Karlsruhe Institute of Technology

Software Design and Quality

ECSA’21 Tutorial: Identifying Confidentiality Violations in Architectural Design Using Palladio

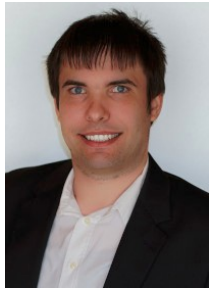
Stephan Seifermann, Maximilian Walter, Sebastian Hahner, Robert Heinrich, Ralf Reussner

Please download the preparation material for the tutorial in advance if you have not done yet.

bit.ly/2U1ZffR

Who are we?

Stephan Seifermann



Maximilian Walter

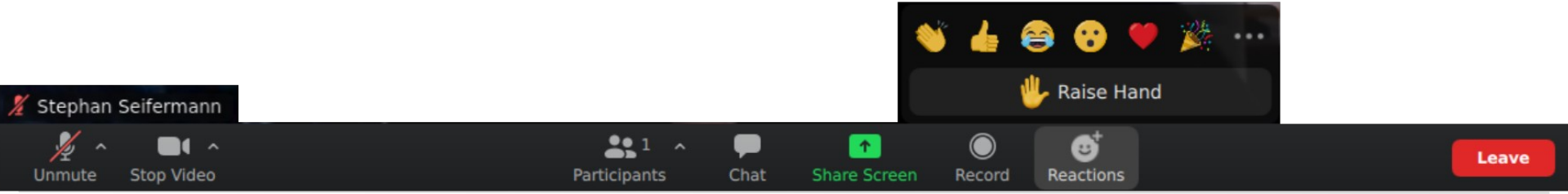
Sebastian Hahner

Robert Heinrich

Ralf Reussner

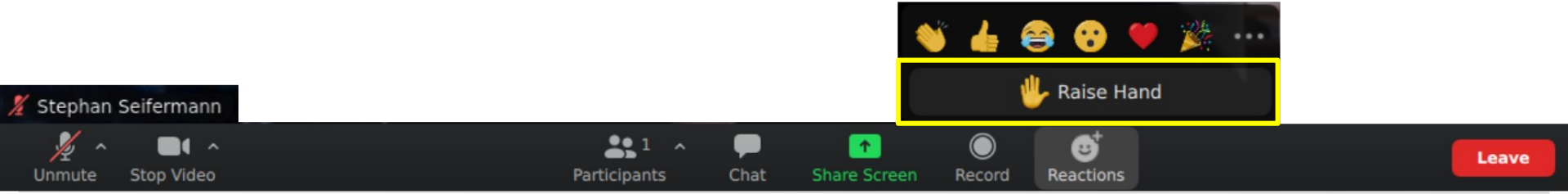
How to Participate at the Tutorial

- Ask questions or make comments whenever they come to your mind
  - Raise your hand
  - Write into the chat
- Mute your microphone to avoid noise
- Video feeds are appreciated
- Try to solve modeling/analysis tasks



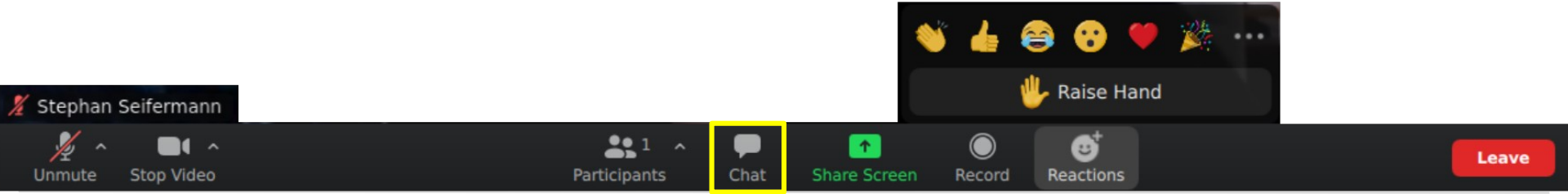
How to Participate at the Tutorial

- Ask questions or make comments whenever they come to your mind
  - Raise your hand
  - Write into the chat
- Mute your microphone to avoid noise
- Video feeds are appreciated
- Try to solve modeling/analysis tasks



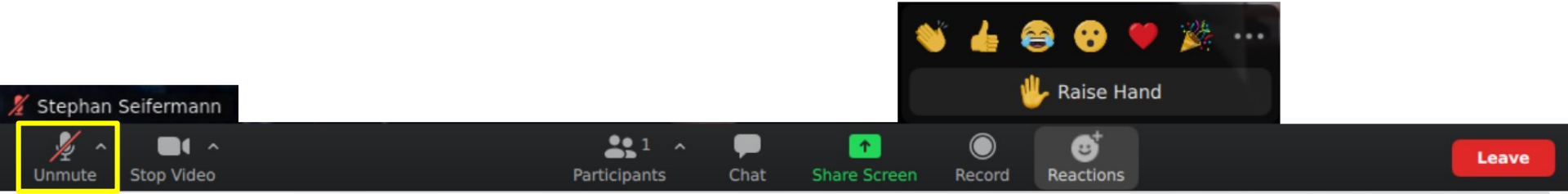
How to Participate at the Tutorial

- Ask questions or make comments whenever they come to your mind
  - Raise your hand
  - Write into the chat
- Mute your microphone to avoid noise
- Video feeds are appreciated
- Try to solve modeling/analysis tasks



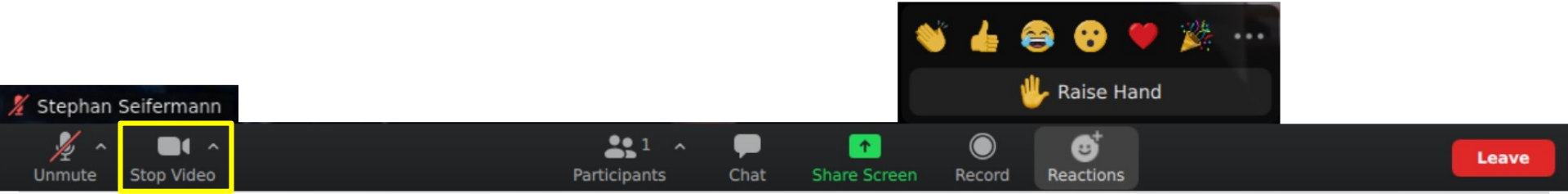
How to Participate at the Tutorial

- Ask questions or make comments whenever they come to your mind
  - Raise your hand
  - Write into the chat
- Mute your microphone to avoid noise
- Video feeds are appreciated
- Try to solve modeling/analysis tasks



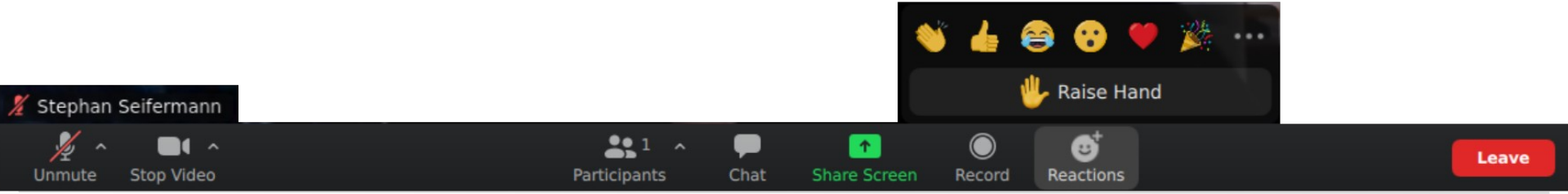
How to Participate at the Tutorial

- Ask questions or make comments whenever they come to your mind
  - Raise your hand
  - Write into the chat
- Mute your microphone to avoid noise
- Video feeds are appreciated
- Try to solve modeling/analysis tasks



How to Participate at the Tutorial

- Ask questions or make comments whenever they come to your mind
  - Raise your hand
  - Write into the chat
- Mute your microphone to avoid noise
- Video feeds are appreciated
- Try to solve modeling/analysis tasks



Background, Expectations, Experience

bit.ly/3iEvMSD

5 min

Tutorial Agenda

- 17:00 – 17:15: Welcoming
- 17:15 – 18:00: Modeling Access Control Using Palladio
- 18:00 – 18:20: Working Session on Modeling Task
- 18:20 – 18:30: Break
- 18:30 – 18:40: Discussion of Modeling Task
- 18:40 – 19:00: Analyzing Access Control Using Palladio
- 19:00 – 19:10: Working Session on Analysis Task
- 19:10 – 19:30: Summary / Future Work / Feedback

Motivation of Security in General

Tech

Yahoo just said every single account was affected by 2013 attack — 3 billion in all

Published Tue, Oct 3 2017 •4:35 PM EDT | Updated Wed, Oct 4 2017 •7:50 AM EDT

Todd Haselton
@robotodd

Share

[1]

Tech • LinkedIn

Massive data leak exposes 700 million LinkedIn users' information

By **Chris Morris**
June 30, 2021 5:49 PM GMT+2

[2]

[1] https://www.cnbc.com/2017/10/03/yahoo-every-single-account-3-billion-people-affected-in-2013-attack.html
[2] https://fortune.com/2021/06/30/linkedin-data-theft-700-million-users-personal-information-cybersecurity/

Motivation of Security in General

Tech

Yahoo just said every single account was affected by 2013 attack — 3 billion in all

Published Tue, Oct 3 2017 •4:35 PM EDT | Updated Wed, Oct 4 2017 •7:50 AM EDT

Todd Haselton
@robotodd

Share

[1]

Tech • LinkedIn

Massive data leak exposes 700 million LinkedIn users' information

By **Chris Morris**
June 30, 2021 5:49 PM GMT+2

[2]

Editors' Pick | May 14, 2021, 06:10am EDT | 5,351 views

Alibaba Posts Operating Loss Of $1.2 Billion Following Antitrust Regulator's Record Fine

Zinnia Lee Forbes Staff
Asia

[3]

[1] https://www.cnbc.com/2017/10/03/yahoo-every-single-account-3-billion-people-affected-in-2013-attack.html
[2] https://fortune.com/2021/06/30/linkedin-data-theft-700-million-users-personal-information-cybersecurity/
[3] https://www.forbes.com/sites/zinnialee/2021/05/14/alibaba-posts-operating-loss-of-12-billion-following-antitrust-regulators-record-fine/

Motivation of Security in General

Tech

Yahoo just said every single account was affected by 2013 attack — 3 billion in all

Published Tue, Oct 3 2017 •4:35 PM EDT | Updated Wed, Oct 4 2017 •7:50 AM EDT

Todd Haselton
@robotodd

Share

[1]

Editors' Pick | May 14, 2021, 06:10am EDT | 5,351 views

Alibaba Posts Operating Loss Of $1.2 Billion Following Antitrust Regulator's Record Fine

Zinnia Lee Forbes Staff
Asia

[3]

Tech • LinkedIn

Massive data leak exposes 700 million LinkedIn users' information

By Chris Morris
June 30, 2021 5:49 PM GMT+2

[2]

Salted Hash- Top security news

By Steve Ragan, Senior Staff Writer, CSO | Jun 18, 2014 1:03 pm PDT

About
Fundamental security insight to help you minimize risk and protect your organization

News

Code Spaces forced to close its doors after security incident

[4]

[1] https://www.cnbc.com/2017/10/03/yahoo-every-single-account-3-billion-people-affected-in-2013-attack.html
[2] https://fortune.com/2021/06/30/linkedin-data-theft-700-million-users-personal-information-cybersecurity/
[3] https://www.forbes.com/sites/zinnialee/2021/05/14/alibaba-posts-operating-loss-of-12-billion-following-antitrust-regulators-record-fine/
[4] https://www.csoonline.com/article/2365062

Motivation of Confidentiality in Architectures

- Security often not considered during software design
  [Assal2018]
- Design issues cause more and more vulnerabilities
  [Kuhn2017] [McGraw2006]
- Fixing design issues late is costly
  [Shull2002]

Motivation of Confidentiality in Architectures

- Security often not considered during software design
  [Assal2018]
- Design issues cause more and more vulnerabilities
  [Kuhn2017] [McGraw2006]
- Fixing design issues late is costly
  [Shull2002]

- Unavailability and lacking integration of tools (amongst others)
  [Davis2013] [Assal2019] [Garavel2020]
- Approaches often only cover one analysis type
  [vanDenBerghe2017]

How do we address these issues?

- Problem: limited analysis support
  - Analysis framework with simple semantics [Seifermann2019]
  - Examples for information flow and access control analyses [Seifermann2021]

[Seifermann2019] Data-driven software architecture for analyzing confidentiality. ICSA'19, p. 1–10.

[Seifermann2021] A unified model to detect information flow and access control violations in software architectures. SECRYPT'21, p. 26–37.

How do we address these issues?

- Problem: limited analysis support
  - Analysis framework with simple semantics [Seifermann2019]
  - Examples for information flow and access control analyses [Seifermann2021]
- Problem: lacking integration
  - Integration approach for ADLs [Seifermann2021]
  - DSL for analysis definition [Hahner2021]

[Seifermann2019] Data-driven software architecture for analyzing confidentiality. ICSA'19, p. 1–10.
[Seifermann2021] A unified model to detect information flow and access control violations in software architectures. SECRYPT'21, p. 26–37.
[Hahner2021] Modeling data flow constraints for design-time confidentiality analyses. ICSA-C'21, p. 15–21.

Learning Objectives

- Understanding of how labels can be used to model confidentiality
  - General idea of analyses based on label propagation
  - Application example: Role-based Access Control (RBAC) analysis
- Being able to use the Palladio-based tooling in confidentiality analyses
  - Modeling aspects relevant for confidentiality
  - Formulating and executing confidentiality analyses

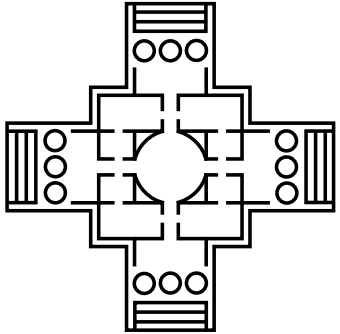
Karlsruhe Institute of Technology

Software Design and Quality

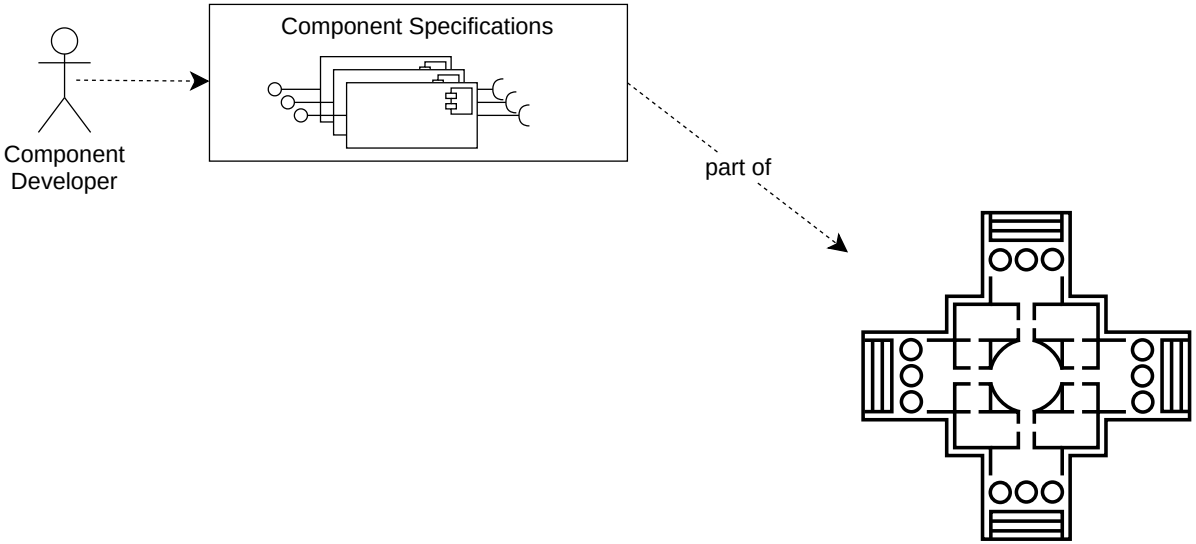
Modeling Access Control Using Palladio

Stephan Seifermann, Maximilian Walter, Sebastian Hahner, Robert Heinrich, Ralf Reussner

