SE-4930: Developing Secure Software

Lab 2: The SQUARE Process[1]

Report due: September 24, 2014 23:59 (One per team)

Introduction

Security Quality Requirements Engineering (SQUARE) provides a means for eliciting, categorizing, and prioritizing security requirements for information technology systems and applications. The focus of this methodology is to build security concepts into the early stages of the development life cycle. The model can also be used for documenting and analyzing the security aspects of fielded systems and for steering future improvements and modifications to those systems.

The complete SQUARE process covers 9 steps, as is shown in the table below, and has been shown to be beneficial in developing secure systems.

Number	Step	Input	Techniques	Participants	Output
1	Agree on definitions	Candidate definitions from IEEE and other standards	Structured interviews, focus group	Stakeholders, requirements engineer	Agreed-to definitions
2	Identify assets and security goals	Definitions, candidate goals, business drivers, policies and procedures, examples	Facilitated work session, surveys, interviews	Stakeholders, requirements engineer	Assets and goals
3	Develop artifacts to support security requirements definition	Potential artifacts (e.g., scenarios, misuse cases, templates, forms)	Work session	Requirements engineer	Needed artifacts: scenarios, misuse cases, models, templates, forms
4	Perform risk assessment	Misuse cases, scenarios, security goals	Risk assessment method, analysis of anticipated risk against organizational risk tolerance, including threat analysis	Requirements engineer, risk expert, stakeholders	Risk assessment results
5	Select elicitation techniques	Goals, definitions, candidate techniques, expertise of stakeholders,	Work session	Requirements engineer	Selected elicitation techniques

[1] Based on material from CERT and the Build Security In Project as well as includes significant material from TECHNICAL REPORT CMU/SEI-2005-TR-009 ESC-TR-2005-009.

		organizational style, culture, level of security needed, cost/benefit analysis, etc.			
6	Elicit security requirements	Artifacts, risk assessment results, selected techniques	Joint Application Development (JAD), interviews, surveys, model-based analysis, checklists, lists of reusable requirements types, document reviews	Stakeholders facilitated by requirements engineer	Initial cut at security requirements
7	Categorize requirements as to level (system, software, etc.) and whether they are requirements or other kinds of constraints	Initial requirements, architecture	Work session using a standard set of categories	Requirements engineer, other specialists as needed	Categorized requirements
8	Prioritize requirements	Categorized requirements and risk assessment results	Prioritization methods such as Analytical Hierarchy Process (AHP), Triage, Win-Win	Stakeholders facilitated by requirements engineer	Prioritized requirements
9	Inspect requirements	Prioritized requirements, candidate formal inspection technique	Inspection method such as Fagan, peer reviews	Inspection team	Initial selected requirements, documentation of decision-making process and rationale

A slightly simplified process, referred to as Square Light involves 5 of these steps, including Agree on definitions, Identify assets and security goals, Perform risk assessment, Elicit security requirements, and Prioritize requirements. In lab, we will be performing a Square Light assessment on your Software Development lab projects. In order to do this, you will need to perform some role playing. Your "adopted" SDL teams will be split, with half of you playing the role of the developers and half playing the role of the client.

Step 1: Agree on definitions

In order to guarantee effective and clear communication throughout the requirements engineering process, the requirements engineering team and stakeholders must first agree on a common set of terminology and definitions. Given the differences in expertise, knowledge, and experience, an arbitrary term may have multiple meanings between the participants of SQUARE. In addition, there may be ambiguity in the level of detail that is assumed for a given term. For instance, one stakeholder may view "access controls" as a set of policies that governs which users may be granted access to which resources. Another stakeholder may view access controls as the software elements in the system that actually implement this functionality. These differences in perspective must be resolved before the process can continue.

Below are a few set of terms that you might want to come to a common definition of during this session.

access control	corruption	honey pot	non-repudiation	spoof
access control list (ACL)	cracker	impact	patch	SQL injection
antivirus software	denial-of-service (DoS) attack	incident	penetration	stakeholder
artifact	disaster recovery plan	incident handling	penetration testing	stealthing
asset	disclosure	insider threat	physical security	survivability
attack	disgruntled em-ployee	integrity	port scanning	target
audit	downtime	interception	privacy	threat
authentication	disruption	interruption	procedure	threat assessment
availability	encryption	intrusion	recognition	threat model
back door	espionage	intrusion detection system (IDS)	recovery	toolkits
breach	essential services	liability	replay attack	Trojan
brute force	exposure	luring attack	resilience	trust
buffer overflow	fabrication	malware	resistance	uptime
cache cramming	fault line attacks	man-in-the-middle attack	risk	victim
cache poisoning	fault tolerance	masquerade	risk assessment	virus
confidentiality	firewall	modification	security policy	vulnerability
control	hacker	non-essential ser-vices	script kiddies	worm

The development team should start by coming up with a list of terms. The stakeholders then should define these terms for the development team.

Step 2: Identifying Assets and Security Goals

The purpose of Step 2 in SQUARE is for the stakeholders to formally agree on a set of prioritized security goals for the project. Without overall security goals for the project, it is impossible to identify the priority and relevance of any security requirements that are generated. In addition, the establishment of security goals scopes the rest of the SQUARE process.

