Trust 4.0: Dataflow-based Trust Modelling and Analysis in Industry 4.0 Systems

Spiros Alexakis (CAS Software AG), Stephan Seifermann (Karlsruhe Institute of Technology)
Fachgruppentreffen GI Architekturen 2019
Trust in Industry 4.0

Supply chains in Industry 4.0 are distributed and complex
- Many participants acting in various roles
- Many information exchanged between participants
- Information exchange vital for production

Trust required between participants
- No confidential information must be shared
- Participants only allowed to see necessary information

Situations might change rapidly
- Information sharing depending on geographical location
- Information sharing required by exceptional events

Introduction ➤ Running Example ➤ Modeling and Analyses ➤ Runtime Enforcement ➤ Conclusion
Project Trust 4.0

**KIT**
- Architectural Data Flow Modeling and Analysis

**CUNI**
- Runtime Access Control Modeling and Analysis

**CAS**
- Requirements
- Privacy-aware decision making

**IMA**
- Requirements
- Privacy-aware sensor gateway

Running Example

Introduction  ➤ Running Example  ➤ Modeling and Analyses  ➤ Runtime Enforcement  ➤ Conclusion
## Running Example

### Concepts

- **Employee’s Homes**
- **Factory Waiting Area**
- **Factory Workplace**

### Running Example

#### Factory Workplace

<table>
<thead>
<tr>
<th>Shift</th>
<th>Start</th>
<th>End</th>
<th>Supervisor</th>
<th>Workers</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROD13</td>
<td>09:00</td>
<td>17:00</td>
<td>Susan</td>
<td>Werner, Winfried</td>
</tr>
</tbody>
</table>

#### 20 min before

#### 5 min before

---

**Introduction** ➔ **Running Example** ➔ **Modeling and Analyses** ➔ **Runtime Enforcement** ➔ **Conclusion**
Running Example

Scenario

<table>
<thead>
<tr>
<th>Shift</th>
<th>Start</th>
<th>End</th>
<th>Supervisor</th>
<th>Workers</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROD13</td>
<td>09:00</td>
<td>17:00</td>
<td>Susan</td>
<td>Werner, Winfried</td>
</tr>
</tbody>
</table>

Employee’s Homes  Factory Waiting Area  Factory Workplace

Running Example

Runtime Enforcement

Conclusion
Running Example

Scenario

<table>
<thead>
<tr>
<th>Employee’s Homes</th>
<th>Factory Waiting Area</th>
<th>Factory Workplace</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Employee’s Homes Image" /></td>
<td><img src="image2.png" alt="Factory Waiting Area Image" /></td>
<td><img src="image3.png" alt="Factory Workplace Image" /></td>
</tr>
</tbody>
</table>

### Shifts

<table>
<thead>
<tr>
<th>Shift</th>
<th>Start</th>
<th>End</th>
<th>Supervisor</th>
<th>Workers</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROD13</td>
<td>09:00</td>
<td>17:00</td>
<td>Susan</td>
<td>Werner, Winfried</td>
</tr>
</tbody>
</table>

---

**Introduction**

- Trust 4.0: Dataflow-based Trust Modelling and Analysis in Industry 4.0 Systems
  - Spiros Alexakis, Stephan Seifermann

**Running Example**

**Modeling and Analyses**

**Runtime Enforcement**

**Conclusion**

Software Design and Quality Group

Institute for Program Structures and Data Organization
Running Example

Scenario

<table>
<thead>
<tr>
<th>Employee’s Homes</th>
<th>Factory Waiting Area</th>
<th>Factory Workplace</th>
</tr>
</thead>
</table>

**Shift** | **Start** | **End** | **Supervisor** | **Workers**
---|---|---|---|---
PROD13 | 09:00 | 17:00 | Susan | Werner Winfried

