2011

Seventh International Workshop on Software Engineering for Secure Systems (SESS 2011)

Seok-Won Lee
University of Nebraska-Lincoln, slee@cse.unl.edu

Mattia Monga
Università degli Studi di Milano, mattia.monga@unimi.it

Jan Jürjens
Dept. of Computer Science TU Dortmund, Jan.Jurjens@cs.tu-dortmund.de

Seventh International Workshop on Software Engineering for Secure Systems (SESS 2011)

Seok-Won Lee
Dept. of Computer Science and Engineering
University of Nebraska-Lincoln
Lincoln, NE 68588-0115, USA
+1-402-472-2184
slee@cse.unl.edu

Mattia Monga
Dip. Informatica e Comunicazione
Università degli Studi di Milano
Via Comelico 39/41 – I-20135
Milan, Italy
+390250316238
mattia.monga@unimi.it

Jan Jürjens
Dept. of Computer Science
TU Dortmund
44221 Dortmund,
Germany
+49 231 755-7953
Jan.Jurjens@cs.tu-dortmund.de

ABSTRACT

The 7th edition of the SESS workshop aims at providing a venue for software engineers and security researchers to exchange ideas and techniques. In fact, software is at core of most of the business transactions and its smart integration in an industrial setting may be the competitive advantage even when the core competence is outside the ICT field. As a result, the revenues of a firm depend directly on several complex software-based systems. Thus, stakeholders and users should be able to trust these systems to provide data and elaborations with a degree of confidentiality, integrity, and availability compatible with their needs. Moreover, the pervasiveness of software products in the creation of critical infrastructures has raised the value of trustworthiness and new efforts should be dedicated to achieve it. However, nowadays almost every application has some kind of security requirement even if its use is not to be considered critical.

Categories and Subject Descriptors

D.2 [**Software Engineering**]; D.4.6., K.6.5. K.4 Security and Protection; Privacy, Regulation

General Terms

Design, Security, Languages, Theory, Verification.

Keywords

Software Engineering, Information Security, Secure Systems.

1. WORKSHOP THEME – Soft and Secure

Nowadays software systems are as flexible as ever: they adapt themselves to the context of operation and their evolving environments. Nevertheless, they should always operate in a secure manner by preserving privacy and trust among the involved parties, even if the dynamic and decentralized nature of these systems poses several challenges in order to protect the exchange of data or services and guarantee the fairness of the system as a whole. Software is at core of most of the business transactions and its smart integration in an industrial setting may be the competitive advantage even when the core competence is outside the ICT field. As a result, the revenues of a firm depend directly on several complex software-based systems.

Thus, stakeholders and users should be able to trust these systems to provide data and elaborations with a degree of confidentiality, integrity, and availability compatible with their needs and software engineers have to be familiar with the risks their design choices pose. All in all almost every application has today some kind of security requirement even if its use is not to be considered critical.

Moreover, the pervasiveness of software products in the creation of critical infrastructures has raised the value of trustworthiness and new efforts should be dedicated to achieve it.

The cases in which no one has the complete control on all the components are increasingly common and relevant: for example, "Mashup" applications pose several new security challenges since the designers could be partially unaware of the information exchanges that the users introduce into the system logic.

Security concerns should be taken into account as early as possible, and not added to systems as an after-thought: this is extremely expensive and it may compromise the design integrity in critical ways. Security features such as cryptographic protocols and tamper resistant hardware cannot be simply added on to transform an insecure product to a secure one. Security solutions and patterns are hard to reuse in different contexts, they crosscut all the system components and a single vulnerability alone might compromise the trustworthiness of the whole system. Thus, not surprisingly, several security holes are recurrent, notwithstanding the experience accumulated by security research in the last decades. Software engineers and practitioners should assimilate basic security techniques and discover new techniques for integrating them in the current practice, while understanding associated costs and benefits. Several well-established software engineering disciplines such as verification, testing, program analysis, process support, configuration management, requirement engineering, etc. could contribute to improving security solutions that sometimes lack a coherent methodological approach. Or, as it is the case of security standards proposed by the Common Criteria [2] or BS7799 [1], present challenges that prevent integration with mainstream software engineering practice. Moreover, applications are increasingly deployed in unanticipated environments and even the "attack surface" of an application can be difficult to assess at design time, for example in the now popular case of virtual hosting in which guest applications share physical resources that might open unwanted communication channels..

ICSE'11, May 21–28, 2011, Waikiki, Honolulu, HI, USA

doi: 10.1145/1985793.1986045

2. WORKSHOP OUTLINE

This year the program committee selected four regular and four position papers to be presented at the workshop. The issues addressed were very diverse, another demonstration of how security cross-cuts all the activities of modern software engineering practice.

