Seminar Topics Winter Term 17/18 - Security and Privacy in the Information Society
Prof. Dr. Dr. h.c. Günter Müller
University of Freiburg

Fields and Topics for the Seminar: Security and Privacy in the Information Society

This seminar has the objective to discuss the role of new technologies in Informatics from a privacy and security perspective with regard to enabling new modes of operation in energy systems, known as smart grids or other modern services, e.g. business processes, or even advanced machine learning applications. A useful management of renewable energy is only possible if demand and supply can be matched. This requires the collection, storage and processing of data, including personal data. In other applications, the detection of fraud or the intention to manipulate user behavior is the core target of contributions.

In the following, we introduce each of these four subject areas, give basic literature and list the corresponding topics.

1. Is there Technology Enabling Privacy in Smart Grids?

The so-called Smart-Grid as a supporting pillar for the success of the energy transformation promises an efficient control of renewable energy. Simultaneously numerous barriers and risk come along with this technological innovation. In particular, the gathering of consumption data by using intelligent meters (Smart meter) required for operation and coordination threatens the households' privacy.

The scenario for attacks on privacy and its risks is part of the work, and largely depends upon your fantasy. The solution and approach to ensure privacy and reduce risk is defined by the papers content. Please apply the paper, discuss the scenario, the method, and the pro and con of the method.

Karwe, Markus, and Günter Müller. "DPIP: A Demand Response Privacy Preserving Interaction Protocol." International Conference on Business Information Systems. Springer, Cham, 2015.

Jawurek, Marek, Florian Kerschbaum, and George Danezis. "SoK: Privacy technologies for smart grids—A survey of options." Microsoft Res., Cambridge, UK (2012).

Soria-Comas, Jordi, and Josep Domingo-Ferrer. "Big data privacy: challenges to privacy principles and models." Data Science and Engineering 1.1 (2016): 21-28. https://link.springer.com/article/10.1007/s41019-015-0001-x

Topic 1: L-diversity: Privacy beyond k-anonymity
http://dx.doi.org/10.1145/1217299.1217302

Topic 2: Basic concepts and taxonomy of dependable and secure computing
http://dx.doi.org/10.1109/TDSC.2004.2

Topic 3: Differential Privacy: A Survey of Results
http://dx.doi.org/10.1007/978-3-540-79228-4_1

Topic 4: Differential privacy under fire
http://static.usenix.org/events/sec11/tech/full_papers/Haeberlen.pdf

Topic 5: Compliance monitor for early warning risk determination
http://link.springer.com/article/10.1007%2Fs11576-008-0079-0

2. Machine Learning: A new Challenge for Privacy?

Machine learning maybe seen as a reversal of long custom where the user learns how the machine works, instead the machine learns from the user exploiting stored data and predicting future behavior. This section offers two topics. By applying machine learning techniques and analysis the normativity of results should be analyzed. The second case is a case study of methods applied by the company Cambridge Analytica regarding the US presidential election. Both topics have the policy – architecture link as a common topic, where the results may depend upon the programmers or the algorithms rather than on humans alone.

Kubat, Miroslav. Introduction + Chapter 1, in: An Introduction to Machine Learning. Springer, 2015. https://link.springer.com/book/10.1007%2F978-3-319-20010-1

Kosinski, Michal, David Stillwell, and Thore Graepel. "Private traits and attributes are predictable from digital records of human behavior." Proceedings of the National Academy of Sciences 110.15 (2013): 5802-5805. http://www.pnas.org/content/110/15/5802.short

Topic 6: Is Analysis and design of Algorithms dependent upon normative intentions?

Use cases in e.g. autonomic driving and TAY from Microsoft, where access to big Data and algorithms for machine learning had effects on the outcome of actions.

Andrejevic, Mark, and Kelly Gates. "Big data surveillance: Introduction." Surveillance & Society 12.2 (2014): 185-196.https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/bds_ed/5135

Kraemer, Felicitas, Kees Van Overveld, and Martin Peterson. "Is there an ethics of algorithms?." Ethics and Information Technology 13.3 (2011): 251-260.

Topic 7: Show examples of personality tests and how they can be used for Big Data and assessment of people's behavior?

Use OCEAN from Psychology to find examples in the net.

https://www.outofservice.com/bigfive/

John, Oliver P., Laura P. Naumann, and Christopher J. Soto. "Paradigm shift to the integrative big five trait taxonomy." *Handbook of personality: Theory and research* 3 (2008): 114-158.

Kosinski, Michal, et al. "Mining big data to extract patterns and predict real-life outcomes." Psychological methods 21.4 (2016): 493.

