Tutorial for Software Quality Management
Summer Term 2010
Dr. S. Wagner
L. Heinemann, S. Islam
11.5.2010

Technische Universität München
Fakultät für Informatik

Tutorial Sheet 3: Quality Requirements

A computer with Internet access is required for this tutorial sheet.

Assignment 1: Security and Privacy Requirements

Background Security and privacy over the last few years have gained huge attention to the industry and research community. Microsoft; for example, focuses its effort to improve quality security and privacy in all its products. Microsoft introduced Security Development Life cycle (SDL) and privacy guidelines for the products. SDL has played a critical role in embedding security and privacy in Microsoft software and culture. For instance, security and privacy are considered in design, development, deployment, and communication.

Microsoft Security Development Lifecycle (SDL) - Version 5.0

http://www.microsoft.com/downloads/details.aspx?FamilyID=7d8e6144-8276-4a62-a4c8-7af77c06b7ac&displaylang=en.

Privacy Guidelines for Developing Software Products and Services http://www.microsoft.com/downloads/details.aspx?FamilyID=c48cf80f-6e87-48f5-83ec-a18d1ad2fc1f&displaylang=en

Assume, you are working as a quality manager in the upcoming project of a company. The company is Microsoft gold certified partner. The project considers developing a web portal. The customer would be able to order the items offered by your company through online portal. A successful order requires valid credentials from the customer through bank or credit cards. The project manager and other main practitioners are agreed to develop the product within the Microsoft platform. You are asked to develop a list of security and privacy requirements by following the guidelines of the Microsoft security development life cycle and privacy.

Hints: The guidelines are large document therefore some hints are given, at which pages you can look on to elicit the requirements.
Microsoft Security Development Lifecycle (SDL) - Version 5.0 : pages 6-7 the basic security and privacy concept during the development, page 21 security recommendation for integration-points security design review and strong log-out and session management, page 67 for design review, page 77 Appendix A privacy at a glance, page 79-80 Appendix B: Security Definitions for Vulnerability Work Item Tracking.

Privacy Guidelines for Developing Software Products and Services: Privacy Guidelines for Developing Software Products and Services: pages 6-8 basic concept of user data and personal

identifiable information including sensitive, pages- 11-13 notice, choice and consent, page 20 data integrity, page 24 web sites and web services, pages 48-49 appendix B security and data protection

Example of security and privacy requirements

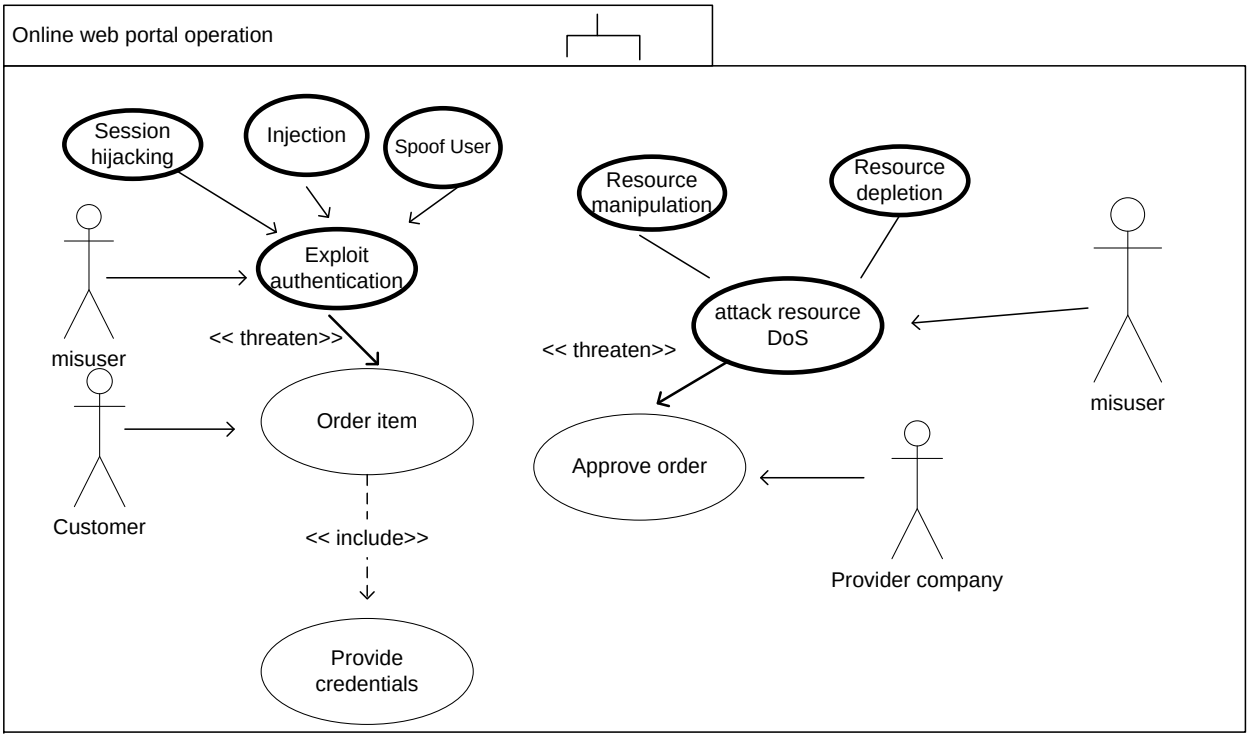
- The web portal components shall provide least privilege while interacting with other components (by following secure by default. However it is a high level security requirement)
- Once the user completes all credential information, to purchase any item, then system shall provide a complete notice about the purchase update. (by following privacy by design. It is a concrete privacy requirement which enforces basic privacy taxonomy)
- The system shall preserve the customer categorized data for the minimum amount of time to support the business purpose and to meet the legal compliance
- The data shall categorize in manner that some sensitive data would not transfer even to the trusted business partners.
- The overall data communication infrastructure shall be secure to protect any malicious activities

Assignment 2: Misuse case using activity based quality model

Background There exist several threats within the project context, stated in assignment 1 (also see page 14-15 security bug and security bug causes). Threat modelling allows to identify threats and vulnerabilities in a given context so that risks associated with the threats are analysed. This eases to refine the initial requirements in a systematic manner. Use activity based quality model in particular an activity tree to specify the attacks. This allows identifying and refining the threats which are later used to construct the misuse case.

Hints: You are free to consider any scenario and threats which is relevant for the application context. Once the activity model is constructed then use it to develop a misuse case. A misuse case is an attacker's use case, which directly threat a valid use case.

Example of Misuse case The figure shows a misuse case for the online web portal high level use case. Here two main threats are considered, i.e., exploit authentication threaten the customer operations and attack resource threaten the provider.


Online web portal operation
Session hijacking
Injection
Spoof User
Exploit authentication
misuser
<< threaten>>
Order item
Customer
<< include>>
Provide credentials
Resource manipulation
Resource depletion
attack resource DoS
<< threaten>>
misuser
Approve order
Provider company