A. Weisbecker, M. Burmester & A. Schmidt (Hrsg.): Mensch und Computer 2015 Workshopband, Stuttgart: Oldenbourg Wissenschaftsverlag, 2015, S. 667-676.

Resilience by Usable Security

Sven Wohlgemuth

Abstract

Resilience is introduced as the new security goal supported with security/safety-related information by data-centric services for predictive risk management in real-time. The problem is that data-centric services threaten resilience. Although privacy as a state of equilibrium and its enforcement with usable security by identity management aims actually at decreasing users' own risk, its use by data-centric services for unilateral information flow control hinders maximizing entropy of information. This work shows that cooperative privacy approximates maximal entropy. For this purpose, this work proposes multilateral information control with an observer as the core software library of identity management.

1 Resilience and Information

Resilience is getting importance as the new security model of societies and information systems for supporting their sustainability by achieving a state of equilibrium in real-time and in spite of incidents of any kind. In 2015, the G7 Summit has decided to strengthen resilience of societies by a predictive climate risk management and a climate risk insurance for their safety and sustainability (G7 Summit 2015). The European Commission prescribes resilience as the security goal of operative risk management for economy (European Commission 2013a) and as a proposal for cybersecurity (European Commission 2013b) and the General European Data Protection Directive (European Commission 2012). All include personal accountability of users on operating an adequate risk management and the authenticity of their reports together with sanctions in case of non-compliance. Data-centric services should predict and prevent safety and security incidents by means of Big Data analytics on security vulnerabilities and incidents for optimizing one's own risk. Their implementation with Internet of Things (ITU 2005), Cloud Computing (Mell and Grance 2011), and machine learning schemes (Wahlster and Müller 2013) should allow scalability.

While data-centric services should improve resilience, they also threaten resilience (Müller et al. 2012). Data-centric services tend to monopolies. It has already been shown that data analytics lead to a competitive advantage in productivity. In order to decrease the error rate of derived statistical information, data-centric services need to increase the entropy of information for their statistics. Users remain, in turn, using data-centric services with an acceptable error rate. This is their lock-in effect. At the same time, data-centric services increase their service portfolio by secondary use of their information and letting their users participate as (open source) software developers. Using additional services increases, in turn, the amount of information of the data-centric service. This network effect increases its market share. Furthermore, a secondary use of information allows to decrease the marginal costs of the data-centric service and force competitors out. On the one side, this increases the error rate of information by a data-centric service. On the other side, the risk of users on using information of a data-centric service remains the same.

This work points out that a cooperative privacy protection as informational self-determination achieves an optimal entropy of information. This, in turn, optimizes each user's own risk (Faisst and Prokein 2005). Technically, a cooperative protection of privacy is possible. Already by now, data-centric services follow information self-determination to protect their information unilaterally by information flow control. With the aim of optimizing entropy of information for a data-centric service and its users, this work proposes multilateral information flow control and a design of a software library of an observer for evaluating and comparing privacy of information processing. Section 2 introduces usable security for privacy in order to technically support resilience. Section 3 reports on the state-of-the-art on usable security by a toolbox of privacy mechanisms according to the AAA trust infrastructure. Section 4 introduces data-centric services as the new privacy phenomenon, since privacy protection is applied by their providers instead of their users. Section 5 discusses cases for information flow control in order to increase entropy of information. It derives the need of a multilateral information flow control with privacy for maximal entropy. Section 6 introduces a design of the observer as the core software library for identity management. Section 7 concludes this work.

2 Multilateral and Usable Security

Resilience aims at preventing system failure by achieving a state of equilibrium of opposite interests for this system and over a certain period of time while taking its dependencies into consideration. Regarding security, Multilateral Security has the same meaning for an information exchange according to its IT protection goals (Rannenberg et al. 1999). It results in a privacy policy on information flow control for privacy as informational self-determination. The protection goal implication results that users have to balance explicitly their interests in accountability and unobservability, whereas the configuration of the others can be derived by an identity manager as the personal security tool (Jendricke and Gerd tom Markotten 2000). Enforcement of a multilateral security setting is, however, not certain by a combination of secure atomic information systems, which implements a data-centric service. Multilateral Security considers users in addition to an information system as a "vulnerability" and source of an incident on information loss, e.g. compromised by malware, and its propagation via dependencies. For information system, this is observed for the Internet of Things and Cloud Computing (BSI 2015). The security model of (Dolev and Yao 1983) proposes cryptography and considers compromised participants of a data-centric service. The enforcement relies on the authentic exchange of cryptographic keys.

