Investigating software security practices

Koen Yskout
Laurens Sion

iMinds-DistriNet, KU Leuven

About us

- Laurens.Sion@cs.kuleuven.be
  PhD student (KU Leuven)
- Koen.Yskout@cs.kuleuven.be
  Post-doctoral researcher (KU Leuven)
- Riccardo.Scandariato@cs.kuleuven.be
  Research expert (KU Leuven) | Professor (Chalmers, SE)
- Wouter.Joosen@cs.kuleuven.be
  Professor (KU Leuven)

DistriNet

iMinds KU LEUVEN

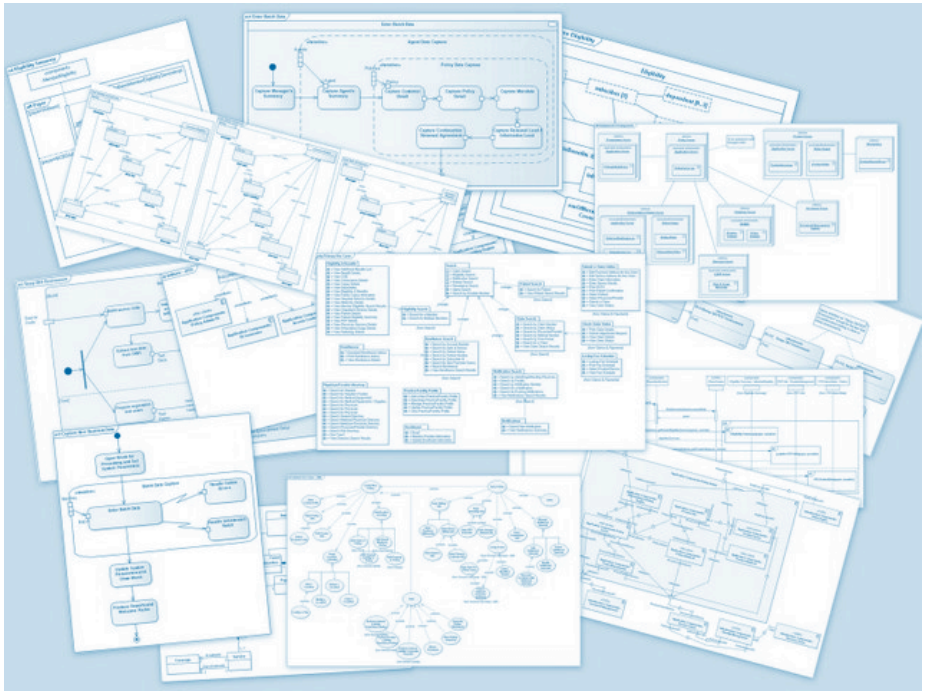
Our research goal

Create

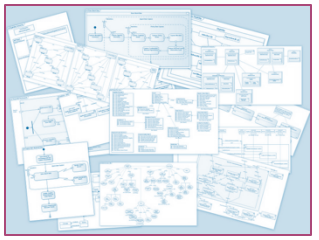
- Representations
- Analysis techniques
- Tools

for managing

- Security and privacy **requirements**
- Security and privacy **design solutions**



Imagine...



Extract model

Analyze

Error: Credit card data can appear in logs as follows:
- Step 1. …

Error: Access to the following interface is unprotected: …

Warning: Client-side session data used but not verified for integrity.

Fix: add encryption, authentication

Note: According to NIST recommendations, your selected key size provides protection until 2030.

Warning: Data encrypted in transit is stored unprotected in: …

Warning: Interceptor needs key to read encrypted requests

Fix

Analyze

Success. The following components are crucial for ensuring the confidentiality of credit card data: …

Generate security documentation

Generate security implementation

We're getting there

- Research approaches exist that offer (parts of) this
  - Secure Tropos / Si*
  - UMLsec
  - SecureUML
  - Secure xADL
  - Secure Object Flows
  - …
- But (as far as we can see) they do not seem to be widely used *in practice*
  - Do *you* use them?

We want to

- Discover *why* existing approaches are *not* used in practice
  - Which features are most interesting?
  - What is missing?
- Develop techniques that can be used in practice
  - Solve actual problems
  - Take real context into account

Step 1: Discover

What?

Collect data on current state of practice

How?

Ask questions to practitioners

Who?

People with *insight* into how their organization handles security and privacy in *requirements and design*

It has been done before

For example, there are studies on

- Quality requirements
- Architectural Description Languages (ADLs)
- Model-Driven Engineering (MDE)
- UML
- Formal methods
- …

in an industrial setting,
based on interviews and questionnaires.

Just one problem

We need access to the right people from industry that want to help us!

You?

What's in it for you?

- Influence on *research* track
  - Make our research matter for your organization
- Influence on *education* track
  - We deliver your next junior employees
  - We can teach them better if we know what they'll do later
- You will be kept informed of the *results*
  - Allows you to compare to the rest of the industry
- We cannot do this without you
  - So we try to limit the effort required from you

Yes, but…

- *“We just do what everybody else does”*
- *“We don’t have explicit security requirements”*
- *“We don’t do anything with security at the design level”*
- …

We want a *representative* overview of the state of practice, so **your input matters!**

Just to be clear

We do *not*

- perform a complete BSIMM/OpenSAMM-style assessment
- rank or compare organizations
- provide advice to your organization
- tell your competitor what you do
  - Nor do we tell you what your competitor does ;-)
- sell you anything

Also, we promise that

- your name
- your organization's name
- the raw response data

remain confidential

Interested?

- Think about who can help us
  - It may be you
  - It may be someone you know
- Practical
  - in-person interview *or* online questionnaire
- Time investment
  - We aim at less than 1 hour
- Interested? Please contact us!

Laurens.Sion@cs.kuleuven.be
Koen.Yskout@cs.kuleuven.be

Questions?

Thank you!