Special Issue on the Economics of Security and Privacy: Guest Editors' Introduction

RAINER BÖHME, University of Innsbruck
RICHARD CLAYTON, University of Cambridge
JENS GROSSKLAGS, Technical University of Munich
KATRINA LIGETT, Hebrew University of Jerusalem
PATRICK LOISEAU, Univ. Grenoble Alpes, CNRS, Inria, Grenoble INP, LIG and MPI-SWS
GALINA SCHWARTZ, University of California at Berkeley

This editorial introduces the special issue on the economics of security and privacy.

CCS Concepts: • **Security and privacy → Human and societal aspects of security and privacy**; **Economics of security and privacy**;

Additional Key Words and Phrases: Security, privacy, economics, incentives, game theory

ACM Reference format:
Rainer Böhme, Richard Clayton, Jens Grossklags, Katrina Ligett, Patrick Loiseau, and Galina Schwartz. 2018. Special Issue on the Economics of Security and Privacy: Guest Editors' Introduction. *ACM Trans. Internet Technol.* 18, 4, Article 47 (November 2018), 3 pages.
https://doi.org/10.1145/3216902

1 INTRODUCTION

The global adoption of the Internet has transformed economies and societies. However, Internet technologies have also resulted in heightened societal concerns about information security and privacy. Insufficient safeguards—actual or perceived—have become a barrier to certain economic activity, and a source of downside risk to growth and sustainability, with possible systemic impact.

Scholars have long realized that choices pertaining to security and privacy affect the world in ways that are not captured within the narrow modeling of engineering systems. In essence, these choices are strategic decisions. Thus, the analysis that is performed should incorporate the models and methods developed in economics and, where applicable, in the behavioral sciences.

The team of guest editors set out to compile a special issue with the aim of highlighting the major achievements and the latest advances in this interdisciplinary research field. A "Call For

Authors' addresses: R. Böhme, Department of Computer Science, Universität Innsbruck, Technikerstraße 21A, 6020 Innsbruck, Austria; email: rainer.boehme@uibk.ac.at; R. Clayton, University of Cambridge, Computer Laboratory, GE21, William Gates Building, JJ Thomson Avenue, Cambridge CB3 0FD, United Kingdom; email: cl.cam.ac.uk; J. Grossklags, Technical University of Munich, Department of Informatics, Boltzmannstraße 3, 85748 Garching, Germany; email: jens.grossklags@in.tum.de; K. Ligett, The Hebew University of Jerusalem, Givat Ram, Jerusalem 91904, Israel; email: katrina@cs.huji.ac.il; P. Loiseau, Laboratoire d'Informatique de Grenoble, Bâtiment IMAG, 700 avenue Centrale, Domaine Universitaire, 38400 St Martin d'Hères, France; email: patrick.loiseau@univ-grenoble-alpes.fr; G. Schwartz, UC Berkeley, Cory Hall, Berkeley, CA 94720, USA; email: schwartz@eecs.berkeley.edu.

1533-5399/2018/11-ART47
https://doi.org/10.1145/3216902

Papers" distributed in 2016 invited authors to submit work pertaining to one of three topic areas: (i) natures and causes of security and privacy risks, (ii) effects of security and privacy risks, and (iii) intervention approaches.

While much research in this field touches all three areas, for example, because effective intervention approaches need valid models of causes and effects, each of the seven articles in this special issue can be seen to advance the state of the art in a particular one of these areas.

The articles have been selected from a set of 53 initial submissions in multiple rounds of a rigorous blind review process. The guest editors are grateful to all the authors and all the volunteer reviewers who participated in this process.

2 OUTLINE OF THE SPECIAL ISSUE

2.1 Natures and Causes of Security and Privacy Risks

This special issue includes one theoretical and one empirical contribution toward understanding the nature of security risk in networked systems.

Starting with the theoretical work, the article entitled "On the Assessment of Systematic Risk in Networked Systems" by Aron Laszka, Benjamin Johnson, and Jens Grossklags studies the propagation of risk in a network. The authors establish and study one-hop and multi-hop propagation models for networked systems under attack, allowing us to infer macroscopic—or systemic, in the jargon of finance—risks from microscopic risk arrival models. Their results could be relevant for the provision and pricing of cyber-insurance products. A particular strength of the work is that it addresses special cases of common real-world networks.