Contact him
Running Example

Scenario

| Employee’s Homes | Factory Waiting Area | Factory Workplace |

<table>
<thead>
<tr>
<th>Shift</th>
<th>Start</th>
<th>End</th>
<th>Supervisor</th>
<th>Workers</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROD13</td>
<td>09:00</td>
<td>17:00</td>
<td>Susan</td>
<td>Werner Winfried</td>
</tr>
</tbody>
</table>

Introduction  ➤  Running Example  ➤  Modeling and Analyses  ➤  Runtime Enforcement  ➤  Conclusion
### Running Example

**Scenario**

<table>
<thead>
<tr>
<th>Location</th>
<th>Shift</th>
<th>Start</th>
<th>End</th>
<th>Supervisor</th>
<th>Workers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee’s Homes</td>
<td>PROD13</td>
<td>09:00</td>
<td>17:00</td>
<td>Susan</td>
<td>Werner</td>
</tr>
<tr>
<td>Factory Waiting Area</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Winfried</td>
</tr>
<tr>
<td>Factory Workplace</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Factory Office</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Runtime Enforcement**

**Conclusion**
Running Example
Security Constraints

Assets
- Locations in factory
- Data about workers

Physical Constraints
- Only workers assigned to shift can access factory 25 min before shift
- Only workers assigned to shift can access workplace 8 min before shift

Virtual Constraints
- Supervisor cannot access personal data of workers
- Supervisor cannot access sensitive personal data of late workers
Trust 4.0 Approach
Overview

Introduction | Running Example | Modeling and Analyses | Runtime Enforcement | Conclusion

14.06.2019
Trust 4.0: Dataflow-based Trust Modelling and Analysis in Industry 4.0 Systems
Spiros Alexakis, Stephan Seifermann

Software Architect

Data Flow Analysis

Sensitivity of Data

Decision Making

Dynamic Policies

Solver

Static Policies

Industry 4.0 System

Context Information

Industry 4.0 Sensors

Software Architecture

Modeling and Analyses
Data Flow Analysis
Overview

Analysis Goals

Architecture → Extended Architecture → Analysis Model → Logic Program → Results

PCM Instance → Data-Centric PCM Instance → Operations Model → Prolog Program → Query Result

Introduction → Running Example → Modeling and Analyses → Runtime Enforcement → Conclusion
Data Flow Analysis
Modeling and Analysis

Worker

WorkerLocation

WorkerLocations

privacy = min(input.privacy, OFFICIAL)

project

: WorkerLocation

privacy = SENSITIVE

filter

WorkerLocation[]

Location

calcDist

WorkerLocation

Distance

privacy = SENSITIVE

input

project

: WorkerLocation

privacy = OFFICIAL

filter

WorkerId

WorkerId

的距离

Workplaces

privacy = OFFICIAL

Distance

privacy = OFFICIAL

Workplaces

Location

Distance

privacy = min(input.privacy, OFFICIAL)

Introduction  ➸ Running Example  ➸ Modeling and Analyses  ➸ Runtime Enforcement  ➸ Conclusion
# Data Flow Analysis

## Results

<table>
<thead>
<tr>
<th>DataId</th>
<th>DataType</th>
<th>PrivacyLevel</th>
<th>EntryPoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>WorkerLocation</td>
<td>SENSITIVE</td>
<td>Worker UC1</td>
</tr>
<tr>
<td>1</td>
<td>WorkerId</td>
<td>NONE</td>
<td>Supervisor UC2</td>
</tr>
<tr>
<td>2</td>
<td>WorkerLocation</td>
<td>SENSITIVE</td>
<td>Supervisor UC2</td>
</tr>
<tr>
<td>3</td>
<td>Location</td>
<td>SENSITIVE</td>
<td>Supervisor UC2</td>
</tr>
<tr>
<td>4</td>
<td>Distance</td>
<td>OFFICIAL</td>
<td>Supervisor UC2</td>
</tr>
</tbody>
</table>

