Towards Usable Cyber Security Requirements

Jose Romero-Mariona: jromerom@uci.edu
Hadar Ziv: ziv@ics.uci.edu
Debra J. Richardson: djr@ics.uci.edu
Dennis Bystritsky: dbystrit@uci.edu

Donald Bren School of Information and Computer Sciences
University of California, Irvine

Outline

- Motivation
- Background
- ROBS in Detail
- SURE Technique
- SURE Requirements
- SURE Testing
- Conclusions
- Future Work
Motivation

- Security risks are increasingly more frequent, widespread, and volatile
- Often, the need for security is realized too late in the software development process
- Traditional Requirements Engineering (RE) approaches are not well suited for security-focused systems
- Specialized approaches to Security Requirements Engineering (SRE) are still in their infancy
- Support for later stages (LSS) of development is especially lacking

Background

- Literature Survey:
  - 12 approaches
  - 5 SRE phases
  - 34 questions total
- Results:
  - Need for a SRE approach that provides Later Stages Support
  - Current approaches lack meaningful testing support
  - Top approaches
    - Original: CLASP and USEr
    - Derived: Misuse Cases
Background

ROBS in Detail

- ROBS- Requirements for an Online Banking System
- Example scenario for application of SURE
  - Secure and Usable Requirements Engineering
  - New SRE approach
  - Aids in deriving testing artifacts from security requirements
ROBS in Detail

One of the security-related features of my online banking system is document access and sharing...

Developer Dennis

SURE- User Analysis

- Software Developer- Target user
- Assumptions
  - Familiar with traditional RE methods like narrative text, shall statements, and use cases
  - Security specification novice- Some knowledge about specifications in general, but needs support
  - Familiar with basic security concepts like threats and attacks
  - Software testing basics- test plan, test cases, etc.
SURE Technique - Requirements

Determine CLASP Activities
- Activity 1- Institute security awareness program
- Activity 3- Manage certification process
- Activity 6- Specify security requirements
- Activity 7- Specify misuse cases
- Activity 12- Research and asses security solutions
- Activity 26- Identify and implement security tests
SURE Technique - Requirements

SURE Security Requirements

Security Requirements Specification


Misuse Cases Specification

Determine Misuse Cases → Misuse Consequences → Possible Threats

Possible System Threats

Stakeholder Input

Progress
SURE Technique - Requirements

Specify Security Requirements

Security Statement 1 (SS1)
"Documents with sensible data are handled which need to be shared"

Security Need 1 (SS1-SN1)
"Need to securely transport documents"

Security Need 2 (SS1-SN2)
"Need to securely store documents"

Security Requirement 1 (SS1-SN1-SR1)
"System shall enforce secure document dispatch"

Security Requirement 2 (SS1-SN1-SR2)
"System shall monitor secure document transmission"

Security Requirement 3 (SS1-SN1-SR3)
"System shall enforce secure document receipt"
SURE Technique - Requirements

Specify Misuse Cases

Misuse Case
“An attacker disguises himself as an access point and intercepts the login information from a system administrator. The attacker then captures a document containing sensitive information.”

Misuse Case Consequence(s)
- Possible loss of sensitive data
- Attacker might gain access to information necessary to infiltrate the system further
- Risk of identity theft

Misuse Case Threat(s)
- Evil-twin attack
- Eavesdropping attack
SURE Technique - Testing

- SRBT foundation
  - Set of 4 security requirements based testing principles
  - 12-step process for SRBT
- Supports
  - Test completion criteria
  - Test case design
  - Test case specification

Conclusions and Future Work

- SURE- New SRE approach
- Supports security requirements specification
- Facilitates test artifact derivation from security requirements
- Implementation- SURE System
- Technique refinement
- Technique/System evaluation