

# Editorial to the Second Workshop on Security and Privacy in Enterprise Computing (InSPEC09)

Rafael Accorsi  
Dept. of Telematics  
University of Freiburg  
Germany

Email: [accorsi@iig.uni-freiburg.de](mailto:accorsi@iig.uni-freiburg.de)

Ernesto Damiani  
Dept. of Computer Technology  
University of Milan  
Italy

Email: [damiani@dti.unimi.it](mailto:damiani@dti.unimi.it)

Frank Innerhofer-Oberperfler  
Research Group Quality Engineering  
University of Innsbruck  
Austria

Email: [frank.innerhofer-oberperfler@uibk.ac.at](mailto:frank.innerhofer-oberperfler@uibk.ac.at)

Florian Kerschbaum  
SAP Research CEC Karlsruhe  
Germany

Email: [florian.kerschbaum@sap.com](mailto:florian.kerschbaum@sap.com)

**Abstract**—The goal of the International Workshop Series on Security and Privacy in Enterprise Computing (InSPEC) is to provide a forum for the discussion of novel research directions and challenges in security and privacy in enterprise computing among the experts from academia and industry. The following introduces the second edition of the workshop in conjunction with the 13th IEEE International EDOC Conference in Auckland, New Zealand.

## I. WORKSHOP CONTEXT

Enterprise computing is a hot topic in applied informatics. Automated, communicating workflows, years ago an unattainable vision in industry, are by now widely adopted. At their implementation level, loosely-coupled services are becoming the new building blocks of enterprise systems and service-oriented architectures combine them in a flexible manner, thereby realizing the adaptivity gained from automated workflows. In addition, with wide adoption of e-commerce, business analytics that exploit multiple, heterogeneous data sources have become an important practical field. Beyond the traditional client-server scenario, ubiquitous computing technologies, such as RFID or sensor networks, change the way business systems interact with their physical environment and hence with end users, e.g. goods in a supply chain and novel personalization possibilities.

The continuous development towards the automation of business processes cast a number of challenges to security and privacy into a yet more complex and relevant context. We are increasingly relying on IT systems for our daily business including essential commodities, such as water and power. The traditional forms of computer security need to be enhanced to address the distributed nature and multiple administrative domains of conducting business. For example, algorithms for incorporating the new business practices need to be identified for access control. Similarly, data confidentiality cannot be provided on the network layer alone anymore, it needs to be built into applications and processes

that span across various domains. The enhanced data sharing calls for innovative algorithms and protocols that respect the users' security needs. Novel cryptographic techniques need to be developed and established ones evaluated for industrial adoption. In addition to the security measures, this new generation of distributed systems requires techniques for ensuring compliance with regulations on governance and privacy of data, including those asserted by government and regulatory agencies.

## II. CONTRIBUTIONS

The InSPEC workshop series sets out to provide a platform for researchers and practitioners to present problems in enterprise computing and novel solutions there. Following the first edition in Munich in 2008, the second edition in Auckland includes the following refereed contributions.

Pearson et al. [1] present a so-called “Accountability Model Tool” to address the problem of capturing data about business processes in order to determine whether they comply with the privacy policies or not. The goal is to detect violations of privacy policies in an automated manner and make subjects accountable for them. While this is traditionally achieved by a posteriori audits [2]–[5] based on secure logging [6], the approach proposed by the authors operate at runtime, generating compliance reports on-the-fly.

## III. PERSPECTIVES

The development that changed the IT industry was the Internet. The ubiquitous availability of connectivity lead to dramatically new forms of interactive computing. One of the newest such developments is cloud computing or software as a service. The low costs of communication combined with the economies of scale on maintenance and computation are a convincing argument for many customers. The huge initial success of many such offerings drives the industry even more into that direction.

Given a service provider hosting the software for many customers collaboration becomes feasible and cheap. There are no longer high integration hurdles and complex communications setups. Instead most of the data is already stored in one database and data exchange mostly becomes an issue of setting the access control policies. From a security researcher's point of view the challenges will shift. Is the cloud service provider the long sought for trusted third party? Can he do something for your data security that distinguishes him in the market from others? Most new industrial software development projects will focus on the cloud and as such should research.

