Dealing with Uncertainty in Architectural Confidentiality Analysis[1]

Sebastian Hahner[2]

Abstract: In a connected world, confidentiality becomes increasingly critical. To cope with confidentiality on a higher abstraction level of software systems, architectural analyses have been proposed. By explicitly modeling data in the system design, the validity of access control policies can be ensured. However, the required information for such analyses is often too imprecise due to the high degree of uncertainty at design-time which results in incomplete and inaccurate policies. In this paper, we describe three key challenges while facing uncertainty and show how software architects could be supported in enhancing confidentiality throughout software design and evolution.

Keywords: Software Architecture; Confidentiality; Access Control; Uncertainty

1 Introduction

With the increasing system connectivity and the growing volume of data, confidentiality has become a crucial quality property of software systems [SHR19]. Confidentiality demands that “information is not made available or disclosed to unauthorized individuals, entities, or processes” [In18]. As implied by *Privacy by Design*, the overall design of a trusted software system should consider confidentiality early and “minimize the amount of personal data processed” [Sc10]. Architectural confidentiality analyses enable architects to evaluate the flow of data by annotating the software architecture [Ka13; Pe19] and to define data flow constraints [Ha20; SHR19] which can be realized using access control policies.

However, details about such policies are usually not specified in the architectural abstraction but added during policy refinement. Here, the high degree of uncertainty regarding the structure, behavior, and usage of the software does not allow one to draw precise conclusions on the confidentiality of the overall system. Cheng et al. [Ch07] explain this problem with unforeseeable tradeoffs while defining policies. Strict policies may reduce the risk of data breaches but may harm the flexibility of software systems, especially in highly dynamic environments like implied by Industry 4.0 [Bu20].

To enable a more comprehensive analysis of confidentiality, uncertainty has to be actively managed in definition and refinement of access control policies. One approach is the

[1] This work is funded by the DFG (German Research Foundation) – project number 432576552, HE8596/1-1 (FluidTrust) and the KASTEL institutional funding.

[2] Karlsruhe Institute of Technology, Am Fasanengarten 5, 76131 Karlsruhe, Germany, sebastian.hahner@kit.edu

classification of uncertainty [Bu20; PM14; Wa03] that enables the modeling of the influence of uncertainty and may guide architects in making design decisions, assumptions and tradeoffs. Additionally, modeling uncertain influences and decisions may result in enhanced documentation which helps the traceability of erroneous assumptions and subsequent faults during software evolution [Re06]. Thus, explicitly relating high-level policies on architectural abstraction level to refined, low-level policies may ease the re-evaluation of changes to the system or its requirements. Last, including uncertainty into the design and refinement process of access control policies may increase the flexibility at runtime when facing unexpected context changes [Bu20].

We motivate this problem based on legal requirements as implied by the *European General Data Protection Regulation* (GDPR) which states that personal data of European citizens is only allowed to be stored and processed on European servers or on servers which ensure "an adequate level of protection" [Co16, Art. 45]. Fig. 1 shows two components which work with personal data. The *Storage Unit* is deployed on a *European Server* which satisfies the GDPR. However, it remains unclear where the *Processing Unit* gets deployed (as indicated by the question mark) which introduces uncertainty. If the *Non-European* gets chosen, an access control system might have to deny the processing of data from the *Storage Unit*.

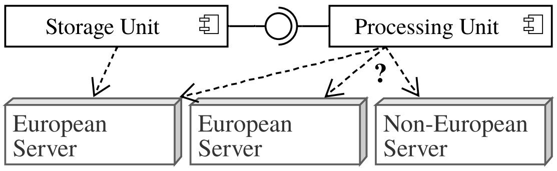

Fig. 1: Simple deployment diagram showing uncertainty

In this paper, we present three key challenges that we have identified regarding confidentiality analysis: The relation of uncertainty and confidentiality in software architectures (**C1**), the modeling of uncertainty while refining access control policies (**C2**) and their verification based on existing confidentiality analyses (**C3**). Our goal is to enhance the quality of policies by uncertainty-aware refinement and verification on architectural abstraction level. The current state of uncertainty classification is summarized in Sect. 2. After describing the three challenges in Sect. 3, we present our vision in Sect. 4. Sect. 5 concludes this paper.

2 Classifying Uncertainty

One approach to cope with uncertainty is its classification, which enables architects to deal with different kinds of uncertainty more accurately. Uncertainty in architectural decisions can be defined as "any departure from the unachievable ideal of complete determinism" [Wa03] and is strongly related to risk [In18]. In this section, we summarize the classifications regarding their relation to confidentiality and access control.

