Karlsruhe Institute of Technology

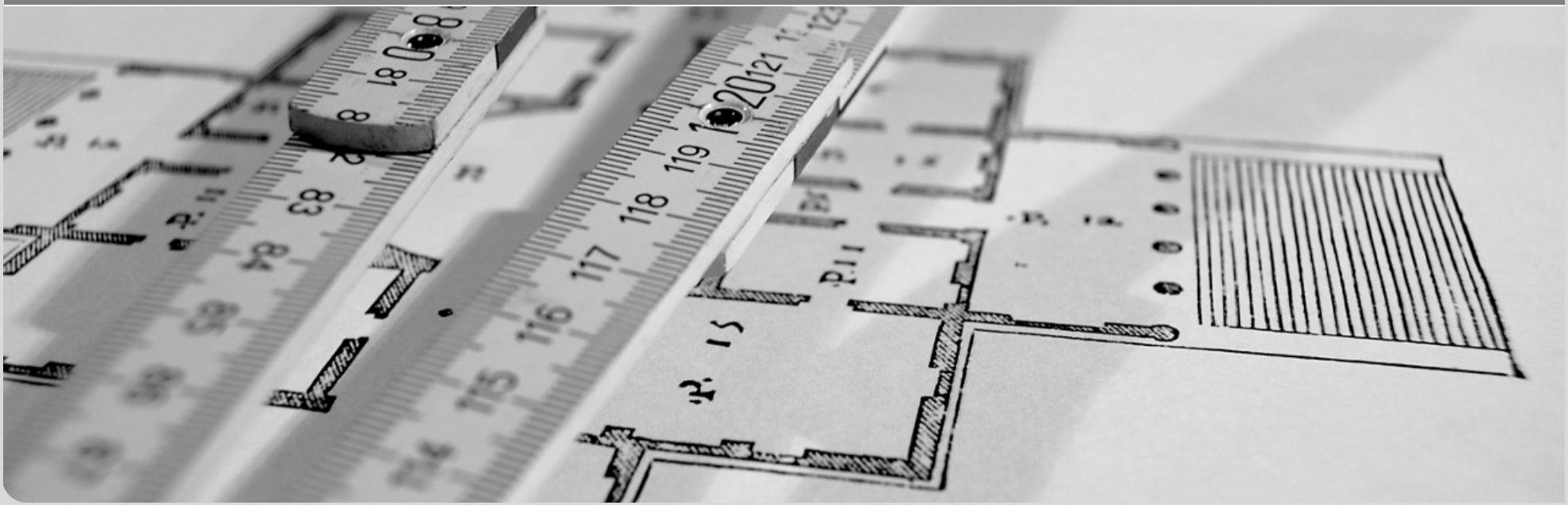
Software Design and Quality

Access Control Verification in Software Systems
Bachelor's thesis

Julian Hinrichs — Advisor: M.Sc. Stephan Seifermann

Reviewer: Prof. Dr. Ralf H. Reussner — Jun.-Prof. Dr.-Ing. Anne Koziolek | September 28, 2018

CHAIR FOR SOFTWARE DESIGN AND QUALITY



Motivation

- Privacy analysis on an architectural level.
- Tool to support a motivated system architect: data-based privacy analysis (DBPA).
- DBPA uses case studies which are difficult to create.
- Existing case studies are usually not usable for DBPA.

Motivation

- Privacy analysis on an architectural level.
- Tool to support a motivated system architect: data-based privacy analysis (DBPA).
- DBPA uses case studies which are difficult to create.
- Existing case studies are usually not usable for DBPA.