Whereas correctness of the security model, cryptographic schemes, and their implementation can be formally verified and certified, usable security has in open information systems not been solved so far. Existing user clients for IT security based on cryptography and the organizational model of a PKI, Pretty Good Privacy (PGP) for the Web of Trust (Whitten and Tygar 1999) and the evaluation of the Signtrust eID client, which has been certified for the German national PKI according to the German Signature Act for qualified electronic signatures, have shown vulnerability for information loss due to a semantic mismatch between the technical security prerequisites of a PKI and users' individual security expertise and interest (Gerd tom Markotten 2002). Even though a user interface would fit to all kind of user classes, the increasing number of dependencies during runtime introduce inevitable, unknown dependencies as a conceptual vulnerability for information loss. The challenge for usable security is to protect identity-related information, which is shared with information systems of other users, before the other one's software code is being executed. Security properties of information systems should be identified before granting access (Müller et al. 2007).

3 ATUS – A Toolkit for Usable Security

Information flow control follows in practice the AAA authorization framework for accounting by authentication and enforcement with electronic identity and authorization with access control (Vollbrecht et al. 2000). Its four use cases (1) *Single Domain Case*, (2) *Roaming*, (3) *Distributed Services*, and (4) *Combining Roaming and Distributes Services* distinguish between an information exchange between two organizations (cases 1 and 2) and via a third party (cases 3 and 4). According to the classification of the AAA authorization framework, state-of-the-art on privacy mechanisms for usable security are classified in the following. The increasing number of dependencies during runtime with a data-centric service introduces inevitable, unknown dependencies as conceptual vulnerability for information loss. Accountability of information is proposed to extend the control system for data-centric services (Wohlgemuth and Müller 2006, Weitzner et al. 2008).

Privacy Policy Framework provides the mathematical model and tools to formalize and verify its instances and their integration in a continuous evolution of communities of trusted users and information systems. It takes the scalability of data-centric services into account by the security model and its enforcement with using adequate risk controls and the in-time response to a change even in a decentralized organization. The security policy model is distributed usage control (Pretschner et al. 2006), since it assumes a decentralized information flow control and allows with obligations modification during run-time without conceptually threatens information. The mathematical model is the general PKI evaluation model (Maurer 1996), since it evaluates authentication of cryptography-base information from a user-centric view as a set of statements on a PKI. This model allows evaluation of several certification paths for the same key, i.e. several origin of information and their aggregation, in order to increase user's confidence in the resulting derived information on privacy. Incidents by configuration are still possible and calls for an operator to detect conflicts of policy rules (Sackmann and Kähmer 2008), model checking of privacy policies (Accorsi 2013), and re-writing (Höhn 2009).

Privacy Authentication refers to distributed trust management (Blaze et al. 1996) in which access to information is granted according to authentication with a certain cryptographic key and its certified authorization with a credential. Trust management has been extended with unobservability by means of revocable non-linkability with pseudonyms and privacy-preserving attribute-based credentials. As an abstraction on cryptography and the PKI, partial identities represent role-based authentication for an information exchange as implemented with the mobile identity manager iManager (Wohlgemuth et al. 2004).

Privacy Authorization specifies a privacy policy on using personal-related information for isolation of an information exchange during run-time (Sonehara et al. 2011). While avoiding loss of control on information when applying trust management on information exchange with a third party, higher cryptographic protocols of DREISAM for non-linkable delegation of rights specify an authorized information exchange during run-time (Wohlgemuth 2008).

Privacy Accountability generates a statement on information loss on a given isolation. In accordance to the communication model of (Shannon 1948), privacy mechanisms have to focus on data traces as edges between nodes and within nodes of a directed communication graph. Secure logging collects and logs system events of single information systems as $evidence_{node}$ on internal information processing while at the same time allowing unobservability by cryptographic based secure logging with user-centric views (Accorsi 2013). Higher cryptographic protocols of DETECTIVE connect the electronic identity of each information provider with the one of the consumer along an isolation. This results in $evidence_{edge}$ while users remain unobservable (Wohlgemuth et al. 2010).

Privacy Accounting derives a *privacy evidence* on information loss of an authorized information processing and so on isolation (Sackmann et al. 2006). At present, *Privacy Accounting* considers privacy evidences separately for each system resulting in $evidence_{node}$ and between systems resulting in $evidence_{edge}$. Regarding authentication, a user combines $evidence_{node}$ and $evidence_{edge}$ with the existing set of (derived) information on authentication, authorization, certification, and reliability of the information sources. For future communication, information is derived on privacy evidences of the past and assumptions for getting a statement on the acceptable security model. An option for its user interface is a privacy dashboard (Zimmermann et al. 2014).

