Karlsruhe Institute of Technology

FluidTrust
Trust by fluid access control in Industry 4.0

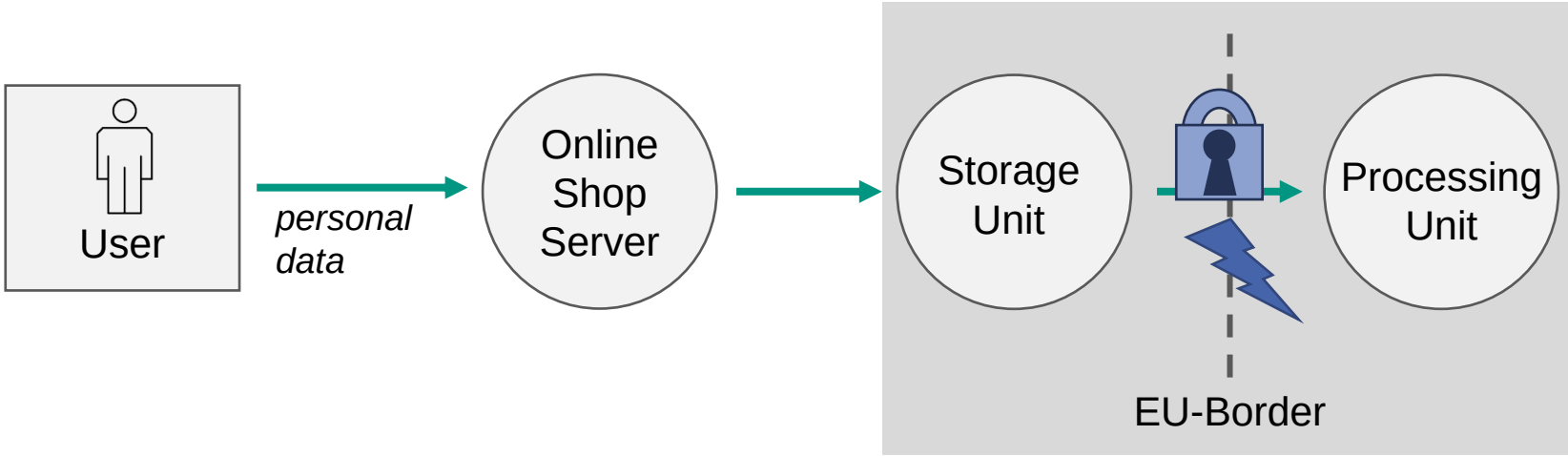
Dealing with Uncertainty in Architectural Confidentiality Analysis

Sebastian Hahner

Motivation

*Dealing with Uncertainty in **Architectural Confidentiality Analysis***

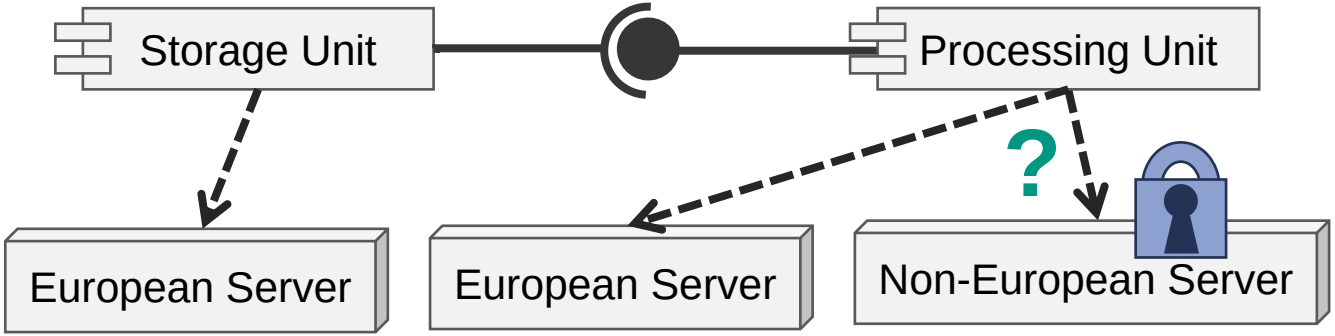
- Data flow-based architectural confidentiality analysis
  e.g., Personal Data is only allowed to be stored and processed on European servers or servers with “an adequate level of protection” (GDPR, Art. 45)



