Accepted Manuscript

Title: Linking data and process perspectives for conformance analysis

Author: Mahdi Alizadeh, Xixi Lu, Dirk Fahland, Nicola Zannone, Wil M.P. van der Aalst

PII: S0167-4048(17)30226-2
DOI: https://doi.org/10.1016/j.cose.2017.10.010
Reference: COSE 1222

To appear in: *Computers & Security*

Received date: 27-3-2017
Revised date: 7-9-2017
Accepted date: 27-10-2017

Please cite this article as: Mahdi Alizadeh, Xixi Lu, Dirk Fahland, Nicola Zannone, Wil M.P. van der Aalst, Linking data and process perspectives for conformance analysis, *Computers & Security* (2017), https://doi.org/10.1016/j.cose.2017.10.010.

*Corresponding author

Email addresses: m.alizadeh@tue.nl (Mahdi Alizadeh), x.lu@tue.nl (Xixi Lu), d.fahland@tue.nl (Dirk Fahland), n.zannone@tue.nl (Nicola Zannone), w.m.p.v.d.aalst@tue.nl (Wil M. P. van der Aalst)

Linking Data and Process Perspectives for Conformance Analysis

Mahdi Alizadeh*, Xixi Lu, Dirk Fahland, Nicola Zannone, Wil M. P. van der Aalst

Eindhoven University of Technology, Eindhoven, Netherlands

Abstract

The detection of data breaches has become a major challenge for most organizations. The problem lies in that fact that organizations often lack proper mechanisms to control and monitor users' activities and their data usage. Although several auditing approaches have been proposed to assess the compliance of actual executed behavior, existing approaches focus on either checking data accesses against security policies (*data perspective*) or checking user activities against the activities needed to conduct business processes (*process perspective*). Analyzing user behavior from these perspectives independently may not be sufficient to expose security incidents. In particular, security incidents may remain undetected or diagnosed incorrectly. This paper proposes a novel auditing approach that reconciles the data and process perspectives, thus enabling the identification of a large range of deviations. In particular, we analyze and classify deviations with respect to the intended purpose of data and the context in which data are used, and provide a novel algorithm to identify non-conforming user behavior. The approach has been implemented in the open source framework ProM and was evaluated through both controlled experiments and a case study using real-life event data. The results show that the approach is able to accurately identify deviations in both data usage and control-flow, while providing the purpose and context of the identified deviations.