Software Engineering for Secure Systems

SESS06 – Secure by design

Danilo Bruschi
Dip. Informatica e Comunicazione
Università degli Studi di Milano
Via Comelico 39/41 – I-20135
Milan, Italy
bruschi@dico.unimi.it

Bart De Win
Katholieke Universiteit Leuven
Celestijnenlaan 200A – B-3001
Leuven, Belgium
bart.dewin@cs.kuleuven.be

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

Categories and Subject Descriptors

D.2.m [**Software Engineering**]: Miscellaneous

General Terms

Security, Design

Keywords

Security requirements, trustworthiness, secure programming, security testing, security usability

1. OUTLINE OF THE THEME AND GOALS

The issue of software security is increasingly relevant in a world where most of our life depends directly on several complex computer-based systems. Today the Internet connects and enables a growing list of critical activities from which people expect services and revenues. In other words, they *trust* these systems to be able to provide data and elaborations with a degree of confidentiality, integrity, and availability compatible with their needs.

Historically, the software engineering community has strived more to obtain validity than trustworthiness. Nowadays, however, software ubiquity in the creation of critical infrastructures and ease of third-party service integration has raised the value of trustworthiness and new efforts should be dedicated to achieve it. In particular, 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. Moreover, security features such as cryptographic protocols and tamper-resistant hardware cannot be simply used to "decorate" applications, to transform an insecure product in a secure one just by this addition. Surprisingly enough, 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 integrate them in the current practice, while understanding associated costs and benefits.

Conversely, computer security still lacks of practical methodological approaches which could help in reducing security exposures in many critical applications. Even well defined formalisms such as the security standards (e.g., Common Criteria [2] and BS7799 [1]), are challenging to integrate with mainstream software engineering practices. In such a context, several well-known software engineering disciplines such as verification, testing, program analysis, process support, configuration management, requirement engineering, etc. could contribute in improving security solutions.

The SESS workshop aims at providing a venue for software engineers and security researchers to exchange ideas and techniques. The first edition was held in conjunction with ICSE2005 [3]. The workshop website is `http://homes.dico.unimi.it/~monga/sess06.html`.

This workshop aims at putting together people from the software engineering and the security fields, with the ambitious goal of fostering a fruitful cross-fertilization between the two communities. As software is going to permeate every aspect of our society, an increasing attention to its social side-effects is needed. Security is obviously an important one, because most of our daily activities assume availability of reliable and trustworthy software systems. The software industry has to deal with the problem of building secure programs in an economic way, but software engineers have not yet matured enough knowledge in the field [4].

ICSE'06, May 20–28, 2006, Shanghai, China.
ACM 1-59593-085-X/06/0005.

2. PROGRAM COMMITTEE

- Elisa Bertino, Center for Education and Research in Information Assurance and Security, Purdue University
- Danilo Bruschi, Università degli Studi di Milano, Italy
- Premkumar T. Devanbu, University of California at Davis
- Bart De Win, Katholieke Universiteit Leuven, Belgium
- Carlo Ghezzi, Politecnico di Milano, Italy
- Charles B. Haley, The Open University, UK
- Richard A. Kemmerer, University of California at Santa Barbara
- Christopher Kruegel, Technische Universitt Wien, Austria
- Mattia Monga, Università degli Studi di Milano, Italy
- Samuel Redwine, James Madison University
- Stuart Stubblebine, Stubblebine Research Labs and University of California at Davis
- Wietse Z. Venema, IBM T.J. Watson Research Center
- John Viega, Secure Software, Inc.
- Giovanni Vigna, University of California at Santa Barbara
- Xiaolan Zhang, IBM T. J. Watson Research Center
- Hengming Zou, Shanghai Jiao Tong University, China

3. REFERENCES

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

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

[3] SESS'05: Proceedings of the 2005 workshop on software engineering for secure systems: building trustworthy applications, 2005. Available at `http://www.acm.org/dl`.

[4] Michael Howard and David LeBlanc. *Writing Secure Code*. Best Practices. Microsoft Press, second edition, 2003.