Electron Markets
DOI 10.1007/s12525-014-0158-6

PREFACE

Security and privacy in business networking

Sven Wohlgemuth · Stefan Sackmann · Noboru Sonehara · A Min Tjoa

Abstract Business networking relies on application-specific quantity and quality of information in order to support social infrastructures in, e.g., energy allocation coordinated by smart grids, healthcare services with electronic health records, traffic management with personal sensors, RFID in retail and logistics, or integration of individuals' social network information into good, services, and rescue operations. Due to the increasing reliance of networking applications on sharing ICT services, dependencies threaten privacy, security, and reliability of information and, thus, innovative business applications in smart societies. Resilience is becoming a new security approach, since it takes dependencies into account and aims at achieving equilibriums in case of opposite requirements. This special issue on 'Security and Privacy in Business Networking' contributes to the journal 'Electronic Markets' by introducing a different view on achieving acceptable secure business networking applications in spite of threats due to covert channels. This view is on adapting resilience to enforcement of IT security in business networking applications. Our analysis shows that privacy is an evidence to measure and improve trustworthy relationships and reliable interactions between participants of business processes and their IT systems. The articles of this special issue, which have been accepted after a double-blind peer review, contribute to this view on interdisciplinary security engineering in regard to the stages of security and privacy requirements analysis, enforcement of resulting security requirements for an information exchange, testing with a privacy-preserving detection of policy violations, and knowledge management for the purpose of keeping business processes resilient.

Keywords Business networking · Resilience · Information exchange · Security · Privacy · Enforcement

Business networking and resilience

At present, one of the most promising visions for business networking is the exploitation of information with information and communication technology (ICT), in particular by Big Data analytics with cyber-physical systems (CPS) (acatech 2011; Wahlster and Müller 2013). IBM calls it 'Smarter Planet' (IBM Corporation 2008), the European Commission (2010) has started the corresponding program 'Horizon 2020—A Digital Agenda for Europe', and Japan proposes the 'Declaration to be the World's Most Advanced IT Nation' (Prime Minister of Japan and His Cabinet 2013). One aim of these initiatives is that systems, such as business networking applications, social infrastructures, and a society become resilient. Changes and vulnerabilities should be identified and analyzed to foresee and prevent incidents of any kind, as well as to react accordingly in acceptable time. Resilient ICT then supports the increased, sustainable welfare of a society.

The key approach for gaining information on vulnerabilities and predicting incidents will be the ability to access and to analyze huge amounts of data in nearly real-time and to implement so-called Big Data analytics successfully. Service providers will collect, aggregate, and analyze data from various sources provided by CPS, e.g., business networks, social

S. Wohlgemuth (✉)
CASED, System Security Lab, Mornewegstr. 32,
64293 Darmstadt, Germany
e-mail: sven.wohlgemuth@trust.cased.de

S. Sackmann
Martin Luther University Halle Wittenberg, Universitätsring 3,
06108 Halle/Saale, Germany

N. Sonehara
National Institute of Informatics, Information and Society Research Division, 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, Japan

A. Tjoa
Vienna University of Technology, Institute for Software Technology, Favoritenstr. 9-11/188, 1040 Wien, Austria

Published online: 14 May 2014

networks, sensors and actuators, as well as governments and citizens. Prominent examples for such innovative business networking applications can be found, e.g., in the domain of energy allocation coordinated by smart grids, healthcare services with electronic records, traffic management with personal sensors and interconnected vehicles, RFID in retail and logistics, individualized manufacturing of goods, as well as personalized services based on an individual's social network.

Such business networking applications share the Internet and its ICT services for global communication. Due to the increasing interdependence of the participating components, incidents may result in highly disruptive impacts. Technical failure, human error, accidents, or cyber-attacks might spread via dependencies and could threaten security and reliability of ICT services, the supported social infrastructures, and, in the end, the welfare and safety of our society. In order to improve the security and reliability of ICT support in this context, several approaches are currently being discussed and implemented. For example, the reform of the EU legal framework for electronic communications added Article 13a addressing security and reliability. It asks public and private service providers to take security measures and provide an incident report flow as an information exchange on vulnerabilities and incidents between providers, national regulatory authorities, the European Union Agency for Network and Information Security (ENISA), and the European Commission. It is proposed that a qualified independent body should audit this information flow. The vision is that such an information exchange of incident reports would safeguard competition and boost consumer choice (European Commission 2009).

