Can Inverse Transparency be Made Compatible With High Data Security Environments?

Bachelor's Thesis

Supervisor: Prof. Dr. Alexander Pretschner
Advisor: Valentin Zieglmeier
Email: {pretschn, zieglmev}@in.tum.de
Phone: +49 (89) 289 - 17834
Starting date: immediately

Informatik 4 – Lehrstuhl für Software und Systems Engineering
Prof. Dr. Alexander Pretschner
Fakultät für Informatik
Technische Universität München

Boltzmannstraße 3
85748 Garching bei München

https://www.in.tum.de/i04/

Context

Recent privacy legislation such as the GDPR and CCPA have lead to data owners becoming more self-sovereign in the handling of their data. Yet, these initiatives still do not lead to a true data sovereignty of individuals. Allowing access to data is still in many cases an "all-or-nothing" affair, with those trying to get access to the data having an information advantage. This is especially problematic in case of employee data, where an inherent power asymmetry and the necessity to use data for business processes reduces the choice of data owners to a minimum.

The concept of "Inverse Transparency" tries to improve upon the existing privacy protections of employees by giving data owners more sovereignty in how their data are used. Its core idea is to enable access to data on a more case-by-case basis, but to monitor all accesses and make those visible to data owners [1]. On the one hand, this can help to raise awareness of data usages and better protect the employee's personal data, on the other hand it may enable usages of data useful to teams and individuals alike.

Depending on the role of the data owner and the data that they produce and handle, different protection techniques are appropriate. Especially for defense contractors, some of the highest requirements for data security and protection exist. This raises an interesting question: Can Inverse Transparency be applied in these contexts? Which specific requirements towards data security and tamper-proofness arise? And is there potential to improve upon these already strict data security standards that exist there?

Goal

The goal of this thesis is to research the applicability of Inverse Transparency to environments with the highest data security requirements, specifically defense contractors. To that end, the student will work with a company partner (from here on "company A") from the defense industry to gather real-world requirements, conceptualize an implementation, and evaluate their solution.

To enable the application of the Inverse Transparency toolchain, the student will tackle one specific issue technically: Handling the different classification levels that data can inhibit [2, 3]. Different requirements towards data security can exist for individual data [4], for computers and networks [3], or for users [5].

The work will be structured into a theoretical, an implementation, and an evaluation phase.

Theoretical phase: Summarize and give an overview over the security requirements towards company A. Contrast with literature and compare to the published works regarding defense contractors around the world. If possible, include specific requirements of company A that go beyond what is given by their customers. Of specific interest is where the current approach of the Inverse Transparency toolchain [1] is insufficient to fulfill those security requirements.

Implementation phase: Extend the Inverse Transparency toolchain to match the security requirements derived from the theoretical phase. As storing highly classified data is subject to very strict regulations, a specific focus will lie on enabling different classification levels based on various properties of the data. Furthermore, developing a security and identity check for users accessing the data will be necessary to follow the "need-to-know" principle. Concretely, this means developing a module for the Overseer that allows for these classifications and identity checks before allowing access to the data and logging it. The concrete implementation can be adapted based on the findings from the theoretical phase.

Evaluation phase: Assess the quality of the developed solution in collaboration with experts from company A. This could mean presenting the solution to data privacy experts, conducting interviews with security experts, or holding workshops with regular employees subjected to the heightened security requirements. If the implemented tools are successfully integrated into the Inverse Transparency toolchain, potentially this could also include an evaluation of its applicability to the high-security work of company A.

Work Plan

1. Research related literature and real-world requirements from company A.
2. Implement an extension to the Inverse Transparency toolchain that enables heightened security requirements.
3. Evaluate the implementation with experts from company A.
4. Document the work in the thesis.

Deliverables

- Source code of the implementation.
- (Anonymized) transcripts of conducted interviews.
- Thesis written in conformance with LMU guidelines.

References

[1] Zieglmeier, Valentin, and Alexander Pretschner. "Trustworthy Transparency by Design." arXiv preprint arXiv:2103.10769 (2021). Available: https://arxiv.org/pdf/2103.10769

[2] Shirey, Robert W. "Defense Data Network Security Architecture." *ACM SIGCOMM Computer Communication Review* 20.2 (1990): 66-72. Available: https://dl.acm.org/doi/abs/10.1145/378570.378710

[3] Kuipers, David, and Mark Fabro. *Control systems cyber security: Defense in depth strategies*. No. INL/EXT-06-11478. Idaho National Laboratory (INL), 2006. Available: https://core.ac.uk/download/pdf/190361396.pdf

[4] Bundesministerium des Innern, für Bau und Heimat. Anlage III Verschlusssachenanweisung – Hinweise zur Einstufung. In: *Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA)*. Available: http://www.verwaltungsvorschriften-im-internet.de/BMI-OESII5-20180810-SF-A003.htm

[5] Bundesministerium der Justiz und für Verbraucherschutz. *Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen (Sicherheitsüberprüfungsgesetz - SÜG)* v. 20.04. 1994 (BGBl. I, S 867), zuletzt geändert durch Gesetz v. 18.07.2017 (BGBl. I, S 2732). Available: https://bmwi-sicherheitsforum.de/ghb/bibliothek/208,0,0,1,0.html