Motivation

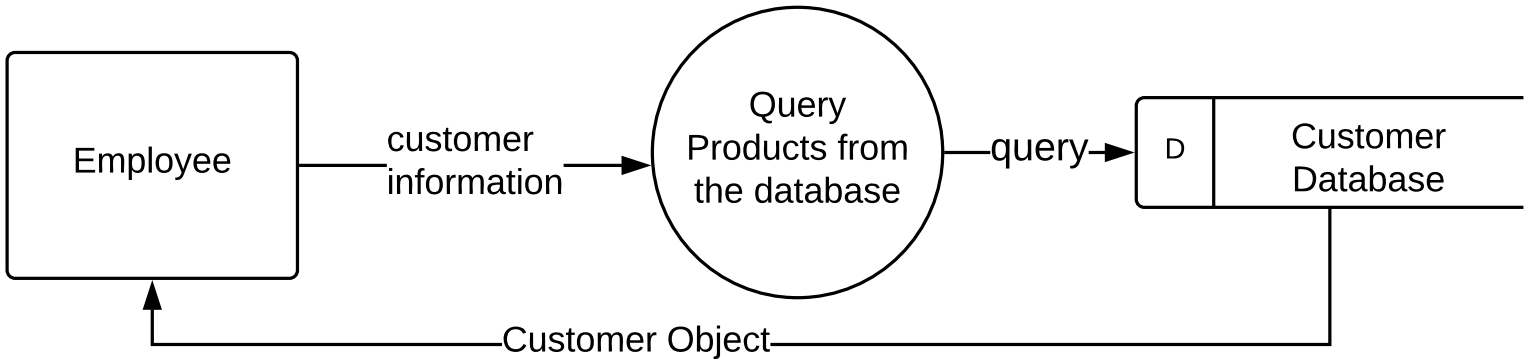
- Privacy analysis on an architectural level.
- Tool to support a motivated system architect: data-based privacy analysis (DBPA).
- DBPA uses case studies which are difficult to create.
- Existing case studies are usually not usable for DBPA.

Motivation

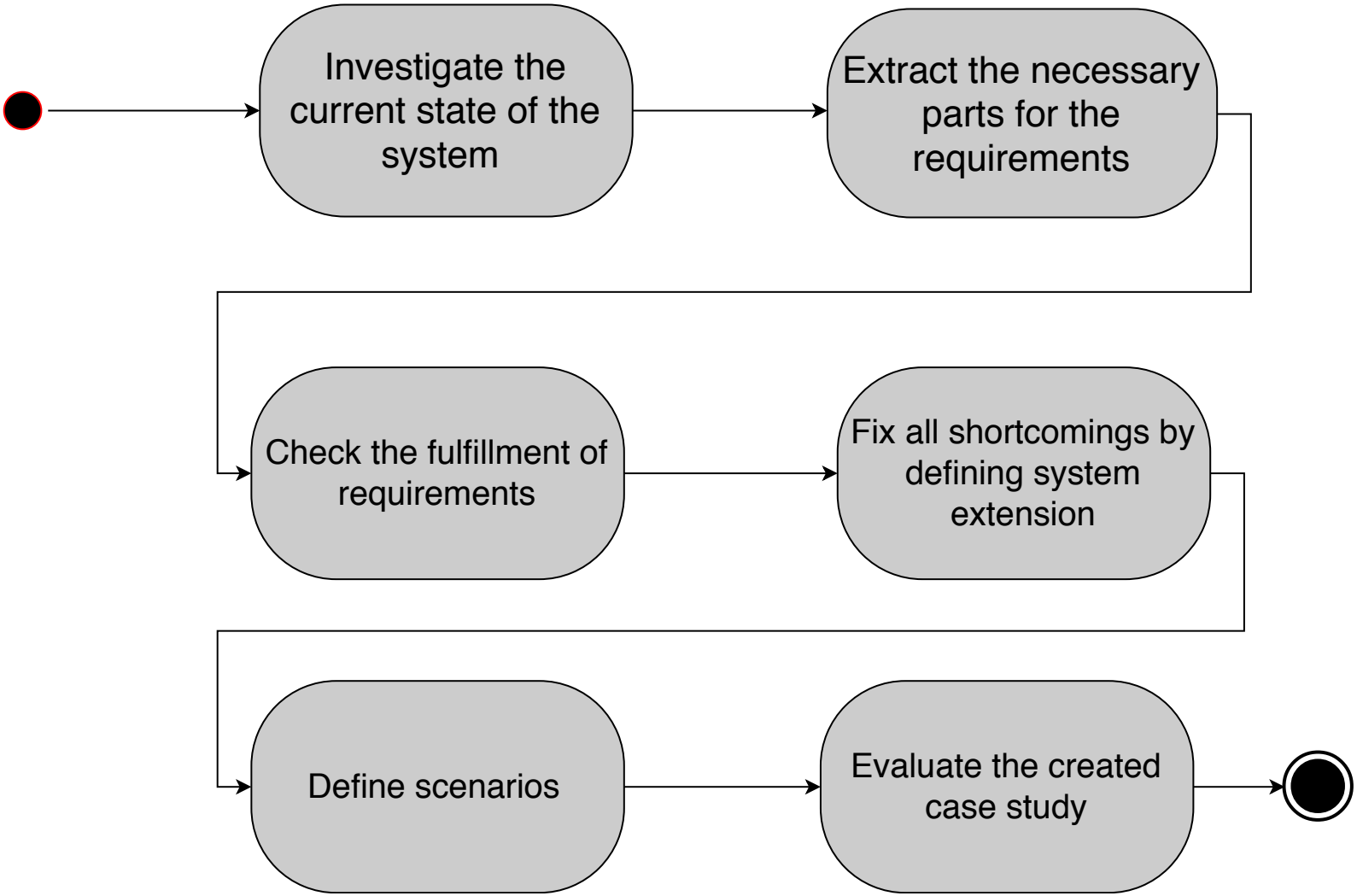
- Privacy analysis on an architectural level.
- Tool to support a motivated system architect: data-based privacy analysis (DBPA).
- DBPA uses case studies which are difficult to create.
- Existing case studies are usually not usable for DBPA.