For improving resilience, a spontaneous exchange of information of acceptable quantity and quality lies at the core of these approaches. While such extensive information exchange and analysis can already be observed in business networking applications (Riemer et al. 2009) in the context of security and reliability it is still in an early stage. However, it would enable service providers to derive information on vulnerabilities and incidents by means of a secondary use of data with machine learning algorithms. In turn such information can be disclosed to other participants, e.g. actuators, who decide and act on this information to improve the security of their services and ICT. On the whole, such service providers and their business networking applications might be of high relevance for improving resilience of critical infrastructures, the emerging CPS, and future business networks.

However, information exchange is also the basis for dependencies between ICT systems—not only in the desired way as realized in business networking applications, but also by creating undesirable vulnerabilities and risks. Unfortunately, not all dependencies of an ICT system can be automatically detected (Wang and Ju 2006) and, thus, they threaten trustworthiness and participation in an information exchange. Therefore, one key issue to be resolved for exploiting the full potential of future business networking is enforcing the individual security and privacy interests of all participants to achieve an acceptable trustworthy information exchange. This implies controlling the usage of information.

Information exchange and intermediaries

In computer science trustworthy information exchange means a reduction of vulnerabilities in the participating ICT systems and their communication in order to reduce the effect of any incident (Avizienis et al. 2004). It also means that participants can formalize a security policy describing their individual security interests and negotiate on an agreed-upon security policy reflecting a compromise or equilibrium respectively (Rannenberg et al. 1999). In such multilateral IT security models protection goals, like accountability and unobservability, become an important part of a 'balanced' security. Enforcing accountability and unobservability can be technically achieved by encryption and authentication schemes supporting pseudonymity, e.g. by identity management (Chaum 1985) or cryptographic key systems (Pfitzmann and Hansen 2010). These approaches depend on confidentiality and integrity of the private key, its accountability to the given identity, and on integrity and consistency of a public key exchange. Even though trusted runtime environments exist (Asokan et al. 2013), security of a cryptographic key exchange without a trusted third party (TTP) has not yet been demonstrated (Freire et al. 2013).

Introducing a third party extends the direct communication model of an information exchange. In practice, the role of a third party acting as an intermediary for an information exchange is manifold. Intermediaries take care of the security and reliability of the communication and of current payments. Successful examples are SWIFT and international clearing systems (Bons et al. 2012). Intermediaries also establish relationships between data providers and data consumers by deriving information based on data collected with their consent. Successful examples here are loyalty card programs in the field of customer relationship management (CRM) or social networks sites. Furthermore, intermediaries can contribute to the usability of an information exchange to enforce the participants' individual security interests. Usability studies of security tools, e.g. PGP (Whitten and Tygar 1999), show that their user interfaces and security concepts are too technical and not intuitive with the result that, as observed in Germany, over 70 % are willing to delegate responsibility for their security to a TTP (DIVSI 2012).

Altogether, intermediaries in the role of TTP can be expected to play an important role with respect to extensive information exchange. However, they also represent a new vulnerability. Since an intermediary is usually involved in several information exchanges with different participants,

dependencies between the intermediary's ICT system and those of the other participants arise during run-time. Hence, a TTP also can be the origin of a possible man-in-the-middle attack with serious consequences for the information exchange. According to Article 13a incident reports in 2013, third party failure has a high impact. Most of the observed incidents have their direct cause in system overload, power cuts, and software bugs (Dekker et al. 2013). The IT security report for Germany in 2011 (BSI 2011) shows a trend from direct attacks to indirect ones via dependencies to the affected ICT system. The report forecasts an increase in attacks by botnets, identity theft, security vulnerabilities, and malware. SCADA, mobile communications, interfaces and storage media, or Cloud Computing systems — all of which are considered to be part of future CPS — show an increased risk potential. A current study of Internet usage in Germany indicates that these threats represent a real hurdle for information exchange. A fear of misuse of personal data is the main reason why the majority of the population in Germany refrains from participating in Internet services (DIVSI 2012).