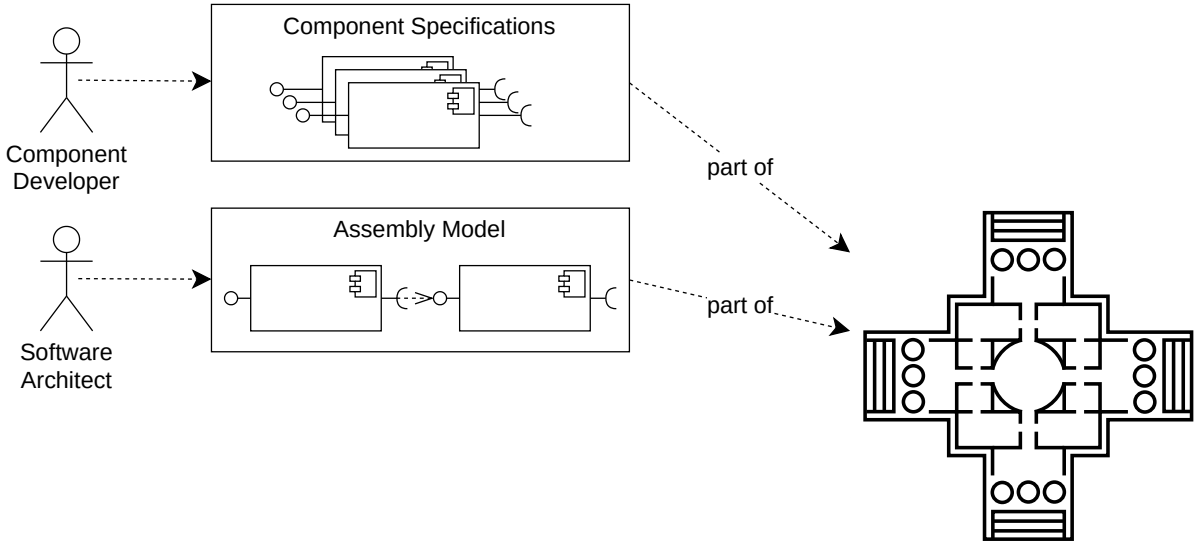
Models and Analyses in Palladio



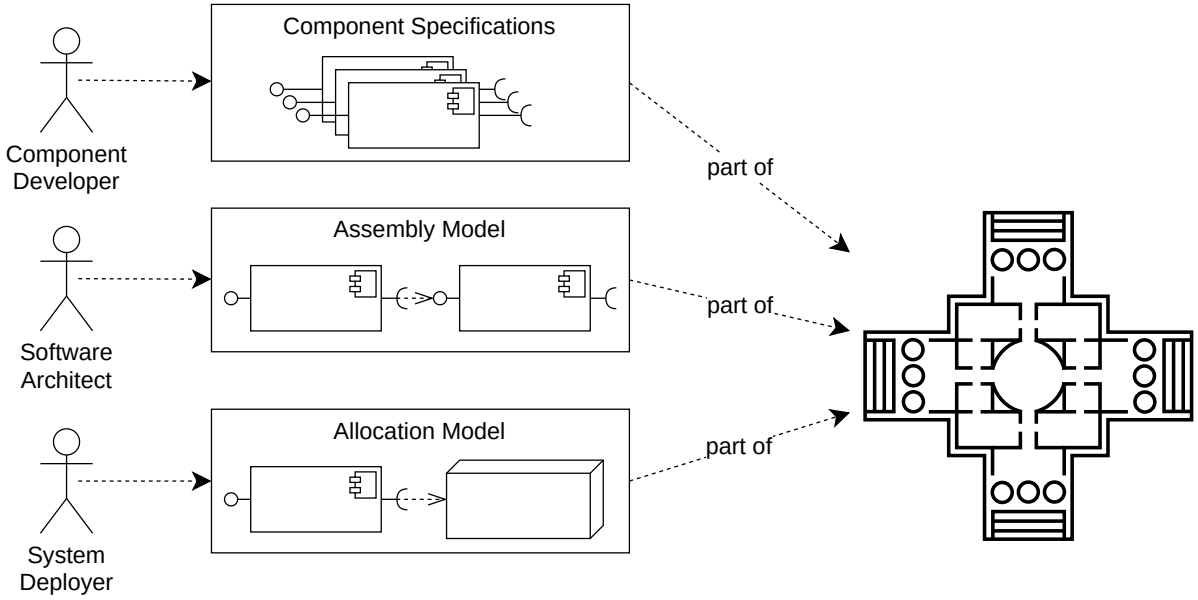
Models and Analyses in Palladio



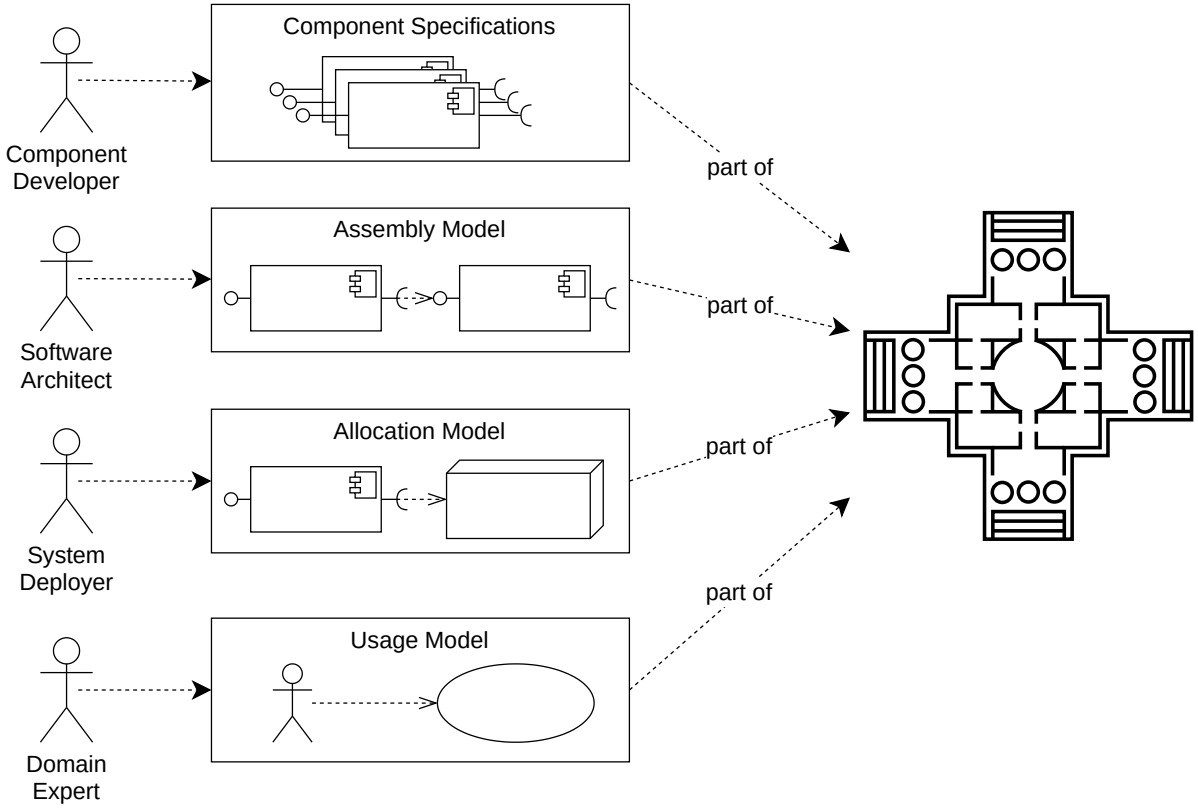
Models and Analyses in Palladio



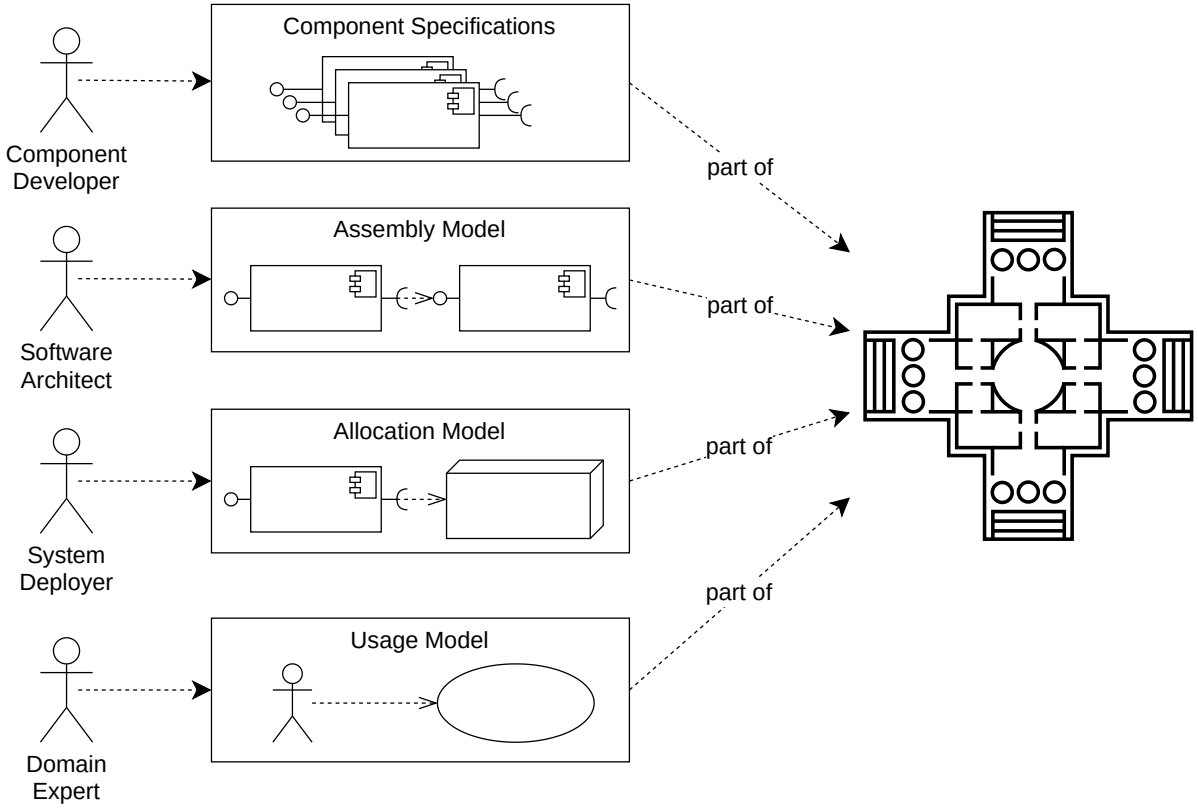
Models and Analyses in Palladio



Models and Analyses in Palladio



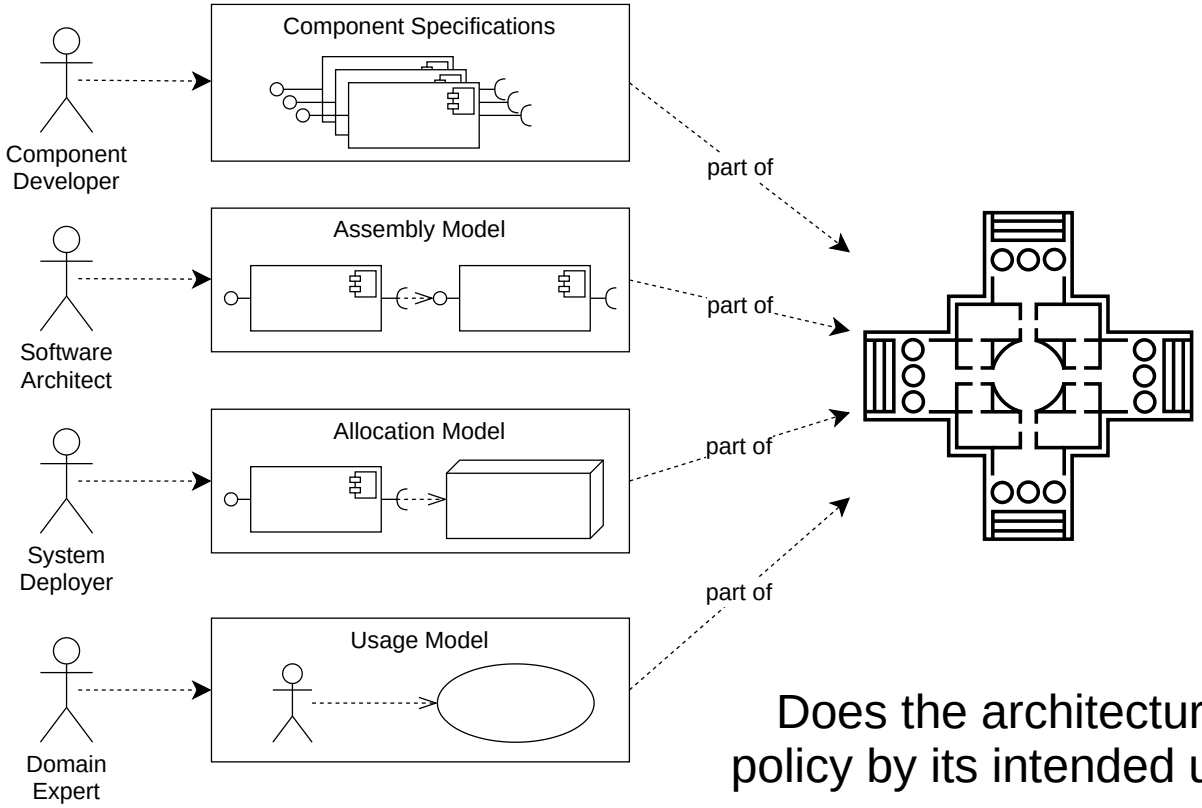
Models and Analyses in Palladio



Quality Predictions

- Performance
- Reliability
- Maintainability
- ...
- **Confidentiality**

Models and Analyses in Palladio



Quality Predictions

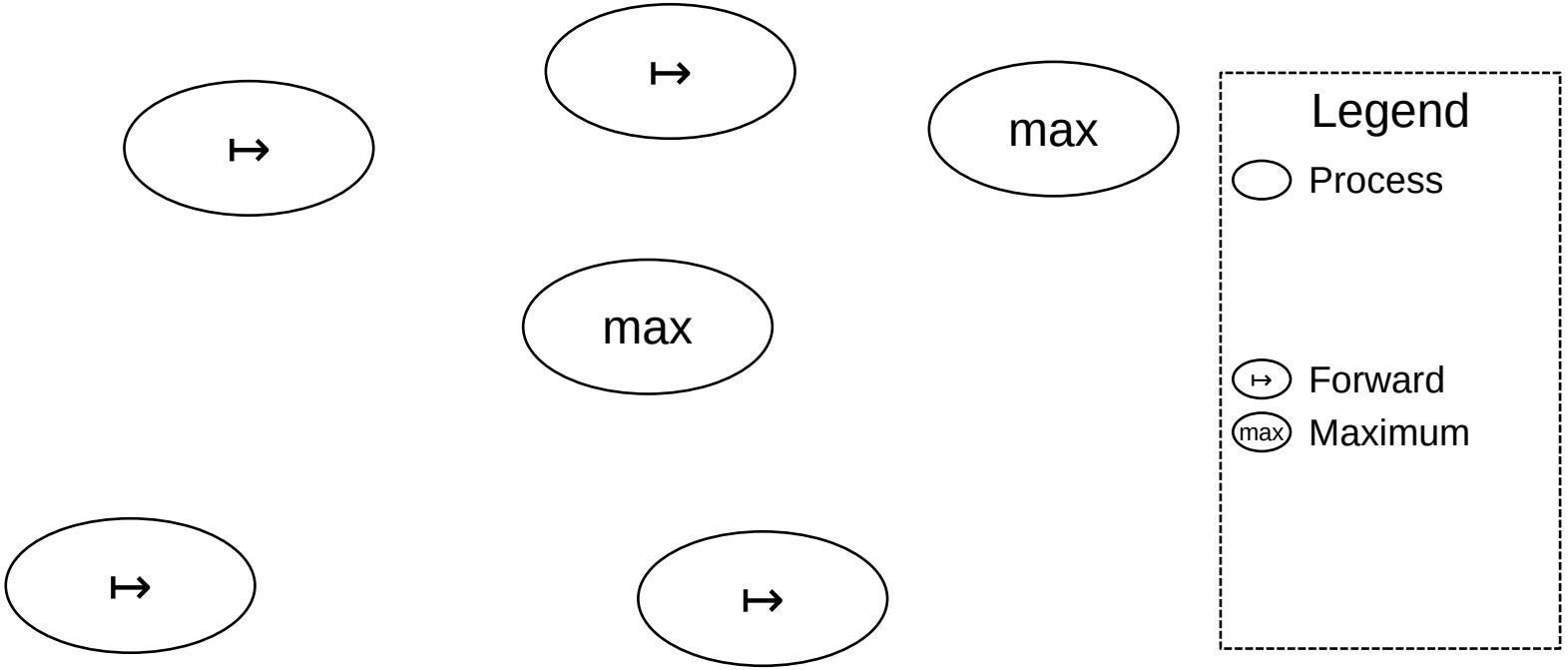
- Performance
- Reliability
- Maintainability
- ...
- **Confidentiality**

Does the architecture violate the confidentiality policy by its intended usage, structure or behavior?