Foundations

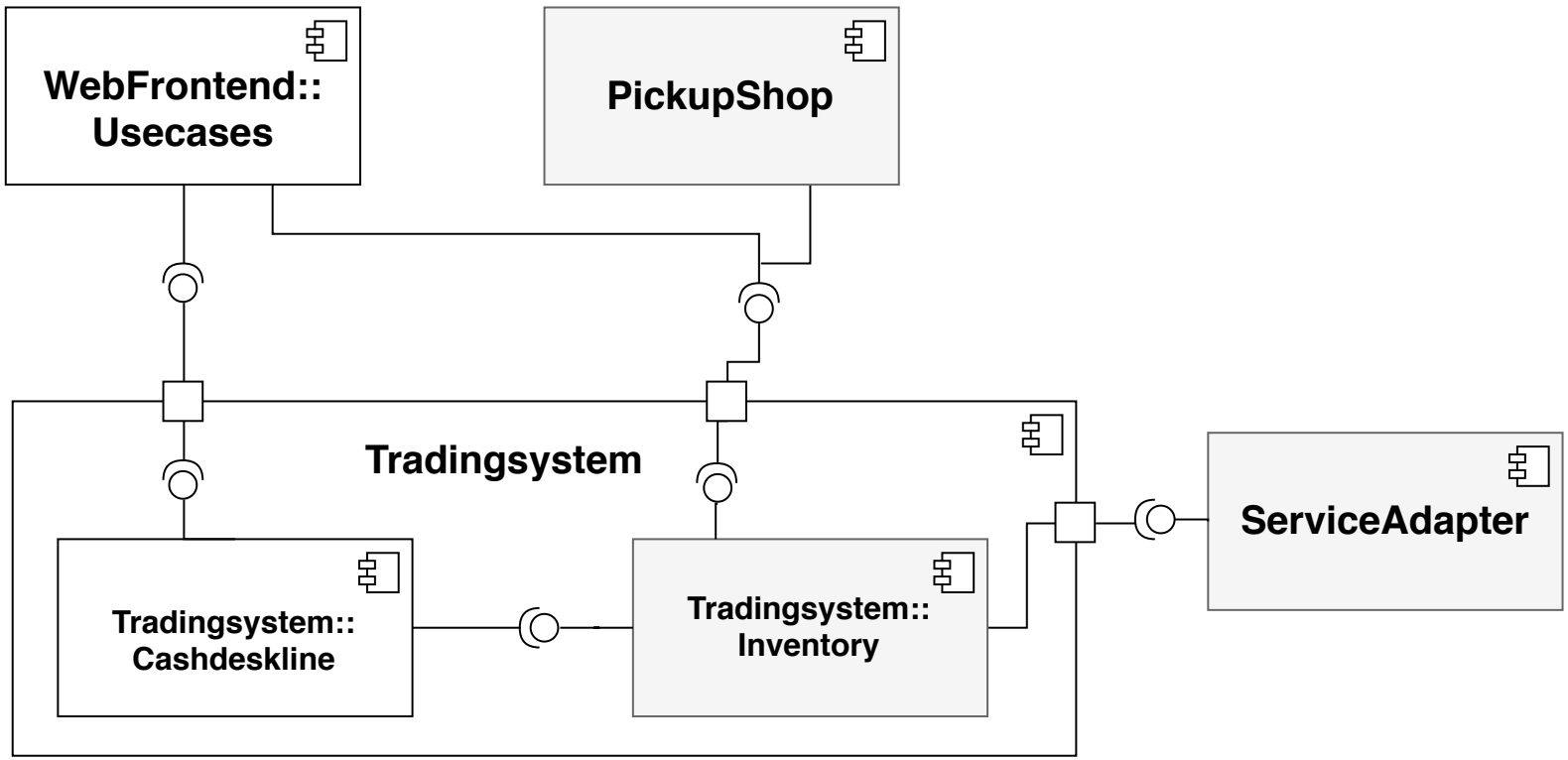
- Security relevant data
  - Data worth protecting within the system.
- Data flows
  - Describe the movement of data and the changes to data in a system.



