often require a strong technical background that limits their usage. In this paper, we formally describe a verification process that enables us to prove security-oriented properties such as confidentiality on block and state machine diagrams of SysML. The mathematical description of the translation of these formally defined diagrams into a ProVerif specification enables us to prove the correctness of the verification method.

11:30-12:00 - The Challenge of Safety Tactics Synchronization for Cooperative Systems

By Elena Lisova and Svetlana Girs (Malardalen University, Sweden)

Given rapid progress in integrating operational and industrial technologies and recent increase in the level of automation in safety related systems, cooperative cyber-physical systems are emerging in a self-contained area requiring new approaches for addressing their critical properties such as safety and security. The notion of tactics is used to describe a relation between a system input and its corresponding response. Cooperative functionalities often rely on wireless communication and incoherent behavior of different wireless channels makes it challenging to achieve harmonization in deployment of systems’ tactics. In this work we focus on safety tactics for cooperative cyber-physical systems as a response to inputs related to both safety and security, i.e., we are interested in security informed safety, and formulate a challenge of synchronization of safety tactics between the cooperating systems. To motivate the requirement on such synchronization we consider a car platoon, i.e., a set of cooperative vehicles, as an example and illustrate possible hazards arising from unsynchronized tactics deployment.

12:15 – 12:45

Round Table and discussions

12:45 – 14:00

Farewell & Lunch