The topics of the papers increasingly focus on model-driven security engineering approaches that concern from the beginning of system conception: transformation of security concerns in requirements engineering phase to design phase [6]; comprehensive security conceptual meta-model [8]; languages for software certification in the complex systems of systems context [4]; or even more towards system implementation: use of least privileges technique to check the violation in a large scale system [5]; the vulnerability prediction models using execution complexity metrics [3]; ideas proposed to allow end users to safely execute new software of uncertain provenance [9].

In addition, some theoretical and practical studies were included: the action refinement theory to guarantee the security properties in communication [7]; theoretical and practical study on a crypto system [10].

It is very encouraging to see that a lot of efforts were put in developing a better design, model and development of security constraints in the system with a larger view and understanding.

A panel program will discuss current challenging issues in the area of secure software engineering by a group of experts from: secure software engineering/ information assurance education; system security, privacy/security requirements, security certification process, and theoretical security research.

3. WORKSHOP ORGANIZATION AND PROGRAM COMMITTEE

3.1 Organizing Committee (Chairs)

- Jan Jürjens, Technical University Dortmund, Germany
- Seok-Won Lee, Univ. of Nebraska-Lincoln, USA
- Mattia Monga, Università degli Studi di Milano, Italy

3.2 Program Committee

- Davide Balzarotti, Eurecom, France
- Andreas Bauer, National ICT Australia, Australia
- Hao Chen, University of California Davis, USA
- Pau-Chen Cheng, IBM TJ Watson Research Center, USA
- Mihai Christodorescu, IBM TJ Watson Research Center
- Dave Clarke, Katholieke Universiteit Leuven, Belgium
- Hyunsook Do, North Dakota State University, USA
- Eduardo Fernàndez-Medina Patón, Universidad de Castilla-La Mancha, Spain
- Donald Firesmith, Software Engineering Institute, USA
- Robin Gandhi, University of Nebraska at Omaha
- Munawar Hafiz, University of Illinois, USA
- Lin Liu, Tsinghua University, China
- Lorenzo Martignoni, Univ. of California at Berkely, USA
- Raimundas Matulevicius, University of Tartu, Estonia
- Sjouke Mauw, University of Luxembourg
- Nancy Mead, Software Engineering Institute, USA
- Haris Mouratidis, University of East London, UK
- William Robertson, University of California, Berkeley, USA
- Thomas Santen, European Microsoft Innovation Center, Germany
- Riccardo Scandariato, Katholieke Universiteit Leuven, Belgium
- Jörg Schreck, Telefonica O2 Munich, Germany
- Wietse Z. Venema, IBM T.J. Watson Research Center
- Liang Xiao, Royal College of Surgeons Ireland, Ireland
- Mohammad Zulkernine, Queens University, Canada

4. ACKNOWLEDGMENTS

The organizers want to thank all the reviewers and the authors for their contribution to a workshop that promises to be very interesting for both the security and the software engineering research community.

5. REFERENCES

[1] The BS7799 / BS 7799 security standard. http://www.thewindow.to/bs7799/

[2] The Common Criteria portal. http://www.commoncriteriaportal.org/

[3] Y. Shin; L. Williams "An Initial Study on the Use of Execution Complexity Metrics as Indicators of Software Vulnerabilities" In Proceedings of the 7th Int'l Workshop on Software Engineering for Secure Systems (SESS), Hawaii, May 2011.

[4] M.T. Gamble; R. Gamble; M.L. Hale "Security Policy Foundations in Context Unity" In Proceedings of the 7th Int'l Workshop on Software Engineering for Secure Systems (SESS), Hawaii, May 2011.

[5] K. Buyens; R. Scandariato; W. Joosen "Composition of least privilege analysis results in software architectures" In Proceedings of the 7th Int'l Workshop on Software Engineering for Secure Systems (SESS), Hawaii, May 2011.

[6] N. Ahmed; R. Matulevicius "Towards Transformation Guidelines from Secure Tropos to Misuse Cases" In Proceedings of the 7th Int'l Workshop on Software Engineering for Secure Systems (SESS), Hawaii, May 2011.

[7] F. Martinelli; I. Matteucci "Preserving Security Properties under Refinement" In Proceedings of the 7th Int'l Workshop on Software Engineering for Secure Systems (SESS), Hawaii, May 2011.

[8] N. Lammari; J-S. Bucumi; J. Akoka; I. Comyn-Wattaiu "A Conceptual Meta-Model for Secured Information Systems" In Proceedings of the 7th Int'l Workshop on Software Engineering for Secure Systems (SESS), Hawaii, May 2011.

[9] J. Davidson et al. "PEASOUP: Preventing Exploits against Software of Uncertain Provenance" In Proceedings of the 7th Int'l Workshop on Software Engineering for Secure Systems (SESS), Hawaii, May 2011.

[10] K. Bae; M. Ahn; H. Lee; J. Ha; S. Moon "Power Analysis Attack and Countermeasure on the Rabbit Stream Cipher" In Proceedings of the 7th Int'l Workshop on Software Engineering for Secure Systems (SESS), Hawaii, May 2011.