Procedure Overview



Investigate the current state of the system



(Heinrich, Rostami, and Reussner 2016)

Requirements

Requirements	
R1	component based system (CBS)
R2	Definition of use cases (UC)
R3	Security relevant data (SRD)
R4	Definition of user roles (UR)
R5	Definition of access rights (AR)
R6	Definition of the type of data processing in the components (TODP)

Procedure: requirements, fulfillment of requirements, fix of shortcomings

R2: UC	✓	13 use cases defined	
R3: SRD	✓	Account data	security relevant
		customer data	security relevant
		system data	security relevant
		P& s data	not security relevant
R4: UR	✓	5 roles defined	
R5: AR	✓	Level 1	full access
		Level 2	used data
		Level 3	own data
R6:TODP	✓	Transmission	
		I/O	
		Rel. algebra	
		Alternation	

Access control matrix and types of data processing

- Access control matrix

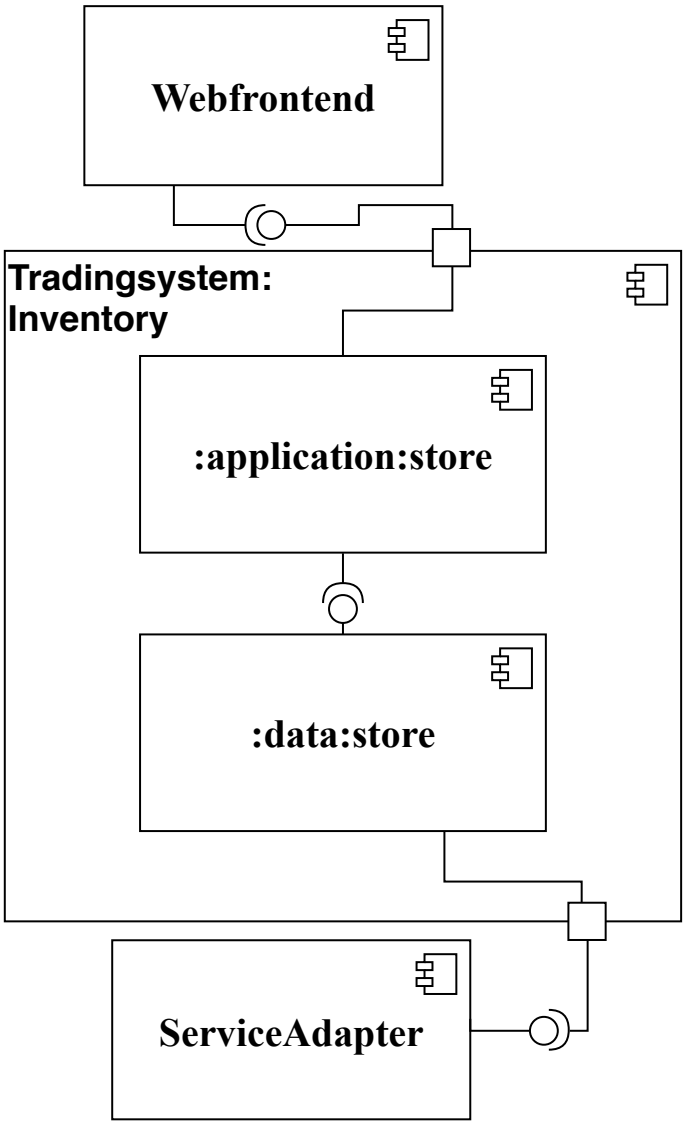
	Webfrontend		TS:Inventory	
StockManager	customer data	4	customer data	4
	account data	3	account data	3
	p&s data	2	p&s data	2
	system data	4	system data	4