Intermediaries can be expected to play a central role in future business networks in the context of providing privacy and security. However, they have to be trusted and, in other words, the less trust required, the better. Therefore, security and privacy mechanisms with a focus on intermediaries and their dependencies as origins of incidents are of interest for exploiting an effective information exchange in business networks. In respect of the realization of an incident report flow, there is no incentive to provide vulnerability information or to report incidents without adequate protection of the disclosed information. For example, a participant reporting a breach of confidentiality would be harmed twice: firstly by the incident itself and secondly by a loss of reputation due to the leakage of the confidential report.

Security models and their enforcement

The security approach to protect information once it has been disclosed to a third party is isolation on the part of the third party. Isolation means that exchanged information should not come into contact with other information exchanges and that the intermediary should not know what information is used in the service or the purpose for which the service is being used by its consumers (Sonehara et al. 2011). Thus, enforcement of isolation means to implement a multilateral trust model to enforce an equilibrium concerning the individual security interests of the participants.

Individual security interests can be enforced by different security models as described in the following. At first, access control models formalize isolation by information flow control for a closed group of participants. Mandatory access control (MAC) security models, e.g. Biba, Bell-LaPadula, or the Chinese Wall Security Policy, are in widespread use (Samarati and de Capitani di Vimercati 2001). They model information flow control to protect data by the use of labels and a pre-defined order. The pre-defined order classifies data and identity of authorized participants as subjects into access classes and formalizes the properties on data access as provisions according to the protection goals of confidentiality or integrity, respectively. However, the protection goal availability of information might not be achieved easily if a MAC policy is deployed for a spontaneous information exchange: the pre-defined order of the security policy would have to be implemented for service providers, leading to confidentiality of the data but also to a restriction of the availability of the services. Hence, a security configuration based on MAC may lead to an incident on availability of information.

Discretionary access control (DAC) where authorizations are granted to the identity of authorized service providers (data consumers) and not according to a security class, is more flexible. However, to date, DAC approaches are not precise enough for a trustworthy spontaneous information exchange. Granting access to data for given exchanges needs to define a group or role for the participants. This, in turn, could grant access to parties of an information exchange who are not participating in it representing a vulnerability regarding confidentiality and integrity of the information exchange.

In contrast, the concept of distributed usage control specifies the confidentiality and integrity of an information exchange and, thus, information flows as data processing by obligations without restricting availability of information (Pretschner et al. 2006). The classification of Hilty et al. (2005) for obligations according to time and distribution shows that obligations are in general not enforceable but can become so at runtime.

Concluding, an instance of a security model for a given isolation formalizes access on data and information, which is mapped to the identities of authorized subjects. According to the security model, security and privacy would be achieved if only authorized identities get access to the information as specified by provisions and obligations of the corresponding security policy and if these identities did in fact represent the corresponding data consumers. Their enforcement is to prevent incidents and to close vulnerabilities.

A further relevant issue for realizing a trustworthy information exchange is the authenticity of the exchanged information. Authenticity of derived information is always subject to a given error probability. Firstly, this is conceptually due to application-dependent statistical model of machine learning schemes (Domingos 2012). Secondly, information relates to a given model, i.e. to a given context, e.g., described by service level agreements and security policies specifying the context of a data processing.

At present, two opposing security concepts for enforcing isolation are under discussion: transparency and control. Transparency of data processing as stated by *Information*

Accountability (Weitzner et al. 2008) follows the concept that data processing should be observed and evaluated with *Transparency-Enhancing Technology (TET)*. TET aims at identifying an incident and its cause in order to decide on the accountability and trustworthiness of the affected participant. In contrast, control on data processing as with *Privacy by Design* (European Commission 2010) considers the possibility of a violation of an isolation and aims at enforcing unobservability. *Privacy-Enhancing Technology (PET)* achieves at least unobservability by pseudonymity. For self-protection further PETs follow the approach of additionally impeding secondary use of information and re-identification of participants for purposes of data processing, which occur after data collection. This may raise additional incidents and, thus, requires transparency in their cause and origin to decide on trustworthiness of the participants.

TET and dependencies

TET aims at enforcing obligations for isolation by observing the current data processing and its compliance to a given security policy. If a policy violation occurs, an anomaly and its cause are analyzed to decide on accountability. It can establish whether the received information has been processed according to the corresponding security policy. A monitor observes data processing of an ICT system and logs it for a data protection audit (Karjoth et al. 2002). If enforcement of isolation of previous information exchanges and vulnerabilities of the ICT system of the data consumer are known, a data provider then can derive information about expected enforcement of isolation.

