Thursday 1 December 2016
10h30
UT2 Jean Jaurès, Maison de la Recherche, Salle D29

Brahim HAMID
Team MACAO - IRIT

Engineering secure systems: patterns, properties, models, analysis and experimental evaluations

Jury:
Pr. Paris AVGERIOU – Univ. Groningue (Rapporteur)
Pr. Bernard COULETTE – Univ. Toulouse Jean-Jaurès (Examinateur)
Pr. Eduardo B. FERNANDEZ – Univ. Floride Atlantique (Examinateur)
Pr. Marianne HUCHARD – Univ. Montpellier (Examinateur)
Pr. Regine LALEAU – Univ. Paris 12 (Rapporteur)
Pr. Yves LEDRU – Univ. Grenoble Alpes (Examinateur)
Pr. Dominique MERY – Univ. Lorraine (Rapporteur)
Pr. Lionel SEINTURIER – Univ. Lille 1 (Rapporteur)

Abstract: System and software security engineering has become a crucial business aspect since organizations are completely dependent on their computer-based systems and invest substantial resources to maintain these systems. Due to the shift from traditional computer systems to the Internet of Things, wireless communication or other interfaces, issues such as sociality, trust, privacy, and delegation of responsibilities has become more closely related to the security of software systems.

These systems have become inter-dependent and connected to the open-world. The risk of exposure becomes a greater challenge due to an increase in the spectrum and probability of cyber-attacks and the impact of a breach on daily life. As a consequence, the security policy of a modern ICT is more dependent on the interaction between the core system (its technological assets) and external entities (other technological assets, people and organizations). This indicates that information and cyber security is not a problem for only a few systems specialists. Currently, almost all white-collar crime and terrorism involves computers or mobile phones, which implies that the involved people, including citizens, need to have awareness and understanding in system security, and in the near future, in computer forensics. However, in most European countries, for instance, ``In France, information and public debate on the threats posed by damage to the security of information systems and its impact on defense and national security, or simply on our daily lives, remain largely underdeveloped."

Therefore, developers of these systems need to 'design for security' and simultaneously balance (trade-off) multiple, interdependent design concerns, such as availability, performance and other architecture quality attributes to economically and quickly build reliable and trustworthy systems. However, in many cases, security engineering and software engineering are considered to be "islands" because these disciplines work independently and their methods and tools are disconnected. This independence causes the architecture and security to be independently handled, which creates tremendous challenges during system development. Therefore, the design of architecture and security need to be investigated in tandem as the engineering of secure systems. Standards are available for securing IT systems. Although they provide minimal guidance to software...
engineers regarding their implementation, they should be applied from the early stage of the conception of a system. Most work has to be manually performed because only a few methodological tools are available to aid the realization. This limitation causes extensive work and substantial extra costs.

The foundation for comprehensive security engineering is a comprehensive understanding of modern systems and technologies and ongoing or previous security incidents and their implications on the underlying critical infrastructure. This understanding includes defining the current structure of the system, i.e., the system architecture, identifying abstract risks and concrete vulnerabilities, and implementing appropriate countermeasures to mitigate risks and vulnerabilities to satisfy both the security and the other architecture's quality attributes. Specification of the deployment plans, identification of the operation needs, agreement with involved stakeholders, plans for training, evaluation and event and incident response and management for the continuity of operations are also taken into account. My contribution in this area concerns engineering secure systems by focusing on the problem of integrating design, realization and management. Notions such as patterns, properties, models, reuse repository, analysis and experimental evaluations can help in the development of well-designed, properly modeled, accurately documented, and well-understood secure systems...