Motivation

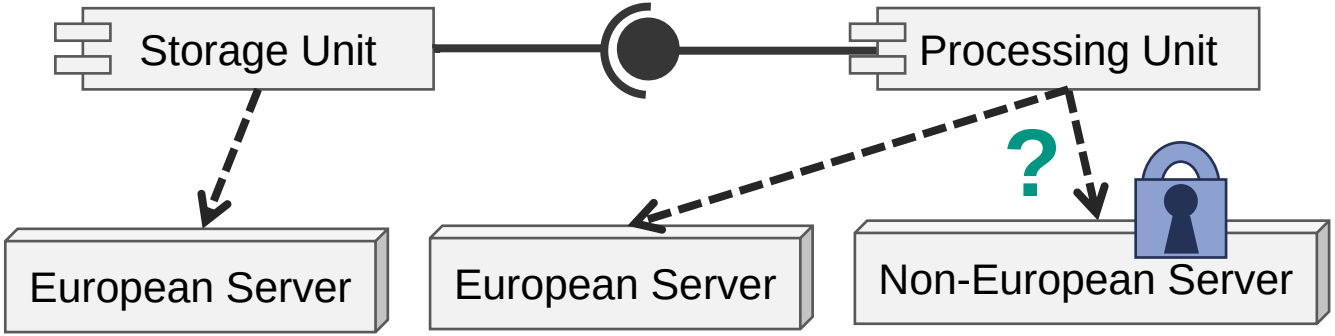
Dealing with Uncertainty *in Architectural Confidentiality Analysis*

- Uncertainty: “any departure from the unachievable ideal of complete determinism” (Walker03)



Challenges

C1: Understanding the relation of uncertainty and confidentiality
C2: Considering uncertainty in architectural modeling
C3: Uncertainty-aware confidentiality analysis



C1: Understanding the relation of uncertainty and confidentiality

Question:

How to systematically examine the impact of ***uncertainty*** and its relation to ***access control policies*** and ***confidentiality***?

Idea:

- Evaluate architectural design decisions
- Reuse existing uncertainty classifications (PerezPalacin14, Bures20)
  - Nature: Epistemic (i.e., lack of knowledge) or aleatory (i.e., randomness)
  - Level: Knowledge, Lack of knowledge, lack of awareness, lack of process
  - Source: Structure, behavior, or environment

C2: Considering uncertainty in architectural modeling

Question:

How to ***refine*** higher-level confidentiality requirements to lower-level access control policies while considering ***uncertainty***?

Idea:

- Include the solutions to **C1** into architectural modeling
- Explicitly model uncertainty, design decisions and assumptions to enable (re-) evaluation, e.g., based on existing ADLs (Reussner16)
- Define refinement process to derive access control policies based on the architectural model and the software architect's input

C3: Uncertainty-aware confidentiality analysis

Question:

How to ***verify*** refined access control policies against modeled architectures by using ***data flow-based confidentiality analyses***?

Idea:

- Include the solutions to **C2** into the verification process
- Combine and process uncertainty which was identified in the refinement
- Adapt existing confidentiality analyses (Seifermann19)
- In the case of confidentiality violations, use the verification results to further refine the derived access control policies

Herausforderungen und Fragestellungen

C1: Verstehen der Beziehung von Ungewissheit und Vertraulichkeit
C2: Ungewissheit in der architekturellen Modellierung berücksichtigen
C3: Vertraulichkeitsanalysen unter Berücksichtigung von Ungewissheit

Fragestellungen zur Diskussion

1. Welche weitere Herausforderungen gibt es zur Behandlung von Ungewissheit in architekturellen Vertraulichkeits-Analysen?
2. Sind die genannten Herausforderungen überhaupt zutreffend?
3. Mit welchen Ansätzen könnte man generell der Ungewissheit in architekturellen Vertraulichkeits-Analysen begegnen?
4. Wie und basierend auf welchen Eingaben können konkrete Zugriffsrichtlinien aus abstrakten Schutzzielen unter Berücksichtigung von Ungewissheit abgeleitet werden?
5. Wie könnte ein Prozess für die (semi-) automatische / manuelle / tool-gestützte Verfeinerung aussehen?

Sources

- **GDPR, Art. 45**: Council of European Union, *“REGULATION (EU) 2016/679 (General Data Protection Regulation)”,* 2016. https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04 (accessed Jan. 19, 2021).

- **Walker03**: W. E. Walker et al., *“Defining uncertainty: a conceptual basis for uncertainty management in model-based decision support”,* Integrated assessment, vol. 4, no. 1, pp. 5–17, 2003.
- **PerezPalacin14**: D. Perez-Palacin and R. Mirandola, *“Uncertainties in the modeling of self-adaptive systems: a taxonomy and an example of availability evaluation”,* in Proceedings of the 5th ACM/SPEC international conference on Performance engineering, New York, NY, USA, Mar. 2014, pp. 3–14
- **Bures20**: T. Bures, P. Hnetynka, R. Heinrich, S. Seifermann, and M. Walter, *“Capturing Dynamicity and Uncertainty in Security and Trust via Situational Patterns”,* in Leveraging Applications of Formal Methods, Verification and Validation: Engineering Principles, Cham, 2020, pp. 295–310, doi: 10.1007/978-3-030-61470-6_18.

