

Covering Your Assets in Software Engineering

Martin Gilje Jaatun and Inger Anne Tøndel
SINTEF ICT

Presented by Martin Gilje Jaatun

Introduction

- An asset is “something of value that deserves protection”
 - We need computer security because we have assets...
- “Everybody” agrees that it is important to identify all relevant assets before embarking on the development of a secure software solution
- “Nobody” actually tells you how to go about identifying these assets
- To quote Tom Lehrer: “I have a modest example here”

Background

- This work is done in the context of the SODA research project, which aims to provide concrete guidance and tools for developing more secure "average" software
- Ideally, our goal is that our suggestions should be used in *all* software development projects, not just the ones where it is "obvious" that security is important
- Keywords: Lightweight, concrete, step-by-step

How-to

- Brainstorming
- Assets from existing documentation
- Categorization and prioritization
 - Customer/system user
 - Confidentiality (1: important 2: maybe 3: not so important)
 - Integrity
 - Availability.... of the asset
 - System developer/owner
 - CIA ...
 - Attacker
 - CIA ...

Brainstorming

- A web-based tool to assist developers in creating more secure software
- Public resource with open content
- Running on server in SINTEF's domain
- Feedback mechanism for users to report experiences
- Security objectives:
 - Integrity of the application
 - SINTEF's IT regulative and security policy
- What are the assets?

Asset table

ASSETS	STAKEHOLDERS' PRIORITY		
	<i>Focus: protection</i> What is most important to protect from stakeholders' point of view?		<i>Focus: attacks</i> What is most interesting/valuable for an attacker?
Description	Customer/ system user	System developer/ owner	Attacker
<asset 1>	<C-? I-? A-?>	<C-? I-? A-?>	<C-? I-? A-?>
<asset 2>	<C-? I-? A-?>	<C-? I-? A-?>	<C-? I-? A-?>
...

Final priority

- Add all priorities for each asset
- Lowest total gives highest overall ranking

Further information

More information about the SODA project can be found here:

<http://www.sintef.com/soda>