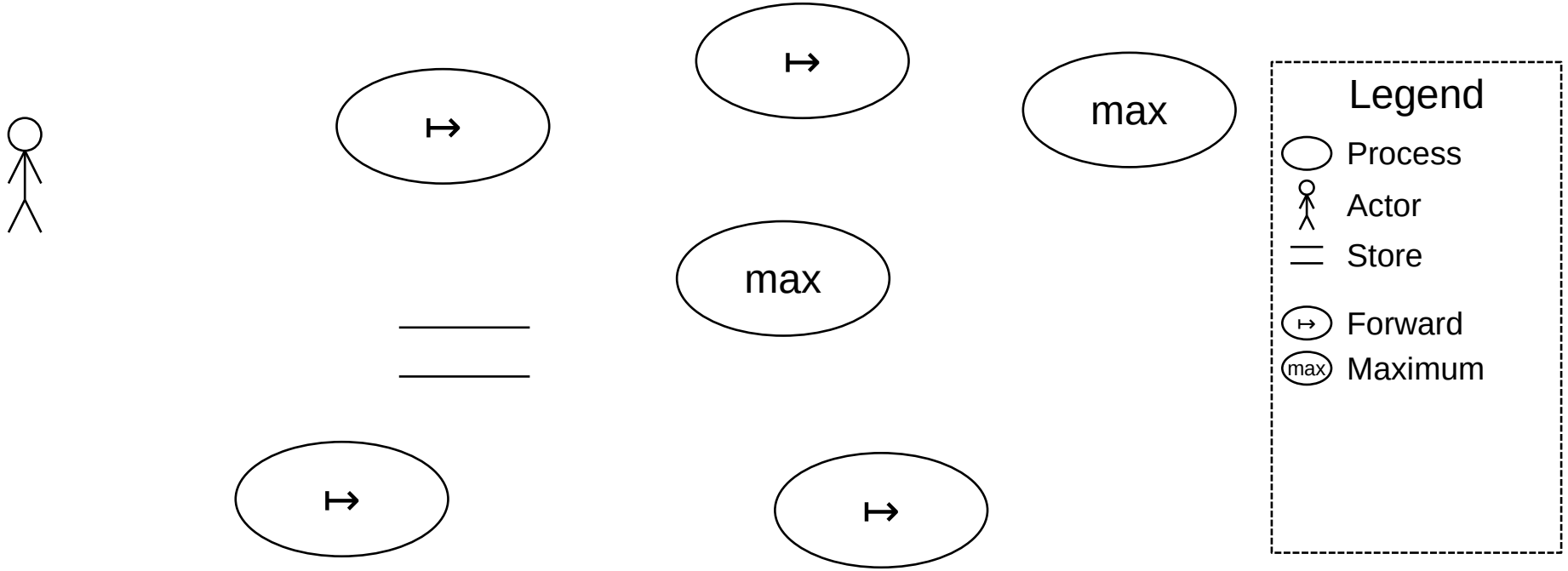
General Idea of Label-based Analyses

Legend

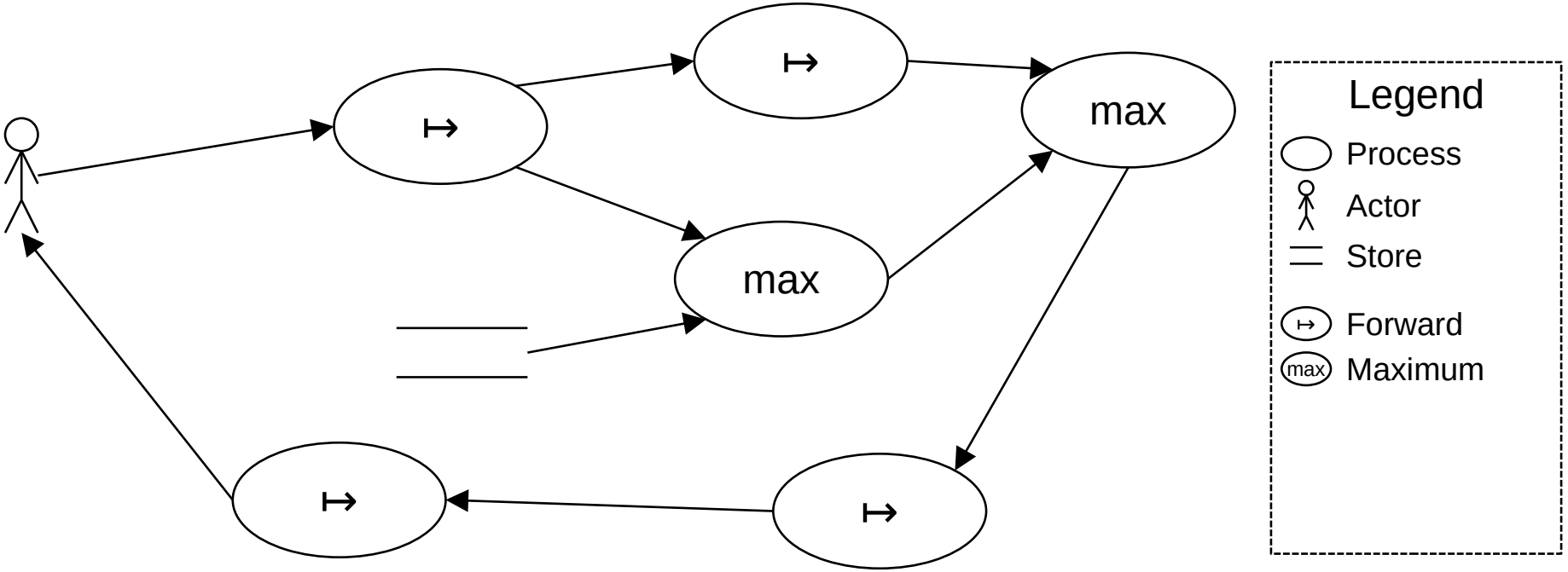
General Idea of Label-based Analyses



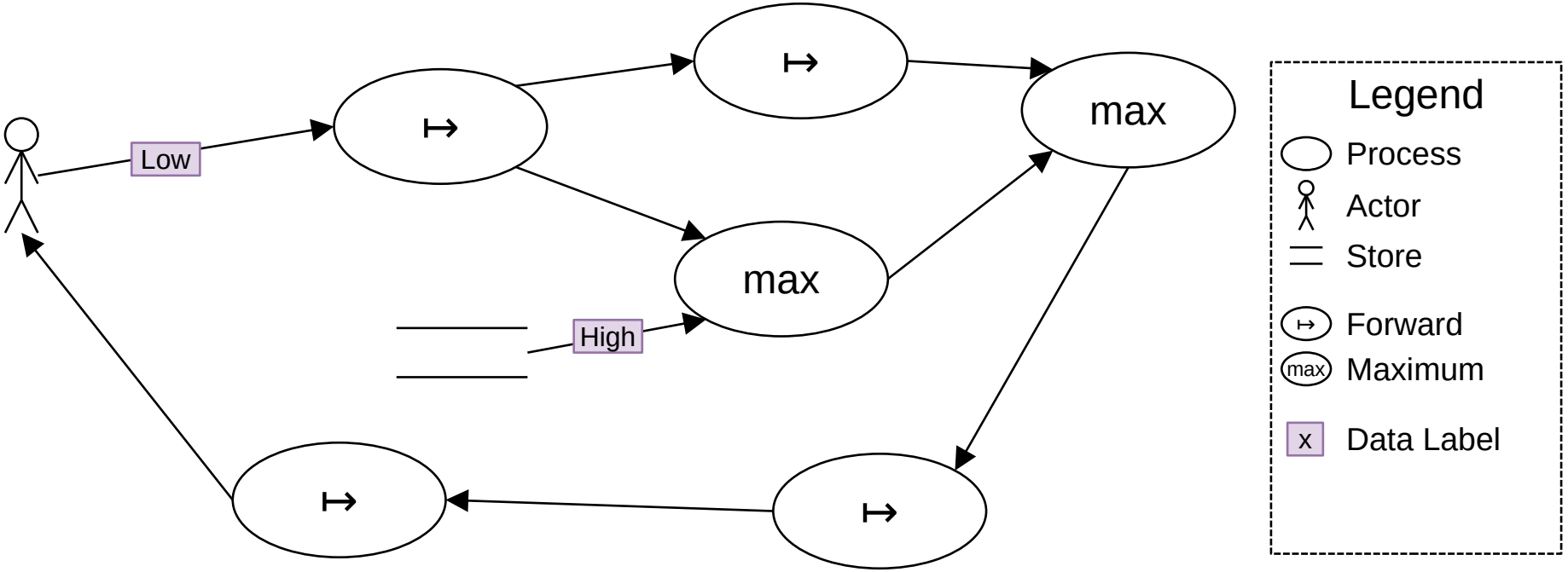
General Idea of Label-based Analyses



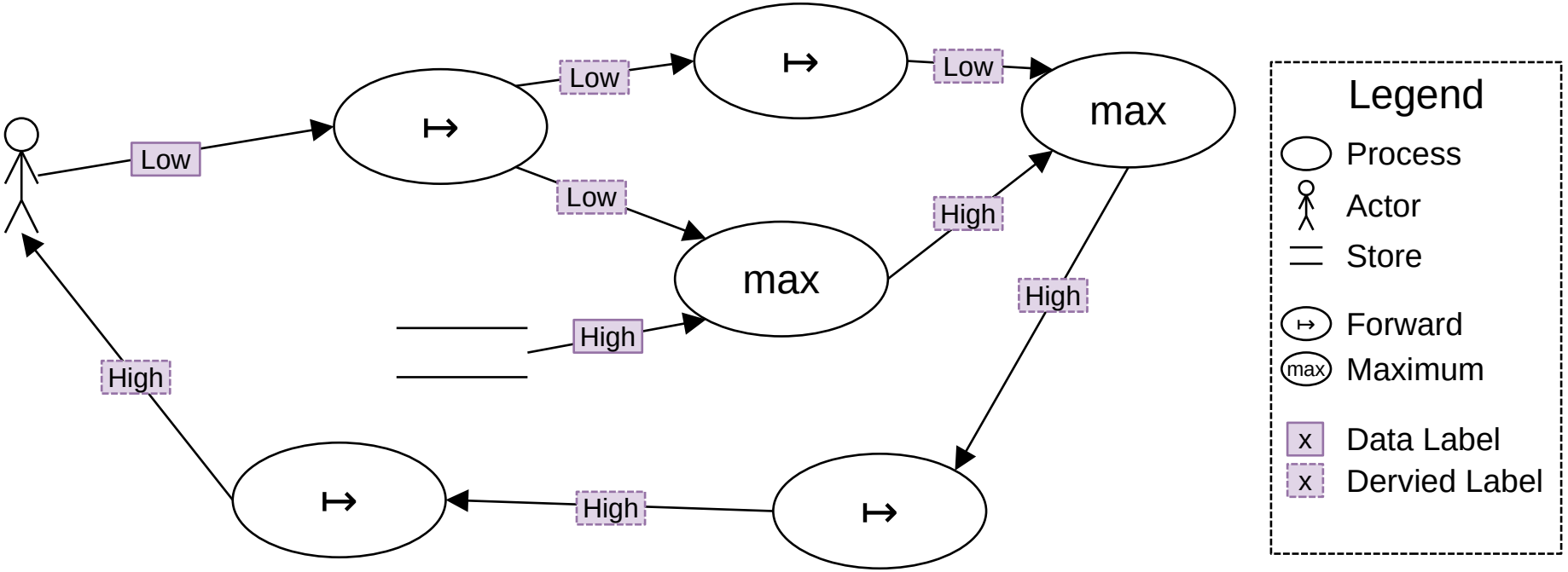
General Idea of Label-based Analyses



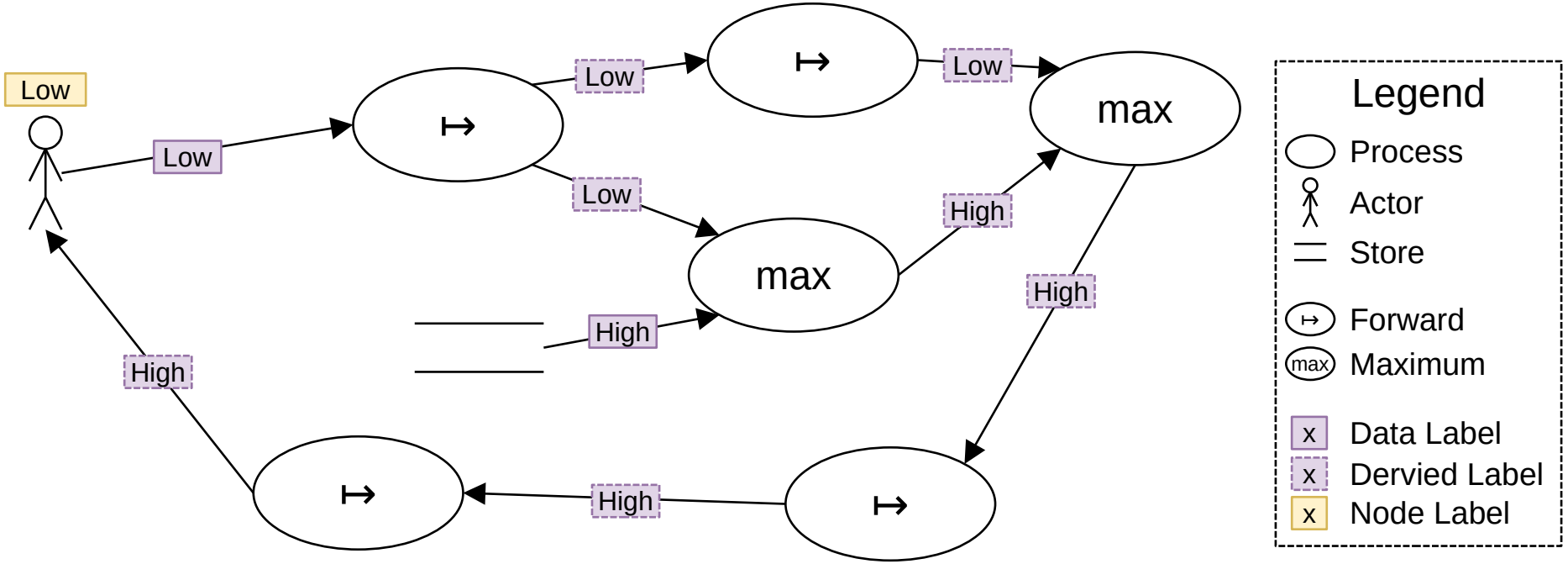
General Idea of Label-based Analyses



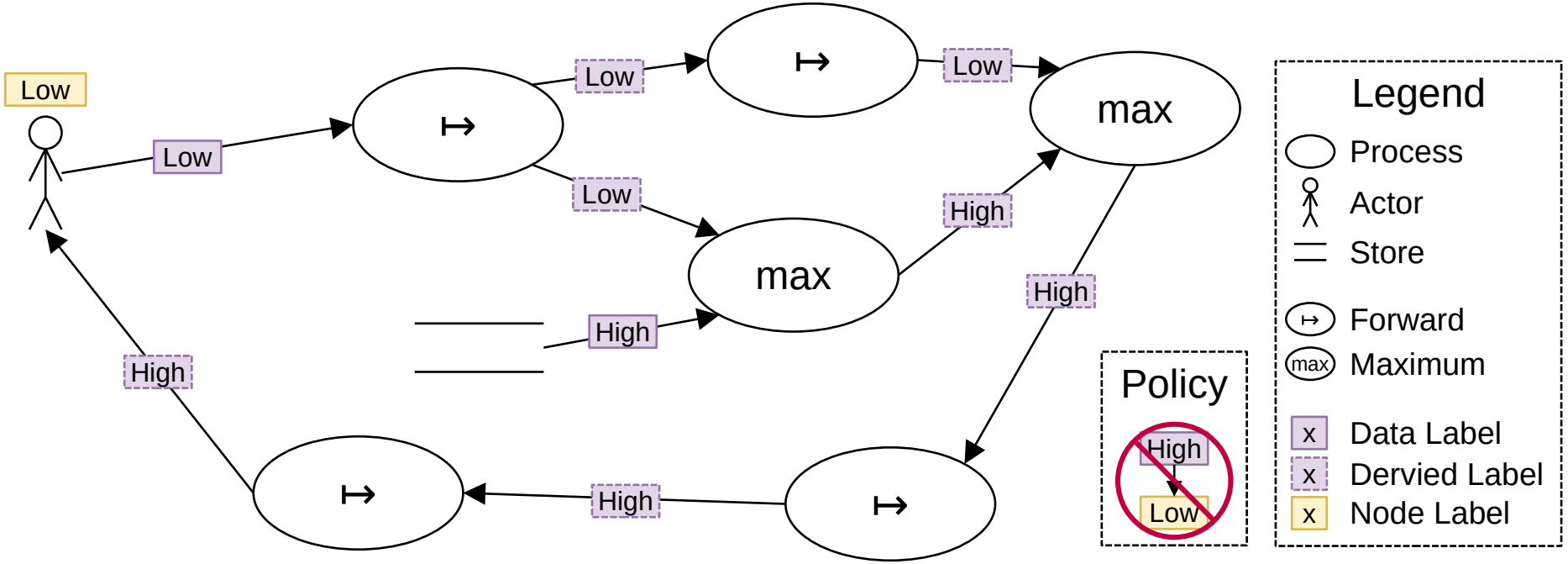
General Idea of Label-based Analyses



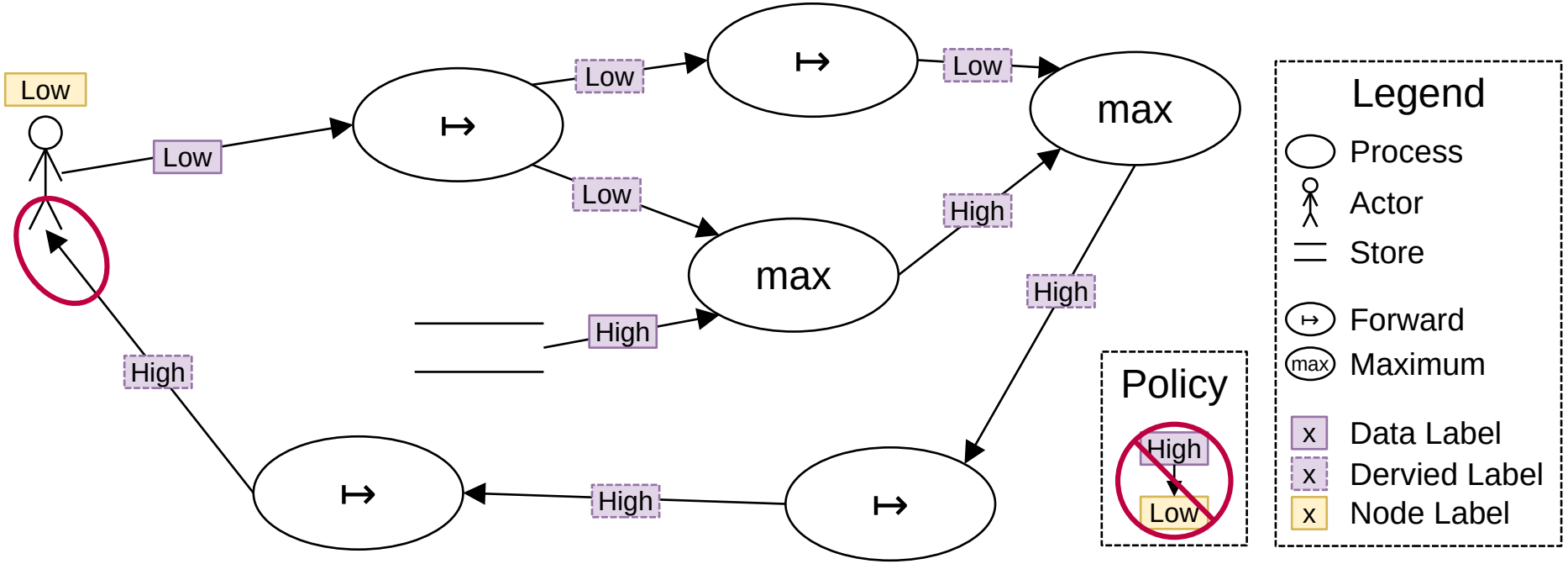
General Idea of Label-based Analyses



General Idea of Label-based Analyses



General Idea of Label-based Analyses



Representing Confidentiality by Labels

- Information flow
  - Data usually has labels (e.g. high/low or tainted) organized in lattices
  - Nodes or users have access to certain labels

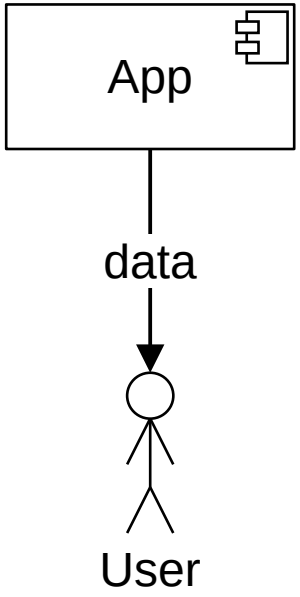
[Seifermann2021] A unified model to detect information flow and access control violations in software architectures. SECRYPT'21, p. 26–37.

Representing Confidentiality by Labels

- Information flow
  - Data usually has labels (e.g. high/low or tainted) organized in lattices
  - Nodes or users have access to certain labels
- Access control (AC)
  - Discretionary AC (DAC): access rights of subjects and objects map to labels
  - Mandatory AC (MAC): policies often similar to information flow policies
  - Role-based AC (RBAC): roles map to labels
  - Attribute-based AC (ABAC): attributes often map to labels

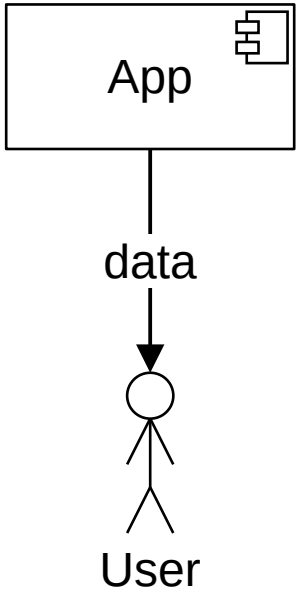
[Seifermann2021] A unified model to detect information flow and access control violations in software architectures. SECRYPT'21, p. 26–37.

Representing RBAC by Labels



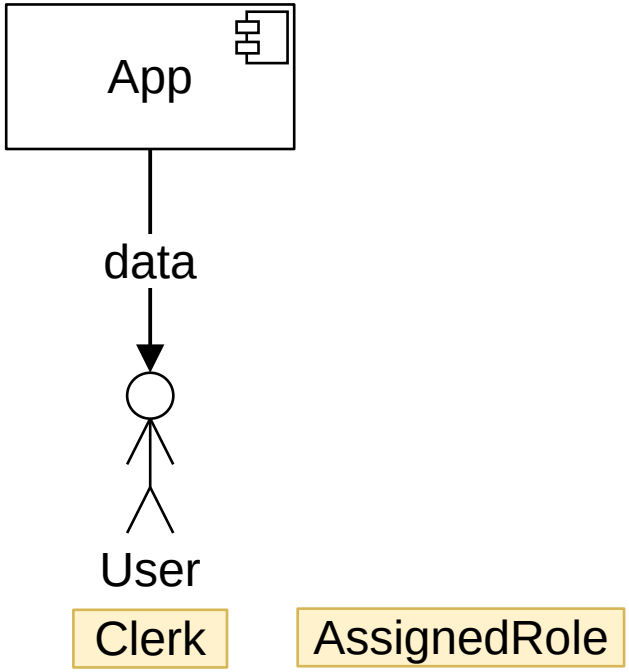
Representing RBAC by Labels

- Policy: Users can access data if they have at least one role that has access to that data



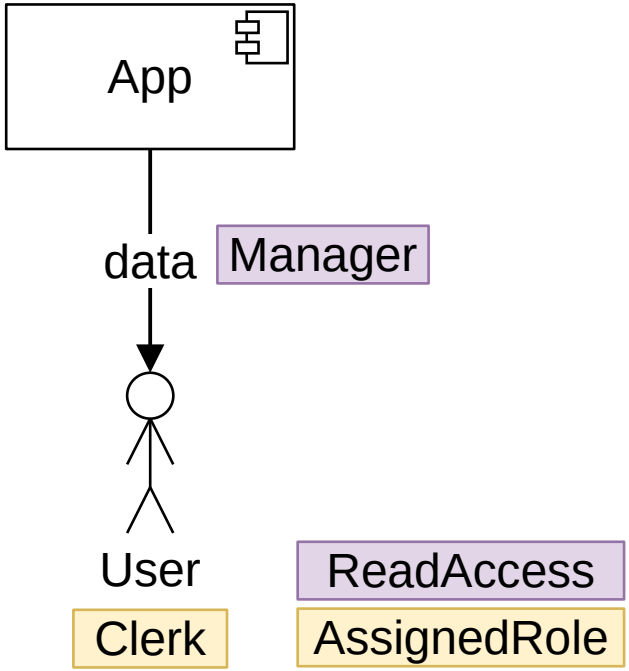
Representing RBAC by Labels

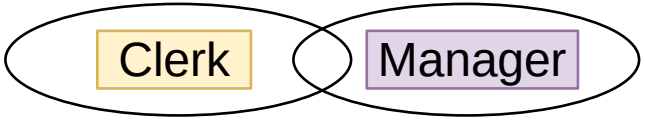
- Policy: Users can access data if they have at least one role that has access to that data
- Relevant labels for policy:
  - Assigned Roles: one label per role



Representing RBAC by Labels

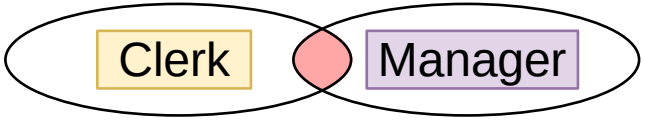
- Policy: Users can access data if they have at least one role that has access to that data
- Relevant labels for policy:
  - Assigned Roles: one label per role
  - Read Access: one label per role

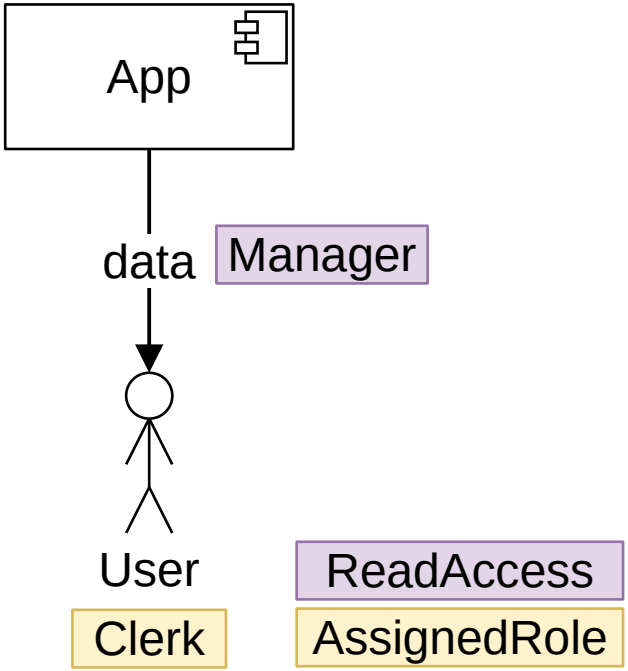




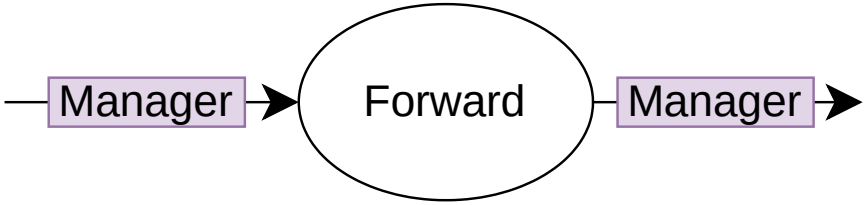
Representing RBAC by Labels

- Policy: Users can access data if they have at least one role that has access to that data
- Relevant labels for policy:
  - Assigned Roles: one label per role
  - Read Access: one label per role
- Violation: Intersection between labels for assigned roles of subjects and read access on data is empty