The systematic development of these privacy mechanisms and their integration in data-centric services needs to take security and usability requirements for the development of Internet applications into account in order to reduce users' individual risk. According to *Privacy by Design*, User-Centric Security Engineering (UCSEC) combines accordingly security engineering with usability engineering by integrating users in the threat and security model for user interface development with standardized criteria (Gerd tom Markotten 2002).

4 The new Privacy Phenomena: Data-Centric Service

With the productivity gain and scalability of data-centric services, IT more and more takes over the control on critical infrastructures of a society. Data-centric services act as adaptive Internet services for a broad spectrum of target user groups. The user interface is multimodal and adaptive to the user (Wahlster 1998). Access to information as the asset and product of data-centric services needs to be controlled according to the security interest of a data-centric service provider. Actually, data-centric services makes already more or less use of the concepts of the presented privacy tools. They isolate information flow by (hardware-based) sandboxes as used for mobile smart devices (Alkassar et al. 2012) The implementation of web browser based interfaces is often open source in order to facilitate access to users as software developers in order to integrate the data-centric service in their application.

The *Privacy Policy Framework* of data-centric services considers access control according to the AAA authorization framework. The formalized representation of trust relationships is by the social graph of their users including their applications. Regarding *Privacy Authentication*, identity management clients are based on cryptography and PKI and partially support pseudonymity of users and non-linkability of credentials. Microsoft U-Prove and the open source electronic identity managers IBM idemix and Shibboleth are examples for pseudonymity and non-linkable credentials whereas PersoApp supports pseudonymity of a user as service consumer. Regarding *Privacy Authorization*, some services support *Roaming* with their integration in other data-centric services. According to the knowledge of the author, none data-centric service supports disclosure of information to a third party with information flow control. *Privacy Accountability* is achieved by internal data provenance for a social graph. *Privacy Accounting* is run by machine learning to construct and adapt social graph to current and future security vulnerabilities and incidents and therewith related security information.

With the exception of *Privacy Authentication*, usability of privacy tools by data-centric services is unilateral. It provides neither information exchange at all, spontaneous information exchange with a third party nor transparency for their users in order to check authentication of information, on the one side. On the other side, their users are accountable for their use. Regulations for protecting electronic communication (European Commission 2014) and amendment for personal information processing (European Commission 2012) exclude accountability for safety, public security, and national interests.

5 Optimizing Information and a State of Equilibrium

The communication model of Shannon defines information and the amount of information of an exchange as its entropy (Shannon 1948). Information is threatened by information loss. In case of an incident, entropy of a given information processing is reduced actively by distortion and noise or passively by information leakage. As countermeasure within the basic communication model, transparency of information processing by an observer is necessary to detect active incidents and their origin in order to restore information (Shannon 1948), whereas encryption is a countermeasure against passive incident during transmission (Shannon 1949). A state of equilibrium cannot be achieved, if only the information consumer controls the information processing. Information flow control requires additionally a feedback system as control for the information provider (Wiener 1961). A control-loop with feedback embraces the information processing of the consumer. The control-loop of an information source gets informative feedback by which the user predicts a critical state and proactively response.

Three cases for entropy exist according to its mathematical definition (Shannon 1949) with $n = 2$ random variables to illustrate entropy in accordance to the two general views on information control of a data-centric service by its users and its provider: $H = -K \sum_{i=1}^{n} p_i log p_i \ with \ K \ is \ a \ positive \ constant.$

Case 1 (trivial) $p_1 = p_2 = 0$: Neither users control nor the provider of a data-centric service controls the information processing. Authentication of information is a matter of trust without the possibility of checking authentication, e.g. compliance to the corresponding regulations. The entropy is zero: $H = 0$

Case 2 (unilateral) $\{\exists! \, p_i > 0 | i, j \epsilon \{n = 2\} \land i \neq j \land \forall j: p_j = 0\}$: Either the provider controls or users control the information processing of a data-centric service. If the user of a data-centric service enforces control, unilateral data economy takes place with anonymity as the worst case in that the user doesn't use this data-centric service and a gain in productivity doesn't take place or this data-centric service stops providing its service. Latter is the risk of the provider. The other case is the unilateral case of information flow control at present by the provider of a data-centric service. In both unilateral cases, information on accountability of information loss and so the individual risk of each user and provider is not optimized. $H = 0$, if the outcome is already known to the provider or users are anonymous, otherwise $H > 0$

