Security Engineering for Ambient Intelligence: A Manifesto

A. Maña, University of Malaga, Spain

C. Rudolph, Fraunhofer Institute for Secure Information Technology, Germany

G. Spanoudakis, City University, UK

V. Lotz, SAP Research, France

F. Massacci, University of Trento, Italy

M. Melideo, Engineering Ingegneria Informatica, Italy

J. S. López-Cobo, ATOS Origin, Spain

ABSTRACT

The scenarios of ambient intelligence introduce a new computing paradigm and set new challenges for the design and engineering of secure and dependable systems. This chapter describes SERENITY, a comprehensive approach to overcome those problems. The key to success in this scenario is to capture security expertise in such a way that it can be supported by automated means. SERENITY’s integral model of ADD — security and dependability (S&D) considers both static and dynamic aspects by relying in two main innovations: (1) the enhanced notion of S&D patterns and integration schemes; and (2) the computer aided run-time monitoring of...
the implemented security solutions. The combination of these innovations lays the foundations of an integrated, solid, flexible, and practical S&D framework for AmI ecosystems. The chapter aims at clarifying the challenges introduced in AmI ecosystems and pointing out directions for research in the different areas involved.

INTRODUCTION

Well in the past millennium, the typical reaction to questions about “information systems security” would have been another question “what is security?” A decade ago the response to the same concern was “security is an added value service, a non-functional requirement.” Only in the last few years has the response become “security must be designed and built-in from the very start.” Although the latter response acknowledges the need for integrating security into the design and development phases of IT, this integration is still lagging behind in practice (Tryfonas, Kiountouzis, & Poulymenakou, 2001). Security engineering capability maturity models, ISO 17799 and other standards detail a classification of properties that a secure system must have but do not actually provide any information on how such properties can be achieved. Even landmark textbooks on security engineering (Anderson, 2001) are often a collection of case studies and do not provide a structured methodology for actually engineering secure systems, no more than a dictionary can be called a grammar.

Today COTS (components off-the-shelf) security services such as encryption, digital signatures, public key infrastructures, etc. and rather standard attack countermeasures such as firewalls, intrusion detection systems, etc. are selectively employed in the attempt to fulfil basic security requirements such as authentication or confidentiality. The usual deployment of those security mechanisms provides an “isolated” functionality, which is not always appropriate for the specific system to be protected and is usually not effective for addressing the potential threats introduced by emerging environments like grid computing and wireless ad-hoc networks. Experience in the development of cryptographic protocols shows that even for relatively small systems, it is difficult and often error-prone to fulfil security requirements by simply combining existing security mechanisms. Even for such a brittle field, there are few and specialized solutions that supports in an automated way the precise identification of security requirements and the correct choice of security mechanisms. Their adoption by IETF protocol designers has still a long way to go (interested readers might have a look at the AVISPA EU project effort into introducing the usage of formal methods into standard security protocols design at www.avispa-project.org).

Designers and users must also face other sources of complexity: the impact of contextual information (e.g., hardware and software configurations of the system), external entities interoperating with the system, legal requirements, social behaviour, etc., can be easily overlooked. As a consequence, expert knowledge in IT security
PKI Deployment Challenges and Recommendations for ICS Networks
www.igi-global.com/article/pki-deployment-challenges-and-recommendations-for-ics-networks/178644?camid=4v1a