

# Security Requirements Engineering: A Survey

Jose Romero-Mariona, Hadar Ziv, and Debra J. Richardson  
Institute for Software Research  
University of California, Irvine  
Irvine, CA 92697-3425  
{jromerom, ziv, djr} @ics.uci.edu

ISR Technical Report # UCI-ISR-08-2

## Abstract

Security has become a primary and prevalent concern for software systems. The past decade has witnessed a tremendous increase in not only the sheer number of attacks but also the ease with which attacks can be performed on systems. We believe that in order to protect a system against harm (intended or not), attention must be given to its requirements. Similar to other system properties and quality attributes, security must be considered from inception, in other words starting with requirements. Security is a nonfunctional requirement (NFR) that is increasingly critical in its importance, unique in its requirements, yet must still be integrated with all other functional and non-functional requirements and mapped into successful architectures, designs, and implementation. Similar to other nonfunctional requirements, the unique nature and demands of security make it difficult and often ineffective to specify security concerns using "general purpose" requirements methods. As a result, several original and derived approaches to security requirements engineering have recently been proposed.

In the following survey we explore a variety of approaches for engineering security-specific requirements. For the purposes of this survey, we decompose security requirements engineering into five more manageable phases, namely, security requirements elicitation, security requirements analysis, security requirements specification, security requirements management, and later stages support for security requirements. We have developed an evaluation framework that focuses on each phase; the evaluation framework is composed of a variety of questions and response criteria designed in order to probe how well existing approaches support each specific security requirements engineering phase.

We survey a total of 12 approaches; there are 6 approaches that have been derived from other approaches in order to address security, and there are 6 approaches that have been developed specifically for security requirements. We apply our evaluation framework to each of the 12 approaches and rank their responses based on a "star count" system. The stars possible for each response range from 0 to 3. 0 stars indicate no support and 3 stars indicate the maximum level of support for that question. Based on the results of the survey, we provide a variety of observations and propose recommendations for improving security requirements engineering. With our survey, we also uncover a variety of areas in security requirements engineering in which there is an evident lack of support; these areas of need will become part of our future work.