Walker et al. [Wa03] present a classification of uncertainty using three dimensions. The *location* describes where the uncertainty manifests itself, e.g., arising from imprecise model definitions or uncertainty on input parameters. The *level* states how much is known about the uncertain influence on a scale from determinism to total ignorance. Regarding the architectural design, tackling reducible uncertainty is considered to be expedient [Bu20]. The *nature* describes the distinction between epistemic and aleatoric uncertainty. While epistemic uncertainty arises due to imperfection of knowledge and may be reduced, aleatoric uncertainty is caused by natural variability from random events and cannot be further reduced. Other classifications describe the *source* of uncertainty [Ga10; PM14]. Regarding access control policies, these can be treated differently, e.g., sensor noise introduces a different kind of uncertainty than upcoming legal regulations. Bures et al. [Bu20] propose the sources *structure*, *behavior* and *environment* to better match the description of software architectures when reasoning about confidentiality and access control.

3 Challenges

In this section, we describe challenges in architectural confidentiality analysis regarding uncertainty in definition, refinement and verification of access control policies. We strive to understand the role of uncertainty and its management in architectural modeling and analysis. This is related to architectural decision making under uncertainty described by Lytra; Zdun [LZ13]. They name the challenges of supporting architects by resolving uncertainty, adapting to different architectural abstraction levels and providing (semi-)automated decision support.

C1: Understanding the relation of uncertainty and confidentiality In order to define uncertainty-aware access control policies which ensure confidentiality, the relation of uncertainty and confidentiality must be systematically examined. Based on existing classifications of uncertainty, architectural design decisions can be evaluated on their uncertainty characteristics and impact on confidentiality. This evaluation includes considering fine-grained levels of uncertainty, e.g., applying fuzzy logic to express partial knowledge when representing and refining policies [Ho92]. The solution to this challenge is considered to be non-trivial due to the versatility of uncertainty. In our motivating example, this uncertainty becomes visible as lack of knowledge regarding the deployment.

C2: Considering uncertainty in architectural modeling The second challenge considers uncertainty in the architectural modeling. Garlan [Ga10] names the challenge of including uncertainty as first-class entity into the design process. Defining a method to integrate the solution to challenge **C1** into the architectural modeling can be helpful to increase the quality of access control policies and to estimate confidentiality on a higher abstraction level. This includes explicitly modeling uncertain influences, e.g., based on existing architectural description languages [Re16] and defining a process for uncertainty-aware access control policy refinement. Handling the combination of uncertainty characteristics in regard to the wide-ranging design decisions is considered to be challenging. In absence of full determinism, every design decision contains assumptions. Not making these assumptions explicit cannot only harm system evolution, but also introduce new uncertainty due to decreasing model accuracy [EM13]. Modeling assumptions and decisions explicitly can reduce costly subsequent faults during the evolution of the system, its policies and its environment [Re16]. In our motivating example, we consider uncertainty regarding the deployment location and make the decision that the *Processing Unit* is either deployed on a *European Server* or a more restrictive access control policy is applied explicit.

C3: Uncertainty-aware confidentiality analysis The third challenge considers the verification of access control policies by using architectural confidentiality analyses. Current data flow-based approaches use annotated architectural models [Ka13; Pe19], e.g., by describing the characteristics of data sources, data sinks and data processing [SHR19]. It is currently unclear how existing approaches can be adapted to verify access control policies against modeled architectures with explicit uncertain parameters. A possible adaption might include combining and weighting multiple influences of uncertainty in modeling and analysis. One approach is to apply fuzzy methods, e.g., by using gradual permission or by delegating access decisions [Bu20]. In our motivating example, confidentiality analyses could help to evaluate under which conditions personal data of European citizens flows to the non-European server to verify the refined access control policy.

4 Vision

In this section, we discuss our vision on how to cope with the challenges described in Sect. 3. We propose to include uncertainty characteristics in architectural modeling and the definition of access control policies and also to extend existing confidentiality analyses. Please note, that this represents an early view and is subject to change in future work.

In order to face challenge **C1**, we propose to gather properties that affect access control policies systematically. This includes, but is not limited to, architectural design decisions. We aim to identify the impact of different aspects of uncertainty on confidentiality as shown in our motivating example. It is unlikely to obtain a comprehensive list due to the complexity of the domain of software architectures and the versatility of uncertainty. However, even the investigation of some aspects may help to guide architects throughout the design and evolution of software systems. It shall be examined whether existing classifications are applicable, e.g., the uncertainty sources in software architectures by Bures et al. [Bu20] or the uncertainty matrix by Walker et al. [Wa03].

To incorporate this knowledge in the architectural modeling and tackle challenge **C2**, we propose a defined refinement process. Starting with imprecise policies based on, e.g., legal requirements as shown in our motivating example, we plan to analyze affected architectural elements and design decisions. Afterwards, architects define policies which can be refined in regard to the architectural model. The resulting policies ensure confidentiality under given assumptions. In our motivating example, restrictive access control policies are only required under the assumption, that the *Non-European Server* is used.