3. Paradigm Shift in Business Process Security?

From the Société Générale scandal with loss of nearly five billion Euro caused by shuffling transactions to more recent scandals, for instance in the automotive industry (e.g. the "Dieselgate") — the increasing number of corporate fraud cases under- line the growing demand for security and control in enterprises and their corresponding information systems. All these frauds and security vulnerabilities could be traced to processes or workflows. This topic discusses process analysis with regard to process management as well as process mining. Classic computer security usually follows the CIA triad, trying to achieve or sustain confidentiality, integrity and availability, or simply "keeping bad things from happening". Security in business processes, however, should also consider to "make good things happen" by reaching the intended goals even if partially the security objectives are endangered.

Marlon Dumas, Marcello La Rosa, Jan Mendling, Hajo A. Remiers: Introduction to Business Process Management, in: Fundamentals of Business Process Management
https://link.springer.com/chapter/10.1007/978-3-642-33143-5_1

Wil M.P. van der Aalst: Process Mining: The Missing Link, in: Process Mining - Data Science in Action.

https://link.springer.com/chapter/10.1007/978-3-662-49851-4_2

Topic 8: Security and Privacy in Business Process Management

Günter Müller, Rafael Accorsi: Why Are Business Processes Not Secure?
https://link.springer.com/chapter/10.1007%2F978-3-642-42001-6_17

Mathias Weske: Business Process Management - Concepts, Languages, Architectures
https://link.springer.com/book/10.1007%2F978-3-642-28616-2

Marlon Dumas, Marcello La Rosa, Jan Mendling, Hajo A. Remiers: Fundamentals of Business Process Management https://link.springer.com/book/10.1007/978-3-642-33143-5

Topic 9: Which connections from „Security and Privacy" can be drawn to Process Mining?

Wil M.P. van der Aalst: Process Mining - Data Science in Action
http://www.springer.com/de/book/9783662498507

Elham RamezaniDirk FahlandWil M. P. van der Aalst: Where Did I Misbehave? Diagnostic Information in Compliance Checking

https://link.springer.com/chapter/10.1007/978-3-642-32885-5_21

4. Assure all Models of Privacy complete Privacy?

Privacy includes the concealment of personal information as well as the ability to control what happens with this information. The right to privacy can be considered either as a basic and inalienable human right, or as a personal right or possession. The following topics may be seen as case studies in presently intensively discussed fields of technology.

Müller, G., et. al. (2013): Privacy threats and their impact, in: Buchmann, J., Internet Privacy, Springer 2013, S. 61-90

Pearson, Tancock, Charlesworth, Siani, David, Andrew. *"The Emergence of Privacy Impact Assessments"* (http://www.hpl.hp.com/techreports/2010/HPL-2010-63.pdf)

Zimmermann, Christian. Chapter 1, 3, 4.3, in:Privacy through accountability. Diss. Dissertation, Albert-Ludwigs-Universität Freiburg, 2016, 2016. https://freidok.uni-freiburg.de/data/11029

Topic 10: Discuss mode of collection of Data with either Google or any other Social net and make a privacy assessment.

https://academic.oup.com/poq/article/80/S1/298/2223402/Filter-Bubbles-Echo-Chambers-and-Online-News

http://www.heinz.cmu.edu/~acquisti/economics-privacy.htm (A. Acquisti)

Topic 11: Does Blockchain Architecture guarantee privacy?

- Satoshi Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System. White paper, 2008. https://bitcoin.org/bitcoin.pdf

- Vitalik Buterin: Ethereum: A Next-Generation Cryptocurrency and Decentralized Application Platform. In: Bitcoin Magazine. 23. January 2014. https://bitcoinmagazine.com/articles/ethereum-next-generation-cryptocurrency-decentralized-application-platform-1390528211/

- Serguei Popov: The Tangle. White paper, 3. April 2016. http://iotatoken.com/IOTA_Whitepaper.pdf

Topic 12: Why is (re)Captcha not sufficient to assure human identification?

- Von Ahn, Luis, et al. "recaptcha: Human-based character recognition via web security measures." Science 321.5895 (2008): 1465-1468.

- Baecher, Paul, et al. "Breaking reCAPTCHA: a holistic approach via shape recognition." IFIP International Information Security Conference. Springer Berlin Heidelberg, 2011.

https://east-ee.com/2017/02/28/rebreakcaptcha-breaking-googles-recaptcha-v2-using-google/

Seminar Topics Winter Term 17/18 - Security and Privacy in the Information Society
Prof. Dr. Dr. h.c. Günter Müller
University of Freiburg

Topic 13: Secure Authentication and Authorization Protocols for Internet of Things – What new privacy and security threats arise?

Rolf H. Weber, Internet of Things – New security and privacy challenges, Computer Law & Security Review, Volume 26, Issue 1, January 2010, Pages 23-30, ISSN 0267-3649, http://doi.org/10.1016/j.clsr.2009.11.008. (http://www.sciencedirect.com/science/article/pii/S0267364909001939)

Dave Neal: The Svakom Siime Eye endoscopic digital dildo is stuffed with security issues. The Inquirer. https://www.theinquirer.net/inquirer/news/3007760/the-svakom-siime-eye-endoscopic-digital-dildo-is-stuffed-with-security-issues