

# 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 information 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 [Lam73]. 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 put on the execution of the process, in particular the confidentiality and non-interferability of pieces of information.

Asserting that the executions of business processes do not allow illegal IF is essential in the context of regulatory compliance [KGM08], which is largely automated by business processes deployed over service-oriented architectures [AMK02]. Most of the compliance requirements, and hence security policies, is concerned with the propagation of sensitive data [BA08], such as personally identifiable information, credit card numbers and the like.

However, the minority of these policies, namely those denoting *safety properties* [Lam77], can be enforced with access control mechanisms based on execution monitors [Sch00]. The majority of the security policies, in particular those expressing non-interference, denote *hyperproperties* for which mechanisms for runtime enforcement do not exist [CS08], nor are there techniques for *a posteriori* analysis of process executions tailored to the detection of illegal IF [Acc08].

As a result of lacking techniques for IF control (IFC), illegal IF arising from *covert channels* – i.e. information channels whose primary purpose is not the transmission of information, but which are misused for this purpose – and *information interference* – i.e. 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 led to policy violations and non-compliance.

Our work investigates approaches for the *a posteriori* analysis of IF in business processes. Resembling a forensic investigation [PBM08] and building on authentic log files recorded during processes’ execution [Acc09], our goal is to advance IFC by developing approaches

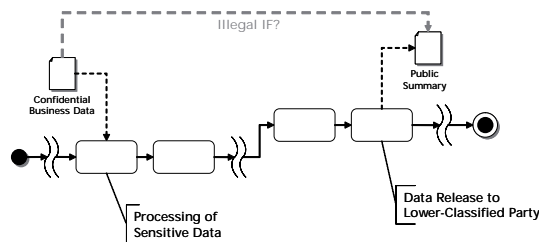


Figure 1: Confinement of data in business processes.

for the analysis of audit trails to detect illegal IF. Put other 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 [ABLY07, CG07].

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 to draw conclusions on secret information, such as the identity of patients [Swe02]. 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 [Acc06, SK99], to-date it is unclear which pieces of information are in fact relevant for the detection of illegal IF [SSA06]. 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 [Tif03], we believe that data mining techniques, in particular those based on mixture models [SSTP07], 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.

## References

- [ABLY07] A. Antón, E. Bertino, N. Li, and T. Yu. A Roadmap for Comprehensive Online Privacy Policy Management. *Comm. ACM*, 50(7):109–116, 2007.
- [Acc06] R. Accorsi. On the Relationship of Privacy and Secure Remote Logging in Dynamic Systems. In S. Fischer-Hübner et al. eds, *Security and Privacy in Dynamic Environments*, vol. 201 of *IFIP Proc.*, pp. 329–339. Springer, 2006.
- [Acc08] R. Accorsi. *Automated Counterexample-Driven Audits of Authentic System Records*. PhD thesis, University of Freiburg, 2008.
- [Acc09] R. Accorsi. Credible Digital Evidence: What Secure Logging Protocols Have to Offer? *Submitted to the IEEE COMPSAC 2009*, 2009.
- [AMK02] S. Aissi, P. Malu, and K. Srivinasan. E-Business Process Modelling: The next big step. *IEEE Computer*, 35(5):55–62, 2002.
- [BA08] T. Breaux and A. Antón. Analyzing Regulatory Rules for Privacy and Security Requirements. *IEEE Transactions on Software Engineering*, 34(1):5–20, 2008.
- [CG07] A. Carlin and F. Gallegos. IT Audit: A Critical Business Process. *IEEE Computer*, 40(7):87–89, 2007.
- [CS08] M. Clarkson and F. Schneider. Hyperproperties. In *Proc. of IEEE Computer Security Foundations Symposium*, pp. 51–65. IEEE Press, 2008.
- [KGM08] M. Kähler, M. Gilliot, and G. Müller. Automating Privacy Compliance with ExPDT. In *Proc. of IEEE Conference on E-Commerce Technology*, pp. 87–94. IEEE Press, 2008.
- [Lam73] B. Lampson. A Note on the Confinement Problem. *Comm. ACM*, 16(10):613–615, 1973.
- [Lam77] L. Lamport. Proving the correctness of multiprocess programs. *IEEE Trans. on Software Engineering*, 3(2):125–143, 1977.
- [PBM08] S. Peisert, M. Bishop, and K. Marzullo. Computer Forensics *In Forensics*. *ACM Operating System Review*, 42(2):112–122, 2008.
- [Sch00] F. Schneider. Enforceable Security Policies. *ACM TISSEC*, 3(1):30–50, 2000.
- [SK99] B. Schneier and J. Kelsey. Security Audit Logs to Support Computer Forensics. *ACM TISSEC*, 2(2):159–176, 1999.
- [SSA06] S. Sackmann, J. Strüker, and R. Accorsi. Personalization in Privacy-Aware Highly Dynamic Systems. *Comm. ACM*, 49(9):32–38, 2006.
- [SSTP07] M. Stritt, L. Schmidt-Thieme, and G. Poepfel. Combining Multi-Distributed Mixture Models and Bayesian Networks for Semi-Supervised Learning. In *Proc. of the Int. Conf. on Machine Learning and Applications*, pp. 354–362. IEEE Computer Society, 2007.
- [Swe02] L. Sweeney. k-Anonymity: A Model for Protecting Privacy. *Int. J. of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(5):557–570, 2002.
- [Tif03] Michael Tiffany. A Survey of Event Correlation Techniques and Related Topics. At <http://www.tiffman.net/netman/netman.pdf>, 2003.