Model-Driven Security

MDsec '12 Workshop at MoDELS 2012, Innsbruck, Austria

Nora Koch
Institut für Informatik, Ludwig-Maximilians-Universität München and NTTDATA, Germany
kochn@pst.ifi.lmu.de

Alexander Knapp
Universität Augsburg, Institut für Informatik, Germany
knapp@informatik.uni-augsburg.de

Geri Georg
Colorado State University, Computer Science Department, U.S.A.
georg@cs.colostate.edu

Marina Egea
Atos Research & Innovation Department, Madrid, Spain
marina.egea@atosresearch.eu

Benoit Baudry
IRISA – INRIA, Campus de Beaulieu, Rennes, France
benoit.baudry@inria.fr

ABSTRACT

We have seen many efforts invested in research on engineering security aspects of software and systems over the last years, but we have also seen spectacular security breaches and privacy leaks in web applications, mobile apps, and enterprise systems. In fact, in both the industrial and the academic context, we are still far from satisfactory, integrative development approaches covering the many different facets of security, such as access control, secure user interaction, privacy, secure protocols, trustworthiness, etc. Model-driven and model-based approaches to security integrate security aspects in the early phases of software development at an abstract level. They thus pave the way to reduce the gap between security requirements and their enforcement mechanisms and to verify security properties on an appropriate level of detail, following the principle of separation of concerns. These approaches allow designers to decouple functional architecture from mechanisms that ensure the security properties of the system. The main objective of this workshop was to bring together researchers and practitioners to discuss the approaches, key issues, innovative applications, and trends in model-driven engineering of secure and trustworthy service composition, software, and systems.

Categories and Subject Descriptors

D.2.1 [**Requirements/Specifications**]: Methodologies; D.2.2 [**Design Tools and Techniques**]; D.4.6 [**Security and Protection**]

General Terms

Design, Security, Theory

MDsec'12, September 30 2012, Innsbruck, Austria
Copyright 2012 ACM 978-1-4503-1806-8/12/09 ...$15.00.

Keywords

Security, design, model-based development, model-driven development

1. INTRODUCTION

The program of the MDsec workshop consisted of four paper sessions and discussions. The paper sessions generally coalesced around the topics of Secure Architectures, Access Control, Secure Development, and Cryptography.

The papers of the first section on Secure Architecture focussed on organisational issues and risk analysis in managing security. They use meta-modeling, refinement and pattern-based techniques to achieve their objectives. The papers of the second session on Access Control proposed model-driven approaches for generating policies for Web applications, monitoring access control policies in networks, and the enforcement of access control in distributed, pervasive systems. Security aspects in collaborative and enterprise models as well as in models of smart cart applications were presented in the third session on Secure Development. These models are used for representing ontologies, generating security code or the formal verification of the code. Finally, the forth section on Cryptography discussed a formal model for deriving a cryptographic orchestrator for secure service composition.

The workshop received 26 submissions on a wide range of topics that span multiple phases of system development. Nine papers were eventually chosen to be presented at the workshop and are included in these proceedings. Each paper was reviewed by three members of the the day, leading to many interesting discussions.

Twenty-two participants attended the workshop over the day, leading to many interesting discussions. Several participants with industrial background contributed their experiences in the field of security to the discussions. They posted as well challenging questions to the presenters and the audience of the workshop.

The main discussion topics are presented in the following sections. Section 2 discusses the roles of models and how they can be made more productive, and Section 3 discusses research directions that our community needs to address.

2. THE ROLE OF MODELS IN SECURITY

We reinforced through discussion that the role of models depends on their intentions, or what they are being used for: e.g. communication with stakeholders or generating code or performing analysis or performing runtime monitoring, etc. However, some researchers have also found that very specific models, such as risk models, may not always be needed. Over time the information they extract regarding a system may be naturally included in other appropriate models. In short, security models may only add value in cases where other models do not take the associated and relevant security issues into account. We have also found that problems can arise if the same language or notation is used in models for these different roles. In general, models that use domain specific languages (DSLs), based on the role that the model plays, are most productive.

We discussed the role of models during runtime system monitoring to some extent, and while no conclusions were drawn, it was noted that this is an interesting application of security modeling, and that there are problems that must be solved "on the fly". In fact, it is not possible explore the state space like we can at design time; in a running system there is no time to determine properties, and therefore analysis must be completely automated.

3. RESEARCH DIRECTIONS

We noted that there are both vertical and horizontal integrations that should be addressed in any research agendas. This is related to the fact that there is a tension between the desire to incorporate new ideas into existing approaches and techniques and the desire to create new approaches that specifically address a focused problem. We would like to propose that some tactics such as model transformations, extensions, and adaptations may be sufficient in many cases to solve a new problem, but we also realize that completely new approaches may also be required in other cases.

These tensions are very evident in the needs to integrate the solutions to problems that were presented at the workshop into more overall system modeling, and to provide additional (perhaps better) links between functional and security modeling. This latter issue is critical — designers and developers often have limited ideas of how to approach security in the systems they are creating. Most current approaches assume that there is some user applying the approach, however security experts need different types of models and for different reasons than software developers: e.g. different modeling at a different level of abstraction. As discussed in the previous section, there is a role for DSLs in these models, and it is probably beneficial to continue creating and standardizing security libraries for software developers to use.

We also discussed whether security is really different from other modeling. Or is this just an artificial distinction? Perhaps security modeling really should be just good modeling, as evidenced from the inclusion of security issues in system models over time that was also discussed in the previous section.

In fact we are seeing variant languages for security across a set of industrial companies. Two examples are similar models and standards for automotive companies, and threat model sharing that is occurring in the UK. In part, these situations work because there is a business interest in exchanging models. However, it should be noted that not all security models are easily exchanged (e.g. threat models). De-facto standardization of formats and model types could be very beneficial to industry in the long run.

A key barrier to both horizontal and vertical integration is that of critical mass. Platforms and forums that allow other researchers to use our models and languages can provide this critical mass in addition to providing valuable feedback regarding usefulness. We also need to be able to incorporate our new ideas into others' existing approaches. These are exactly the goals of the NESSoS EU project: to provide a platform for knowledge exchange, based on researchers' experiences, and a tool platform for plug-ins. The tools in NESSoS are all prototypes and the platform is intended solely as an exchange experience.

4. ACKNOWLEDGMENTS

We would like to thank the MODELS Workshop Chairs for their help in the planning and delivery of the MDsec workshop at MODELS 2012, and the ACM support for these proceedings. We would also like to thank all of the authors who submitted their research to this workshop, and the PC members who reviewed the papers and helped make the difficult decisions regarding which papers were accepted to the workshop. Our thanks also go to all the participants who made the workshop a success. Finally, we would like to thank our sponsors, the NESSoS and Aniketos EU projects, and Atos, INRIA, SAP, Thales, and TSSG, who supported us in this effort.