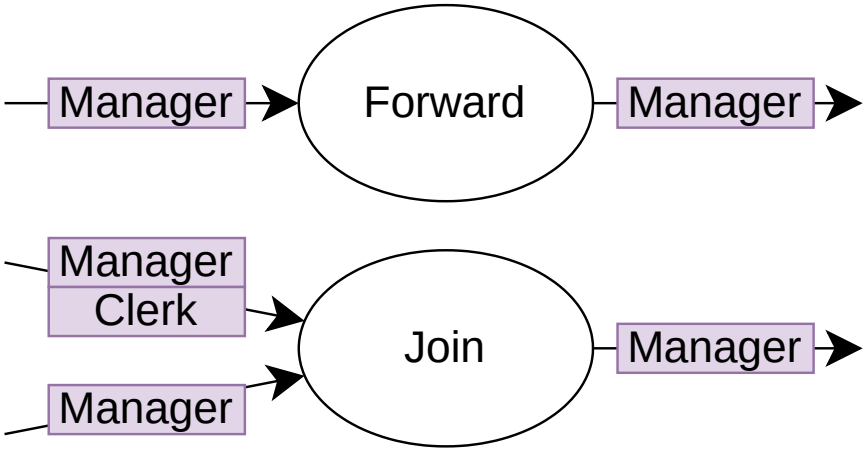




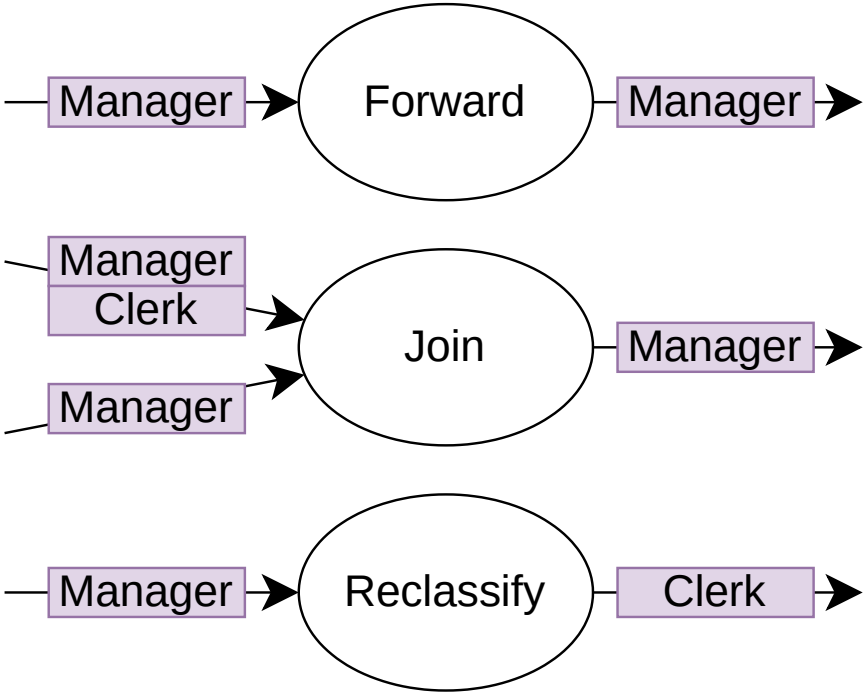
RBAC Behaviors in Label Propagation



RBAC Behaviors in Label Propagation

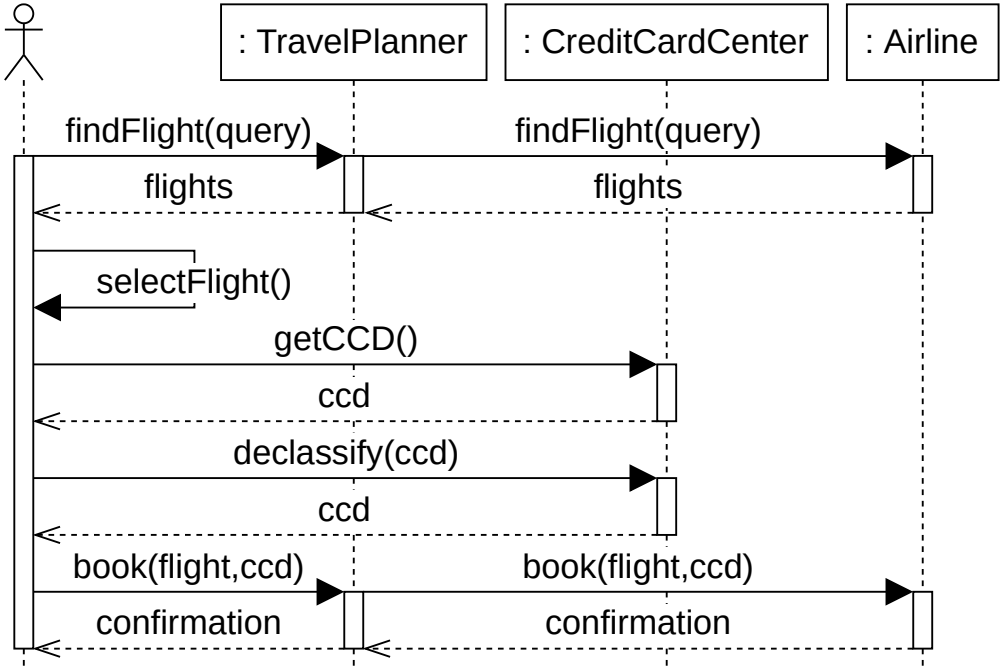


RBAC Behaviors in Label Propagation

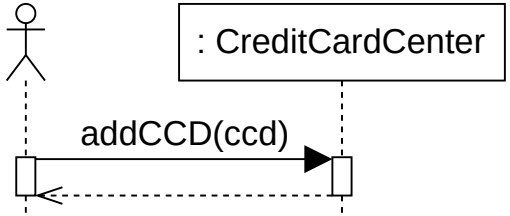


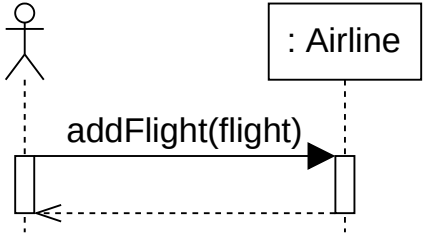
Simplified Travel Planner System

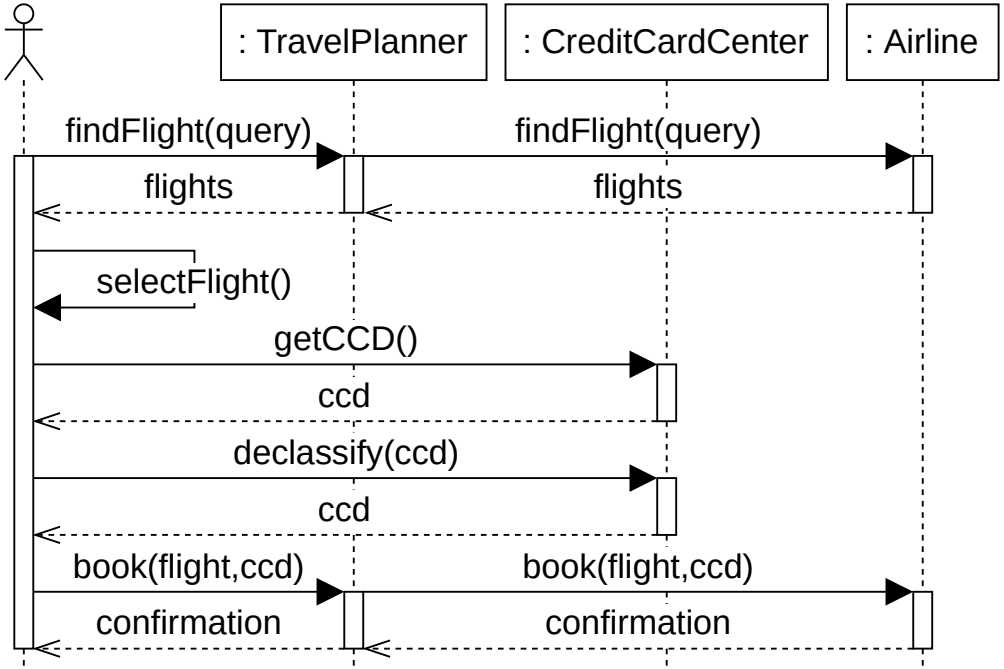
- User uses two apps to search for and book a flight
  - TravelPlanner
  - CreditCardCenter
- Airline provides flight information and processes booking
- Requirement: Credit card data only accessible to user