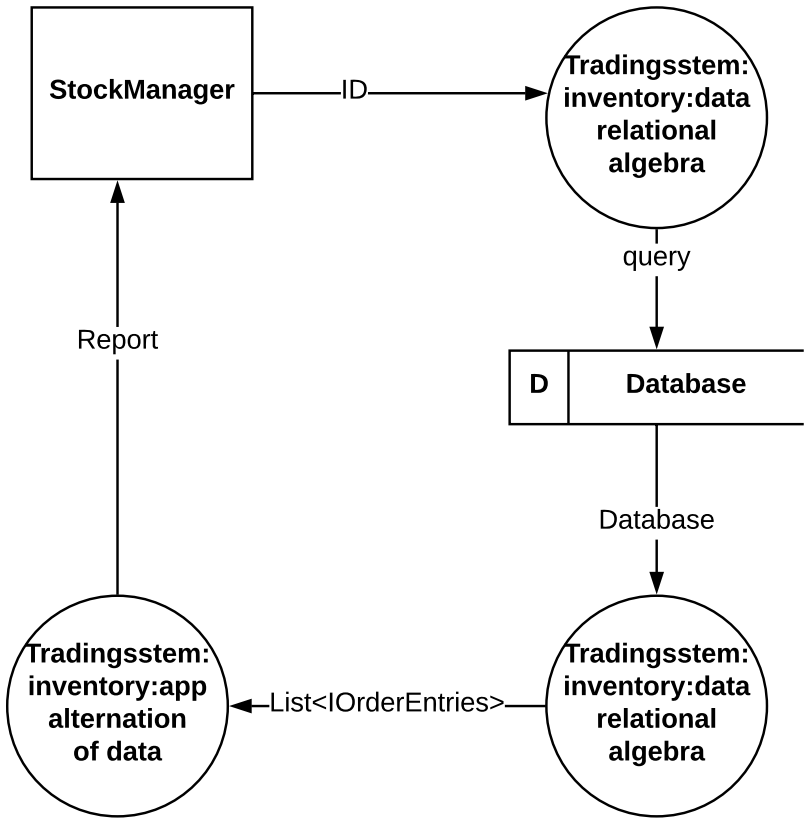
(Evered and Bögeholz 2004)