Turning to the empirical side, the article entitled "Rotten Apples or Bad Harvest? What We Are Measuring When We Are Measuring Abuse?" by Samaneh Tajalizadehkhoob, Rainer Böhme, Carlos Gañán, Maciej Korczyński, and Michel Van Eeten studies abuse levels at web hosting providers. More specifically, how much are these abuse levels determined by the security efforts of providers versus other inherent characteristics of the providers (both technical and socio-economical)? The authors find that a significant part of the abuse level can be explained by characteristics such as number of websites co-located on the same server, the popularity of the websites, or the price charged. Their results challenge the conventional wisdom that (the lack of) security effort is a major factor in abuse. A particular strength of the article is the use of a sophisticated statistical analysis based on the concept of statistical twins that seems to be promising.

2.2 Effects of Security and Privacy Risks

In the corporate world, the worst effect a security breach can have is to kick you out of business. No industry knows this better than the thriving ecosystem surrounding crypto-currencies. The article entitled "Revisiting the Risks of Bitcoin Currency Exchange Closure" by Tyler Moore, Nicolas Christin, and Janos Szurdi seeks to understand the determinants of Bitcoin exchange closures. To this end, they present and analyze new data on exchange opening and closing dates, trading volumes, breaches, and exchange security features. Perhaps the most interesting takeaway from the article is the finding that breaches do not automatically imply exchange closure. The results of this work should be of interest to all those using or studying Bitcoin or related currencies, and it may provide lessons about the roles of various security features.

Turning from security breaches to privacy threats, the tracking of consumer behavior is a major concern. The article entitled "Fine-Grained Control over Tracking to Support the Ad-Based Web Economy" by Javier Parra-Arnau, Jagdish Prasad Achara, and Claude Castelluccia advances the hypothesis that fine-grained control over per-web-page tracking can strike a meaningful tradeoff between user privacy and the Internet economy. To this end, the authors develop web

plugins for Chrome and Firefox that classify web content and accordingly block or allow trackers while users browse the web. The authors then perform an experimental evaluation of the plug-ins, including an economic analysis. The article stood out for the substantial system developed in order to understand fine-grained tracking in the wild.

2.3 Intervention Approaches

The special issue is completed by three works that may guide intervention measures. First, staying on the issue of tracking, the article entitled "Measuring Third-Party Tracker Power across Web and Mobile" by Reuben Binns, Jun Zhao, Max Van Kleek, and Nigel Shadbolt quantitatively examines market concentration for web and mobile third-party trackers. One surprising finding is the comparison between the web and mobile markets, where they find that even identical services use very distinct trackers across the two platforms. A particular strength of the work is the development and application of new metrics for market concentration, which could become a useful tool for those attempting to regulate third-party trackers.

The second article entitled "PrivacyCheck: Automatic Summarization of Privacy Policies Using Data Mining" by Razieh Nokhbeh Zaeem, Rachel L. German, and K. Suzanne Barber presents a browser plugin that automatically extracts structured information from textual privacy policies. The plugin uses machine learning to identify different risk factors and quantifies the risk levels for those factors (10 factors ranked on a scale from 1 to 3). The proposed framework for privacy explanations is intuitive and understandable for end users; hence, it can help people to navigate privacy policies. A particular strength of this work is that the authors create a new dataset, which is one of the biggest to date in the field and contains significant manual work from domain experts.

Finally, the paper entitled "Should Credit Card Issuers Reissue Cards in Response to a Data Breach?: Uncertainty and Transparency in Metrics for Data Security Policymaking" by James T. Graves, Alessandro Acquisti, and Nicholas Christin empirically investigates the aggregate cost/benefits (called social cost) of reissuing credit cards in response to credit card data breaches in comparison with waiting until any actual frauds occur. They find that reissuing cards may have lower social costs than waiting until fraud is attempted, which should cause some existing policies to be reviewed. A particular strength of the article is that it uses a variety of statistical models and methods as well as data sources to derive the key result and quantify its robustness.