Privacy Risk Analysis

Synthesis Lectures on Information Security, Privacy, & Trust

The Synthesis Lectures Series on Information Security, Privacy, and Trust publishes 50- to 100-page publications on topics pertaining to all aspects of the theory and practice of Information Security, Privacy, and Trust. The scope largely follows the purview of premier computer security research journals such as ACM Transactions on Information and System Security, IEEE Transactions on Dependable and Secure Computing and Journal of Cryptology, and premier research conferences, such as ACM CCS, ACM SACMAT, ACM AsiaCCS, ACM CODASPY, IEEE Security and Privacy, IEEE Computer Security Foundations, ACSAC, ESORICS, Crypto, EuroCrypt and AsiaCrypt. In addition to the research topics typically covered in such journals and conferences, the series also solicits lectures on legal, policy, social, business, and economic issues addressed to a technical audience of scientists and engineers. Lectures on significant industry developments by leading practitioners are also solicited.

Trust in Social Media
Jiliang Tang and Huan Liu
2015

Physically Unclonable Functions (PUFs): Applications, Models, and Future Directions
Christian Wachsmann and Ahmad-Reza Sadeghi
2014

Usable Security: History, Themes, and Challenges
Simson Garfinkel and Heather Richter Lipford
2014

Reversible Digital Watermarking: Theory and Practices
Ruchira Naskar and Rajat Subhra Chakraborty
2014

Mobile Platform Security
N. Asokan, Lucas Davi, Alexandra Dmitrienko, Stephan Heuser, Kari Kostiainen, Elena Reshetova, and Ahmad-Reza Sadeghi
2013

Security and Trust in Online Social Networks
Barbara Carminati, Elena Ferrari, and Marco Viviani
2013

RFID Security and Privacy
Yingjiu Li, Robert H. Deng, and Elisa Bertino
2013

Hardware Malware
Christian Krieg, Adrian Dabrowski, Heidelinde Hobel, Katharina Krombholz, and Edgar Weippl
2013

Private Information Retrieval
Xun Yi, Russell Paulet, and Elisa Bertino
2013

Privacy for Location-based Services
Gabriel Ghinita
2013

Enhancing Information Security and Privacy by Combining Biometrics with Cryptography
Sanjay G. Kanade, Dijana Petrovska-Delacrétaz, and Bernadette Dorizzi
2012

Analysis Techniques for Information Security
Anupam Datta, Somesh Jha, Ninghui Li, David Melski, and Thomas Reps
2010

Operating System Security
Trent Jaeger
2008

Privacy Risk Analysis

Sourya Joyee De and Daniel Le Métayer

ISBN: 978-3-031-01221-1 paperback
ISBN: 978-3-031-02349-1 ebook

DOI 10.1007/978-3-031-02349-1

A Publication in the Morgan & Claypool Publishers series
SYNTHESIS LECTURES ON INFORMATION SECURITY, PRIVACY, & TRUST

Lecture #17
Series Editors: Elisa Bertino, *Purdue University*
Ravi Sandhu, *University of Texas, San Antonio*
Series ISSN
Print 1945-9742 Electronic 1945-9750

Privacy Risk Analysis

Sourya Joyee De and Daniel Le Métayer
Inria, Université de Lyon

SYNTHESIS LECTURES ON INFORMATION SECURITY, PRIVACY, & TRUST #17

ABSTRACT

Privacy Risk Analysis fills a gap in the existing literature by providing an introduction to the basic notions, requirements, and main steps of conducting a privacy risk analysis.

The deployment of new information technologies can lead to significant privacy risks and a privacy impact assessment should be conducted before designing a product or system that processes personal data. However, if existing privacy impact assessment frameworks and guidelines provide a good deal of details on organizational aspects (including budget allocation, resource allocation, stakeholder consultation, etc.), they are much vaguer on the technical part, in particular on the actual risk assessment task. For privacy impact assessments to keep up their promises and really play a decisive role in enhancing privacy protection, they should be more precise with regard to these technical aspects.

