FORTES: Forensic Information Flow Analysis of Business Processes⋆
(Extended Abstract)

Rafael Accorsi and Günter Müller

Department of Telematics
University of Freiburg, Germany
{accorsi,mueller}@iig.uni-freiburg.de

Abstract. This extended abstract outlines the **FORTES** project for the forensic analysis of information flow properties. **FORTES** claims that information flow control can be made usable as a core of an audit-control system. For this purpose, it reconstructs workflow models from secure log files (i.e. execution traces) and, applying security policies, analyzes the information flows to distinguish information flows according to their relevance. **FORTES** thus cannot prevent security policy violations, but by detecting them with well-founded analysis, improve the precision of audit controls and the generated certificates.

Approximately 70% of all business processes in use today rely on automated workflow systems for their execution [16]. Despite the growing expenses in the design of advanced tools for secure and compliant deployment of workflows, an exponential growth of dependability incidents persists [8, 11, 12]. One reason for this fact is that traditional mechanisms based on access control models fail to enforce security properties unless they are fully known at design time. Concepts beyond access control focusing on information flow control [17] or usage control [13] open up new paradigms to design security mechanisms for reliable and secure IT-based workflows.

Information flow control semantically specifies reliable and secure workflows, where reliability is the guarantee to continuously deliver correct services [5] and security is a composite of the protection goals confidentiality, integrity, and availability [14]. Workflows satisfying both reliability and security requirements are called dependable. However, the "control" part of all approaches based on "information flow" has so far been poorly achieved in terms of practical enforceable mechanisms. In traditional information flow control with formal verification and program analysis, any relationship (so-called *interference*) between an observable event (*low*) of a workflow and a secret or classified event (*high*) happening over a (covert) channel [10] denotes an error, but none of these approaches can distinguish between security-relevant and security-irrelevant relationships in a

---

⋆ This extended abstract has been presented in April 2010 at the Dagstuhl Workshop 10141 on Distributed Usage Control organized by Sandro Etalle, Alexander Pretschner, Ravi Sandhu and Marianne Winslett.

business sense. This makes the resulting systems unfeasibly restrictive in many application scenarios [15].

FORTES approaches covert channel analysis from a forensic perspective. It claims that information flow control can be made usable as a core of an audit system. Today, "manual" audits issue a certificate where an entrusted third-party asserts conformant business behaviour. Certificates are generated following "semi-formal best practice" approaches and lack well-founded, automated analysis [6, 7]. Approaches to automating audit focus largely on the simple pattern-matching of audit-trails and policies [1, 9] and, more recently, on the use of extensional policies with basic forms of clustering of audit-trails [3, 4]. This fails to capture subtle attacks caused by interferences [12].

FORTES applies information flow analysis for the analysis of logs files. For this purpose, **FORTES** reconstructs workflow models from secure log files [2] (i.e. execution traces) and, applying security policies, analyzes the detected information flows to distinguish security-relevant from security-irrelevant interferences and covert channels. **FORTES** thus cannot prevent security policy violations, but it detects them with well-founded analysis. **FORTES** issues automatically generated, semantically meaningful certificates based upon reconstructed workflow models, the specification of dependability requirements (policies), and the analysis of execution traces (secure logs).

References

1. R. Accorsi. Automated privacy audits to complement the notion of control for identity management. In E. de Leeuw, S. Fischer-Hübner, J. Tseng, and J. Borking, editors, *Policies and Research in Identity Management*, volume 261 of *IFIP*, pages 39–48. Springer-Verlag, 2008.
2. R. Accorsi. Safekeeping digital evidence with secure logging protocols: State of the art and challenges. In *Proceedings the IEEE Conference on Incident Management and Forensics*, pages 94–110. IEEE Press, 2009.
3. R. Accorsi and T. Stocker. Automated privacy audits based on pruning of log data. In *Proceedings of the IEEE Conference on Enterprise Distributed Object Computing*, pages 175–182, 2008.
4. R. Accorsi and C. Wonnemann. Auditing Workflow Executions against Dataflow Policies. In *Lecture Notes in Business Information Processing*, volume 47, pages 207–217. Springer-Verlag, 2010.
5. A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr. Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing*, 1(1):11–33, 2004.
6. J. Bace and C. Rozwell. Understanding the components of compliance. Gartner Research Paper, July 2006.
7. A. Carlin and F. Gallegos. IT audit: A critical business process. *IEEE Computer*, 40(7):87–89, July 2008.
8. W. Diffie. Information security: 50 years behind, 50 years ahead. *Communications of the ACM*, 51(1):55–57, January 2008.
9. J. Kuri, G. Navarro, L. Mé, and L. Heye. A pattern matching based filter for audit reduction and fast detection of potential intrusions. In *Recent Advances in*

Intrusion Detection, volume 1907 of *Lecture Notes in Computer Science*, pages 17–27. Springer-Verlag, 2000.

10. B. Lampson. A note on the confinement problem. *Communications of the ACM*, 16(10):613–615, October 1973.

11. L. Lowis and R. Accorsi. Finding vulnerabilities in SOA-based business processes. *IEEE Transactions on Service Computing*, 2010. To appear.

12. G. Müller, R. Accorsi, S. Höhn, and S. Sackmann. Sichere Nutzungskontrolle für mehr Transparenz in Finanzmärkten. *Informatik Spektrum*, 33(1):3–13, February 2010.

13. A. Pretschner, M. Hilty, and D. Basin. Distributed usage control. *Communications of the ACM*, 49(9):39–44, September 2006.

14. K. Rannenberg, A. Pfitzmann, and G. Müller. Sicherheit, insbesondere mehrseitige Sicherheit. In G. Müller and A. Pfitzmann, editors, *Mehrseitige Sicherheit in der Kommunikationstechnik*, pages 21–30. Addison-Wesley, 1997.

15. P. Ryan, J. McLean, J. Millen, and V. Gligor. Non-interference: Who needs it? In *Proceedings of the IEEE Computer Security Foundations Workshop*, pages 237–238. IEEE Computer Society, 2001.

16. S. Sackmann and J. Strüker. Eine stille Revolution in deutschen Unternehmen. Number IV in Electronic Commerce Enquête. 2005.

17. F. Schneider, G. Morrisett, and R. Harper. A language-based approach to security. In R. Wilhelm, editor, *Informatics – 10 years back. 10 years ahead*, volume 2000 of *Lecture Notes in Computer Science*, pages 86–101. Springer-Verlag, 2001.