Case 3 (multilateral) $p_1 = p_2 = \frac{1}{2}$: Both users and the provider of a data-centric service control in cooperation the information processing by informative feedback. Entropy of information processing of a data-centric service is maximized: $H = log n; here \ H = log 2$ as long as it is information. If all data is known to users and provider without change, the data-centric service is not required anymore. However, Shannon and Wiener both assume for control by transparency the origin of an information loss during transmission. Whereas this assumption holds in closed information systems, where each state transition can be observed, this is not the case for data-centric services (BSI 2015). Actually, this calls for multilateral information flow control with cooperative privacy in protecting one's own valuable information and information processing by unobservability while controlling the information processing of the other participants indirectly by deriving statistical statements on anomalies in nodes and edges of an information exchange as privacy evidences. Since technical privacy mechanisms as risk control approximate a state of equilibrium but might not achieve it due to unknown incidents, non-technical risk controls as legal regulations and economic instruments should complement multilateral information flow control for optimizing one own's risk.

In general for the multilateral case, the random variables have the same probability. Each user needs to compare his privacy evidences on the data-centric service with the one of the others. Collaborative benchmarking allows such a comparison in accordance to the threat model of Multilateral Security and Dolev and Yao with the assumption of a compromised or untrusted data-centric service and homomorphic encryption (Kerschbaum 2011). This requires a formalization of privacy mechanisms for risk control and their effect on a privacy evidence as key performance indicators and its values. Since multilateral information flow control allows users of data-centric services to increase entropy stepwise by data economy, it supports community building of a *Web of Trust with productivity advantage by data-centric services.*

6 Core Software Library for Identity Management

This design of the core software library for implementing the observer is derived from a general cryptographic key management library (Wohlgemuth 1999). Figure 1illustrates its design of an observer as a data-centric service.

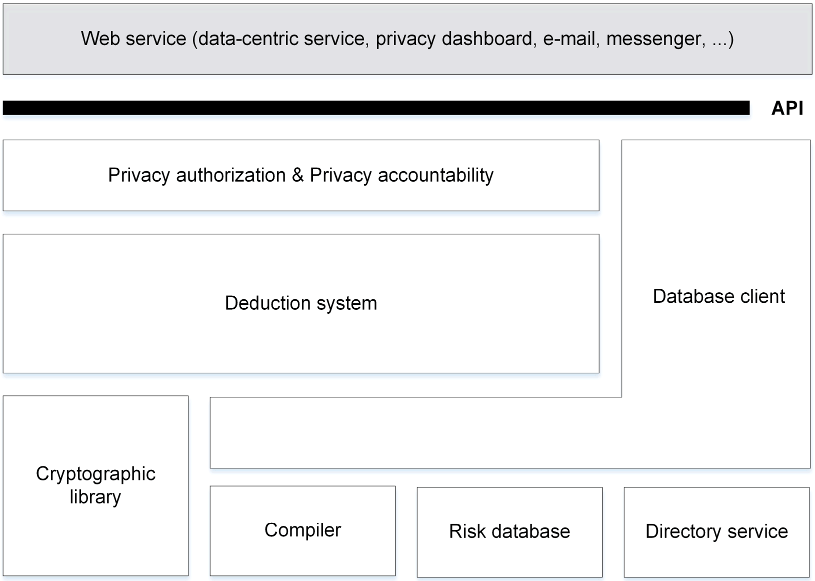
Web service (data-centric service, privacy dashboard, e-mail, messenger, ...)
API
Privacy authorization & Privacy accountability
Deduction system
Database client
Cryptographic library
Compiler
Risk database
Directory service

Figure 1 Design of the observer as core software library of identity management.

The *Privacy authorization & Privacy accountability* module offers variations for evaluating privacy evidences. They relate to authentication information about a cryptographic key, an identity, authorization, and strategies for isolation at a given point of time. It implements the cryptographic protocols for non-linkable delegation of rights, secure logging of an electronic identity, data provenance between electronic identities, and the collective benchmarking protocol. It calls the *Deductive system* and transforms its results for the privacy dashboard.

