International Workshop on Privacy Engineering

http://ieee-security.org/TC/SPW2015/IWPE

May 21st, 2015 at the Fairmont, San Jose, CA

Co-located with 36th IEEE Symposium on Security and Privacy

9:00-09:20	**Welcome, introductions and opening remarks**
09:20–10:20	**Privacy: Plural, Contextual, Contestable but not Unworkable. Invited talk by Deirdre K. Mulligan (UC Berkeley)** The scholarly literature presents a dizzying array of diverging definitions of privacy. Privacy is equally ambiguous in practice, where it is invoked to protect a wide range of interests based on an equally wide range of justifications. While the frequency and intensity of privacy debates are evidence of its salience to contemporary life, its contestability has intensely troubling practical consequences. Privacy is decreed too fickle and indeterminate to be advanced through legislative, regulatory, and technical means. Ambiguity becomes an excuse for disregarding privacy claims—despite visceral and broad appeal, and vociferous support. In this talk, I argue that privacy is an "essentially-contested concept," and that its contestability is a source of value and power that ought to be preserved. I then explore the power of a multi-dimensional analytic of privacy for advancing our understanding of privacy's meaning in specific contexts and contests. Using the analytic to unpack privacy claims in high-profile privacy cases reveals the complex array of privacy concepts raised by technical change. Privacy's essential contestability is key to its ongoing relevance and utility in political and social life but leveraging it requires analytical tools that help us ensure that efforts at design focus on the right privacy in a given context.  ***Deirdre K. Mulligan*** *is an Associate Professor in the School of Information at UC Berkeley, co-Director of the Berkeley Center for Law & Technology, Chair of the Board of Directors of the Center for Democracy and Technology, a Fellow at the Electronic Frontier Foundation, and Policy lead for the NSF-funded TRUST Science and Technology Center. Prior to joining the School of Information in 2008, she was a Clinical Professor of Law, founding Director of the Samuelson Law, Technology & Public Policy Clinic, and Director of Clinical Programs at the UC Berkeley School of Law (Boalt Hall). Mulligan's current research agenda focuses on information privacy and security, including exploring users' conceptions of privacy in the online environment and their relation to existing theories of privacy. Her comparative study of privacy practices in large corporations in five countries, conducted with UC Berkeley Law Prof. Kenneth Bamberger, will be published by MIT press this fall.*
Morning Coffee Break	
10:50–12:20	**Session: Systematizing privacy engineering goals** **PRIPARE: Integrating Privacy Best Practices into a Privacy Engineering Methodology** Nicolás Notario, Alberto Crespo, Yod Samuel Martín García, José M. Del Álamo, Daniel Le Métayer, Thibaud Antignac, Antonio Kung, Inga Kroener and David Wright *Data protection authorities worldwide have agreed on the value of considering privacy-by-design principles when developing privacy-friendly systems and software. However, on the technical plane, a profusion of privacy-oriented guidelines and approaches coexists, which provides partial solutions to the overall problem and aids engineers during different stages of the system development lifecycle. As a result, engineers find difficult to understand what they should do to make their systems abide by privacy by design, thus hindering the adoption of privacy engineering practices. This paper reviews existing best practices in the analysis and design stages of the system development lifecycle, introduces a systematic methodology for privacy engineering that merges and integrates them, leveraging their best features whilst addressing their weak points, and describes its alignment with current standardization efforts.*

	Protection Goals for Privacy Engineering Marit Hansen, Meiko Jensen and Martin Rost *Six protection goals provide a common scheme for addressing the legal, technical, economic, and societal dimensions of privacy and data protection in complex IT systems. In this paper, each of these is analyzed for state of the art in implementation, existing techniques and technologies, and future research indications.* **Privacy by Design in Federated Identity Management** Rainer Hörbe and Walter Hötzendorfer *Federated Identity Management (FIM), while solving important scalability, security and privacy problems of remote entity authentication, introduces new privacy risks. By virtue of sharing identities with many systems, the improved data quality of subjects may increase the possibilities of linking private data sets; moreover, new opportunities for user profiling are being introduced. However, FIM models to mitigate these risks have been proposed. In this paper we elaborate privacy by design requirements for this class of systems, transpose them into specific architectural requirements, and evaluate a number of FIM models with respect to these requirements. The contributions of this paper are a catalog of privacy-related architectural requirements, joining up legal, business and system architecture viewpoints, and the demonstration of concrete FIM models showing how the requirements can be implemented in practice.*
Lunch	
13:20–13:30	**Best paper award ceremony**
13:30–14:30	**Privacy as a safety critical concept, Ian Oliver (Nokia Networks)** Privacy's place in software engineering development is tentatively made at best. Yet the effects of information leakage, an improperly made audit and so on are known to be expensive in monetary, legal and other terms. We present here learnings made in adopting ideas from safety-critical systems and disciplines where safety is a first-class concept, such as aviation and medicine. We outline our rationale and describe our experiences - both good and bad - and the necessary concepts that must be understood for successful application of such ideas.  ***Dr Ian Oliver** is a security specialist within Nokia Networks working on Network Function Virtualisation, 5G, Security and Privacy, He also holds a Research Fellow position at the University of Brighton working with the Visual Modelling Group. Prior to these he has worked as the privacy architect and officer for Here and Nokia Services; and for eleven years at Nokia Research Centre working with Semantic Web, UML, formal methods and hardware-software co-design. He has also worked at Helsinki University of Technology and Aalto University teaching formal methods and modelling with UML. He holds over 40 patents in areas such as The Internet of Things, semantic technologies and privacy. He is the author of the book Privacy Engineering: A data flow and ontological approach. More information can be found here: http://www.privacyengineeringbook.net*
14:30–15:10	**Session: Technologies for user-management of privacy** **Extending the Power of Consent with User-Managed Access** Eve Maler *The inherent weaknesses of existing notice-and-consent paradigms of data privacy are becoming clear, not just to privacy practitioners but to ordinary online users as well. The corporate privacy function is a maturing discipline, but greater maturity often equates just*

