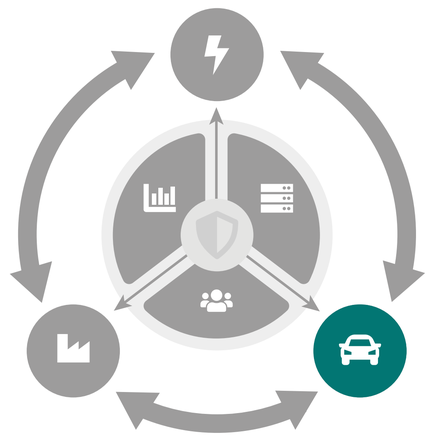
Karlsruhe Institute of Technology

P1T3

Information Flow Control by-Construction for Component-based Systems

R. C. Rønneberg, C. Gerking, I. Schaefer
(Dependability, Mobility Systems Security, Software Engineering)



Motivation and Research Questions

- Modern mobility systems increasingly handle sensitive information about road users
- Software needs to ensure that the sensitive information is not leaked
- Privacy concerns are often addressed late in the software development cycle

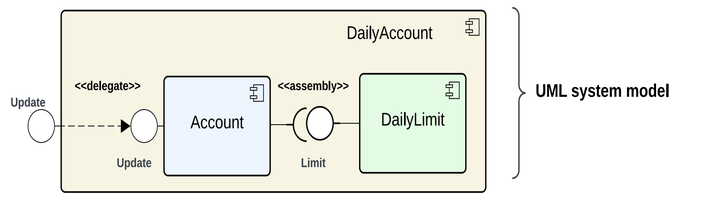
➡ How to define an incremental approach to building secure component-based systems?

Impact

- A **novel** approach combining **component-based** SE with **information flow control** and **CbC**
- Strong **privacy guarantees** for users and a **practical development process** for **developers**
- **Open-source implementation** of the tool support

Research Activities and Results

- Development process from high-level system design to implementation
- Information flow specification in a component description language
- Secure composition via formal conditions



Declare sub-components / Information Flow specification / Component compositions

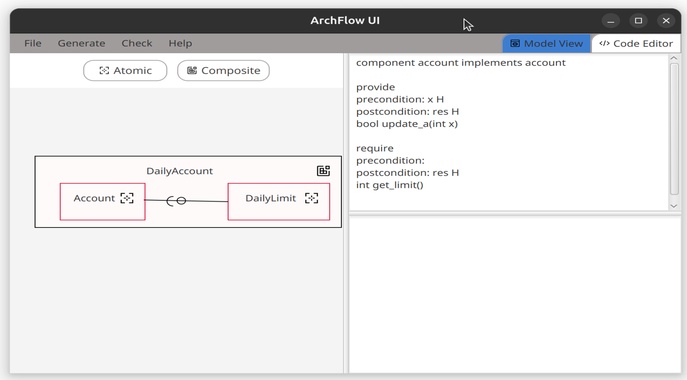
```
component DailyAccountImpl implements
DailyAccount {

 //Sub-components
 component Account
 component DailyLimit

 //Provided method
 update
 pre: public x
 post: public x, private res
 in: x: int
 out: res: bool

 //Compositions
 delegate update -> Account.update
 assembly Account.getLimit ->
DailyLimit.getLimit
}
```

```
component AccountImpl implements
Account {

 //Required method
 getLimit
 pre:
 post: secret res
 in: void
 out: res: int

 //Provided method
 update
 pre: public x
 post: public x, secret res
 in: x: int
 out: res: bool

}
```

```
component DailyLimitImpl implements
DailyLimit {

 //Provided method
 getLimit
 pre:
 post: public res
 in: void
 out: res: int
}
```

Component description

- Open-source tool support available on GitHub

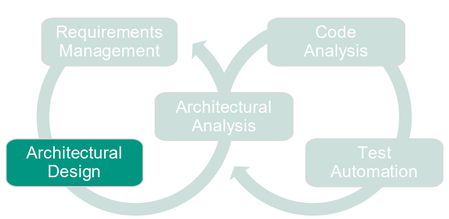


- Next steps:
  - Concurrent communication with active objects
  - Quantitative information flow specifications

Publications

- Exact and Efficient Bayesian Inference for Privacy Risk Quantification. In: SEFM 2023.
- Quantitative Information Flow Control by Construction for Component-based Systems. In: ECSA 2023.
- Information Flow Control by Construction in Asynchronous Systems. Master thesis 2024.
- Scaling IFbC to Component-based Software Architectures. In: FORTE 2025.

links to:



KASTEL