To handle challenge **C3**, we propose to connect the previously described refinement to existing data flow analyses. Depending on the class and impact of uncertainty, it might be sufficient to analyze confidentiality for few, representative cases. Alternatively, we consider the use of fuzzy logic as proposed by Bures et al. [Bu20]. Fuzzy methods have been previously used both for privacy policies [Pl15] and access control [Ch07].

5 Conclusion

In this paper, we described three challenges regarding the consideration of confidentiality in design and evolution of software systems. These challenges evolve around the subject of uncertainty. We presented existing classifications of uncertainty and discussed their applicability in confidentiality analysis. Last, we discussed our planned approach which includes the refinement of higher-level access control policies and their verification based on architectural data flow analyses.

References

[Bu20] Bures, T.; Hnetynka, P.; Heinrich, R.; Seifermann, S.; Walter, M.: Capturing Dynamicity and Uncertainty in Security and Trust via Situational Patterns. In: Leveraging Applications of Formal Methods, Verification and Validation: Engineering Principles. Pp. 295–310, 2020.

[Ch07] Cheng, P.-C.; Rohatgi, P.; Keser, C.; Karger, P. A.; Wagner, G. M.; Reninger, A. S.: Fuzzy Multi-Level Security: An Experiment on Quantified Risk-Adaptive Access Control. In: 2007 IEEE Symposium on Security and Privacy (SP '07). Pp. 222–230, 2007.

[Co16] Council of European Union: REGULATION (EU) 2016/679 (General Data Protection Regulation), 2016.

[EM13] Esfahani, N.; Malek, S.: Uncertainty in Self-Adaptive Software Systems. In: Software Engineering for Self-Adaptive Systems II: International Seminar, Dagstuhl Castle, Germany, October 24-29, 2010 Revised Selected and Invited Papers. Pp. 214–238, 2013.

[Ga10] Garlan, D.: Software engineering in an uncertain world. In: Proceedings of the FSE/SDP workshop on Future of software engineering research - FoSER '10. the FSE/SDP workshop. P. 125, 2010.

[Ha20] Hahner, S.: Domain-specific Language for Data-driven Design Time Analyses and Result Mappings for Logic Programs, Master's Thesis, 2020.

[Ho92] Hosmer, H. H.: Using fuzzy logic to represent security policies in the multipolicy paradigm. ACM SIGSAC Review 10/4, pp. 12–21, 1992.

[In18] International Organization for Standardization: ISO/IEC 27000:2018(E) Information technology – Security techniques – Information security management systems – Overview and vocabulary, Standard, 2018.

[Ka13] Katkalov, K.; Stenzel, K.; Borek, M.; Reif, W.: Model-Driven Development of Information Flow-Secure Systems with IFlow. In: 2013 International Conference on Social Computing. Pp. 51–56, 2013.

[LZ13] Lytra, I.; Zdun, U.: Supporting architectural decision making for systems-of-systems design under uncertainty. In: Proceedings of the First International Workshop on Software Engineering for Systems-of-Systems. Pp. 43–46, 2, 2013.

[Pe19] Peldszus, S.; Tuma, K.; Struber, D.; Jurjens, J.; Scandariato, R.: Secure Data-Flow Compliance Checks between Models and Code Based on Automated Mappings. In. 2019 ACM/IEEE 22nd International Conference on Model Driven Engineering Languages and Systems (MODELS). Pp. 23–33, 2019.

[Pl15] Platenius, M. C.; Arifulina, S.; Petrlic, R.; Schäfer, W.: Matching of Incomplete Service Specifications Exemplified by Privacy Policy Matching. In: Advances in Service-Oriented and Cloud Computing. Pp. 6–17, 2015.

[PM14] Perez-Palacin, D.; Mirandola, R.: 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. Pp. 3–14, 2014.

[Re06] Refsgaard, J. C.; van der Sluijs, J. P.; Brown, J.; van der Keur, P.: A framework for dealing with uncertainty due to model structure error. Advances in Water Resources 29/11, pp. 1586–1597, 2006.

[Re16] Reussner, R. H.; Becker, S.; Happe, J.; Heinrich, R.; Koziolek, A.; Koziolek, H.; Kramer, M.; Krogmann, K.: Modeling and Simulating Software Architectures: The Palladio Approach. The MIT Press, 2016.

[Sc10] Schaar, P.: Privacy by design. Identity in the Information Society 3/2, Publisher: Springer, pp. 267–274, 2010.

[SHR19] Seifermann, S.; Heinrich, R.; Reussner, R.: Data-Driven Software Architecture for Analyzing Confidentiality. In: 2019 IEEE International Conference on Software Architecture (ICSA). Pp. 1–10, 2019.

[Wa03] Walker, W. E.; Harremoës, P.; Rotmans, J.; Van Der Sluijs, J. P.; Van Asselt, M. B.; Janssen, P.; Krayer von Krauss, M. P.: Defining uncertainty: a conceptual basis for uncertainty management in model-based decision support. Integrated assessment 4/1, Publisher: Taylor & Francis, pp. 5–17, 2003.