	to greater regulatory compliance. At a time when many users are disturbed by the status quo, new trends in web security and data sharing are demonstrating useful new consent paradigms. Benefiting from these trends, the emerging standard User-Managed Access (UMA) allows apps to extend the power of consent. UMA corrects a power imbalance that favors companies over individuals, enabling privacy solutions that move beyond compliance **Decentralizing Privacy: Using Blockchain to Protect Personal Data** Guy Zyskind, Oz Nathan and Alex 'sandy' Pentland *The recent increase in reported incidents of surveillance and security breaches compromising users' privacy call into question the current model, in which third-parties collect and control massive amounts of personal data. Bitcoin has demonstrated in the financial space that trusted, auditable computing is possible using a decentralized network of peers accompanied by a public ledger. In this paper, we describe a decentralized personal data management system that ensures users own and control their data. We implement a protocol that turns a blockchain into an automated access-control manager that does not require trust in a third party. Unlike Bitcoin, transactions in our system are not strictly financial – they are used to carry instructions, such as storing, querying and sharing data. Finally, we discuss possible future extensions to blockchains that could harness them into a well-rounded solution for trusted computing problems in society.*
Afternoon Coffee Break	
15:40–16:30	**Session: Surveillance, privacy and infrastructure** **Reviewing for Privacy in Internet and Web Standard-Setting** Nick Doty *The functionality of the Internet and the World Wide Web is determined in large part by the standards that allow for interoperable implementations; as a result, the privacy of our online interactions depends on the work done within standard-setting organizations. But how do the organizational structure and processes of these multistakeholder groups affect the engineering of values such as privacy? This paper reviews the history of considerations for security and privacy in Internet and Web standard-setting; the impact of Snowden surveillance revelations and reactions to them; and some trends in how we review for privacy in Internet and Web standards.* **Privacy Principles for Sharing Cyber Security Data** Gina Fisk, Calvin Ardi, Neale Pickett, John Heidemann, Mike Fisk, Christos Papadopoulos *Sharing cyber security data across organizational boundaries brings both privacy risks in the exposure of personal information and data, and organizational risk in disclosing internal information. These risks occur as information leaks in network traffic or logs, and also in queries made across organizations. They are also complicated by the trade-offs in privacy preservation and utility present in anonymization to manage disclosure. In this paper, we define three principles that guide sharing security information across organizations: Least Disclosure, Qualitative Evaluation, and Forward Progress. We then discuss engineering approaches that apply these principles to a distributed security system. Application of these principles can reduce the risk of data exposure and help manage trust requirements for data sharing, helping to meet our goal of balancing privacy,*

International Workshop on Privacy Engineering

http://ieee-security.org/TC/SPW2015/IWPE

May 21st, 2015 at the Fairmont, San Jose, CA

Co-located with 36th IEEE Symposium on Security and Privacy

	organizational risk, and the ability to better respond to security with shared information.
16:30–17:35	**Session: Evaluating engineering methods for PETs** **Choose Wisely: A Comparison of Secure Two-Party Computation Frameworks** Jan Henrik Ziegeldorf, Jan Metzke, Martin Henze and Klaus Wehrle *Secure Two-Party Computation (STC), despite being a powerful tool for privacy engineers, is rarely used practically due to two reasons: i) STCs incur significant overheads and ii) developing efficient STCs requires expert knowledge. Recent works propose a variety of frameworks that address these problems. However, the varying assumptions, scenarios, and benchmarks in these works render results incomparable. It is thus hard, if not impossible, for an inexperienced developer of STCs to choose the best framework for her task. In this paper, we present a thorough quantitative performance analysis of recent STC frameworks. Our results reveal significant performance differences and we identify potential for optimizations as well as new research directions for STC. Complemented by a qualitative discussion of the frameworks' usability, our results provide privacy engineers with a dependable information basis to take the decision for the right STC framework fitting their application.* **Tor Experimentation Tools** Fatemeh Shirazi, Matthias Goehring and Claudia Diaz *Tor is the most popular anonymity network, used by more than 2 million daily users. Engineering privacy enhancing tools such as Tor requires extensive experimentation in order to test attacks, evaluate the effects of changes to the Tor software or analyze statistical data on the Tor network. Since research should not be performed on the live Tor network, various techniques have been employed for Tor research, including small-scale private Tor networks, simulation and emulation. In this paper, we provide an overview and discussion of existing techniques and tools used for Tor experimentation by categorizing techniques and highlighting advantages and limitations of each tool. The goal of this paper is to provide researchers with the necessary information for selecting the optimal Tor research tool depending on their specific requirements and possibilities.*
17:35–17:45	**Wrap-up and concluding remarks**