- Operations matrix

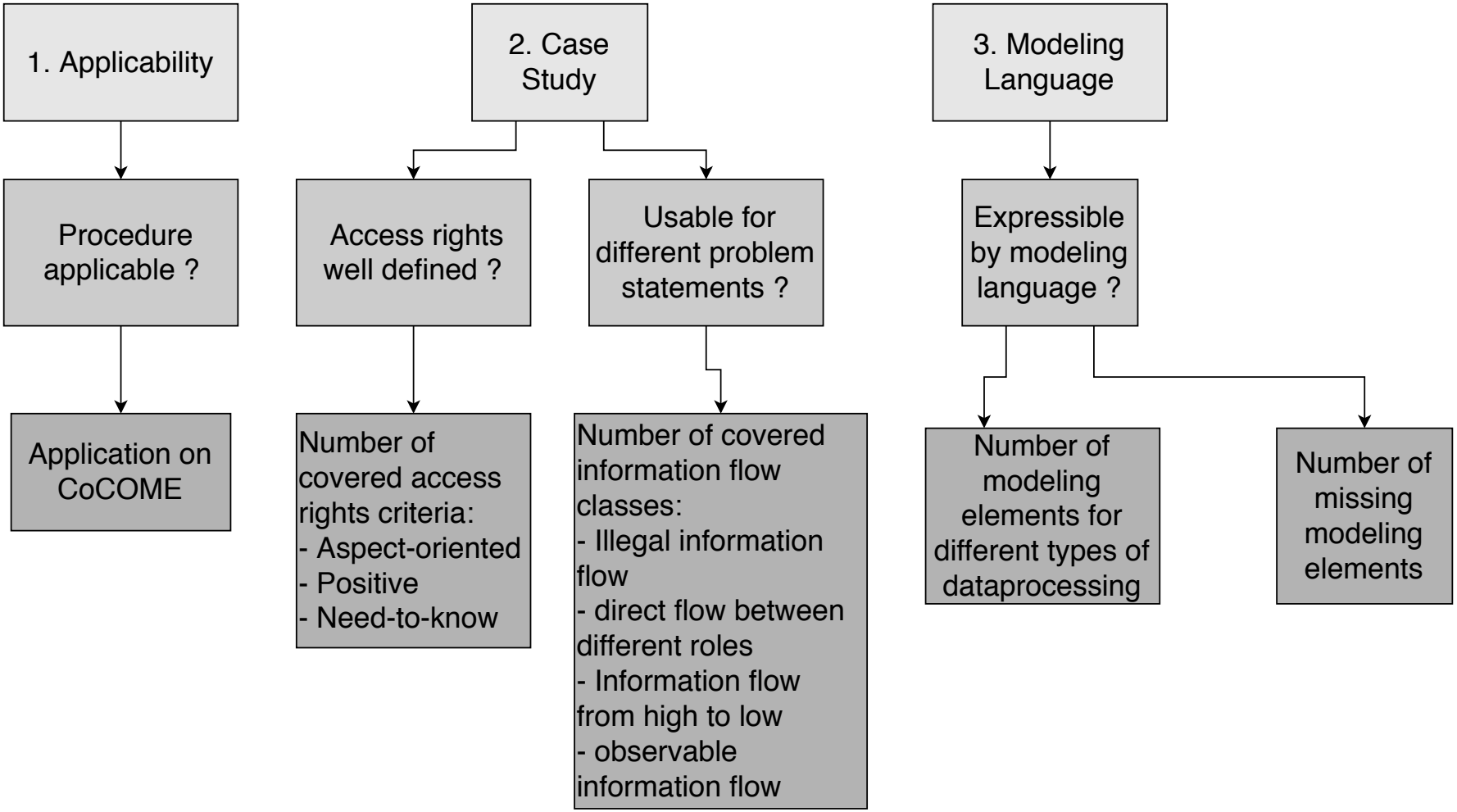
	customer	account	P& S	system
Webfrontend	transmit	transmit	I/O, transmit	n/a

Procedure: Definition of a Scenario





Goal-Question-Metric plan



(Basili and Weiss 1984)

Evaluation of the case study

Access Rights	fulfilled ?
Aspect-oriented	✓
Positive	✓
Need-to-know	✓

(Evered and Bögeholz 2004)

- Used problem statement: Non-influence = non-interference + non-leakage.

Data flow	fulfilled
Illegal information flow	✓
Information flow from high to low	✓
Direct information flow between roles	✗
Observable information flow	✗

(Oheimb 2004)

Evaluation of the case study

Access Rights	fulfilled ?
Aspect-oriented	✓
Positive	✓
Need-to-know	✓

(Evered and Bögeholz 2004)

- Used problem statement: Non-influence = non-interference + non-leakage.

Data flow	fulfilled
Illegal information flow	✓
Information flow from high to low	✓
Direct information flow between roles	✗
Observable information flow	✗

(Oheimb 2004)

Threats to validity

Internal	External	Construct	Conclusion
II, III	I	II	III

- I: Not applied to various systems.
- II: Not all criteria for good access rights are checked. (Evered and Bögeholz 2004)
- III: Not all information classes are modeled.

Threats to validity

Internal	External	Construct	Conclusion
II, III	I	II	III

- I: Not applied to various systems.
- II: Not all criteria for good access rights are checked. (Evered and Bögeholz 2004)
- III: Not all information classes are modeled.

