Detective Information Flow Analysis for Business Processes*

Rafael Accorsi and Claus Wonnemann
Department of Telematics, University of Freiburg
{accorsi|wonnemann}@iig.uni-freiburg.de

Abstract: We report on ongoing work towards *a posteriori* detection of illegal information flows for business processes, focusing on the challenges involved in doing so. Resembling a forensic investigation, our approach aims at analyzing the audit trails resultant from the execution of the business processes, locating informations flows that violate the (non-functional) requirements stipulated by security policies. The goal is to obtain fine-grained evidence of policy compliance with respect to information flows.

Information flow (IF) characterizes the transfer of information from a classified container h to a public container l during the execution of a process. A "container" can be a logical or physical device, such as a process instance, network socket, or variable. An IF is labeled "illegal" whenever it violates the security policies expressing the non-functional requirements placed on the execution of the process, in particular the confidentiality and non-interferability of pieces of information.

Assuring that the executions of business processes do not allow illegal IF is essential in the context of regulatory compliance, which is largely automated by business processes deployed over service-oriented architectures. Most of the compliance requirements, and hence security policies, are concerned with the propagation of sensitive data, such as personally identifiable information, credit card numbers and the like.

However, only the minority of these policies, namely those denoting *safety properties*, can be enforced with access control mechanisms based on execution monitors. The majority of the security policies, in particular those expressing non-interference, denote *hyperproperties* for which mechanisms for runtime enforcement do not exist, nor are there techniques for *a posteriori* analysis of process executions tailored to the detection of illegal IF.

As a result of lacking techniques for IF control (IFC), illegal IF arising from *covert channels* – information channels whose primary purpose is not the transmission of information, but which are misused for this purpose – and *information interference* – the extraction of sensitive information from a set of accumulated data items or events – may go undetected. This leads to a situation in which the executions of a process, and the process itself, may be thought as complying with the security policies, whereas a thorough analysis for illegal IF could prove the opposite: IF leads to policy violations and non-compliance.

We investigate approaches for the a posteriori analysis of IF in business processes. Resembling a forensic investigation and building on authentic log files recorded during the

*See http://www.informatik.uni-freiburg.de/~accorsi/publications.html for a version containing the references.

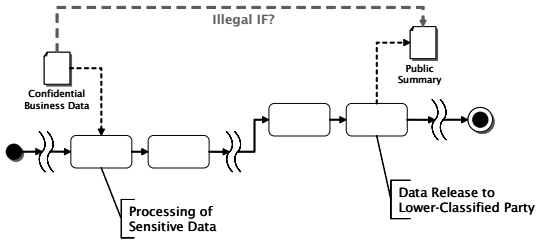

Figure 1: Confinement of data in business processes.

execution of processes, our goal is to advance IFC by developing approaches for the analysis of audit trails to detect illegal IF. Put another way, we investigate an approach for *a posteriori* IFC. In doing so, we do not prevent illegal IF; instead, we support the detection of illegal IF, considerably improving the state of the art audit mechanisms.

The threat of illicit information disclosure arises, for instance, when medical records are released in (assumedly) anonymized form, or when a company releases public statements that are based on confidential business data, as schematically depicted in Figure 1. Here, it must be ensured that data made public does not allow conclusions on secret information to be drawn, such as the identity of patients. Eventually, our approach either returns a proof of adherence to the policies, or gives evidence on violations and their circumstances.

To do so, we develop notions of IF for this setting and corresponding analysis techniques. Specifically, we currently focus on the following research issues:

- *Formalizations of IF properties for business processes.* We evaluate different formalizations of non-interference for their adequacy in a business process context. Further, we search for IF definitions apart from non-interference that capture additional covert channels (e.g. probabilistic and timing channels) and inference of data. A medium-term goal is to devise a language for the expression of hyperproperties, allowing the specification of a multitude of IF properties for business processes.

- *Data selection.* The basis for the analysis is log data recorded by the business process execution engine. While mechanisms for secure logging exist, it is unclear to date which pieces of information are in fact relevant for the detection of illegal IF. One of our efforts is thus to select the log data to be collected for the analysis.

Upcoming research challenges include, among others, the development of appropriate *analysis algorithms* and *accuracy measurement*. As for analysis algorithms, in considering hyperproperties, an analysis must look at *sets* of traces, interconnecting the events therein according to the IF policy. While this can happen by event correlation, we believe that data mining techniques, in particular those based on mixture models, allow for a more precise analysis of audit trails. Accuracy measurement subsumes *precision assessment* and *error estimation*: while false negatives must be ruled out, false positives are to be minimized and their occurrence quantified in a formal way.