Eliciting Security Requirements using Reusable Features from Use Cases
Imano Williams | Xiaohong Yuan
Department of Computer Science, North Carolina A&T State University

Introduction

An ontology is a conceptualization of knowledge that supports semantic relations. Security Requirements are constraints on the functionality of the system.

Problem:
Ontologies [2-4] currently being used in Security Requirements Engineering pose the following problems:
1) novices may have difficulty with eliciting security requirements based on the ontology
2) security requirements are dependent on the ontology used

Objectives:
1) Identify reusable features in use cases that can be used to elicit security requirements
2) Use the reusable features to create concepts and attributes for our ontology
3) Illustrate security requirements elicitation using the proposed ontology with a simple use case

Method

Rationale:
1) The concepts are directly derived from the use cases.
2) The concepts do not require novices to have an expert understanding of software security

Below are the steps used to create the ontology

Steps to Create Ontology
1. Collected Use Case documents
2. Organized Use Cases based on their functionality
3. Selected Common Reusable Features
4. Analyzed Use Case for Reusable Features
5. Created Ontology based on Reusable Features

Preliminary Results

Concepts(attributes) from reusable features in step 5 (Fig.1):
1) Data (sensitive or insensitive): asset that use case receives and/or submits in the application, e.g. SSN, name, etc
2) Data Transmission Type (transmit): transmit between the client and the server
3) Data Storage (plain or encrypted): data is stored in the application
4) Location (authenticated or unauthenticated): use case web page location
5) Relationship (sibling, child or parent): The relation between two or more use cases
6) Use Case Keywords (N/A): use cases’ similar nouns and verbs words
7) User’s Interaction (multiple-steps or single-step): how the purpose of a use case is completed
8) Purpose (major or minor): importance to the business needs

Future Work
1) Create more relationships/axioms for concepts/attribute
2) Address the completeness and validity of the ontology by using experts, documents, and existing ontologies as sources
3) Address the usability of the ontology, in user study with students in a traditional software engineering course
4) Implement ontology using specific language (OWL, SysML) with a specific tool, such as Protege

Acknowledgement

This work is partially supported by National Science Foundation under the grant HRD-1332504. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

References


Security Concerns:
1) Username and password stolen by attacker when submitting
2) User without valid username and password gets access

Security Requirements Elicited:
1) Sensitive username and password should be transmitted securely
2) System should deny invalid username and passwords
3) Sensitive username and password should be securely stored

Fig. 2: Sample has_A Relationships of the ontology concepts

Fig. 1: Steps to create ontology