Lecture Notes in Computer Science 7398

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Jim Blythe Sven Dietrich
L. Jean Camp (Eds.)

Financial Cryptography and Data Security

FC 2012 Workshops, USEC and WECSR 2012
Kralendijk, Bonaire, March 2, 2012
Revised Selected Papers

Springer

Volume Editors

Jim Blythe
USC Information Sciences Institute
4676 Admiralty Way, Suite 1001
Marina del Rey, CA 90292, USA
E-mail: blythe@isi.edu

Sven Dietrich
Stevens Institute of Technology
Computer Science Department
1 Castle Point on Hudson
Hoboken, NJ 07030, USA
Email address: spock@cs.stevens.edu

L. Jean Camp
414 E First St
Bloomington, IN 47401, USA
Email address: ljeanc@gmail.com

ISSN 0302-9743
ISBN 978-3-642-34637-8
DOI 10.1007/978-3-642-34638-5

e-ISSN 1611-3349
e-ISBN 978-3-642-34638-5

Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012950705

CR Subject Classification (1998): C.2, K.4.4, K.6.5, D.4.6, E.3, J.1

LNCS Sublibrary: SL 4 – Security and Cryptology

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

This volume contains the papers from the two workshops held along with the 16th International Conference on Financial Cryptography and Data Security, in Bonaire on March 2nd, 2012.

USEC 2012: Workshop on Usable Security

The goal of the workshop on Usable Security was to engage on all aspects of human factors and usability in the context of security. Many aspects of data security combine technical and human factors. If a highly secure system is unusable, users will move their data to less secure but more usable systems. Problems with usability are a major contributor to many high-profile security failures today.

However, usable security is not well aligned with traditional usability for three reasons. First, security is rarely the desired goal of the individual. In fact, security is usually orthogonal and often in opposition to the actual goal. Second, security information is about risk and threats. Such communication is most often unwelcome. Increasing unwelcome interaction is not a goal of usable design. Third, since individuals must trust their machines to implement their desired tasks, risk communication itself may undermine the value of the networked interaction. For the individual, discrete technical problems are all understood under the rubric of online security (e.g., privacy from third parties' use of personally identifiable information, malware). A broader conception of both security and usability is therefore needed for usable security.

USEC 2012 brought together researchers already engaged in this interdisciplinary effort with others from areas such as HCI, artificial intelligence, theoretical computer science, law, and industry experts.

There were 13 submissions. Each submission was reviewed by at least 2, and on average 3, program committee members. The committee decided to accept 8 papers. Our thanks to the members of the program committee, the indefatigable chair of FC Angelos Keromytis, the IFCA board, participants, and all who submitted their works.

July 2012

Jim Blythe
Jean Camp

USEC 2012 Program Committee

Sadia Afroz	Drexel University
Ross Anderson	University of Cambridge
Matt Bishop	UC Davis
Pamela Briggs	Northumbria University
Tamzen Cannoy	PGP
Rachna Dhamija	Usable Security Systems
Chris Demchak	US Naval War College
Neil Gandal	Tel Aviv University
Seymour Goodman	Georgia Tech
Peter Gutmann	University of Auckland
Raquel Hill	Indiana University
Tiffany Hyun-Jin Kim	Carnegie Mellon
Brian LaMacchia	Microsoft
William Lehr	MIT
Andrew Patrick	Office of the Privacy Commissioner of Canada
Angela Sasse	University College London
Daniel Schutzer	Financial Services Roundtable
Mark Seiden	MSB Associates
Hovav Shacham	UC San Diego
Sara Sinclair	Google
Sean Smith	Dartmouth College
Gene Spafford	Purdue University
Frank Stajano	University of Cambridge
Sid Stamm	Mozilla
Douglas Stebila	Queensland University of Technology
Nicholas Weaver	ICSI Berkeley
Tara Whalen	Carleton University

WECSR 2012: Workshop on Ethics in Computer Security Research

The third Workshop on Ethics in Computer Security Research (WECSR 2012, http://www.cs.stevens.edu/ spock/wecsr2012/), organized by the International Financial Cryptography Association (IFCA, http://www.ifca.ai/), was held in Kralendijk, Bonaire, Dutch Antilles, on March 2, 2012. It was part of the third multi-workshop event co-located with Financial Cryptography 2012.

The goal was to continue searching for a new path in computer security that is acceptable for institutional review boards at academic institutions, as well as compatible with ethical guidelines for professional societies or government institutions. One such major step is the publication of the Menlo Report in the United States Federal Register in Fall 2011, the equivalent of the Belmont Report for this domain.

We mixed the two papers and one panel selected from five submissions with a keynote talk and one invited panel. Each submission was reviewed by at least 5 program committee members. The program committee carefully reviewed the submissions during an online discussion phase in fall 2011. I would like to thank the program committee for their work and suggestions. We like to thank all submitters for their papers and efforts.

The workshop brought together about 15 participants, including computer security researchers, practitioners, policy makers, and legal experts. We joined efforts with the co-located USEC 2012 workshop for the keynote talk by Ross Anderson and the afternoon panel on the ethics of data sharing moderated by Lenore Zuck. The relaxed Bonaire atmosphere allowed for many continued discussions beyond the day itself, including the evening island bus tour.

I would like to thank Angelos Keromytis, Rafael Hirschfeld, Burton Rosenberg, Tyler Moore, and Moti Yung for their hard work and help in organizing this workshop. A special thanks goes to Ross Anderson for a timely intervention. *Masha danki* (thank you very much) to Sara Matera for her support in making the local arrangements. Last but not least my gratitude also goes to the participants, who traveled to this remote island in the Netherlands Antilles close to Venezuela, where Papiamento is spoken. I look forward to many more discussions at future instances of the workshop.

July 2012 Sven Dietrich

WECSR 2012 Program Committee

John Aycock	University of Calgary
Michael Bailey	University of Michigan
Elizabeth Buchanan	University of Wisconsin-Stout
Aaron Burstein	UC Berkeley
Jon Callas	Indiana University
Nicolas Christin	Carnegie Mellon University
Michael Collins	RedJack, LLC
Marc Dacier	Symantec Research
Rachna Dhamija	Usable Security Systems
Sven Dietrich	Stevens Institute of Technology
Roger Dingledine	The Tor Project
David Dittrich	University of Washington
Kenneth Fleischmann	University of Maryland
Maritza Johnson	Columbia University
Erin Kennneally	sdsc / caida / elchemy
Engin Kirda	Intitut Eurecom
Christian Kreibich	ICSI
Howard Lipson	CERT, Software Engineering Institute, CMU
John Mchugh	RedJack LLC and University of North Carolina
Perry Metzger	University of Pennsylvania
Angelos Stavrou	George Mason University
Michael Steinmann	Stevens Institute of Technology
Lenore Zuck	University of Illinois in Chicago

Table of Contents

The Workshop on Usable Security (USEC 12)

The Workshop on Ethics in Computer Security Research (WECSR 12)