Secure Software Design in Practice
ARES – SECSE Workshop

Per Håkon Meland and Jostein Jensen
SINTEF Information and Communication Technology
Department of Security, Safety and System Development
{Per.H.Meland, Jostein.Jensen}@sintef.no
Increasing number of vulnerabilities in software

Vulnerability statistics from CERT CC
Increasing number of vulnerabilities in software

"Software is the biggest problem in computer security today" … “the problem is growing”


Vulnerability statistics from CERT CC
Increasing number of vulnerabilities in software

“Software is the biggest problem in computer security today” … “the problem is growing”


“What the heck is going on, and why is the problem getting worse instead of better?”

Increasing number of vulnerabilities in software

“Software is the biggest problem in computer security today.”
“the problem is growing”


The target group is the ordinary "developer-on-the-street"

- not primarily interested in (or knowledgeable about) security
- must focus on designing/implementing as much functionality as possible before the deadline and on budget.
The SODA assumptions

1. A developer will not try to learn or memorize security knowledge prior to starting the development.

2. There should be no significant change in the way developers work.

3. There must be good tool support that enhances security during development, preferably integrated into the current development tools.
SODA during architecture and design
Threat modeling

- Plan and evaluate from an attacker’s point of view and based on your assets.
- Results in a threat model document
- Not solely connected to the design phase
Security design guidelines

- Describes “good security hygiene”-knowledge\(^1\)
  - Span from less formal best practices, principles and rules-of-thumb to different kinds of policies, rules, regulations and standards

- Forcing too much theoretical information about ways to incorporate security is not very efficient \(^2\)

- We have applied the SODA assumptions on:
  - Security design principles
  - Security patterns

---

Security design principles

- Proven rules for improving the security posture of an application
  - E.g. the *principle of least common mechanism* states that mechanisms used to access resources should not be shared.

- **SODAWeb** is a tool that does a rough filtering based on your current project
Security patterns

- A security pattern is a well-understood solution to a recurring security problem
- Many types of patterns
  - Structural, behavioural and creational security patterns, antipatterns, mini-pattern, procedural patterns.
- SODAWeb provides:
  - An structured overview
  - XMI templates for security design patterns
Security design pattern template

```
InterceptingValidator - EA
```

```
File Edit View Project Diagram Element Tools Add-Ins Settings Window Help
```

```
Toolbox
```

```
Class Elements
```

```
- Package
- Class
- Interface
- Enumeration
- Table
- Signal
- Association
```

```
Class Relation...
```

```
- Common
```

```

```
```

```
Start Page
```

```
*Class Model
```

```
Ready
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
```

```
Example: Instantiation in an EPR
Security design review

“An architecture and design review helps you validate the security-related design features of your application before you start the development phase”¹

Have fresh blood look at and question the design artifacts that have been produced so far.

Use SODAWeb to find the most relevant checklists (see the example in Table 3)

Summary and further work

- Have a set of specific and hands-on techniques and tools
- We are pretty compliant with the SODA assumptions
- Need more tuning
  - Student experiments – effort vs effect
- We would like to share security models in a more automated way
  - EU FP7: SHIELDs