Data leakage prevention aims at confidentiality of data processing. However, a monitor cannot consider more than one trace and is vulnerable to covert channels as seen by virtualization in Cloud Computing (Ristenpart et al. 2009). This is an example of the vulnerability of data confidentiality via a dependency even though the service provider grants access to his services to authorized identities only. If confidentiality is not the highest priority for an information exchange but rather integrity, consensus protocols are an approach to tolerate incidents while resulting in a consensus of authentic information. Preferably different implementations of the same information exchange run in parallel. Consensus protocols assume an information exchange also between these implementations, e.g. by an unknown, inevitable dependency. However, it is impossible for consensus protocols to result in a consensus in the asynchronous timing model, if only one of the participating systems fails during the protocol run (Fischer et al. 1985). Adding extensions such as randomization, failure detectors, or strong primitives for shared-memory lead to consensus protocols coping with failed systems due to delayed or failed data transfer but not for malicious incidents. This is the case with timing restricting consensus protocols (Gärtner 1999). Consensus protocols for a synchronous model cope with failed systems up to a certain number of compromised ICT systems, even if they send different messages to other systems (Pfitzmann and Waidner 1992). However, they restrict availability of the participating ICT systems. This is a vulnerability for any other information exchange with a dependency on this ICT system and out of the scope of the threat model of consensus protocols.

Latest research approaches aim at retaining detected anomalies by evidence on the current model of data processing. That means they reconstruct the current model but without restricting availability. Secure logging and evidence (Sackmann et al. 2006) consider transparent data processing of separated ICT systems and restrict access to logged data to authorized identities only. Process mining (Van der Aalst 2012) extends monitoring of the activities of an information exchange between ICT systems. The assumptions are completeness and authenticity of logged events, whereas confidentiality of the logged data in accordance to granting access on these observations to authorized identities is assured (Accorsi 2011). A variation of process mining is data provenance, which also documents the history of data and additionally their value by 'sticking' it to the data and derived information (Buneman et al. 2001). Schemes are inversion of data processing and annotation of data. Inversion depends on knowledge of the granted access decisions and the output data. This relates to the same completeness assumption as for secure logging and process mining. Annotation labels data so that the model of data processing can be re-constructed if a mapping to the data exists. However, current means for data provenance by annotation either assume centralized monitoring of the complete information exchange or are suitable for some kind of data without the derived information. Furthermore, data provenance can detect an information leakage and its cause only if the leaked information has been found together with evidence on its history (Wohlgemuth et al. 2010).

Data provenance and secure logging as a components for each ICT system under investigation can in principle be used to check the integrity and origin of information by the reconstructed model and its comparison to the security policy. This reconstructed model in turn should extend the model of the applied machine learning scheme. In order to detect an identity theft, it may not be sufficient to reconstruct the model of this data processing, since it ends at the identity. It may also be necessary to check whether an anomaly in the usage of this identity exists regarding the information exchange under investigation.

PET and dependencies

After converting obligations into provisions, PET enforces them while considering violations of confidentiality of isolation. The assumption is an idealized threat model assuming ICT systems as being correct whereas trustworthiness of participants is uncertain. PET impedes re-identification,

secondary use, and non-authorized profiling according to the master identity of a participating party. It can be achieved by restricting availability of information or the information itself (Gilliot et al. 2009). This, in turn, threatens Big Data analytics with an increase of its error probability by introducing faulty information or the non-availability of sufficient quantity, whereas this does not depend on the type of machine learning scheme (Biggio et al. 2012; Huang et al. 2011).

Encryption protects information before access has taken place. However, after decryption, protection is no longer provided and information can be leaked via an unknown dependency. Identity management with anonymized credentials achieves accountability and unobservability as long as further disclosure to third parties is not considered (Camenisch and Lysanskaya 2001). A non-linkable delegation of rights achieves unobservability and accountability in an information exchange with an intermediary under the assumption that the modeled recipient of the information as the last data consumer in its exchange is trustworthy and its ICT system has no vulnerability (Wohlgemuth and Müller 2006). However, this is not realistic for a spontaneous information exchange with an intermediary.

