Short Abstract: A Survey on Log Audits that Detect Privacy Violations

Jenni Reuben, Leonardo A. Martucci, and Simone Fischer-Hübner*

Karlstad University
651 88 Karlstad, Sweden
[firstname.lastname]@kau.se

Auditing is a standard practice for compliance monitoring. Legislations and regulations, such as HIPAA (Health Insurance Portability and Accountability Act), the Swedish Data Patient Act and the EU Data Protection Directive 95/46/EC mandate service providers to implement security mechanisms such as audit controls to record system activities, i.e., audit trails, for later review. The analysis of audit trails, which are collection of log entries, for privacy compliance is referred to as privacy auditing. However the manual analysis of audit trails is a time consuming and error-prone activity and does not usually scale well, therefore automating the analysis of the audit trails to detect non-compliance to privacy legislation, privacy regulation, and privacy preferences is essential.

There are number of mechanisms proposed in the literature for the automatic verification of audit trails for detecting privacy violations. However, there exists no scientific review work until now that systematically compiles, summarizes, and evaluate the state-of-the-art in this area. So, in this work, we conducted a systematic literature review. We survey the existing proposals, and classify them according to a taxonomy.

The taxonomy considers the underlying mechanisms and techniques used in the automatic verification process and attempts to organize similar proposals into discrete groups. We observed that the underlying technical building blocks of privacy auditing solutions are very similar to intrusion detection techniques. As a result, the proposed solutions for privacy violation detection are classified into two main categories: privacy misuse detection and privacy anomaly detection. This is similar to intrusion detection system taxonomies, which is further investigated in our final paper. Furthermore, we evaluate the existing approaches, point out their strengths and limitations in the final paper. In addition we also propose a second taxonomy that is based on privacy principles instead of only on technical solutions.

* This research was funded by SmartSociety and A4Cloud, two research projects of the Seventh Framework Programme for Research of the European Community under grant agreements no. 600854 and no. 317550.