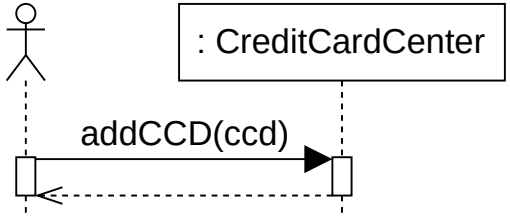
Simplified Travel Planner System

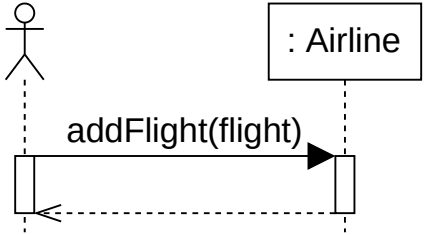


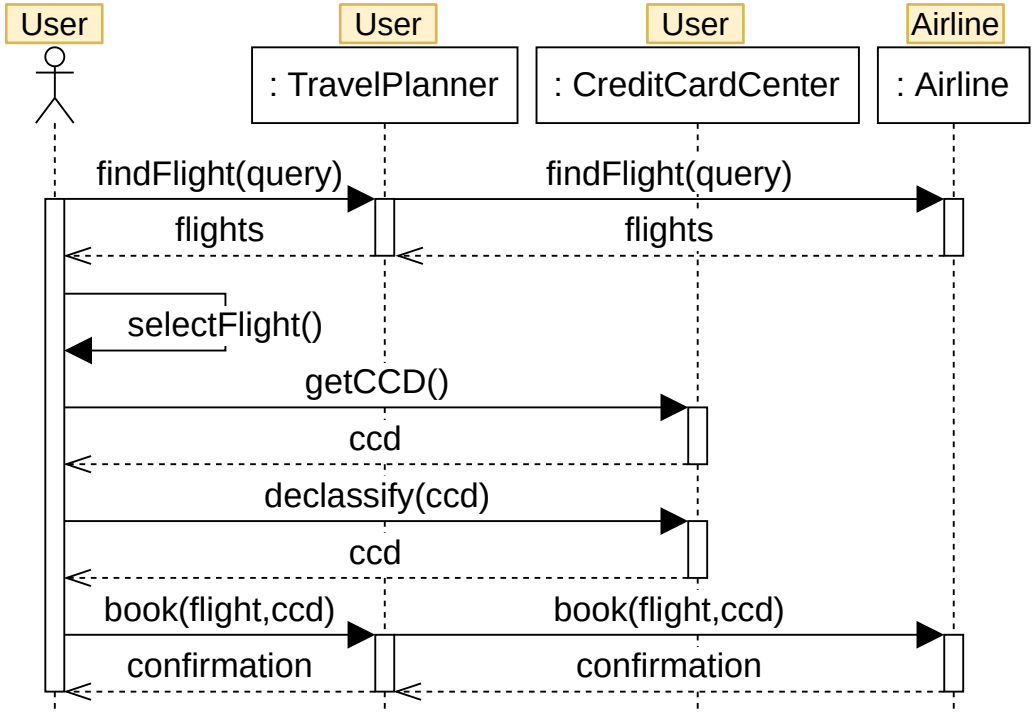




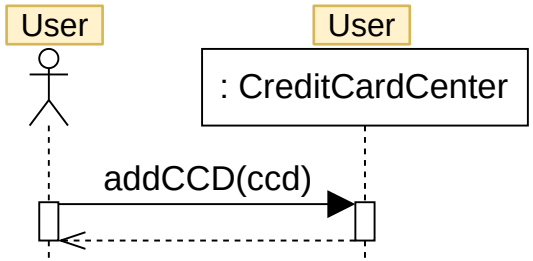
Simplified Travel Planner System

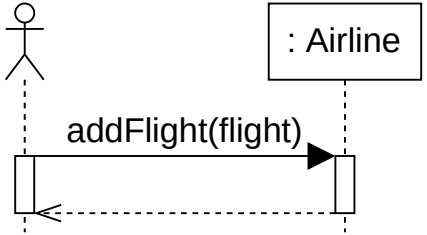


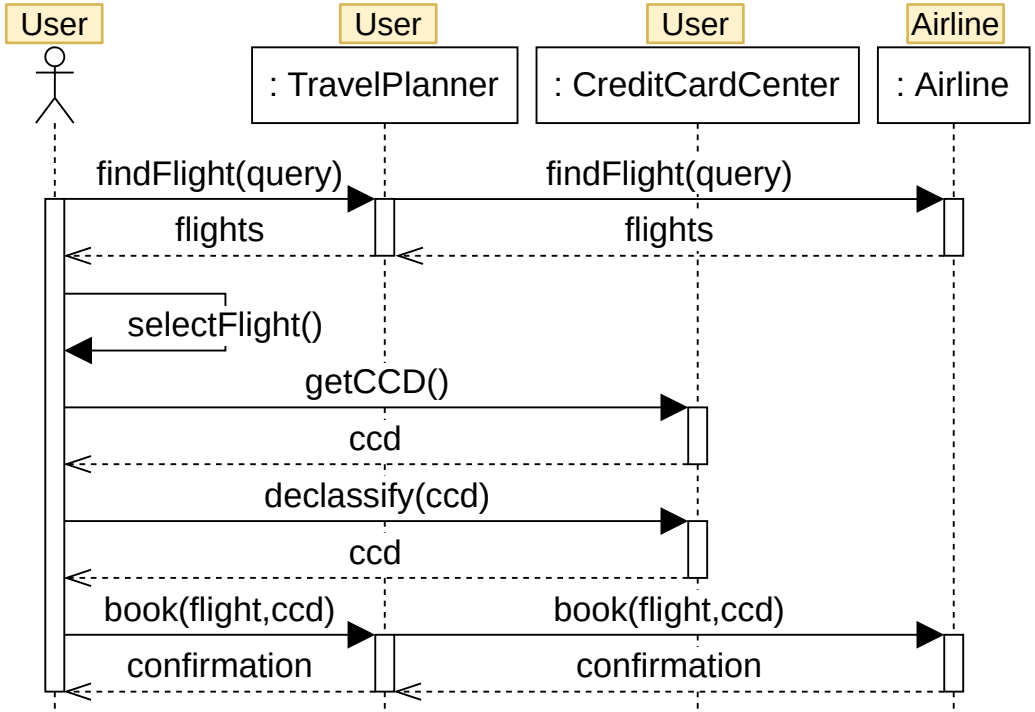




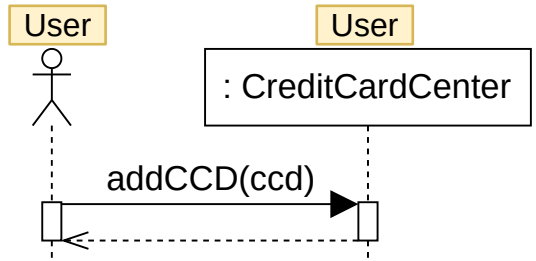
Simplified Travel Planner System

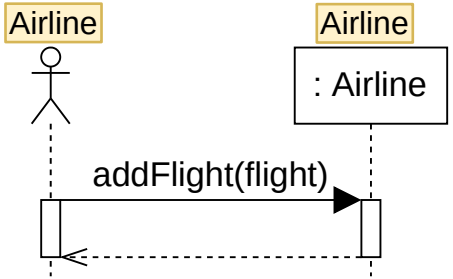


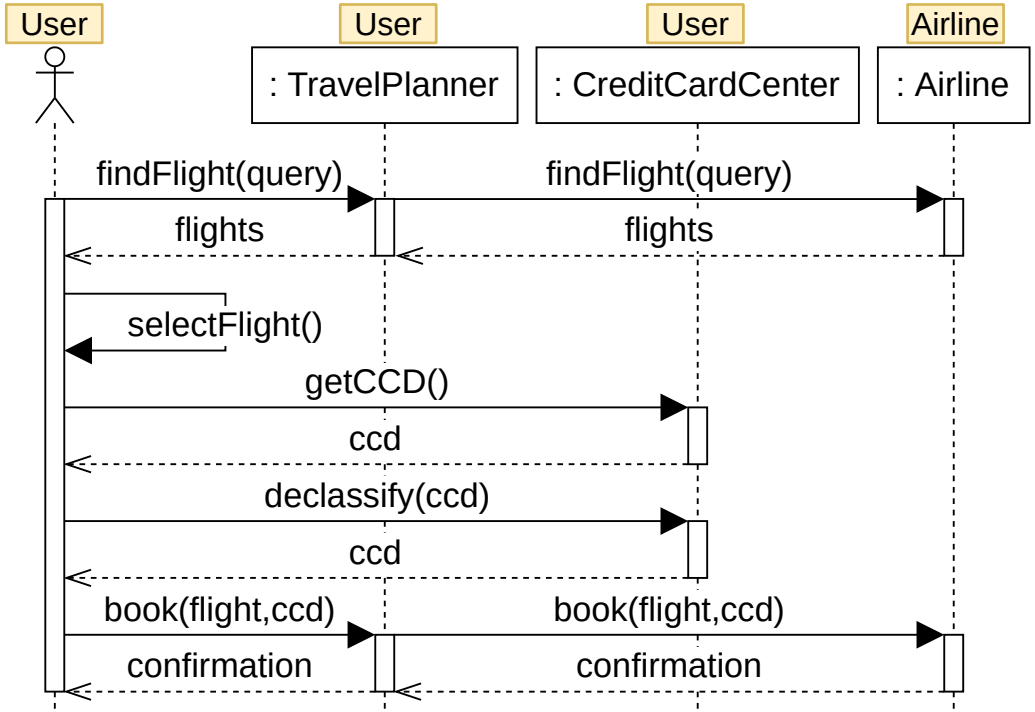




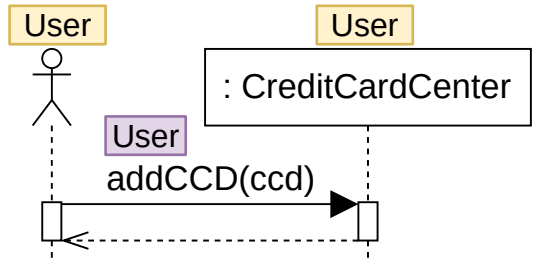
Simplified Travel Planner System

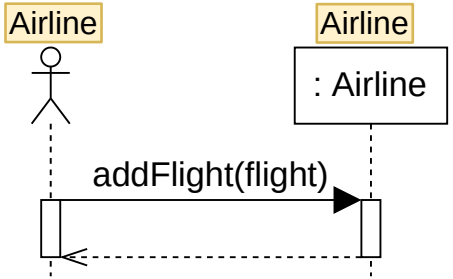


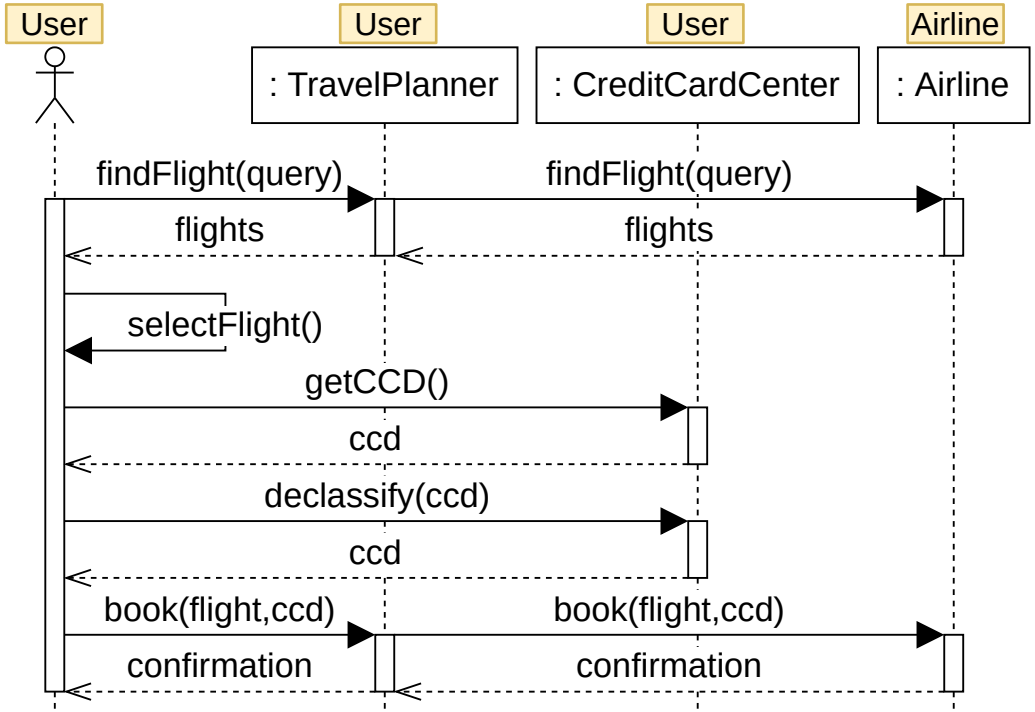




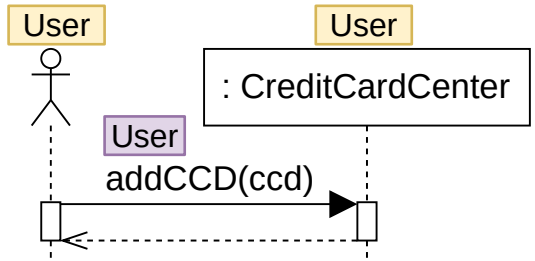
Simplified Travel Planner System

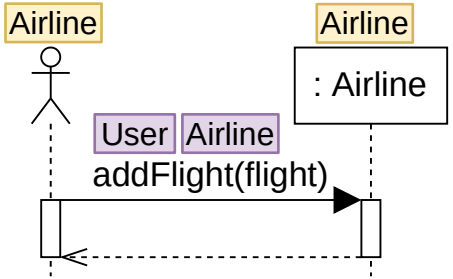


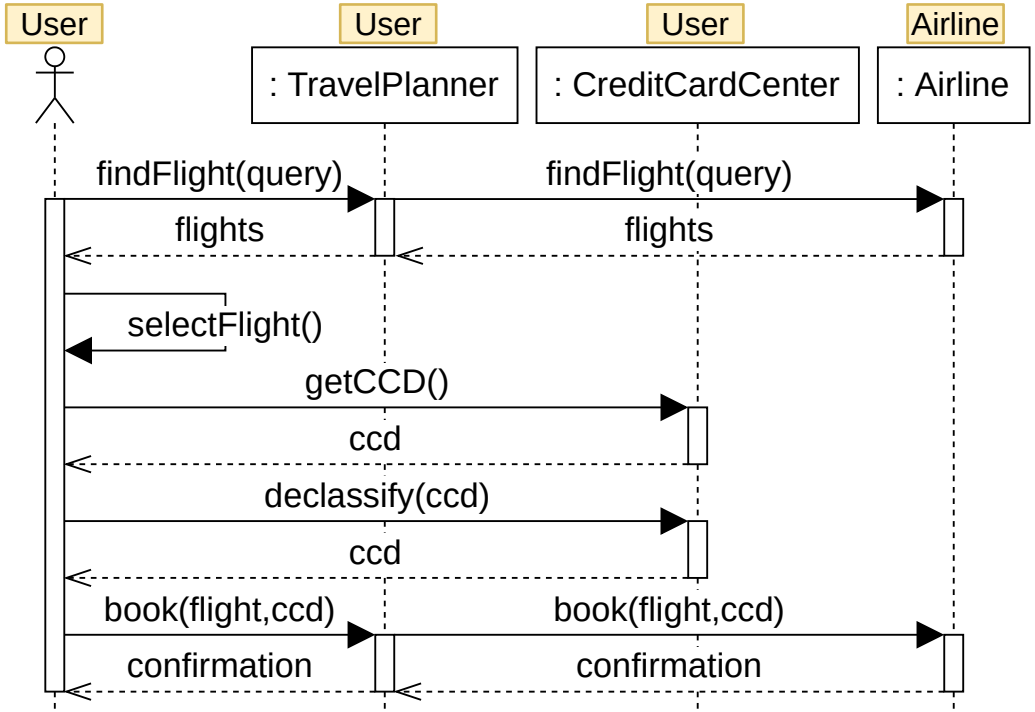




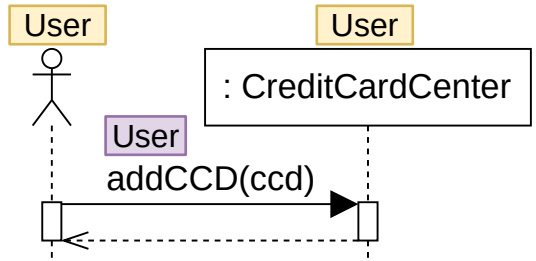
Simplified Travel Planner System

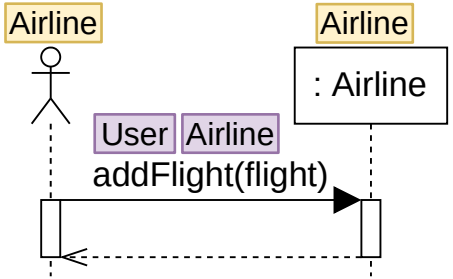


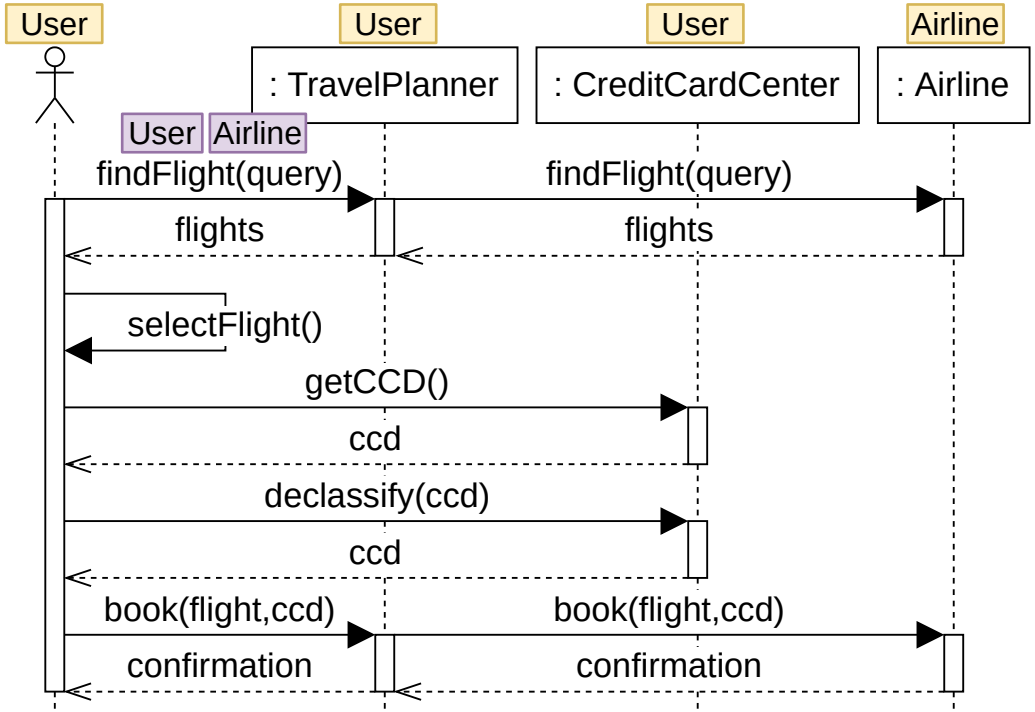




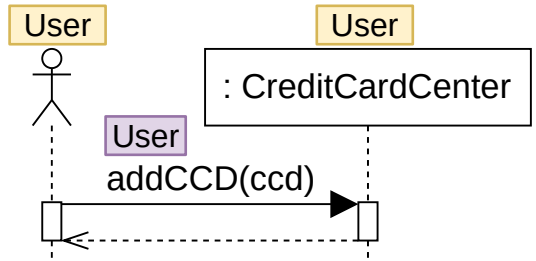
Simplified Travel Planner System

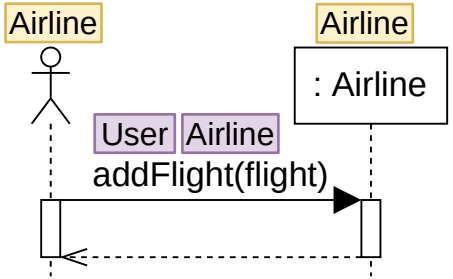


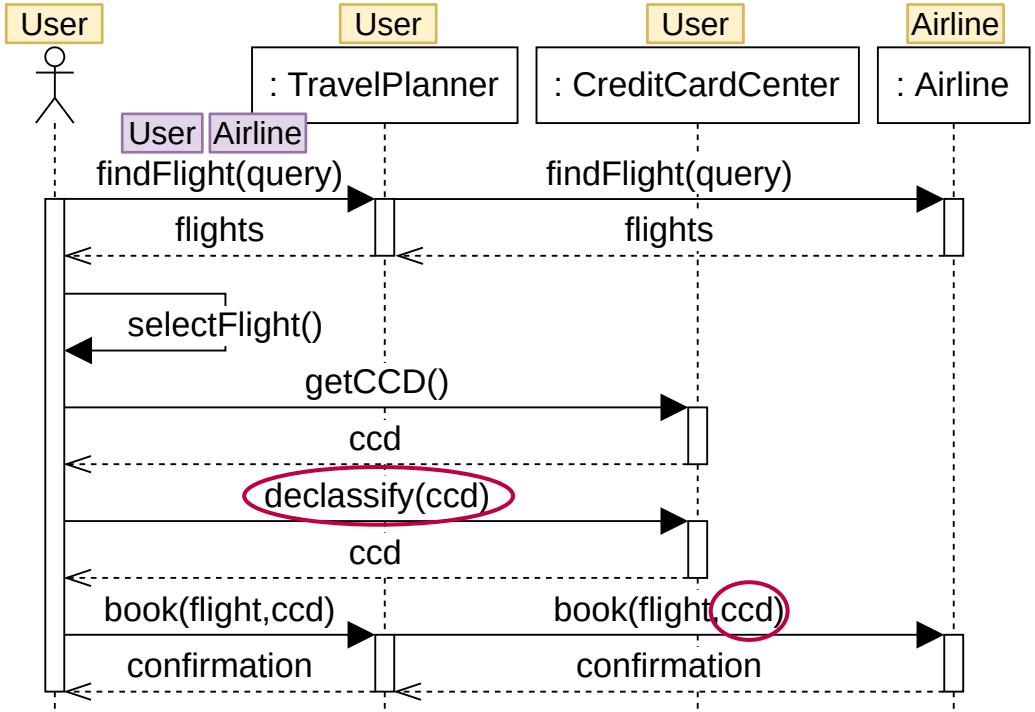




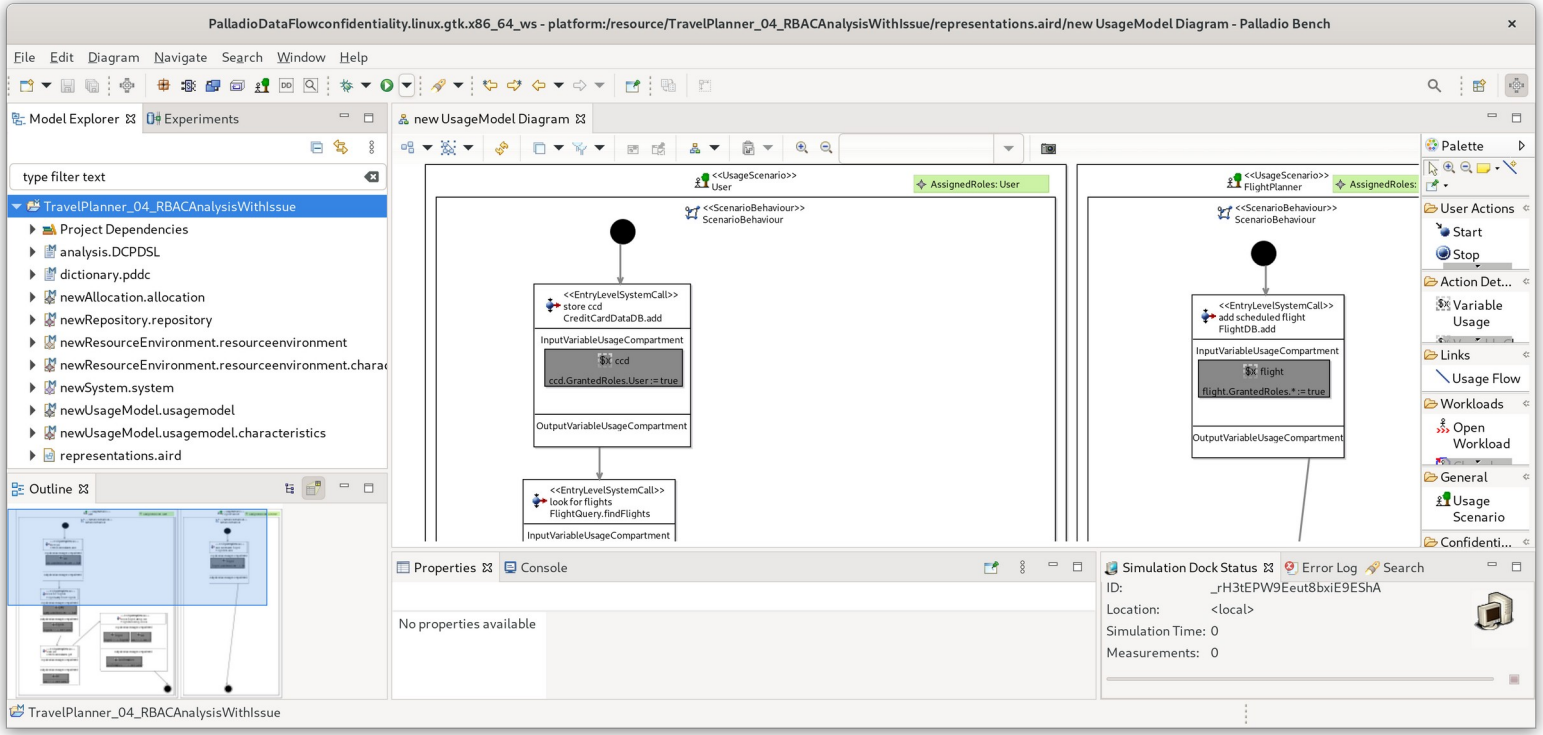
Simplified Travel Planner System







Live Demonstration of Modeling

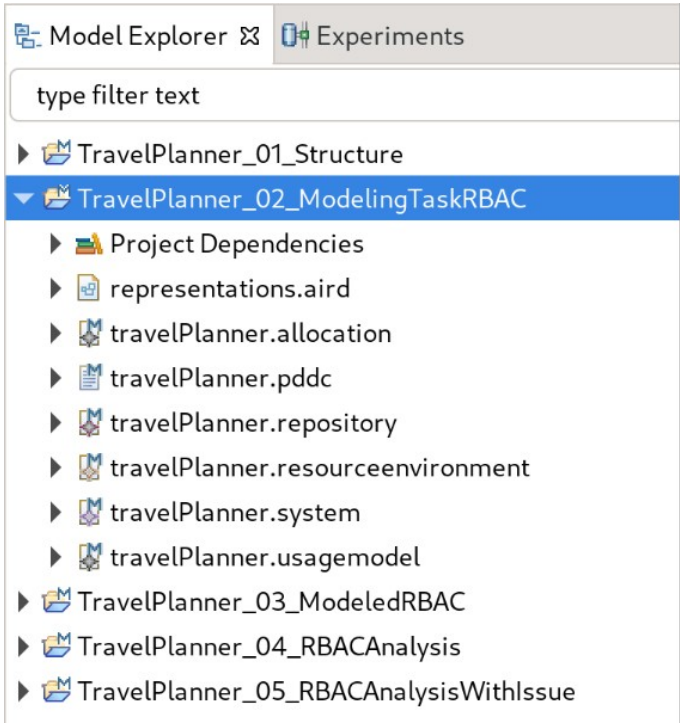


Overview on Modeling Task

- Complete provided TravelPlanner model to prepare RBAC analysis

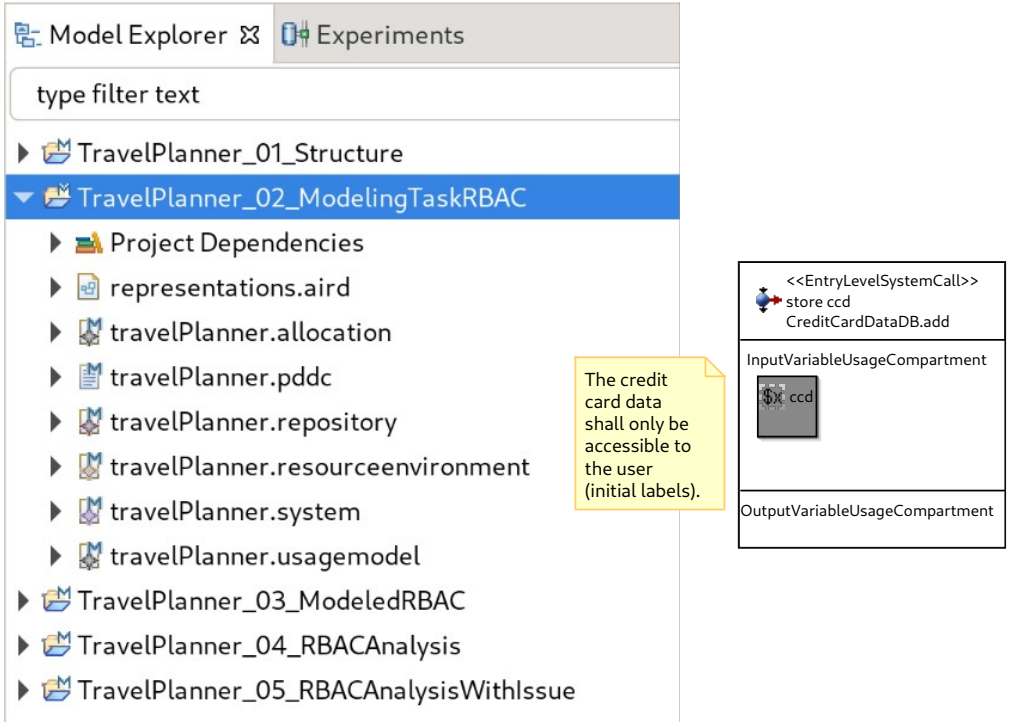
Overview on Modeling Task

- Complete provided TravelPlanner model to prepare RBAC analysis
- Use second modeling project as starting point for task



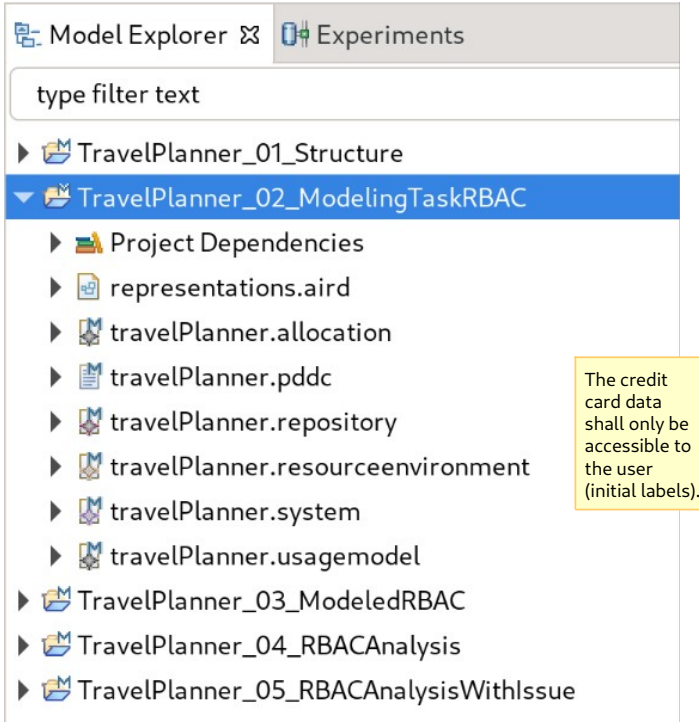
Overview on Modeling Task

- Complete provided TravelPlanner model to prepare RBAC analysis
- Use second modeling project as starting point for task
- Consider hints in yellow notes

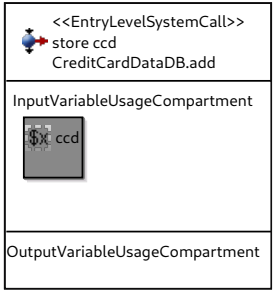


Overview on Modeling Task

- Complete provided TravelPlanner model to prepare RBAC analysis
- Use second modeling project as starting point for task
- Consider hints in yellow notes
- Follow the provided instructions

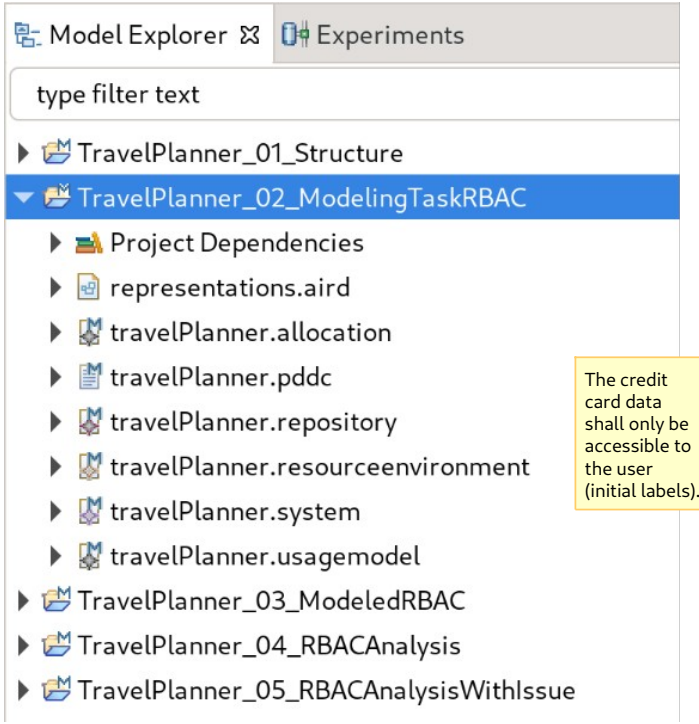


The credit card data shall only be accessible to the user (initial labels).

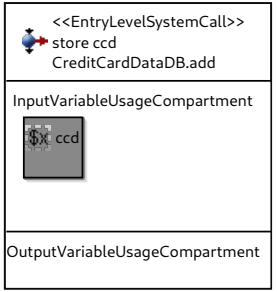


Overview on Modeling Task

- Complete provided TravelPlanner model to prepare RBAC analysis
- Use second modeling project as starting point for task
- Consider hints in yellow notes
- Follow the provided instructions
- Check your solution by comparing it with the third modeling project



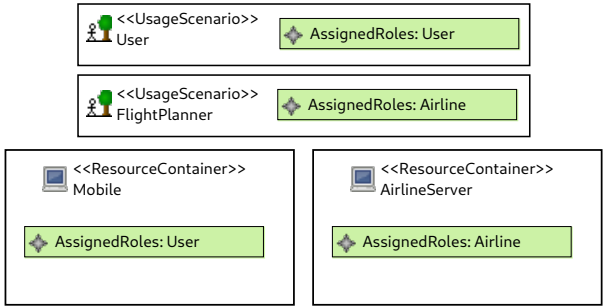
The credit card data shall only be accessible to the user (initial labels).