Our analysis of dependencies in a spontaneous information exchange and today's mechanisms to enforce its security model in accordance with the security and privacy interests of the participants shows that an incident and its propagation to a secure ICT system is always possible. On one hand, it is possible that an attacker can control the identity of this participant. On the other hand, strengthening transparency by consensus protocols or confidentiality by PET with reducing the information raises an incident on dependent information exchanges.

Homomorphic encryption schemes (Dolev and Yao 1983) enforce confidentiality and integrity of information and, at the same time, preserve its availability. Their general suitability is uncertain due to their required computing performance of the cryptographic scheme and a mismatch in abstraction of the information (Naehrig et al. 2011).

Resilience as an approach for IT security and privacy

At present security and privacy in business networking is based on a system and threat model, which includes a limited set of possible information exchanges and incidents. It considers expected states and dependencies including those, which have already passed. A partial model can be achieved for any subsystem, which does not change for an adequate time. However, this is not reality for many actual business networking applications which are highly dynamic and agile. Since vulnerabilities from dependencies arise during run-time and cannot be completely known and predicted, the 'pure' model-based approach is not adequate for preventing and reacting in this context. It is not (at least not efficiently) possible to model all possible changes and incidents and, thus, security with 'pure' model-based approaches will have to follow changes in business networks and their underlying technology.

Extending 'pure' model-based security and privacy approaches to the dynamic and unforeseeable context of actual business networking means having to address these vulnerabilities and dependencies. The general view then changes from achieving 'pure' security to preserving an acceptable level of service of a system that corresponds to a compromise of the individual security and privacy interests of the participants in an information exchange. Preserving an acceptable level of service of a system requires constantly adapting its dependencies to incidents (Holling 2001), a concept that is also known as resilience. However, a general statement on the resilience of a system cannot be made. It corresponds to a certain incident and the ability of a system to recover within a certain time for response and composite costs and risks (Haimes 2009). Since neither individual security and privacy interests (and compromises) nor vulnerabilities remain identical over time, an adaption of security and privacy enforcement is required.

Thus, it is worth thinking about improving security and privacy in business networking by using methods and tools that support resilience of social infrastructures, i.e. in particular Big Data analytics and information exchange on incidents. For data providers and data consumers approaches are required that allow both to balance the benefit and the level of service, respectively, the security or privacy risk associated with information exchange. This means that, e.g., a data provider should be able to check before an information exchange takes place whether a data consumer might violate obligations for the information exchange. Vice versa, a data consumer should be able to check a priori of an information exchange whether the received information is the expected one and the data provider has followed the agreed-upon security policy for this information exchange. From an economic theory point of view, this leads to an asymmetric information situation that can usually be solved (or at least improved) by signalling or screening mechanisms (Furubotn and Richter 2005). Thus, new technical approaches that address the reduction of information asymmetry are being discussed as suitable methods and tools for improving security and privacy in business networking.

ICT Resilience — a signaling and screening architecture

To empower data providers and data consumers to assess and balance the benefit and risk of entering an information exchange, classical security methods and tools should be complemented by methods and tools that support their decision making. To reduce information asymmetry, signalling components should give a participant a tool to generate evidence on his actual data usage to prove trustworthiness according to the corresponding obligations, as well as establish a reputation over

several information exchanges. In turn, a screening component should give a participant a tool to prove that exchanged information has been used as intended (or not). These tools are to be combined with accountability and an (economic) incentive system that allows each participant to evaluate the value of an information exchange according to the security configuration, the achievable level of, e.g. unobservability or accountability, and individual risk preferences.

In accordance with our analysis and adapting current approaches for resilience to security and privacy in business networking, we use the following five components to categorize methods and tools, as well as open research issues for *ICT Resilience*.

