

Table of Contents

Economics of Information Security I

- Mitigating Inadvertent Insider Threats with Incentives 1
Debin Liu, XiaoFeng Wang, and L. Jean Camp
- Deterring Online Advertising Fraud through Optimal Payment in
Arrears 17
Benjamin Edelman

Anonymity and Privacy I

- Privacy-Preserving Information Markets for Computing Statistical
Data 32
Aggelos Kiayias, Bülent Yener, and Moti Yung
- Achieving Privacy in a Federated Identity Management System 51
Susan Landau, Hubert Le Van Gong, and Robin Wilton
- Data Hemorrhages in the Health-Care Sector 71
M. Eric Johnson

Private Computation

- Solving Linear Programs Using Multiparty Computation 90
Tomas Toft
- Private Intersection of Certified Sets 108
Jan Camenisch and Gregory M. Zaverucha
- Privacy-Preserving Classifier Learning 128
Justin Brickell and Vitaly Shmatikov

Economics of Information Security II

- Investments and Trade-offs in the Economics of Information Security ... 148
Christos Ioannidis, David Pym, and Julian Williams
- Blue versus Red: Towards a Model of Distributed Security Attacks 167
Neal Fultz and Jens Grossklags

Authentication and Identification

- Optimised to Fail: Card Readers for Online Banking 184
Saar Drimer, Steven J. Murdoch, and Ross Anderson

Expecting the Unexpected: Towards Robust Credential Infrastructure	201
<i>Shouhuai Xu and Moti Yung</i>	
Optical DNA	222
<i>Deepak Vijaywargi, Dave Lewis, and Darko Kirovski</i>	
Panel	
Passwords: If We're So Smart, Why Are We Still Using Them?	230
<i>Cormac Herley, P.C. van Oorschot, and Andrew S. Patrick</i>	
Fraud Detection	
Defeating Cross-Site Request Forgery Attacks with Browser-Enforced Authenticity Protection	238
<i>Ziqing Mao, Ninghui Li, and Ian Molloy</i>	
Evil Searching: Compromise and Recompromise of Internet Hosts for Phishing	256
<i>Tyler Moore and Richard Clayton</i>	
Detecting Denial of Service Attacks in Tor	273
<i>Norman Danner, Danny Krizanc, and Marc Liberatore</i>	
Auctions	
Cryptographic Combinatorial Securities Exchanges	285
<i>Christopher Thorpe and David C. Parkes</i>	
Cryptographic Combinatorial Clock-Proxy Auctions	305
<i>David C. Parkes, Michael O. Rabin, and Christopher Thorpe</i>	
Secure Multiparty Computation Goes Live	325
<i>Peter Bogetoft, Dan Lund Christensen, Ivan Damgård, Martin Geisler, Thomas Jakobsen, Mikkel Krøigaard, Janus Dam Nielsen, Jesper Buus Nielsen, Kurt Nielsen, Jakob Pagter, Michael Schwartzbach, and Tomas Toft</i>	
Anonymity and Privacy II	
Coercion Resistant end-to-end Voting	344
<i>Ryan W. Gardner, Sujata Garera, and Aviel D. Rubin</i>	
Relations Among Privacy Notions	362
<i>Jens-Matthias Bohli and Andreas Pashalidis</i>	
Author Index	381