This book is an excellent resource for anyone developing and/or currently running a risk analysis as it defines the notions of personal data, stakeholders, risk sources, feared events, and privacy harms all while showing how these notions are used in the risk analysis process. It includes a running smart grids example to illustrate all the notions discussed in the book.

KEYWORDS

privacy, personal data, data protection, risk, analysis, impact, harm, vulnerability, countermeasure, anonymization, law, legal, regulation

Contents

Preface

Risk analysis and risk management are common approaches in areas as varied as environment protection, public health and computer security. In some sense, one may also argue that the original purpose of data protection laws was to reduce the risks to privacy posed by the development of new technologies [58]. In Europe however, the current Data Protection Directive [47] does not rely heavily on privacy risk analysis or Privacy Impact Assessment (PIA).[1] The situation is going to change dramatically with the new General Data Protection Regulation (GDPR) [48], which shall apply from May 25, 2018.

The GDPR represents a fundamental shift from an administrative process based on *a priori* controls to a risk-based accountability approach in which PIAs[2] play a key role. The virtues of the risk-based approach to privacy have been praised by many authors and stakeholders [26]. The main practical benefit expected from the approach is an increased effectiveness in terms of privacy protection: risk assessment makes it possible to focus on the most significant problems and to calibrate measures based on the estimated risks. Organizations also appreciate the fact that legal requirements can be implemented with greater flexibility. Another argument in favor of the risk-based approach is the observation that it is more and more difficult to draw a clear line between anonymous data and personal data, or between sensitive data and non-sensitive data. For this reason, there is a growing view that the only way forward is to go beyond dual visions in this matter and to rely on assessments of actual risks rather than fixed definitions and obligations [120, 128].

However more nuanced views have also been expressed on this topic. For example, the Working Party 29 [6] stresses that the risk-based approach should never lead to a weakening of the rights of the individuals: the rights granted to the data subject should be respected regardless of the level of risk (right of access, erasure, objection, etc.). The fundamental principles applicable to data controllers should also remain the same (legitimacy, data minimization, purpose limitation, transparency, data integrity, etc.), even if they can be scalable (based on the results of a risk assessment). In addition, the risk-based approach should consider not only harms to individuals but also general societal impacts.

Some privacy advocates also fear that the flexibility provided by the risk-based approach is abused by some organizations, and risk assessment is perverted into a self-legitimation exercise [57]. To avoid this drift and ensure that the risk-based approach really contributes to improving privacy, a number of conditions have to be met. First and foremost, the analysis has to be rigorous, both from the technical point of view and from the procedural point of view. The

[1] The notion is even not referred to explicitly in the text of the Directive.
[2] More precisely, the GDPR uses the wording "Data Protection Impact Assessment."

methodology used for the analysis should be clearly defined, as well as the assumptions about the context and the potential privacy impacts. This is a key requirement to ensure that the results of a privacy risk analysis are trustworthy and can be subject to independent checks.

However, if existing PIA frameworks and guidelines [160, 161, 163] provide a good deal of details on organizational aspects (including budget allocation, resource allocation, stakeholder consultation, etc.), they are much vaguer on the technical part, in particular on the actual risk assessment task.

A key step to achieve a better convergence between PIA frameworks geared toward legal and organizational issues on one hand and technical approaches to privacy risk analysis on the other hand, is to agree on a common terminology and a set of basic notions. It is also necessary to characterize the main tasks to be carried out in a privacy risk analysis and their inputs and outputs.

The above objectives are precisely the subject of this book. The intended audience includes both computer scientists looking for an introductory survey on privacy risk analysis and stakeholders involved in a PIA process with the desire to address technical aspects in a rigorous way. We hope that the reader will have as much pleasure in reading this book as we had in putting it together.

Sourya Joyee De and Daniel Le Métayer
August 2016

Acknowledgments

We thank our colleagues of the PRIVATICS research group in Grenoble and Lyon, in particular Gergely Ács and Claude Castelluccia for their comments on an earlier draft of this book and many fruitful discussions on privacy risk analysis. This work has been partially funded by the French ANR-12-INSE-0013 project BIOPRIV and the Inria Project Lab CAPPRIS.

Sourya Joyee De and Daniel Le Métayer
August 2016