- A *Usage Control Policy Tool Box* aims at formalizing isolation patterns for expected information exchanges and anti-isolation patterns for classes of anomalies of an isolation. On one hand, this is required for expressing the interest of the parties involved in an information exchange. On the other hand, this is a basis for detecting anomalies, incidents, and policy violations, as well as for generating correct incident reports and their exchange. The set of patterns should be extensible to cater for newly detected patterns during runtime and for previously unknown interferences and results.
- *Privacy Control* aims at self-protecting against information leakage. The real identities of data providers should remain unobservable when information is going to be disclosed to third parties. This requires, e.g., identity management supporting pseudonymity and non-linkable delegation of rights. Pseudonymity should be revocable in case of provable fraud.
- *Privacy Forensics* aims at deriving evidence on isolation by the most probable data processing including its dependencies and its classification to an anomaly pattern. A data provenance scheme could derive such evidence. However, since internal dependencies of an external ICT system are usually not known, supervised machine learning in combination with labeled evidence could be useful for deriving the probabilities of possible information exchange. Since not all kind of data can be annotated, mechanisms of unsupervised machine learning should also be researched according to their suitability.
- *IT Risk Analysis* aims at evaluating and combining both types of evidence to result in a qualitative (or quantitative) statement on isolation, on information exchanges and, thus, on security and privacy in the corresponding business networking application. This component should consider results from, e.g., the Big Data analytics and information exchange on incidents. Based on the results of the risk analysis, an information exchange can be balanced, i.e. the corresponding security policies and compromises can be decided according to all the participants' risk preferences.
- *System Evolution* aims at automatic improvement of the security configuration for an isolation and replacement of compromised ICT systems or participants, respectively. A removal of systems implies revocation of rights, which can be, e.g. realized by revocation mechanisms for credentials. In the case of accessed data, information has to be removed along the subsequent data trace or at least made useless. Data provenance and data mining technologies can support auditing whether this information has indeed been removed.

We do not wish to claim that these five components are the silver bullet to achieving *ICT Resilience*, however, we expect that they can provide an initial categorization for topics that address security and privacy in future business networking. Summarizing, an ICT system providing a signaling-and-screening architecture of *ICT Resilience* is by itself a business networking application in providing 'security-as-a-service' with all its dependencies, vulnerabilities, and possibilities to violate the privacy interests of data providers. Since security and privacy cannot be guaranteed by technology alone, other means should foster the participation of individuals and correctness of their data and services. Data protection acts combined with adequate incentives are one option, however, they require reliable methods and tools for signaling and screening of actual behavior of all participants without harming their privacy and security interests. We see the challenges as interesting areas for research and finding solutions as a prerequisite for exploiting the potential of business networking applications relying on extensive data processing.

Papers within ICT Resilience

All papers of this special issue contribute to one of the presented components of *ICT Resilience*. Dehling and Sunyaev ('Secure provision of Patient-Centered Health Information Technology Services in Public Networks—Leveraging Security and Privacy Features Provided by the German Nationwide Health Information Technology Infrastructure') address the component *Usage Control Policy Toolbox*. They investigate security and privacy in business networking using the example of patient-centered health ICT services (PHS) based on the German infrastructure *gematik*. They identify security and privacy requirements of PHS, which could serve as a starting point for specifying isolation patterns for an information exchange of patients' health data between medical service providers and third parties.

Gogoulos, Antonakopoulou, Lioudakis, Mousas, Kaklamani, and Venieris ('On the design of a privacy aware authorization engine for collaborative environment') also address the component *Usage Control Policy Toolbox* with a proposal for enforcing isolation of cross-organization information exchanges. Their authorization engine derives

authorizations for data processing from a semantic model in accordance with the privacy and security interests of the participants.

Kieseberg, Schrittwieser, Mulazzani, Echizen, and Weippl ('An algorithm for collusion-resistant anonymization and fingerprinting of sensitive microdata') refer to *Privacy Forensics* in case of the disclosure of anonymized information to third parties. They present a k-anonymization scheme, which tags anonymized information by the procedure of their anonymization. Their evaluation considers colluding data consumers with the aim of non-authorized re-identification of the related identity to this information.

Rechert, von Suchodoletz, and Valizada ('Take Care of Your Belongings Today—Securing Accessibility to Complex Electronic Business Processes') address accessibility of information for the purpose of keeping business processes resilient. Since the outcome and costs of reconstructing archived information with the configuration of the corresponding instance of a business process are difficult to estimate, their proposal is to emulate their reconstruction in possible future data processing environments using software. The aim is to identify clearly defined and controllable preservation strategies, which should be integrated in current business processes. This forecasting and emulation approach is one option for supporting the continuous learning of isolation and anti-isolation patterns for *IT Risk Analysis*.

We thank all authors for their valuable submissions, reviewers and senior editors for the thorough and constructive comments and recommendations, and the editorial office for their support in editing this special issue.