Related to connectivity and cloud computing is the fact that we now connect business processes and the services realizing such a services. One issue in doing so is that of *compatibility*, which aims at showing that communicating business processes are able to achieve the goals they have been designed for [7]. Broken down to standard computer science properties, this means demonstrating, e.g., the absence of deadlocks and starvation. Another issue is that of *security*: assuming processes achieve the intended business goals, do they achieve them safely? That is, do they comply with the basic security and privacy policies? The traditional way of doing so has focused on access control and authentication. With the rise of cloud computing though, the *usage* and *information flow* control, and associated *risk management and quantification* has become of essential relevance [8], [9]. In particular, information flow control [10] and evidence generation [11] have been receiving attention. In this setting, the task is that of identifying potential information leaks and illegal propagation, as well as of devising methods of closing these leaks are challenging.

#### REFERENCES

- [1] S. Pearson, P. Rao, T. Sander, A. Parry, A. Paull, S. Patruni, V. Dandamudi-Ratnakar, and P. Sharma, "Scalable, accountable privacy management for large organizations," in *Proceedings of the EDOC International Workshop on Security and Privacy in Enterprise Computing*. IEEE Computer Society Press, 2009.
- [2] S. Sackmann, J. Strüker, and R. Accorsi, "Personalization in privacy-aware highly dynamic systems," *Communications of the ACM*, vol. 49, no. 9, pp. 32–38, September 2006.
- [3] R. Accorsi, "Automated privacy audits to complement the notion of control for identity management," in *Policies and Research in Identity Management*, ser. IFIP Conference Proceedings, E. de Leeuw, S. Fischer-Hübner, J. Tseng, and J. Borking, Eds. Springer-Verlag, 2008, vol. 261, pp. 39–48.
- [4] —, "Automated counterexample-driven audits of authentic system records," Ph.D. dissertation, University of Freiburg, 2008.
- [5] R. Accorsi and T. Stocker, "Automated privacy audits based on pruning of log data," in *Proceedings of the EDOC International Workshop on Security and Privacy in Enterprise Computing*. IEEE Computer Society Press, 2008.
- [6] R. Accorsi, "On the relationship of privacy and secure remote logging in dynamic systems," in *Security and Privacy in Dynamic Environments*, ser. IFIP Conference Proceedings, S. Fischer-Hübner, K. Rannenberg, L. Yngström, and S. Lindskog, Eds. Springer-Verlag, 2006, vol. 201, pp. 329–339.
- [7] W. M. P. van der Aalst, A. J. Mooij, C. Stahl, and K. Wolf, "Formal methods for web services, 9th international school on formal methods for the design of computer, communication, and software systems, sfm 2009, bertinoro, italy, june 1-6, 2009, advanced lectures," ser. Lecture Notes in Computer Science, M. Bernardo, L. Padovani, and G. Zavattaro, Eds., vol. 5569. Springer, 2009, pp. 42–88.
- [8] R. Accorsi and C. Wonnemann, "Detective information flow analysis for business processes," in *BPSC*, ser. LNI, W. Abramowicz, L. A. Maciaszek, R. Kowalczyk, and A. Speck, Eds., vol. 147. GI, 2009, pp. 223–224.
- [9] R. Accorsi, Y. Sato, and S. Kai, "Compliance-monitor zur frühwarnung vor risiken," *Wirtschaftsinformatik*, vol. 50, no. 5, pp. 375–382, 2008.
- [10] C. Wonnemann, R. Accorsi, and G. Müller, "On information flow forensics in business application scenarios," in *Proc. of the IEEE COMPSAC*. IEEE Computer Press, 2009, pp. 324–328.
- [11] R. Accorsi, "Safekeeping digital evidence with secure logging protocols: State of the art and challenges," in *Proceedings of the Conference on IT Security Incident Management & IT Forensics*, GI. IEEE Computer Society, 2009.