Steps to Complete Modeling Task

- Assign roles to users and resources
  - Add characteristics to UsageScenarios
  - Add characteristics to ResourceContainers

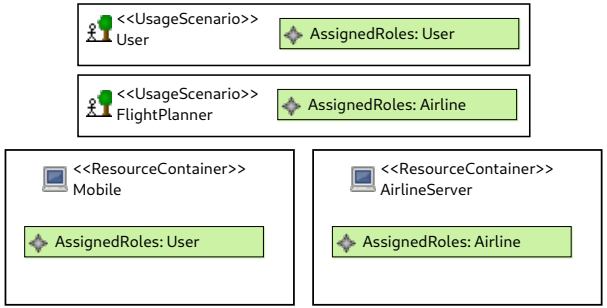
```
enumCharacteristicType AssignedRoles using Roles
```



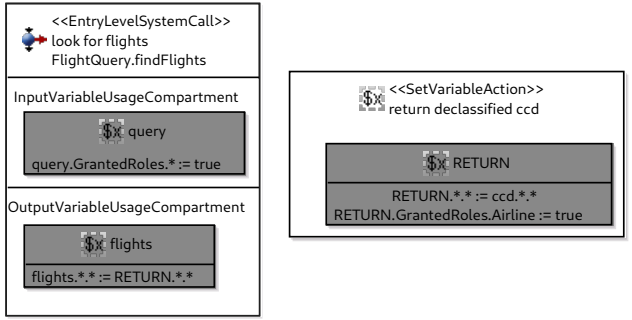
Steps to Complete Modeling Task

- Assign roles to users and resources
  - Add characteristics to UsageScenarios
  - Add characteristics to ResourceContainers
- Add the missing assignments in usage
  - CreditCardCenterDB:add
  - FlightQuery:findFlights
- Add the missing assignments in SEFFs
  - CreditCardCenterLogic:declassifyForAirline
  - TravelPlanner:findFlights

```
enumCharacteristicType AssignedRoles using Roles
```




```
enumCharacteristicType GrantedRoles using Roles
```

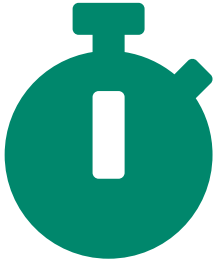


Resources for Modeling Task

Palladio Tooling

Task Instructions

Cheat Sheet



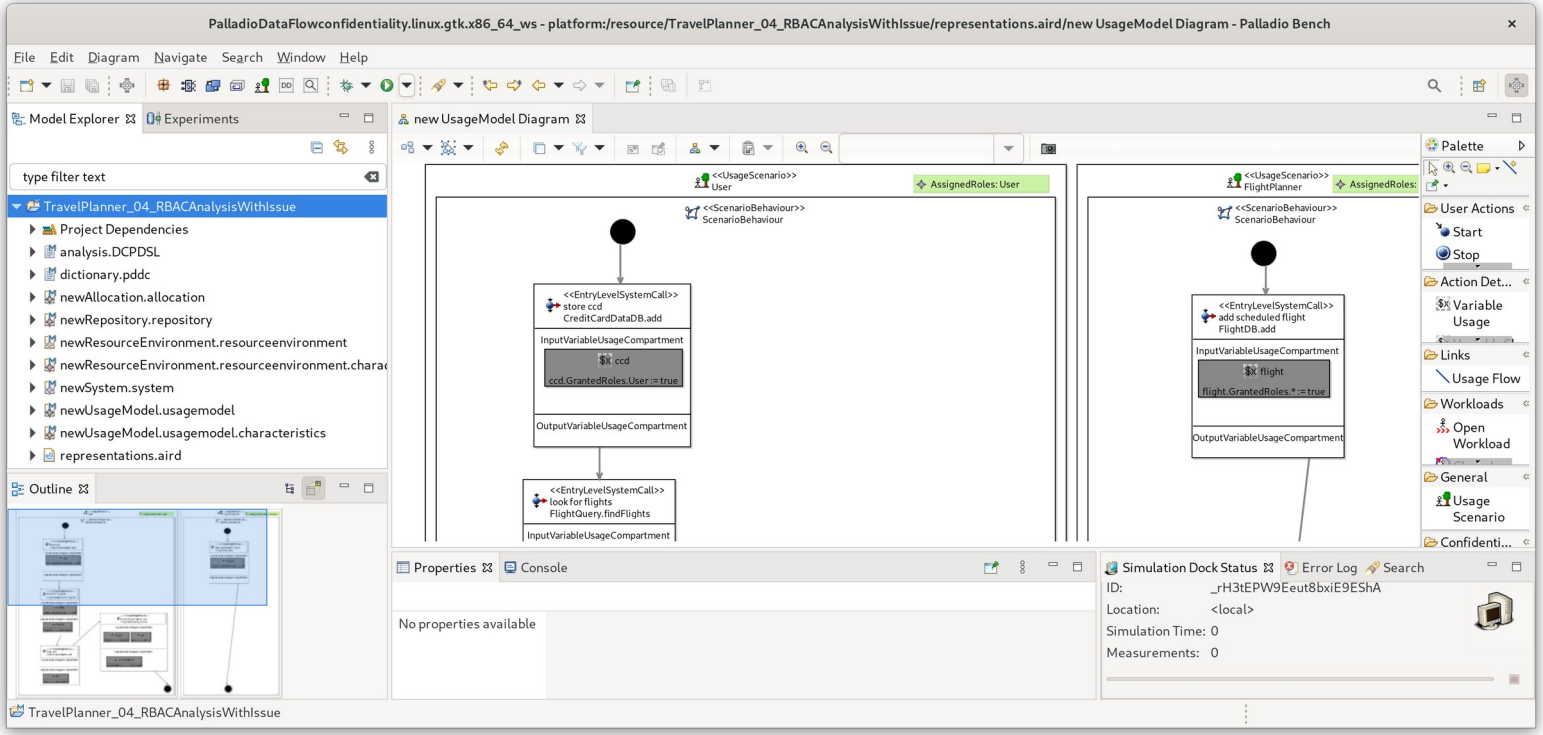
20 min

bit.ly/2U1ZffR

Break

- 17:00 – 17:15: Welcoming
- 17:15 – 18:00: Modeling Access Control Using Palladio
- 18:00 – 18:20: Working Session on Modeling Task
- **18:20 – 18:30: Break**
- 18:30 – 18:40: Discussion of Modeling Task
- 18:40 – 19:00: Analyzing Access Control Using Palladio
- 19:00 – 19:10: Analysis Task
- 19:10 – 19:30: Summary / Future Work / Feedback

Discussion of Modeling Task



Karlsruhe Institute of Technology

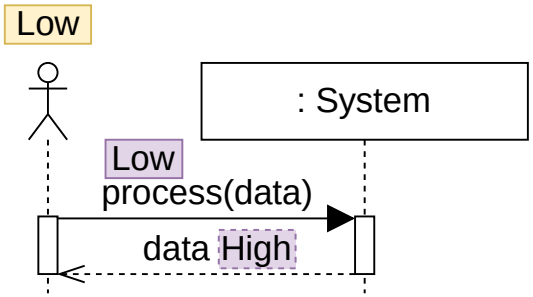
Software Design and Quality

Analyzing Access Control Using Palladio

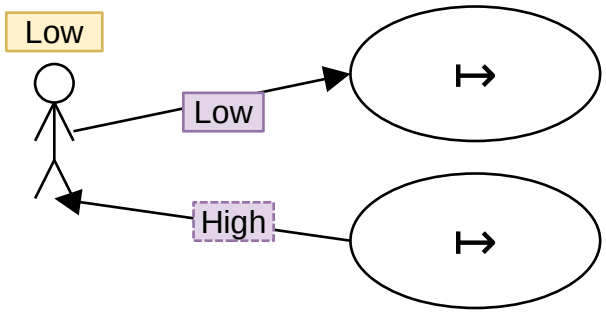
Stephan Seifermann, Maximilian Walter, Sebastian Hahner, Robert Heinrich, Ralf Reussner

Motivation

Software Architecture

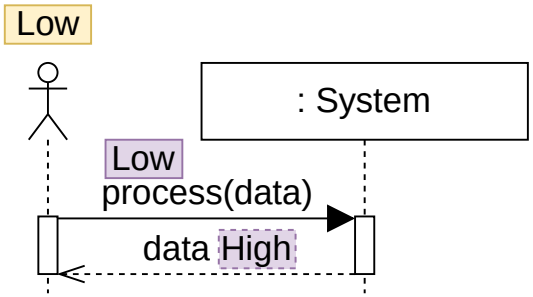


Analysis Formalism



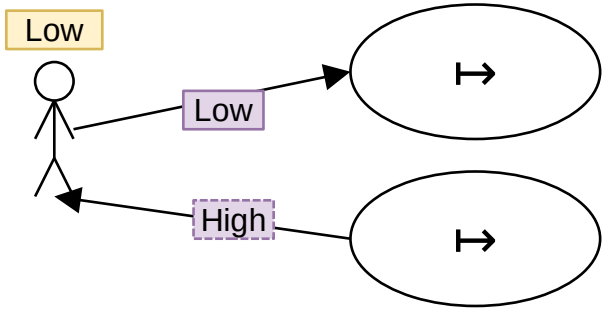
Motivation

Software Architecture

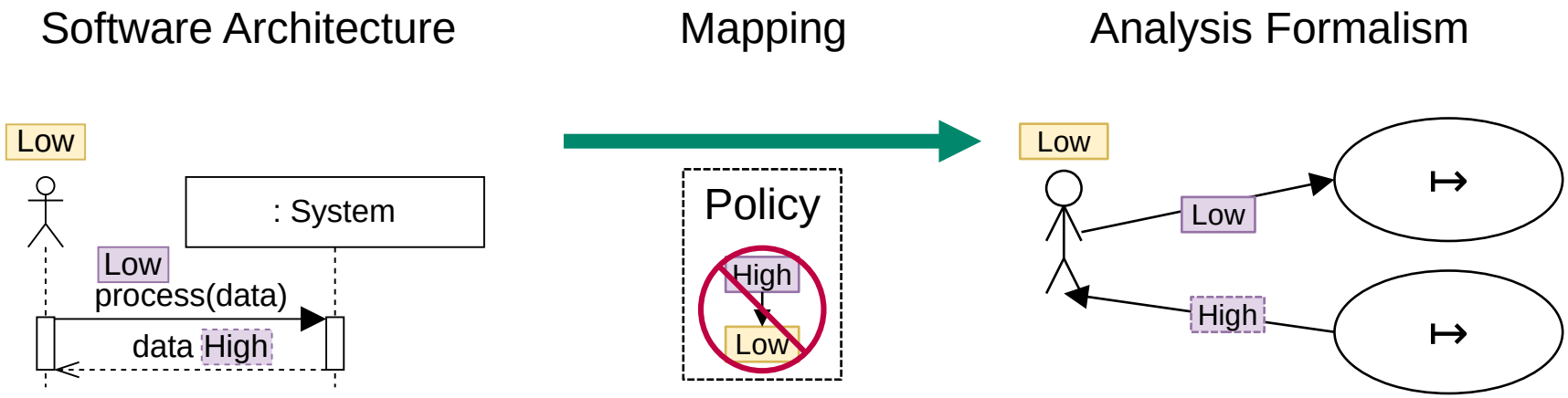


Mapping

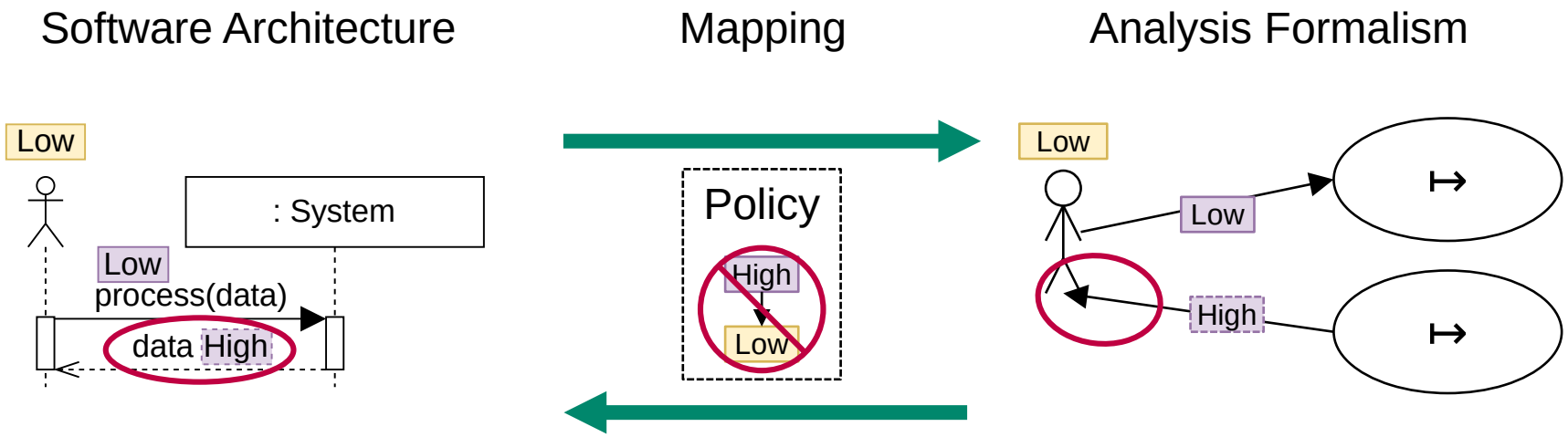
Analysis Formalism



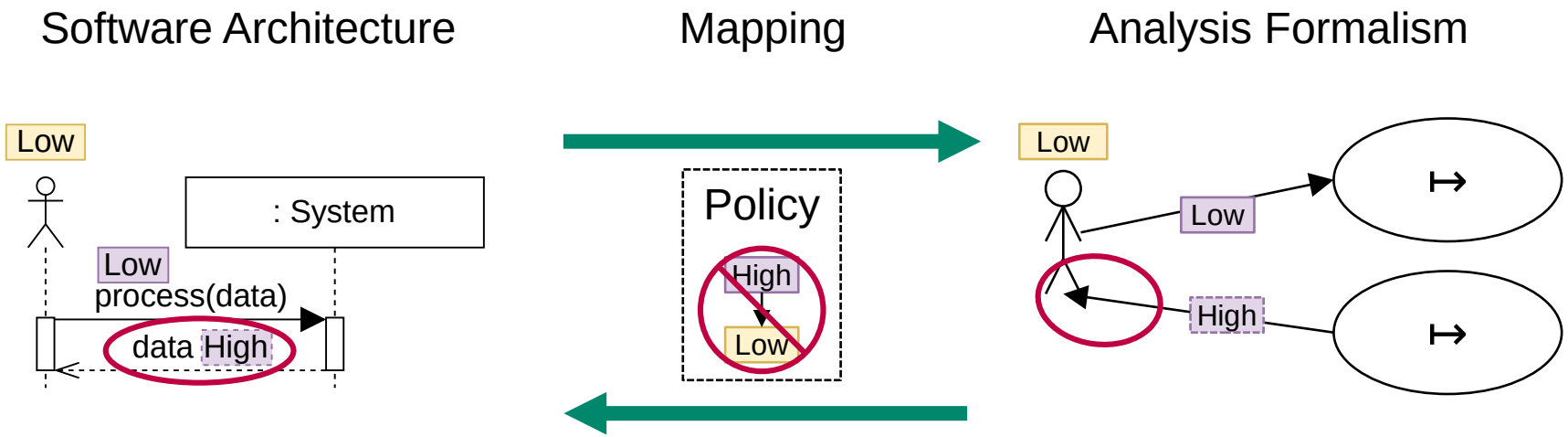
Motivation


Software Architecture
Mapping
Analysis Formalism
Low
: System
Low
process(data)
data High
Policy
High
Low
Low
Low
High

Motivation


Software Architecture
Mapping
Analysis Formalism
Low
: System
Low
process(data)
data High
Policy
High
Low
Low
Low
High

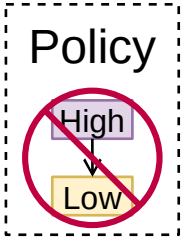
Motivation



Problem: Gap in Abstraction

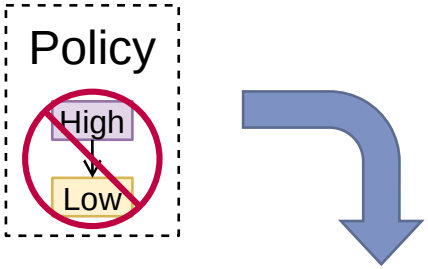
Specification of Data Flow Constraints

- Data flow constraints are specified on architectural abstraction level together with the annotated architecture



Specification of Data Flow Constraints

- Data flow constraints are specified on architectural abstraction level together with the annotated architecture
- A domain-specific language provides the required concepts to formulate such constraints [Hahner2021]



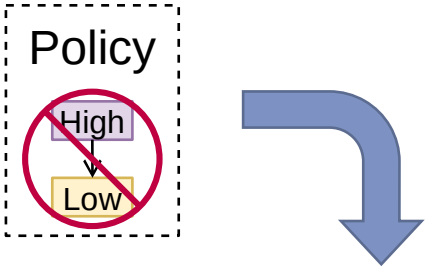
***Constraint**: „Data labeled high is not allowed to flow to components labeled low“*

```
constraint RestrictHigh {
 data.attribute.level.high
   NEVER FLOWS
 component.property.level.low
}
```

[Hahner2021] Modeling data flow constraints for design-time confidentiality analyses. ICSA-C’21, p. 15–21.

Specification of Data Flow Constraints

- Data flow constraints are specified on architectural abstraction level together with the annotated architecture
- A domain-specific language provides the required concepts to formulate such constraints [Hahner2021]
- The specified constraints are mapped together with the annotated architecture

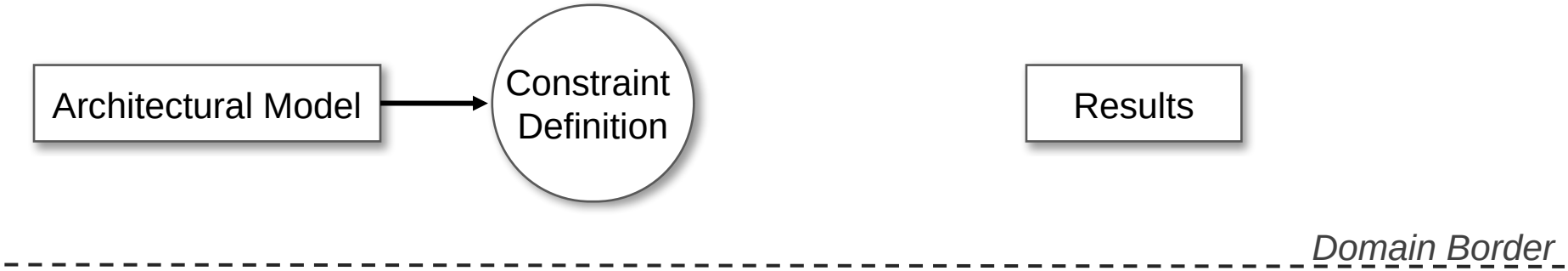


***Constraint**: „Data labeled high is not allowed to flow to components labeled low“*

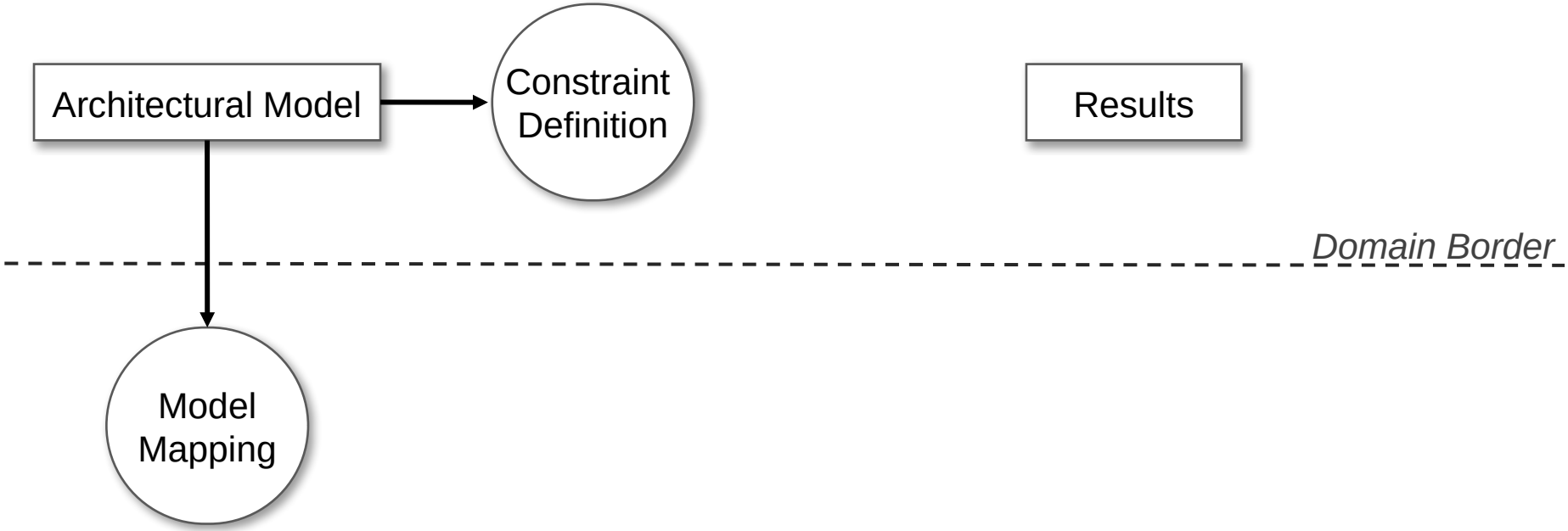
```
constraint RestrictHigh {
 data.attribute.level.high
   NEVER FLOWS
 component.property.level.low
}
```

[Hahner2021] Modeling data flow constraints for design-time confidentiality analyses. ICSA-C’21, p. 15–21.