References

acatech (Ed.). (2011). Cyber-physical systems. Driving force for innovation in mobility, health, energy and production, acatech—National Academy of Science and Engineering, *acatech POSITION PAPER*, http://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Publikationen/Stellungnahmen/acatech_POSITION_CPS_Englisch_WEB.pdf. Accessed 27 Feb 2014.

Accorsi, R. (2011). BBox: A distributed secure log architecture. *7th European Conference on Public-Key Infrastructures, Services and Applications (EuroPKI'10)*, pp. 109–124.

Asokan, N., Davi, L., Dmitrienko, A., Heuser, S., Kostiainen, K., Reshetova, E., et al. (2013). Mobile platform security—Synthesis lectures on information security, privacy, and trust. Morgan & Claypool Publishers.

Avizienis, A., Laprie, J.-C., Randell, B., & Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing, 1*(1), 11–33. IEEE.

Biggio, B., Nelson, B., & Laskov, P. (2012). Poisoning attacks against support vector machines. *29th Int. Conf. on Machine Learning (ICML)*.

Bons, R. W. H., Alt, R., Lee, H. G., & Weber, B. (2012). Banking in the internet and mobile era. *EM – Electronic Markets, 22*(4), 197–202. Springer.

Bundesamt für Sicherheit in der Informationstechnik (BSI)—Federal Office for Information Security. (2011). The IT security situation in Germany in 2011, BSI, https://www.bsi.bund.de/EN/Publications/SecuritySituation/SecuritySituation_node.html. Accessed 27 Feb 2014.

Buneman, P., Khanna, S., & Tan, W. C. (2001). Why and where: A characterization of data provenance. *ICDT 2001*, LNCS 1973. Springer, pp. 316–330.

Camenisch, J., & Lysanskaya, A. (2001). An efficient system for non-transferable anonymous credentials with optional anonymity revocation. *EUROCRYPT'01*, LNCS 2045. Springer, pp. 93–118.

Chaum, D. (1985). Security without identification: transaction systems to make big brother obsolete. *Communications of the ACM, 28*(10), 1030–1044. ACM.

Dekker, M., Karsberg, C., & Lakka, M. (2013). Annual incident reports 2012—analysis of article 13a incident reports. European Union Agency for Network and Information Security (ENISA), http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2012. Accessed 27 Feb 2014.

Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI). (2012). DIVSI Milieu study on trust and security on the Internet, condensed version, https://www.divsi.de/publikationen/studien/divsi-milieu-studie/. Accessed 27 Feb 2014.

Dolev, D., & Yao, A. C. (1983). On the security of public key protocols. *IEEE Transactions on Information Theory, 29*(2), 198–208. IEEE Computer Society.

Domingos, P. (2012). A few useful things to know about machine learning. *Communications of the ACM, 55*(10), 78–87. ACM.

European Commission. (2009). Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services. *Official Journal of the European Communities, L 337*, 37–69.

European Commission. (2010). A digital agenda for Europe. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM 245 final/2.

Fischer, M. J., Lynch, N. A., & Paterson, M. S. (1985). Impossibility of distributed consensus with one faulty process. *Journal of the ACM, 32*(2), 374–382. ACM.

Freire, E., Hofheinz, D., Kiltz, E., & Paterson, K. (2013). Non-interactive key exchange. *PKC 2013*. LNCS 7778, Springer, pp. 254–271.

Furubotn, E. G., & Richter, R. (2005). *Institutions and economic theory: The contribution of the new institutional economics* (2nd ed.). Ann Arbor: University of Michigan Press.

Gärtner, F. (1999). Fundaments of fault-tolerant distributed computing in asynchronous environments. *ACM Computing Surveys, 31*(1), 1–26. ACM.

Gilliot, M., Matyas, V., & Wohlgemuth, S. (2009). Privacy and identity. *The Future of Identity on the Information Society*. Springer, pp. 351–390.

Haimes, Y. Y. (2009). On the definition of resilience in systems. *Risk Analysis, 29*(4), 498–501. Society for Risk Analysis.

Hilty, M., Basin, D., & Pretschner, A. (2005). On obligations. *ESORICS'05*, LNCS 3679, Springer, pp. 98–117.

Holling, C. S. (2001). Understanding the complexity of economic, ecological, and social systems. *Ecosystems, 4*(5), 390–405. Springer.

