Tracking Jira Data Accesses through the Database Layer

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

Fakultät für Informatik
Lehrstuhl 4
Software & Systems Engineering
Prof. Dr. Alexander Pretschner

Boltzmannstraße 3
85748 Garching bei München

Tel: +49 (89) 289 - 17834
https://www4.in.tum.de

Context

The research project "Inverse Transparency" examines a new form of data privacy. In short, all data accesses are allowed, but accesses are logged and made visible to so-called data owners. We define a data owner roughly as either the person creating a datum, or the person a datum relates to in content. For example, a dossier written by Sally containing personal information about Frank is owned by both Sally and Frank.

We evaluate different approaches to tracking data accesses in a tamper-proof and persistent way. Different layers of the access are looked at, from analysis tools creating knowledge to the lower-level access.

Goal

This thesis looks at the tracking of data accesses through the database layer. We focus on the tool Jira Software[1] as well as the database system Microsoft SQL Server[2] to limit the scope, but the work should aim to be generalizable to other tools accessing the data stored in the database.

One possible approach would be to utilize database auditing. Database auditing means observing user actions in a database to ensure that only allowed actions are taken. SQL auditing is available multiple SQL database systems, among them Microsoft SQL Server[3] and PostgreSQL[4].

The work will comprise three steps: First, the feasibility of tracking data accesses through database auditing and other means is evaluated and compared with other means to track data accesses. Second, a proof-of-concept tool is implemented to programmatically create and update auditing rules, as well as extract tracked data accesses. Optionally, the solution may look into limiting possible data accesses while maintaining functionality of Jira Software. Finally, the implemented tool is to be evaluated regarding the functionality (Are all expected data accesses traceable? How does the coverage compare to higher-layer solutions?) as well as performance (execution time of queries, maximum frequency of information retrieval, ...).

Work Plan

1. Research and discuss the feasibility of tracking data accesses through database auditing.
2. Implement a tool to create and update audit rules.
3. Add functionality to extract tracked data accesses.
4. (Optional) Add functionality to limit possible data accesses at the database layer.
5. Evaluate the implementation.
6. Document of the work in the thesis.

Deliverables

- Source code of the implementation.
- Thesis written in conformance with TUM guidelines.

References

[1] Natan, Ron Ben. *Implementing database security and auditing*. Elsevier, 2005.

[2] Motwani, Rajeev, Shubha U. Nabar, and Dilys Thomas. "Auditing SQL queries." *Proc. of the 24th ICDE*. IEEE, 2008.

[3] Kaushik, Raghav, and Ravi Ramamurthy. "Efficient auditing for complex SQL queries." *Proc. of the 2011 SIGMOD*. ACM, 2011.

[1] https://www.atlassian.com/software/jira
[2] https://www.microsoft.com/sql-server
[3] https://docs.microsoft.com/sql/relational-databases/security/auditing
[4] https://www.pgaudit.org/