The *Deductive system* is the core part. It implements the evaluation model for the user's view on a PKI by a graph. The user instruments the evaluation system by the isolation policy and risk scenario for the required entropy of the given data-centric service. During a run of an evaluation, trust relationships between users and evidences on information loss will be identified and derived. If a required evidence is not available, the *Deductive system* queries it from a trusted user, a vulnerability database, or a database for isolation patterns by using the module *Directory client*. If a comparison on isolation and entropy with another data-centric service is required, the *Deductive system* starts a benchmarking process via the module *Query*. Feedback from a query will be transformed to a logical statement by the *Compiler*. Before processing an evidence, its validity is checked against time and revocation. Privacy evidences and isolation patterns are stored in the *Directory service* and *Risk database*, respectively.

The *Cryptographic library* provides the cryptographic primitives for the higher authentication, authorization, and data provenance protocols. The *Directory client* is the interface to non-volatile memory. It serves as a reference monitor for enforcing authorized access requests. It supports the evaluation of the *Deductive system* with retrieving the certification chains on keys, authorization and revocation. Whereas the *Directory service* considers electronic identities and evidences on information loss, the *Risk database* supports the logic representation of isolation and operates as an application framework for the *Deductive system*. The *Compiler* serves for interoperability of information and for import and export of logical statements.

7 Conclusion

Resilience and privacy with usable security are not "standalone applications" but require adaptive communities for cooperation between acceptable trusted users and correct information systems. The proposed multilateral information flow control architecture as a data provenance system with user-centric identity management should serve as a workbench for resilience. A challenge is to bootstrap multilateral information flow control while underlying inevitable vulnerabilities. Complementing non-technical risk controls need to be developed with the support of the workbench. The author welcomes cooperation on a trustworthy base.

Acknowledgement

I would like to thank Günter Müller for the valuable discussions, Kai Rannenberg for letting me participate as a visiting researcher, and the reviewers for their constructive comments.

References

Alkassar, A., Schulz, S., Stüble, S. & Wohlgemuth, S. (2012). Securing Smartphone Compartments: Approaches and Solutions. In: *ISSE 2012*. Heidelberg: Springer, pp. 260-268.

Accorsi, R. (2013). A secure log architecture to support remote auditing. *Mathematical and Computer Modelling 57(7-8)*, 1578-1591.

Blaze, M., Feigenbaum, J. & Lacy, J. (1996). Distributed Trust Management. In: *IEEE Symposium on Security and Privacy 1996*. Oakland, CA: IEEE, pp. 164–173.

BSI (2015). *The State of IT Security in Germany 2014*. Bundesamt für Sicherheit in der Informationstechnik/ Federal Office for Information Security (BSI).

Dolev, D. & Yao, A.C. (1983). On the Security of Public Key Protocols. *IEEE Transactions on Information Theory 29(2)*, 350-357

European Commission (2012). *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. COM(2012) 11 final.

European Commission (2013). REGULATION (EU) No 575/2013 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 June 2013 on prudential requirements for credit institutions and investment forms and amending Regulation (EU) No 648/2012. *Official Journal of the European Union, L 176*, 1-337.

European Commission (2013). *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* JOIN (2013) 1 final.

European Commission (2014). REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal markets and repealing Directive 1999/93/EC. *Official Journal of the European Communities, L 257*, 73-114.

Faisst, O. & Prokein, O. (2005). An Optimization Model for the Management of Security Risks in Banking Companies. In Müller, G. & Kwei-Jay. L. (eds.): *CEC 2005*. Los Alamitos: IEEE, pp. 266-273.

G7 Summit (2015). *Leaders' Declaration G7 Summit 7-8 June 2015*. Think Ahead. Act Together, An morgen denken. Gemeinsam handeln. The Federal Government.

Gerd tom Markotten, D. (2002). *User-Centered Security Engineering*. NordU2002-The 4:rd EurOpen/USENIX Conference.

Höhn, S. (2009). Model-based reasoning on the achievement of business goals. In: *SAC '09*. New York: ACM, pp. 1589-1593.

ITU (2005). *ITU Internet Reports 2005: The Internet of Things*. International Telecommunication Union.

Jendricke, U. & Gerd tom Markotten, D. (2000). Usability meets security – the Identity-Manager as your personal security assistant for the Internet. In: *ACSAC'00*. IEEE, pp. 334-353.

Kerschbaum, F. (2011). Secure and Sustainable Benchmarking in Clouds. *Business & Information Systems Engineering 3(3)*, 135-143.

Maurer, U. (1996). Modeling a Public-Key Infrastructure. In: Martella, G., Kurth, H., Montolivo, E. & Bertino, E. (eds.): *ESORICS 1996*. Heidelberg: Springer, pp. 325-350.