Huang, L., Joseph, A. D., Nelson, B., Rubenstein, I., & Tygar, J. (2011). Adversarial Machine Learning. *4th ACM Workshop on Security and Artificial Intelligence*, ACM, pp. 43–58.

IBM Corporation. (2008). A mandate for change is a mandate for smart. IBM Smarter Planet, https://www.ibm.com/smarterplanet/global/

files/us__en_us__overview__68655_08_522_11092012.pdf. Accessed 27 Feb 2014.

Karjoth, G., Schunter, M., & Waidner, M. (2002). Platform for enterprise privacy practices: Privacy-enabled management of customer data. *2nd International Conference on Privacy-Enhancing Technologies (PET'02)*. Springer, pp. 69–84.

Naehrig, M., Lauter, K., & Vaikuntanathan, V. (2011). Can homomorphic encryption be practical? *3rd ACM Workshop on Cloud Computing Security (CCSW'11)*, ACM, pp. 113–124.

Pfitzmann, A., & Hansen, M. (2010). Anonymity, unlinkability, unobservability, pseudonymity, and identity management—A consolidated proposal for terminology. *Anon Terminology v0.34*, TU Dresden and ULD Schleswig-Holstein, http://dud.inf.tu-dresden.de/Anon_Terminology.shtml. Accessed 27 Feb 2014.

Pfitzmann, B., & Waidner, M. (1992). Unconditional byzantine agreement for any number of faulty processes. *STACS'92*, LNCS 577, Springer, pp. 339–350.

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

Prime Minister of Japan and His Cabinet. (2013). Declaration to be the world's most advanced IT nation. Strategic headquarters for the promotion of an advanced information and telecommunications network society, http://japan.kantei.go.jp/policy/it/2013/0614_declaration.pdf. Accessed 27 Feb 2014.

Rannenberg, K., Pfitzmann, A., & Müller, G. (1999). IT security and multilateral security. *Multilateral Security in Communications—Technology, Infrastructure, Economy.* Addison-Wesley-Longman, pp. 21–29.

Riemer, K., Steinfield, C., & Vogel, D. (2009). eCollaboration: on the nature and emergence of communication and collaboration technologies. *EM – Electronic Markets, 19*(4), 181–188. Springer.

Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. (2009). Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds. 16th ACM CCS, ACM, pp. 199–212.

Sackmann, S., Strüker, J., & Accorsi, R. (2006). Personalization in privacy-aware highly dynamic systems. *Communications of the ACM, 49*(9), 32–38. ACM.

Samarati, P., & de Capitani di Vimercati, S. (2001). Access control: Policies, models, and mechanisms. *FOSAD 2000*. LNCS 2171, Springer, pp. 134–196.

Sonehara, N., Echizen, I., & Wohlgemuth, S. (2011). Isolation in cloud computing and privacy-enhancing technologies. *Special Issue 'Sustainable Cloud Computing' BISE, 3*(3), 155–162. Gabler.

Van der Aalst, W. (2012). Process mining. *Communications of the ACM, 55*(8), 76–83. ACM.

Wahlster, W., & Müller, G. (2013). Placing humans in the feedback loop of social infrastructures – NII research strategies on cyber-physical systems. *Informatik Spektrum, 36*(6), 520–529. Springer.

Wang, C., & Ju, S. (2006) The dilemma of covert channels searching. *Information Security and Cryptology – ICISC 2005*, LNCS 3935, Springer, pp. 169–174.

Weitzner, D. J., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J., & Sussman, G. J. (2008). Information accountability. *Communications of the ACM, 51*(6), 82–87. ACM.

Whitten, A., & Tygar, J. D. (1999). Why Johnny can't encrypt: A usability evaluation of PGP 5.0', *8th USENIX Security Symposium Volume 8 (SSYM'99)*, pp. 169–184.

Wohlgemuth, S., & Müller, G. (2006). Privacy with delegation of rights by identity management, *ETRICS 2006*, LNCS 3995, Springer, pp. 175–190.

Wohlgemuth, S., Echizen, I., Sonehara, N., & Müller, G. (2010). Tagging disclosures of personal data to third parties to preserve privacy. *SEC 2010*, IFIP AICT 330, IFIP, pp. 241–252.