Public summary of PhD-thesis of Mahdi Alizadeh
PhD-defense date: 19 November 2018

Auditing of user behavior: Identifying, analyzing and understanding deviations

In our society, the collection and use of personal data is increasing (e.g. electronic health records, financial data and demographic data used in E-government). Protecting these data is a serious and urgent issue. Traditional security mechanisms such as access control are preventive and very rigid and are not suitable for dynamic environments such as hospitals. For that reason, organizations often employ flexible protection mechanisms to deal with unexpected circumstances. These mechanisms often allow users to deviate from process models and security policies. For instance, most healthcare systems support a 'break-the-glass' procedure that allows users to bypass access control rules in emergency situations. However, this flexibility may be misused by users, accidentally or maliciously. Regardless of user intent, data misuse may have serious consequences for organizations, including financial and reputation loss. That is why organizations should have mechanisms in place to monitor user behavior and identify possible data misuses.

Current behavior analysis mechanisms typically fail to take advantage of end-to-end process models and process mining approaches. If tailored to security purposes, this type of user behavior analysis has the potential to provide more comprehensive results. This thesis proposes approaches for analyzing user behavior and identifying possible deviations from specifications.

We address four challenges. The first challenge is related to the accurate identification of deviations from the expected process. We propose an approach that analyzes past executions of the process and learns how the process behaves when reaching a certain state. Based on the insights obtained from this analysis, we can provide probable explanations of why a certain process execution does not conform to expectations. The second challenge is related to analyzing observed behavior by looking from the perspectives of both the data and the process. We propose a solution for conformance checking that links the data and process perspectives, for more accurate identification of deviations and more comprehensive diagnostics. The third challenge is to provide high-level diagnostics about frequent deviant behaviors to analysts. To address this challenge, we propose a solution to discover frequent anomalous patterns, which represent recurrent deviant behaviors that often occur together. This type of output can allow analysts to focus on deviant behaviors at a higher level of abstraction, instead of analyzing each instance individually. The fourth challenge is to analyze user behavior and to identify users who are behaving abnormally. For this purpose, we propose a solution to compare a user's behavior with that of her peers. This solution analyzes user actions collectively rather than independently, which could make it possible to identify attacks that span multiple actions.

We evaluated the proposed approaches with synthetic and real-life datasets. The results of our experiments showed that our approaches can identify deviations accurately and provide insightful and helpful diagnostics about user behavior to analysts. The insights obtained from these approaches can be used for different purposes. For example, to mitigate the risks of possible attacks, correct the behavior of users who do not follow the expected specifications, or to redesign a process model to better reflect how the process is used in reality. All of which contribute to a safer digital environment.

Title of PhD-thesis: Auditing of user behavior: Identifying, analyzing and understanding deviations. Supervisors: Prof.dr. Milan Petković, Eindhoven University of Technology, Prof.dr.ir. Wil van der Aalst, Eindhoven University of Technology, Dr. Nicola Zannone, Eindhoven University of Technology. Other main parties involved: Philips, Amsterdam Medical Center.