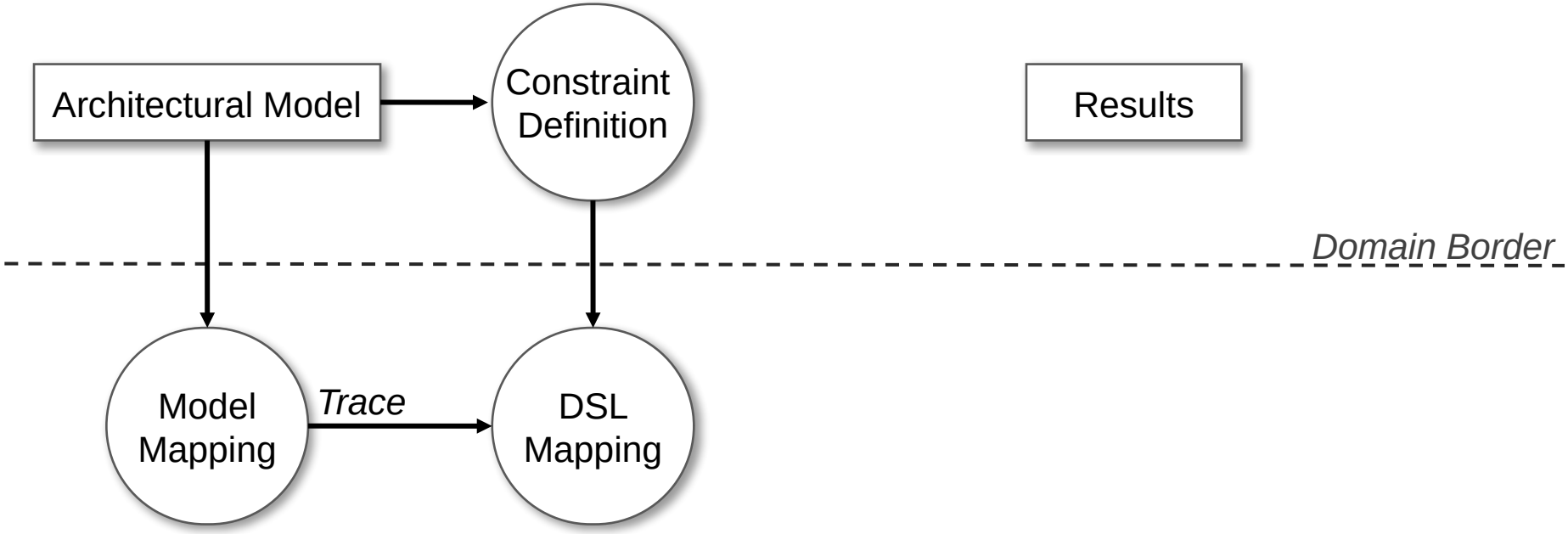
Bridging the Abstraction Gap



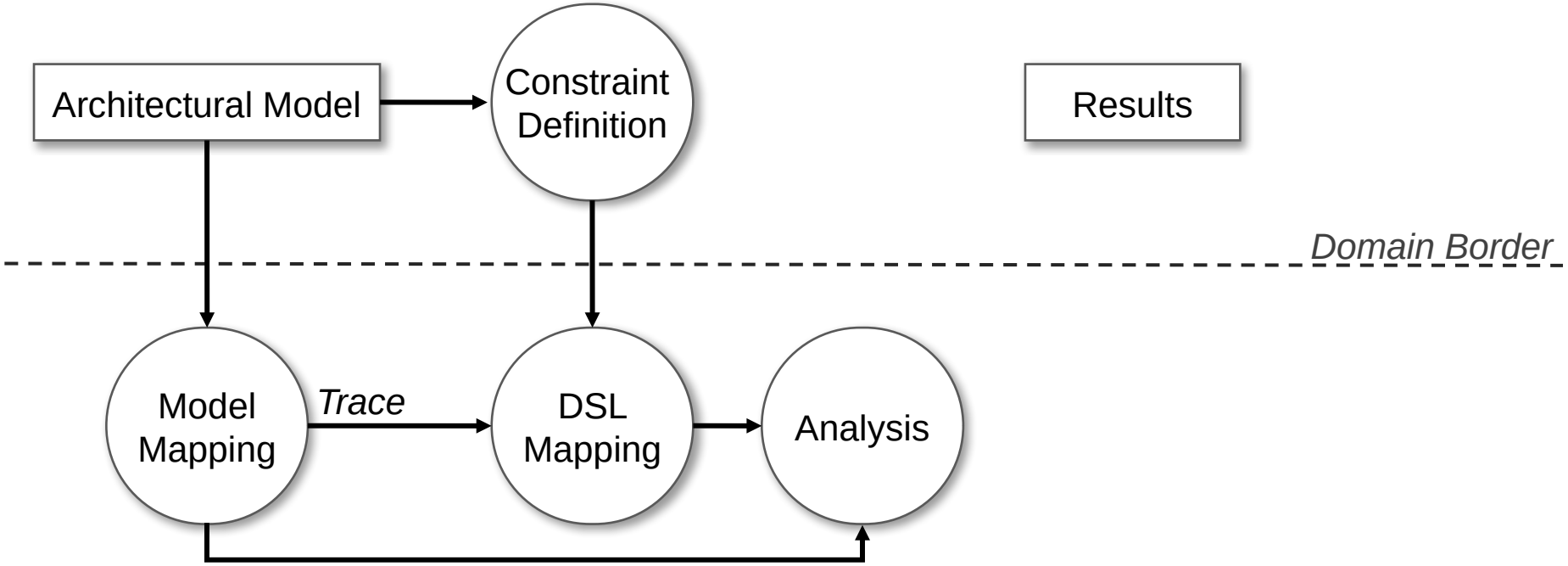
Bridging the Abstraction Gap



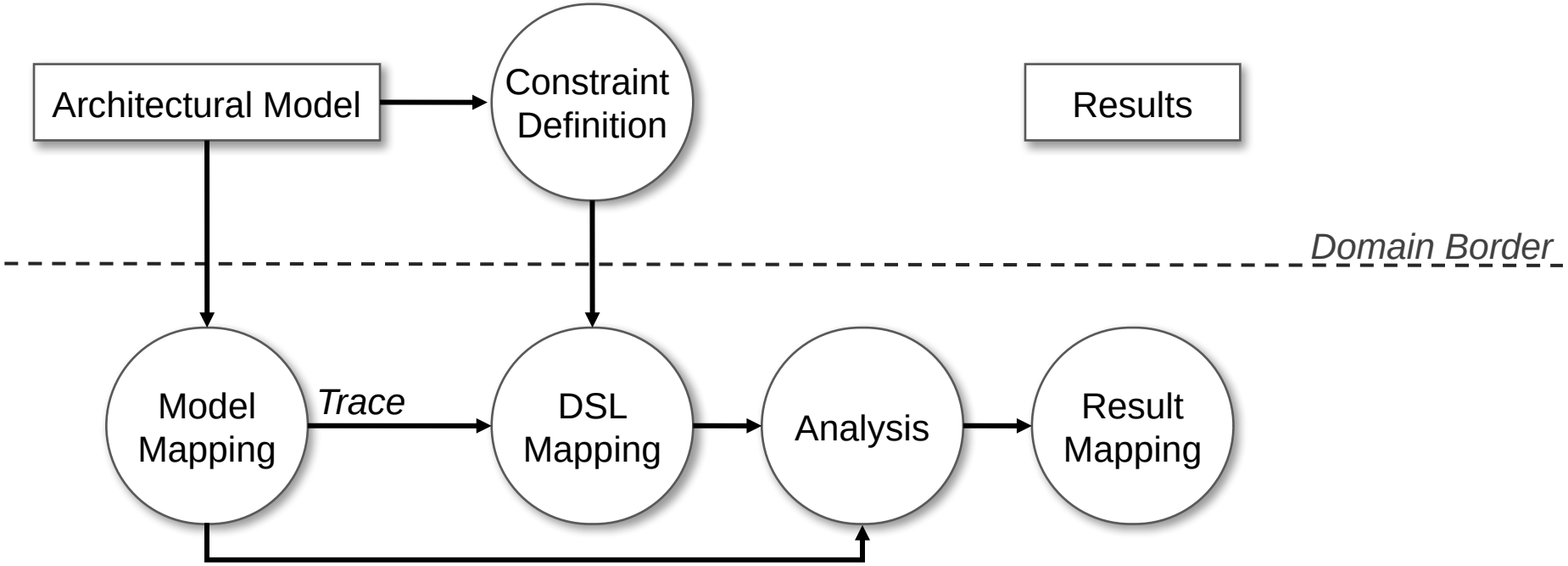
Bridging the Abstraction Gap



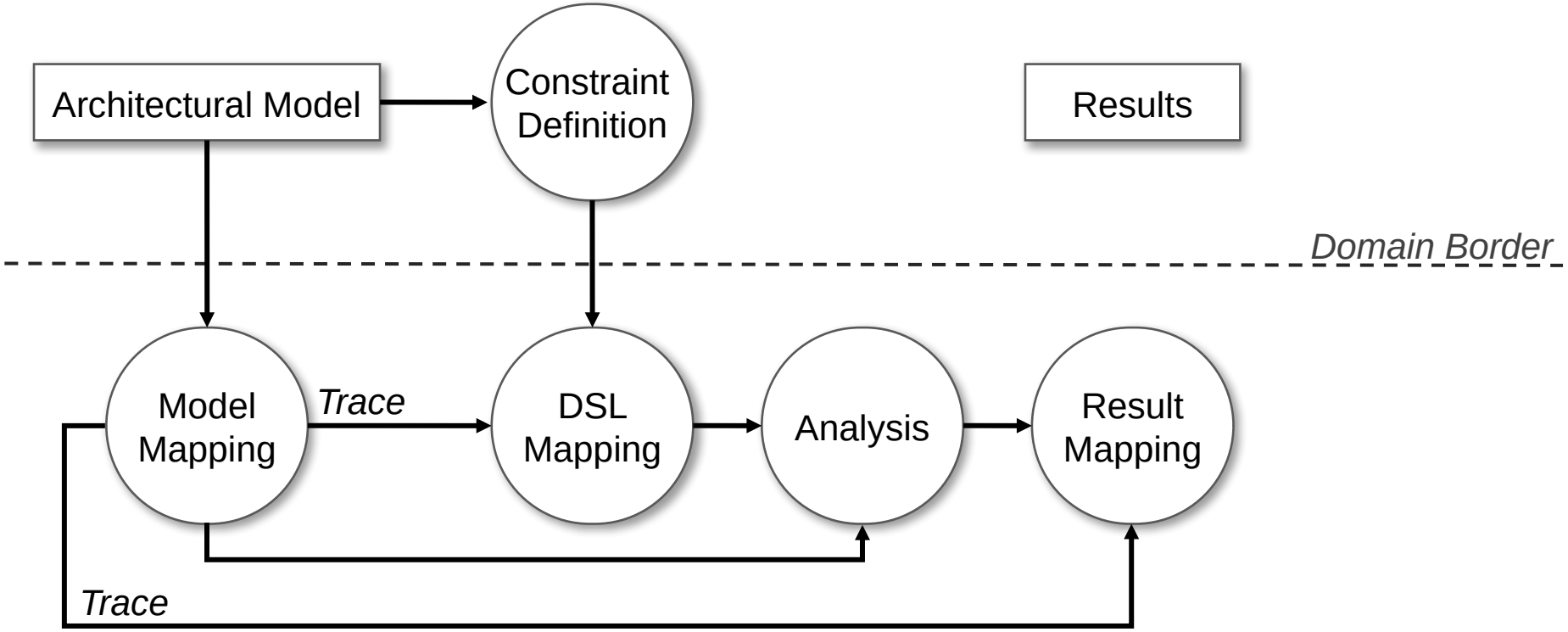
Bridging the Abstraction Gap



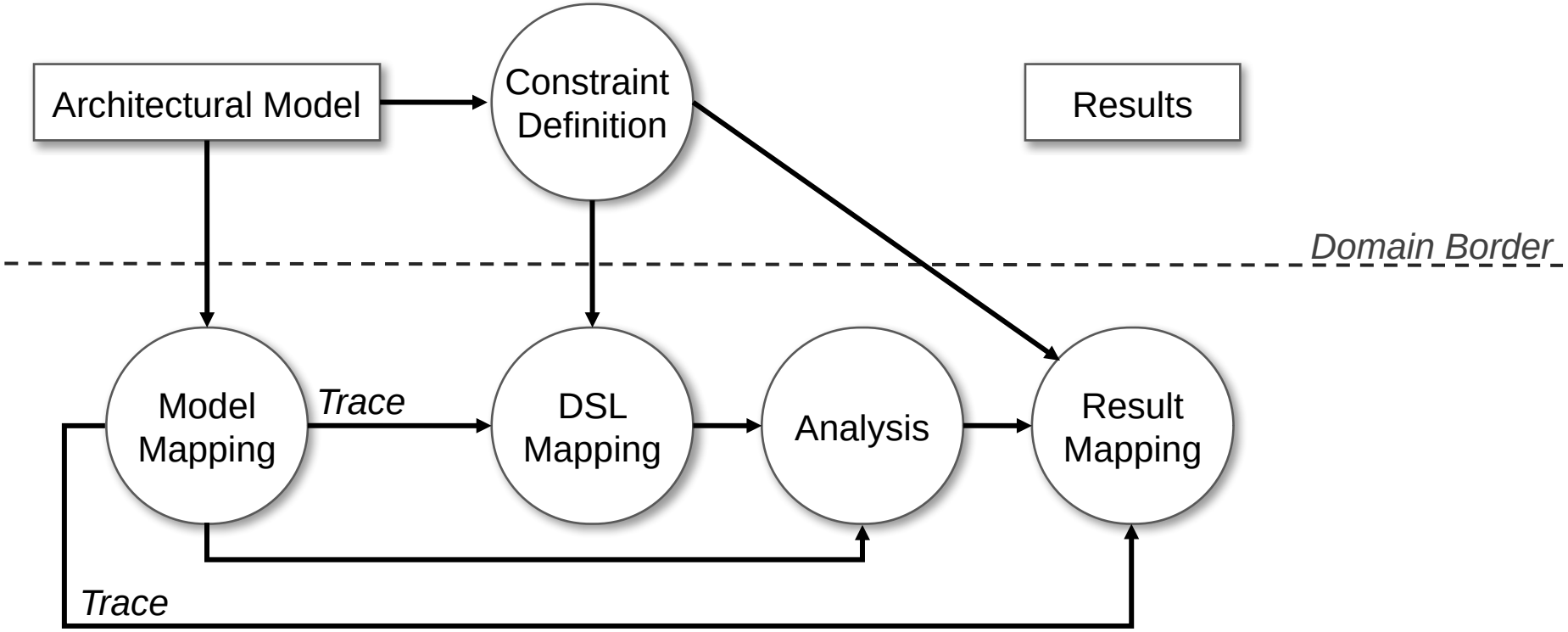
Bridging the Abstraction Gap



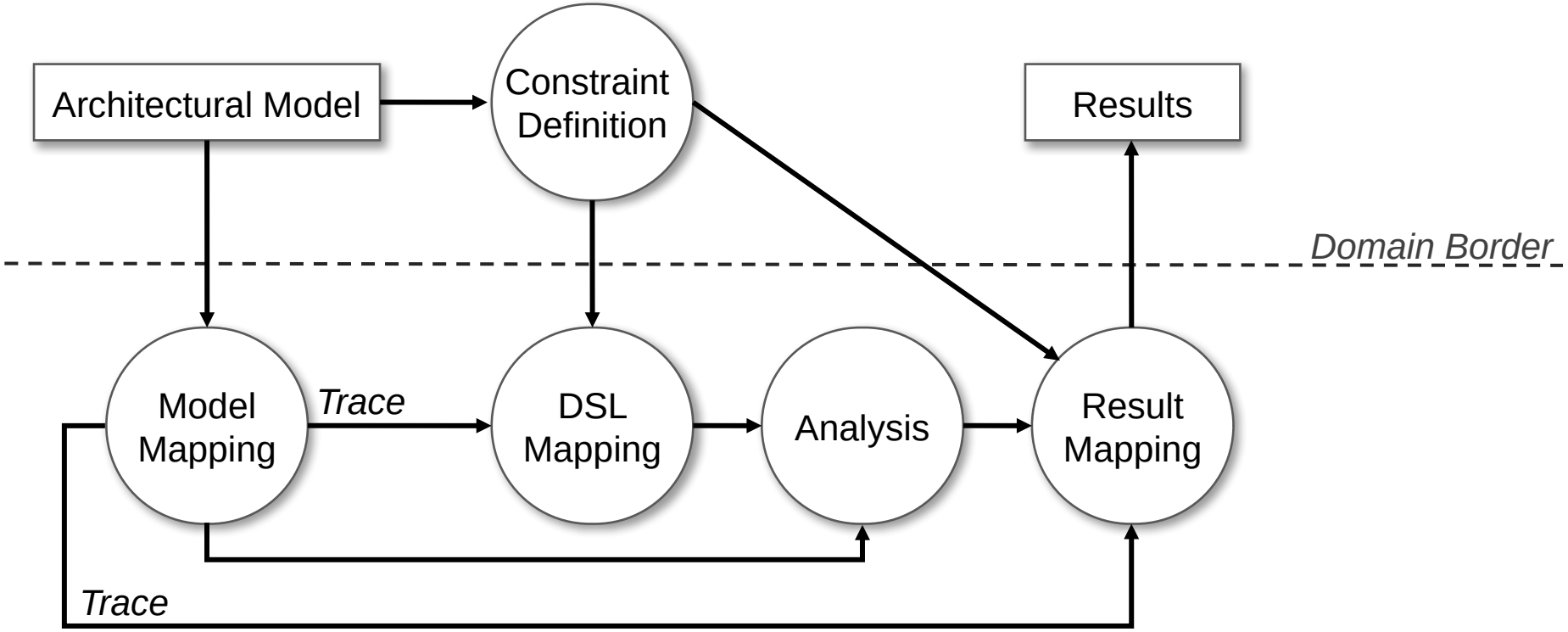
Bridging the Abstraction Gap



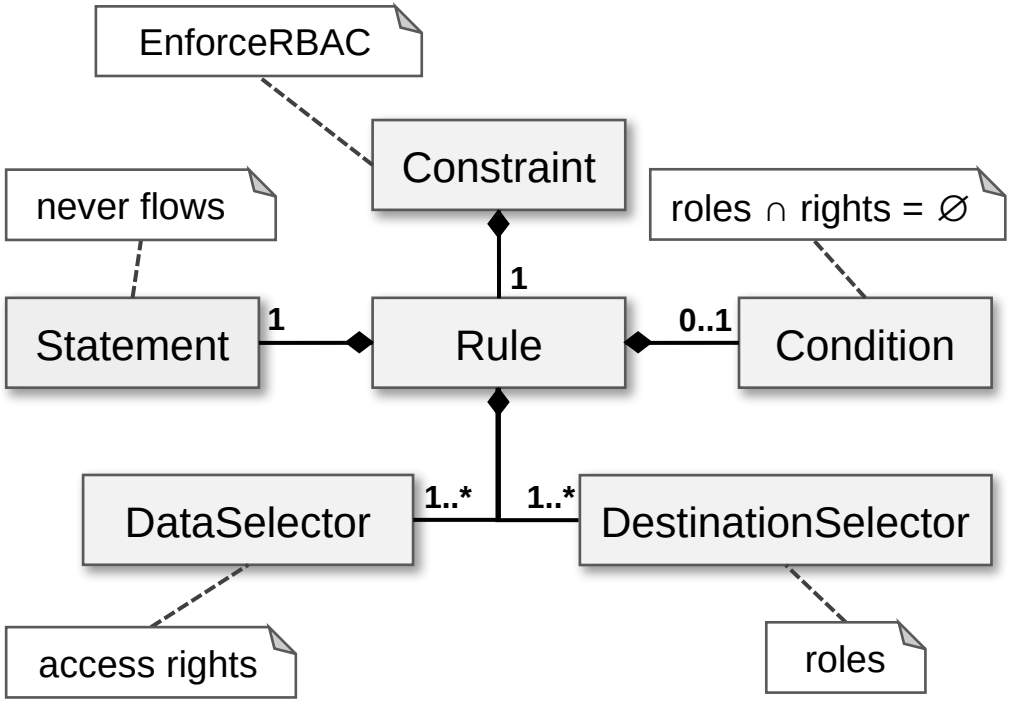
Bridging the Abstraction Gap



Bridging the Abstraction Gap

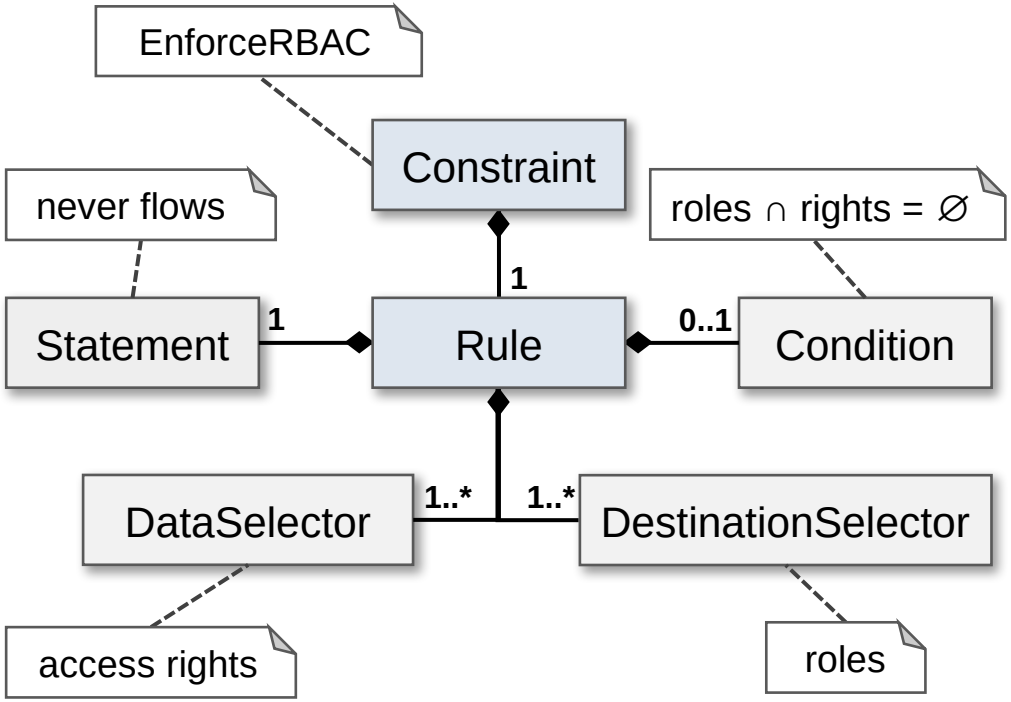


Representing RBAC by the Constraint DSL



Constraint: *„Data is only allowed to flow to components with authorized roles“*

Representing RBAC by the Constraint DSL



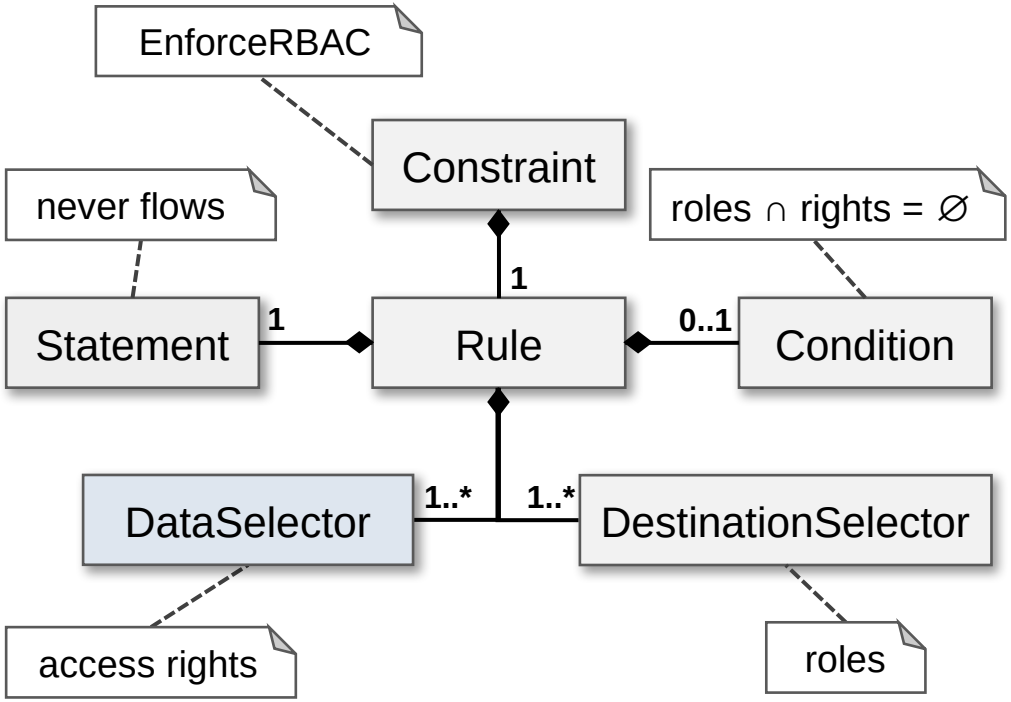
***Constraint**: „Data is only allowed to flow to components with authorized roles“*

```
constraint EnforceRBAC {



}
```

Representing RBAC by the Constraint DSL



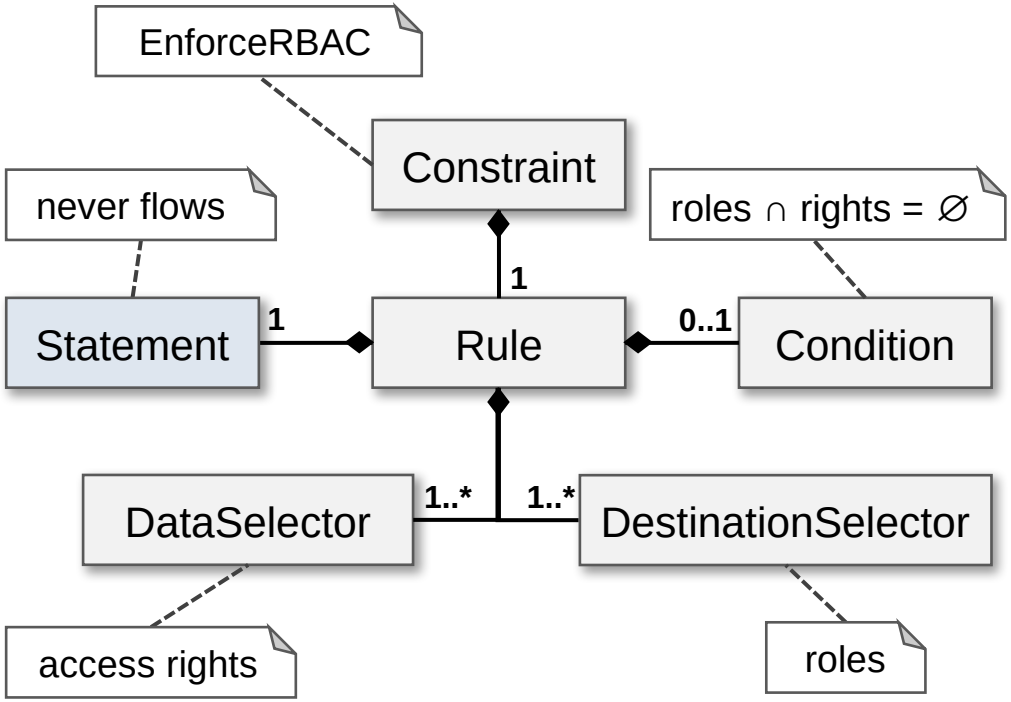
Constraint: *„Data is only allowed to flow to components with authorized roles“*

```
constraint EnforceRBAC {
 data.attribute.GrantedRoles.$rights{}



}
```

Representing RBAC by the Constraint DSL



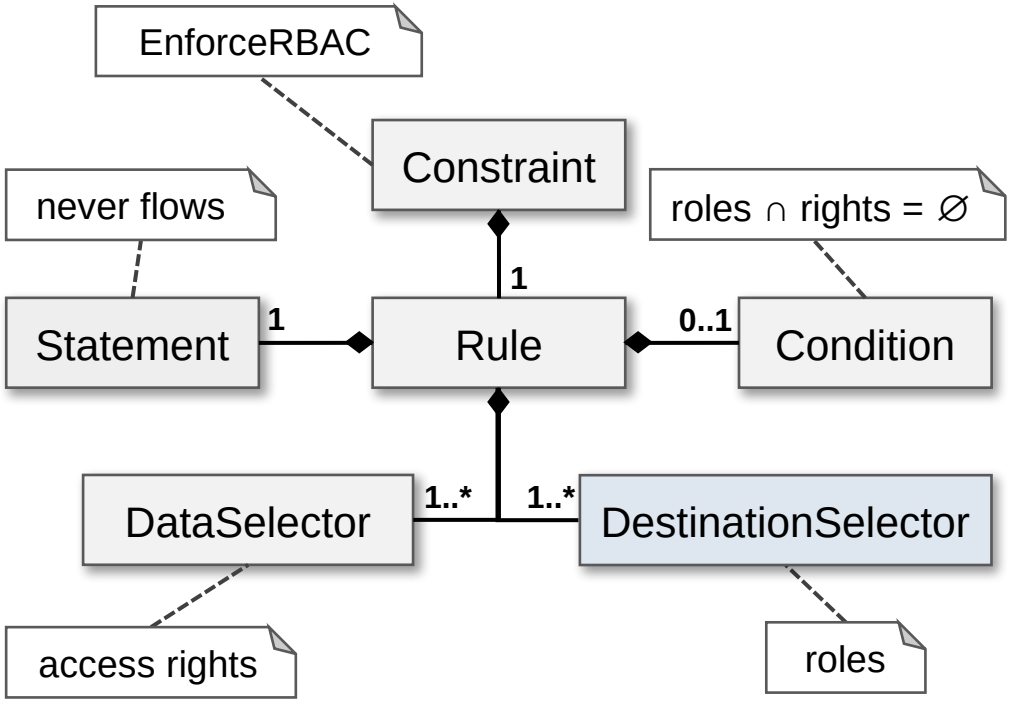
***Constraint**: „Data is only allowed to flow to components with authorized roles“*

```
constraint EnforceRBAC {
 data.attribute.GrantedRoles.$rights{}
   NEVER FLOWS



}
```

Representing RBAC by the Constraint DSL

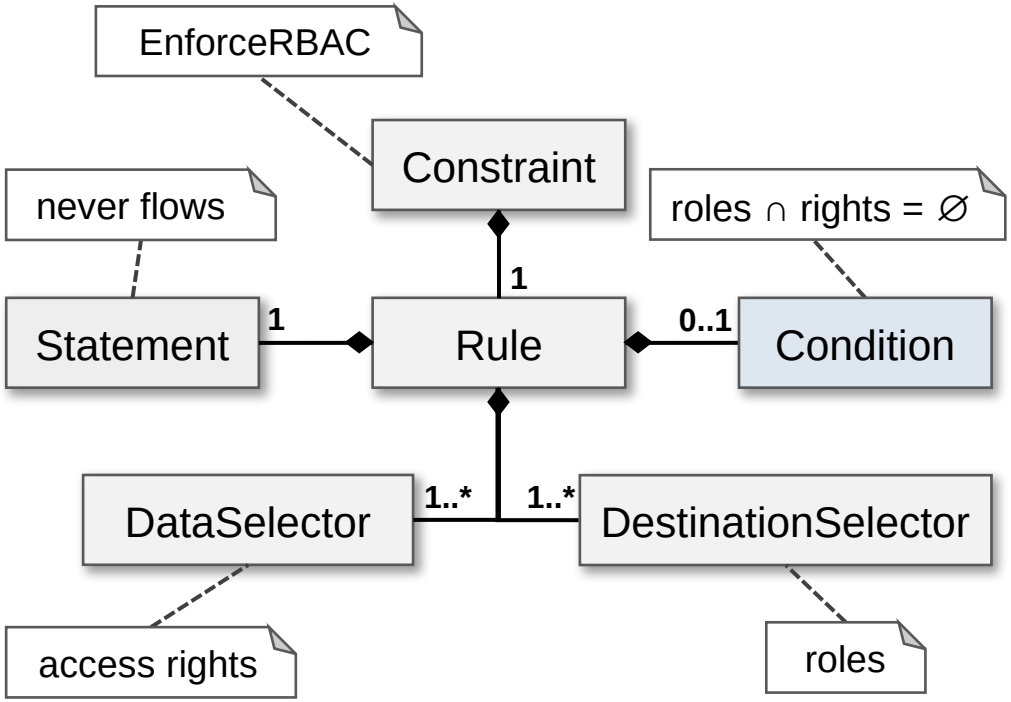


***Constraint**: „Data is only allowed to flow to components with authorized roles“*

```
constraint EnforceRBAC {
 data.attribute.GrantedRoles.$rights{}
   NEVER FLOWS
 component.property.AssignedRoles.$roles{}


}
```

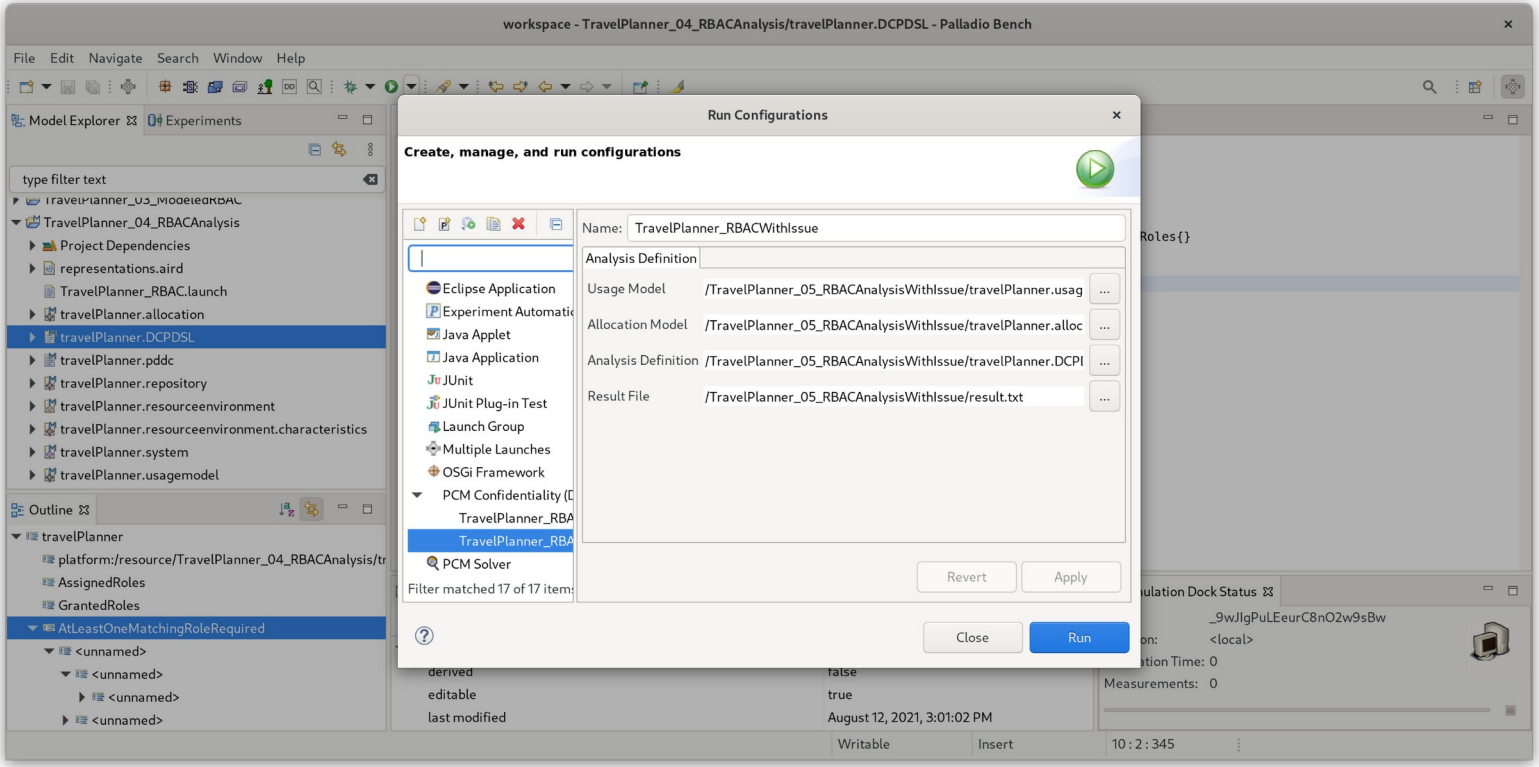
Representing RBAC by the Constraint DSL



***Constraint**: „Data is only allowed to flow to components with authorized roles“*

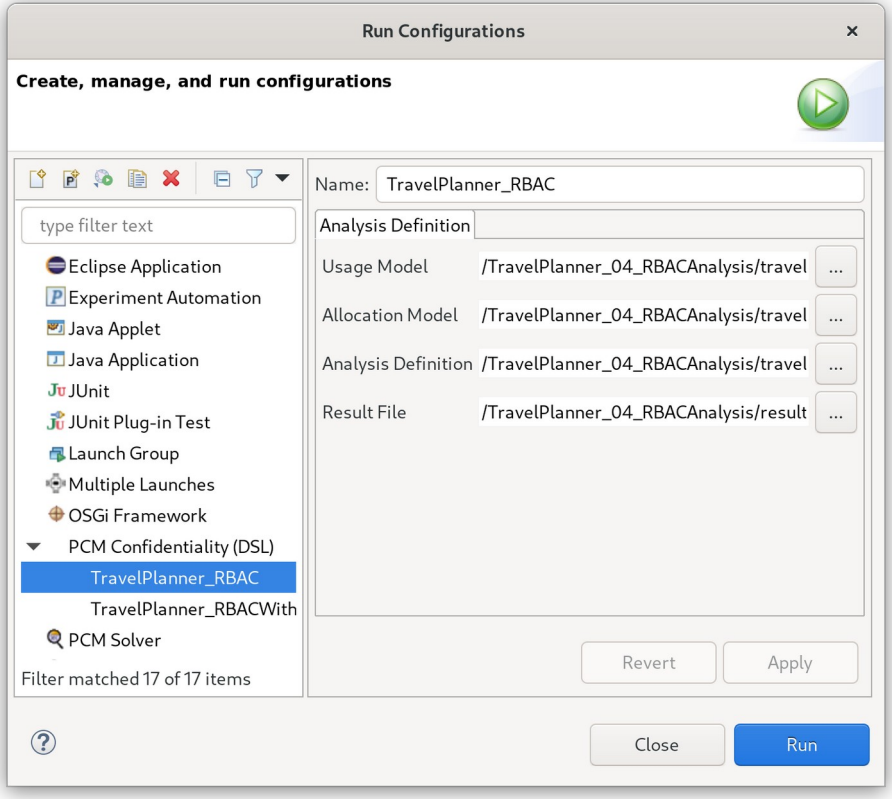
```
constraint EnforceRBAC {
 data.attribute.GrantedRoles.$rights{}
   NEVER FLOWS
 component.property.AssignedRoles.$roles{}
   WHERE
 isEmpty(intersection(rights,roles))
}
```

Live Demonstration of Analysis



Overview on Analysis Task

- Run the predefined RBAC analysis on the TravelPlanner system
  - with an issue (project 04)
  - without an issue (project 05)
- Follow the provided instructions
  - Create and run a new launch configuration for project 04
  - Run the configuration for project 05
  - Have a look at the results

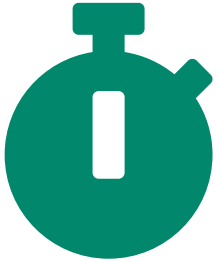


Resources for Analysis Task

Palladio Tooling

Task Instructions