Related Work

- Case studies are commonly used in other fields than computer science, like health care, sociology, law, etc. (Zucker 2009)
- **Similarities**
  - Investigating a concrete characteristics for a scope.
  - Requirements for the procedure (use more than one source, etc). (Zucker 2009)
- **Differences**
  - Usually the solutions to a problem are investigated, we examine the data processing in a concrete system (Jürjens 2008)
- A related publication: A Case Study in Access Control Requirements for a Health Information System (Evered and Bögeholz 2004)
  - Definition criteria to measure good access rights.
  - Created a case study for a much smaller scope, where basic steps for a procedure where shown.
  - Comparison on a high level.

Future work

- Method
  - Apply the method to other systems (e.g Travelsystem (Katkalov et al. 2013)) and create further case studies.
- Case study
  - **short term work**
    - Evaluate the criteria *concise* and *clear*.
    - Define additional scenarios to cover all information flow classes.
  - **long term work**
    - Evaluate the criteria *fundamental* and *efficient*.
    - Definition of further information flow classes other than non-influence out.
    - Using the case study for a data based privacy analysis.

PIBA

- Problem
  - Usable case studies for DBPA are difficult to create.
- Idea
  - Introduce a method for creating usable case studies for DBPA approaches.
- Benefit
  - Ensure compliance for privacy on an architectural level by evaluating system with DBPA.
- Actions
  - Create a method for the creation of case studies.
  - Apply the method to a system.
  - Evaluate the created case study.

References I

Victor R. Basili and David M. Weiss. “A Methodology for Collecting Valid Software Engineering Data”. In: *IEEE Trans. Software Eng.* 10.6 (1984), pp. 728–738. DOI: 10.1109/TSE.1984.5010301. URL: https://doi.org/10.1109/TSE.1984.5010301.

Mark Evered and Serge Bögeholz. “A Case Study in Access Control Requirements for a Health Information System”. In: *ACSW Frontiers 2004, 2004 ACSW Workshops - the Australasian Information Security Workshop (AISW2004), the Australasian Workshop on Data Mining and Web Intelligence (DMWI2004), and the Australasian Workshop on Software Internationalisation (AWSI2004) . Dunedin, New Zealand, January 2004*. 2004, pp. 53–61. URL: http://crpit.com/confpapers/CRPITV32Evered.pdf.

References II


Robert Heinrich, Kiana Rostami, and Ralf Reussner. “The CoCoME Platform for Collaborative Empirical Research on Information System Evolution”. In: (2016).


Jan Jürjens. “Model-based Security Testing Using UMLsec: A Case Study”. In: *Electr. Notes Theor. Comput. Sci.* 220.1 (2008), pp. 93–104. DOI: 10.1016/j.entcs.2008.11.008. URL: https://doi.org/10.1016/j.entcs.2008.11.008.


Kuzman Katkalov et al. “Model-Driven Development of Information Flow-Secure Systems with IFlow”. In: *International Conference on Social Computing, SocialCom 2013, SocialCom/PASSAT/BigData/EconCom/BioMedCom 2013, Washington, DC, USA, 8-14 September, 2013*. 2013, pp. 51–56. DOI: 10.1109/SocialCom.2013.14. URL: https://doi.org/10.1109/SocialCom.2013.14.

References III

David von Oheimb. “Information Flow Control Revisited: Noninfluence = Noninterference + Nonleakage”. In: *Computer Security - ESORICS 2004, 9th European Symposium on Research Computer Security, Sophia Antipolis, France, September 13-15, 2004, Proceedings*. 2004, pp. 225–243. DOI: 10.1007/978-3-540-30108-0_14. URL: https://doi.org/10.1007/978-3-540-30108-0%5C_14.

Donna M. Zucker. “How to Do Case Study Research”. In: *Teaching Research Methods in the Social Sciences* (2009).

Evaluation Modeling language

Meta model	possible ?
relational algebra	yes
I/O operations	yes
Transmission of data	yes
Change of access rights	yes
Alternation of data	yes
ACM in system model	no

Operations matrix complete

Types of data processing	customer	account	p& s	system
Webfrontend	transmit	transmit	I/O transmit	n/a
PickupShop	transmit	transmit	I/O, transmit	n/a
Tradingsystem: inventory:app	change transmit	change transmit	change	n/a
Tradingsystem: inventory:data	rel. algebra operations	rel. algebra operations	rel. algebra operations	change
Tradingssystem: cashdeskline	change transmit	non-existent	change transmit	n/a