A Security Requirements Approach for Web Systems

Daniel Méndez
with Stefan Wagner, Klaus Lochmann, Shareeful Islam

Technische Universität München, Germany

Quality Assessment in Web
June 22th, 2009
Relevance of Security

- Over 6,000 reported vulnerabilities in 2008 *
- Results in average loss of $456,700 per year for each company **
- Most affected: public accessible web systems

Secure web systems begin with specification of security requirements

→ Although, there are many Requirements Engineering (RE) approaches for web systems, security requirements are mostly neglected.

* CERT-Report / CMU
** E-Crime Watch Survey
Problem Statement: Security and Security Requirements

- David A. Garvin, 1984: „Quality is a complex multifaceted concept. It is also the source of great confusion...“

- Especially true for security requirements (specifications), as they:
  - depend on many technological factors
  - depend on economic factors

- Security requirements often neglected, especially in practice

- Consequences:
  - Ambiguous specifications of security requirements
  - Difficult implementation
  - Difficult quality assurance

Need for a structured and economical reasonable RE approach
Outline

- Quality Requirements
- Available Security Approaches and Contemporary Needs
- Proposed Approach
- Activity-Based Quality Model (ABQM)
- Case Study
- Conclusions
Quality Requirements

- Part of „non-functional“ requirements
- Describe aspects beyond functionality, although functional requirements can often be derived
- Often based on Quality Models (e.g. ISO Std. 9126)
- Often reduced to abstract quality attributes

* Martin Glinz

- **Critique:**
  - Usage Scenarios and possible attacks often not available from the beginning ("I know it when I see it")
  - Missing methodological guidance for refinement to an assessable abstraction level (depending on e.g. technological factors of future system)
Sketching Proposed Approach

- Define a RE Process, based on an activity-based quality model

- Philosophy: “Quality is how good human (usage) activities are supported and / or prevented by the system”

- Quality models in general benefit:
  - Clear understanding on quality and common vocabulary
  - Basis for reusing assessable (quality) requirements

Steering Theme: Only specify what:
- customers really need / are ready to invest for;
- developers can unambiguously interpret & measure
Activity-Based Quality Model

Boehm et al. (1978)

- Augmentability
- Structuredness
- Communicativeness
- Accessibility
- Self-Descriptiveness
- Conciseness
- Legibility

- Maintainability
  - Modifiability
  - Modification
  - Testability
  - Testing
  - Understandability
  - Understanding

- Maintenance
- Testing
- Understanding
Maintenance

Modification

Testing

Understanding
What properties of the system and its environment take influence on the activities, thus the quality?

Impact

[Structure | Conformity] + [Understanding]
In a Nutshell: Using the ABQM for Security Requirements Reuse

Activities (Attacks) → Negative Impact („prevents“) → Facts

Activities:
- Physical Attack
- Exploitation Attack
- Injection Attack
- Format String Injection
- SQL Injection
- Parameter Injection
- Script Injection
- Embedding Scripts in Nonscript Elements
- Embedding Scripts in HTTP Headers
- Embedding Scripts in HTTP Query Strings

Facts:
- System Data
- Functionality Dynamics
- Static Structure
- Cookie
- HTTP Request
- Cryptographic Support
- File Handling
- Resource Allocation
- Web Page
- ...
Tackling Deficiencies of SREP

- Supports identification of use cases and attacks using **activity tree** (tackles IKIWISI)
- Supports refinement of requirements to assessable level using **entity tree**
Case Study: Design

I: Elaborate reuse repository
- CAPEC
- BSI - Modules
- CWE
- Available Requirements
- ...

II: Apply to Project

Attack Patterns

Available Requirements
Case Study: Results

- **Study 1** applied to Tomcat 6.0:
  - Research Question: “How many of published vulnerabilities would have been avoided?”
  - Results:
    - 16 of 19 published vulnerabilities could be associated with entries in the ABQM
    - 100% reuse ratio regarding cross-site scripting and session hijacking

- **Study 2** applied to real-life projects at Capgemini sd&m AG *
  - Research Question: “How many security requirements of one project can be reused in another project?”
  - Results:
    - 19 requirements in the repository could be reused
    - 11 requirements had to be elaborated in addition
    - 19 requirements were completely missing in project 2 and were overtaken in addition from the repository

* Master thesis Markus Luckey
Conclusions

- We applied activity-based quality models to RE processes for requirements reuse
- Effective support of elicitation and refinement of security requirements
- Evaluated in large development projects

- Currently: Elaboration of domain-specific quality models and standardisation in the project QuaMoCo (www.quamoco.de)
  (TU München, Capgemini sd&m, Itestra, Siemens, Fraunhofer IESE, SAP)
Thank you for your attention.