Initially, different stakeholders will likely have different security goals. For example, a member of human resources may be concerned about maintaining the confidentiality of personnel records, whereas a stakeholder in finance may be concerned with ensuring that financial data is not modified without authorization. The security goals of the stakeholders may also conflict with one another. A security-conscious stakeholder may place high importance on strong security controls for the system, which in turn may hamper overall system performance. Decreased performance might likely be at odds with the goals of the marketing department. Step 2 in the SQUARE process serves to eliminate such conflicts and align all of the stakeholders' interests.

The security goals of the project must be in clear support of the project's overall business goal, which also must be identified and enumerated in this step. On average, stakeholders should attempt to brainstorm to come up with approximately half a dozen security goals for the project, with more or less depending on the scale of the project. More sophisticated techniques for mapping high-level business requirements to low-level requirements can be found in Core Security Requirements Artefacts [Moffett 04] and "Mapping Mission-Level Availability Requirements to System Architectures and Policy Abstractions".

Some of this is related to the work you did last week in defining the assets of your system. However, more likely, this is a more advanced approach.

Step 3: Perform Risk Assessment

The purpose of this step in the SQUARE process is to identify the vulnerabilities and threats that face the system, the likelihood that the threats will materialize as real attacks, and any potential consequences of an attack. Without a risk assessment, organizations can be tempted to implement security requirements or countermeasures without a logical rationale. For instance, the stakeholders may decide that encryption is a necessary component of their system without fully understanding the nature of the problem that encryption can solve. The risk assessment also serves to prioritize the security requirements at a later stage in the process.

After the threats have been identified by the risk assessment method, they must be classified according to likelihoods. Again, this will aid in prioritizing the security requirements that are generated at a later stage. For each threat identified, a corresponding security requirement can identify a quantifiable, verifiable response. For instance, a requirement may describe speed of containment, cost of recovery, or limit to the damage that can be done to the system's functionality.

Elicit Security Requirements

The requirements engineering team must select an elicitation technique that is suitable for the client organization and project. Although this task may appear to be straightforward, it is often the case that multiple techniques will likely work for the same project. The difficulty is in choosing a technique that can adapt to the number and expertise of stakeholders, size and scope of the client project, and expertise of the requirements engineering team. It is extremely unlikely that any single technique will work for all projects under all circumstances, though previous experience has shown that the Accelerated Requirements Method (ARM) has been successful in eliciting security requirements.

The Accelerated Requirements Method (ARM) is a technique that has been designed to elicit, categorize, and prioritize security requirements. Therefore, ARM stretches over Steps 6, 7, and 8 in the SQUARE process.

At the heart of ARM is the step known as "Brainstorm, Organize, and Name (BON)." In this step, the requirements engineering team and stakeholders meet to develop the initial security requirements. To start the session, the team asks the stakeholders the "focus question," which was crafted to tie to the previously established goals, objectives, and scope of the project. An example focus question might be: "An important security requirement of the project is _____"

Based on their professional experience and security knowledge, the participants are asked to write down seven important security requirements on scratch paper within the time limit of seven minutes.

Afterwards, the team asks each participant to write down their top three security requirements on cards within three minutes. The team then collects the cards and put the candidate security requirements on the wall.

The stakeholders then looked through the candidate security requirements generated during the brainstorming session and observed whether any duplicate or inadequate security requirements were produced. They reflect on what they thought were important and defended their own opinions amongst each other. After discussion and debate, redundant or inappropriate requirements are removed.

Prioritize Requirements

In most cases, the client organization will be unable to implement all of the security requirements due to lack of time, resources, or developing changes in the goals of the project. Thus, the purpose of this step in the SQUARE process is to prioritize the security requirements so that the stakeholders can choose which requirements to implement and in what order. The results of Step 4, the risk assessment, and Step 7, categorization, are crucial inputs to this step.

During prioritization, some of the requirements may be deemed to be entirely unfeasible to implement. In such cases, the requirements engineering team has a choice: completely dismiss the requirement from further consideration, or document the requirement as "future work" and remove it from the working set of project requirements. This decision should be made after consulting with the stakeholders.

Lab Activities

During lab, you are going to go through a SQUARE light simulation using your SDL projects as a starting point. A document showing potential examples of the outcomes for each step is available on the course website.

Task	Exit Criteria	Duration
Agree on Definitions	Both teams should agree on and record the same definition	15 minutes
Identify, agree on, and prioritize security goals	Both teams should identify, agree on, and prioritize the security goals Assumption: Both teams have already agreed on a common business goal	15 minutes
Identify Risks, evaluate, and prioritize	Risks should be identified, evaluated, and prioritized. Risks should be evaluated based on severity and probability as well as the cost and likelihood of success of the mitigation.	15 minutes
Agree on Security Requirements	Both teams have to discuss and finalize the requirements Requirements should be quantifiable and verifiable	20 minutes
Prioritize requirements	Prioritization could be an unstructured, informal discussion or a structured one For this workshop, we will restrict the prioritization to an informal discussion.	15 minutes

Deliverables

Report

Each team is to submit a simple report in pdf format. The report should contain

1. The names of all team members, the date, and the assignment
2. A brief, one paragraph summary of the lab and what was learned
3. Results from each lab activity

4. Things gone right and things gone wrong. Provide a brief, one paragraph summary, of the things that went right with this exercise and the things that went wrong with this exercise.
5. Comments on the examples provided.