- **Reussner16**: R. H. Reussner et al., *Modeling and Simulating Software Architectures: The Palladio Approach*. The MIT Press, 2016.
- **Seifermann19**: S. Seifermann, R. Heinrich, and R. Reussner, *“Data-Driven Software Architecture for Analyzing Confidentiality”,* in 2019 IEEE International Conference on Software Architecture (ICSA), Hamburg, Germany, Mar. 2019, pp. 1–10, doi: 10.1109/ICSA.2019.00009.

Karlsruhe Institute of Technology

FluidTrust
Trust by fluid access control in Industry 4.0

Dealing with Uncertainty in Architectural Confidentiality Analysis

Ergebnisse der Diskussion

Weitere Herausforderungen

- Ungewissheit erkennen (und Umgang mit nicht erkannter Ungewissheit)
- Ungewissheit klassifizieren, kategorisieren, abschätzen, quantifizieren
  - Ungewissheiten nach Größe & schwere der Auswirkungen ordnen
  - Ungewissheit aus Mangel an Kompetenz vs. Mangel an Information
  - Sinnvolle Wertebereiche verwenden, Prozent z.B. oft nicht sinnvoll
- Variabilitätsraum (Dimensionen und Stärke von Änderungen) identifizieren
- Ergebnisraum (z.B. Annahmen, Entscheidungen) definieren
- Passende Abstraktionsebene für sinnvolle Analysen finden
- Qualitative vs. Quantitative Analysen
- Generalisierbarkeit von Lösungen

Offene Probleme mit Herausforderungen

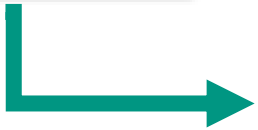
- Mehr Präzision bei vorhanden Herausforderungen notwendig
- Ungewissheit (und ihre Dimensionen) muss sauber definiert werden
- Wo findet der Prozess statt? Vor/Mit/Nach Modellierung?
  Auch im Bezug auf Prozessmodelle, z.B. iterativ oder Wasserfallmodell
- Warum die identifizierte Ungewissheit nicht sofort beheben?
- Bringt der Ansatz genug Vorteile um den Aufwand zu rechtfertigen?
- Ist Ungewissheit im Kontext von Vertraulichkeit etwas
  besonderes oder sollte es eher allgemeiner betrachtet werden?
- Verwandt: “SeeMe”-Modellierung, “UMLsec change”

Ableitung von Zugriffsrichtlinien

Wie?
- Dekomposition
- Expertensystem
- Ansätze aus der Variabilitätsforschung und Probabilistic Model Checking

Auch bedenken:
- Traceability
  - Schutzziel ⇨ Richtlinie
  - Anfrage ⇨ Richtlinie
  - Welche Rollen, Daten?

Abstraktes Schutzziel



Zugriffskontrollmodell z.B. RBAC, ABAC

Was (von was, zu was)?
- Von Regularien
  - Gesetztestexte
  - Organisationsrichtlinien
  - …
- Design- und Architekturelemente

Weitere Bewertungskriterien von Ungewissheit

- Ungewissheit in System vs. Ungewissheit des Modellierers
- Ungewissheit aus Mangel an Kompetenz vs. Mangel an Information
- Schwere der Auswirkungen bzw. vorhandenes Risiko
- Einschätzung der Gewissheit in Annahmen bzw. Entscheidungen durch Modellierer
- Unterscheidung zwischen fixen Werten, Bereichen, gar keinem Wissen?
- Wie sicher ist die Eintrittswahrscheinlichkeit?
- Wie zukunftstauglich sind Entscheidungen?
- Wort-Case, Best-Case Annahmen
- Zeitpunkt der Entscheidung: Entwurfszeit, Deployment, Laufzeit
- Ziele der Vertraulichkeitsmodellierung? (z.B. Vertraulichkeit)

⇨ Vorhandene Klassifikationen ggf. nicht ausreichend

⇨ Was ist zielführend zu dokumentieren bzw. zu modellieren?
(Pragmatischer Ansatz: Was nicht hilft, wird nicht klassifiziert & dokumentiert)

Weitere Überlegungen

- Cone of Uncertainty
- Agile Verfahren
  - Ungewissheit muss explizit gemacht werden und dann entschieden basierend auf Zielvorstellungen
  - Benennung aller Ungewissheiten & Potenzial.
  - Last Responsible Moment. Entscheidungen z.B. durch Parameter und Weichen in die Laufzeit verschieben (⇨ adaptive / dynamische Richtlinien)
- Eindrücke aus der Praxis:
  - Tool-gestützt nicht anwendbar, eher z.B. Checkliste oder Guidelines ⇨ Lösung muss leichtgewichtig sein
  - Data Catalog: Scannen von existierenden Systemen / Finden bzw. Monitoren von Datenflüssen (Nur für grob-granulare Analysen über Systemgrenzen hinweg geeignet)