Mell, P. & Grance, T. (2011). *The NIST Definition of Cloud Computing. NIST Special Publication 800-145*. National Institute of Standards and Technology – NIST.

Müller, G., Flender, C. & Peters, M. (2012). *Vertrauensinfrastruktur und Privatheit als ökonomische Fragestellung*. In: Buchmann, J. (ed.): Internet Privacy Eine multidisziplinäre Bestandsaufnahme/A multidisciplinary analysis. Acatech STUDIE, pp. 143-188.

Müller, G., Gilliot, M. & Wohlgemuth, S. (2007). *Abschlussbericht des DFG-Schwerpunktprogramms "Sicherheit in der Informations- und Kommunikationstechnik" (SPP 1079), Sprecher: Prof. Dr. Günter Müller Universität Freiburg.* Technical report, Albert-Ludwigs University Freiburg, Germany.

Pretschner, A., Hilty, M. & Basin, D. (2006). Distributed usage control. *CACM 49(9) special issue Müller, G. (ed.) Privacy and security in highly-dynamic systems*, 39-44.

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

Sackmann, S. & Kähmer, M. (2008). ExPDT: Ein Policy-basierter Ansatz zur Automatisierung von Compliance. *WIRTSCHAFTSINFORMATIK 50(5)*, 366-374.

Sackmann, S. Strüker, J. & Accorsi, R. (2006). Personalization in privacy-aware highly dynamic systems. *CACM 49(9) special issue Müller, G. (ed.) Privacy and security in highly-dynamic systems*, 32–38.

Shannon, C.E. (1948). A mathematical theory of communication. *The Bell System Technical Journal 27(3)*, 379-423.

Shannon, C.E. (1949). Communication Theory of Secrecy Systems. *The Bell System Technical Journal 28(4)*, 656-715.

Sonehara, N., Echizen, I. & Wohlgemuth, S. (2011). Isolation in Cloud Computing and Privacy-Enhancing Technologies. *Business & Information Systems Engineering 3(3)*, 155-162.

Vollbrecht, J., Calhoun, P., Farrell, S., Gommans, L., Gross, G., de Bruijn, B., de Laat, C., Holdrege, M. & Spence, D. (2000). *AAA Authorization Framework – RfC 2904*. Network Working Group.

Wahlster, W. (1998). Adaptive Internet-Dienste. In: Jähnichen, S. (ed.): *Informationstechnik im Zeitalter des Internet*. Velbert: Online Verlag, 201 -211.

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.

Weitzner, D.J., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J. & Sussman, G.J. (2008). Information Accountability. *CACM 51(6)*, 82-87.

Whitten, A. & Tygar, J.D. (1999). Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In: *8th USENIX Security Symposium*. Washington D.C., pp. 169-184.

Wiener, N. (1961). *Cybernetics: or control and communication on the animal and the machine, second edition.* Cambridge: The MIT Press.

Wohlgemuth, S. (1999). Schlüsselverwaltung – Objektorientierter Entwurf und Implementierung. *Informatiktage 1999 Fachwissenschaftlicher Informatik-Kongress der GI*. Leinfelden: Konradin Verlag R. Kohlhammer GmbH.

Wohlgemuth, S., Echizen, I., Sonehara, N. & Müller, G. (2010). Tagging Disclosures of Personal Data to Third Parties to Preserve Privacy. In: Rannenberg, K., Varadharajan, V. & Weber, C. (eds.): *IFIP SEC 2010*. Heidelberg: Springer, pp. 241–252.

Wohlgemuth, S. Jendricke, U., Gerd tom Markotten, D., Dorner, F. & Müller, G. (2004). Sicherheit und Benutzbarkeit durch Identitätsmanagement. In Spath, D. & Haasis, K. (eds.): *doIT Software-Forschungstag 2003, Aktuelle Trends in der Softwareforschung*. Stuttgart: IRB Verlag, pp. 241-260.

Wohlgemuth, S. & Müller, G. (2006). Privacy with Delegation of Rights by Identity Management. In: Müller, G. (ed.): *ETRICS 2006*. Heidelberg: Springer, pp. 175-190.

Zimmermann, C., Accorsi, R. & Müller, G. (2014). Privacy Dashboards: Reconciling Data-Driven Business Models and Privacy. In Mulliner, C., Weippl, E. & Teufel, S. (eds.): *ARES 2014*. CPS: IEEE, pp. 152-157.

Kontaktinformationen

Sven Wohlgemuth, Dr.; E-Mail: wohlgemuth@acm.org