...
Dynamic Policies
Overview

Introduction ➔ Running Example ➔ **Modeling and Analyses** ➔ Runtime Enforcement ➔ Conclusion

- **Entities**
  - Privacy Levels
    - **Ensembles**
      - Definition
        - Optimized
          - Instantiation
            - Ensembles
              - Instances
                - Rule
                  - Filtering
                    - Applicable
                      - Rules

**Dynamic Policies Overview**

**Overview**

**Introduction**

**Running Example**

**Modeling and Analyses**

**Runtime Enforcement**

**Conclusion**

**Entities** ➔ Privacy Levels ➔ Ensembles ➔ Optimized ➔ Instantiation ➔ Ensembles ➔ Instances ➔ Rule ➔ Filtering ➔ Applicable ➔ Rules
Decision Making

- **Grants**
  
  allow(shift.foreman, "read.personalData.phoneNo", workersThatAreLate)
  allow(shift.foreman, "read.distanceToWorkPlace", workersThatAreLate)

- **Constraints**

  deny(shift.foreman, "read.personalData", workers, PrivacyLevel.ANY)
  deny(shift.foreman, "read.personalData", workersPotentiallyLate, PrivacyLevel.SENSITIVE)

- **Privacy Levels**

  - Distance to work place, and phone number are official
  - Remaining personal data of worker (e.g. date of birth) is private

---

Introduction  
Running Example  
Modeling and Analyses  
Runtime Enforcement  
Conclusion
Trust 4.0-enabled enforcement architecture

Introduction  ➔  Running Example  ➔  Modeling and Analyses  ➔  Runtime Enforcement  ➔  Conclusion

14.06.2019  Trust 4.0: Dataflow-based Trust Modelling and Analysis in Industry 4.0 Systems  
Spiros Alexakis, Stephan Seifermann

Software Design and Quality Group  
Institute for Program Structures and Data Organization

Trust 4.0

- enabled enforcement architecture

Running Example

Modeling and Analyses

Conclusion

Runtime Enforcement

Introduction

WeShare

Trust 4.0 Models

TACM 4.0

CAS Open instance

IoT platform

CAS SmartAia

IMA Sensors

Factory

MQTT  OPC-UA

WeSpaces

CAS OpenSync

Open synchronisation

IMA

Enerchart

WeShare

Trust 4.0 Models

TACM 4.0

CAS Open instance

IoT platform

CAS SmartAia

IMA Sensors

Factory

MQTT  OPC-UA
WeShare for supply chains

Introduction ➔ Running Example ➔ Modeling and Analyses ➔ Runtime Enforcement ➔ Conclusion
Privacy-oriented IoT data transfer (internal view)
Privacy-oriented IoT data transfer (restricted view)
Enerchart Charts based on restricted view

Introduction  Running Example  Modeling and Analyses  Runtime Enforcement  Conclusion
Incorporating trust in Industry 4.0 is challenging
- Rapid changes require reactions
- Complex communication patterns make policies complex

Trust 4.0 supports aspect of access control
- Define bottom line security policies
- Define runtime policies considering context
- Evaluate policies on context changes

Future Work
- Evaluation in industrial context
- Consideration of unforeseen context changes
Introduction: Factory, user with Shield, sync

Running Example: Lock (open/closed)

Dynamic Policies: Sync

Conclusion: Factory, shield, fast forward
Image References
Approach Overview

- Icons made by Freepik (https://www.freepik.com) from Flaticon (https://www.flaticon.com) are licensed by CC 3.0 BY
  - Compasses, Speedometer, Numbering Icons

- Icons made by Dave Gandy (https://www.flaticon.com/authors/dave-gandy) from Flaticon (https://www.flaticon.com) are licensed by CC 3.0 BY
  - Cog Wheels Icon

- Icons made by Icongeek26 (https://www.flaticon.com/authors/icongeek26 from Flaticon (https://www.flaticon.com) are licensed by CC 3.0 BY
  - Clipboard Icons