Cheat Sheet



10 min

bit.ly/2U1ZffR

Conclusion of Tutorial

Stephan Seifermann, Maximilian Walter, Sebastian Hahner, Robert Heinrich, Ralf Reussner

Summary

- Many confidentiality analyses can be expressed by label propagation
  - Overview on information flow and access control analyses
  - In-depth: Role-based Access Control (RBAC)
- Palladio is capable of representing and analyzing confidentiality
  - Flexible analysis framework based on characteristics representing labels
  - Tool support in modeling as well as creating and executing analyses
  - Underlying analysis formalism hidden from users

Future Work

- Conceptual
  - Consideration of dynamically changing execution contexts [Boltz2020]
  - Consideration of uncertainty in design decisions and policies [Hahner2021b]
- Tooling
  - Full modeling and analysis support in UI
  - Integration in Palladio mainline development process

[Boltz2020] Context-Based Confidentiality Analysis for Industrial IoT. SEAA'20, p. 589–596.
[Hahner2021b] Architectural access control policy refinement and verification under uncertainty. ECSA'21 DocSym, accepted.

User Survey

- Short survey on aspects affecting possible future use of approach
- 9 questions, 10-15 minutes
- Anonymous but raw data will be (most probably) published

bit.ly/3n4an8c

15 min

Feedback

bit.ly/3nbWDIv

5 min

Follow Up Pointers

User Survey
Open til September, 19th

bit.ly/3n4an8c

Doctoral Symposium
Tuesday, 16:30

Architectural Access Control Policy Refinement and Verification under Uncertainty

by Sebastian

Fluid Trust Project

bit.ly/2WYT9hi

References

- **[Assal2018]**
  Assal and Chiasson: Security in the Software Development Lifecycle, SOUPS’18, pp. 281-296, 2018.
- **[Assal2019]**
  Assal and Chiasson: 'Think secure from the beginning': A Survey with Software Developers, CHI’19, pp. 1-13, 2019.
- **[Davis2013]**
  Davis et al.: Study on the Barriers to the Industrial Adoption of Formal Methods, FMICS’13, pp. 63-77, 2013.
- **[Garavel2020]**
  Garavel et al.: The 2020 Expert Survey on Formal Methods, FMICS’20, pp. 3-69, 2020.

References

- **[Kuhn2017]**
  Kuhn et al.: It Doesn’t Have to Be Like This: Cybersecurity Vulnerability Trends, IT Professional 19(6), pp. 66-70, 2017.
- **[McGraw2006]**
  McGraw: Software Security - Building Security In, Addison-Wesley, 2006.
- **[Shull2002]**
  Shull et al.: What we have learned about fighting defects, METRIC’02, pp. 249-258, 2002.
- **[vanDenBerghe2017]**
  van den Berghe et al.: Design notations for secure software: a systematic literature review, SoSym 16(3), pp. 809-831, 2017.