Real-Life Cryptographic Protocols and Standardization

Preface

This workshop, “Real-Life Cryptographic Protocols and Standardization,” is intended to gather the experiences of the designers and implementers of cryptographic protocols that are deployed in real-life systems. Designing and implementing real-life systems puts forth many challenges – not only technical issues regarding the use of hardware and software, but also usability, manageability, interoperability and timing to deploy the system. Designing to fulfil all these restrictions while not degrading security frequently requires tremendous efforts. The resulting cryptographic protocols may not always be interesting at the theoretical cryptography level, but the documentation of the challenges they face and the ways such challenges were met are important to be shared with the community. Standardization also promotes the use of cryptographic protocols where the best practices from these experiences are condensed in a reusable way.

We were happy to organize the second workshop in conjunction with the Financial Cryptography and Data Security Conference 2011 in St. Lucia. The selected papers focus on real-life issues and discuss all the design criteria and relevant implementation challenges. We hope the proceedings from the series of this workshop serve as a place where researchers and engineers find the documentation of the necessary know-how for designing and implementing secure systems that have a tangible impact in real life; ultimately, we hope that this contributes to a future generation of usable real-life systems where security would be one of their intrinsic qualities.

April 2011

Kazue Sako

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. The first results are beginning to appear, such as initial drafts of the Menlo Report, the equivalent of the Belmont Report for this domain.

We mixed the three papers and one panel selected from six submissions with two invited papers and one invited panel. Each submission was reviewed by at least four Program Committee members. The Program Committee carefully reviewed the submissions during an online discussion phase in fall 2010. I would like to thank the Program Committee for their work. We would like to thank all submitters for the papers and efforts, and hope that the comments received from the reviewers will allow them to progress with their work.

The workshop brought together about 35 participants, including computer security researchers, practitioners, policy makers, and legal experts, and fostered often fervent ethical and philosophical debates among participants, in order to shape the future of ethical standards in the field. The relaxed local atmosphere allowed for many continued discussions beyond the day itself, including the island excursion the following day kindly organized by the Local Arrangements Chair Fabian Monrose.

I would like to thank George Danezis, Steven Murdoch, Rafael Hirschfeld, Andrew Patrick, Jon Callas, Burton Rosenberg, and last but not least Fabian Monrose for their hard work and help in organizing this workshop. Many thanks also to those who traveled far to this island in the Eastern Caribbean.

I look forward to many more discussions at future instances of the workshop.

March 2011

Sven Dietrich
Organization

The 15th International conference on Financial Cryptography and Data Security (FC 2011) was organized by the International Financial Cryptography Association (IFCA).

Organizers

General Chair
Steven Murdoch  
University of Cambridge, UK

Local Arrangements Chair
Fabian Monrose  
University of North Carolina Chapel Hill, USA

Real-Life Cryptographic Protocols and Standardization

Program Chair
Kazue Sako  
NEC

Program Committee

Josh Benaloh  
Microsoft Research
Aline Gouget  
Gemalto and CryptoExperts
Hongxia Jin  
IBM Almaden
Aggelos Kiayias  
University of Connecticut
Helger Lipmaa  
Cybernetica AS and Tallinn University
Sandra Marcello  
Thales
Jean-Francois Misarsky  
Orange Labs
David Naccache  
ENS
Kaisa Nyberg  
Aalto University and Nokia
Satoshi Obana  
NEC
Pascal Paillier  
Gemalto and CryptoExperts
Benny Pinkas  
Bar Ilan University
Ahmad-Reza Sadeghi  
TU Darmstadt and Fraunhofer SIT
Kazue Sako  
NEC
Workshop on Ethics in Computer Security Research

Program Chair
Sven Dietrich  
Stevens Institute of Technology

Program Committee

Michael Bailey  
University of Michigan
Elizabeth Buchanan  
University of Wisconsin-Stout
Aaron Burstein  
University of California Berkeley
Nicolas Christin  
Carnegie Mellon University
Michael Collins  
RedJack, LLC
Marc Dacier  
Symantec Research
Roger Dingledine  
The Tor Project
David Dittrich  
University of Washington
Kenneth Fleischmann  
University of Maryland
Rachel Greenstadt  
Drexel University
Erin Kenneally  
UC San Diego/CAIDA/Elchemy
Engin Kirda  
Northeastern University
Howard Lipson  
CERT, Software Engineering Institute, CMU
John Mchugh  
RedJack LLC and University of North Carolina
Peter Neumann  
SRI International
Vern Paxson  
ICSI and LBNL
Len Sassaman  
K.U. Leuven ESAT-COSIC
Angelos Stavrou  
George Mason University
Michael Steinmann  
Stevens Institute of Technology
Paul Syverson  
Naval Research Laboratory

Sponsors

Gold  
Office of Naval Research Global
Silver  
Research in Motion
Bronze  
East Caribbean Financial Holding
Google
In Kind  
Lime
WorldPay
Financial Services Technology Consortium BITS
Table of Contents

Financial Cryptography and Data Security Workshops

Real-Life Cryptographic Protocols and Standardization

Cryptographic Protocols: From the Abstract to the Practical to the Actual (Invited Talk) ................................................. 1
   Moti Yung

Toward Real-Life Implementation of Signature Schemes from the Strong RSA Assumption ............................................. 3
   Ping Yu and Rui Xue

Detailed Cost Estimation of CNTW Attack against EMV Signature Scheme ................................................................. 13
   Tetsuya Izu, Yoshitaka Morikawa, Yasuyuki Nogami, Yumi Sakemi, and Masahiko Takenaka

Fast Elliptic Curve Cryptography in OpenSSL ........................................... 27
   Emilia Käsper

Cryptographic Treatment of Private User Profiles ............................. 40
   Felix Günther, Mark Manulis, and Thorsten Strufe

An Introspection-Based Memory Scraper Attack against Virtualized Point of Sale Systems .................................................. 55
   Jennia Hizver and Tzi-cker Chiueh

A Study on Computational Formal Verification for Practical Cryptographic Protocol: The Case of Synchronous RFID Authentication ................................................................. 70
   Yoshikazu Hanatani, Miyako Ohkubo, Shin’ichiro Matsuo, Kazuo Sakiyama, and Kazuo Ohta

   Daniel Hartung and Christoph Busch

Exploration and Field Study of a Password Manager Using Icon-Based Passwords .......................................................... 104
   Kemal Bicakci, Nart Bedin Atalay, Mustafa Yuceel, and P.C. van Oorschot
# Table of Contents

## Workshop on Ethics in Computer Security Research

- Ethical Issues in E-Voting Security Analysis (Invited Talk) .......................... 119  
  *David G. Robinson and J. Alex Halderman*
- Computer Security Research with Human Subjects: Risks, Benefits and Informed Consent .................................................. 131  
  *Maritza L. Johnson, Steven M. Bellovin, and Angelos D. Keromytis*
- Human Subjects, Agents, or Bots: Current Issues in Ethics and Computer Security Research (Panel Statements) .................... 138  
  *John Aycock, Elizabeth Buchanan, Scott Dexter, and David Dittrich*
- Enforced Community Standards for Research on Users of the Tor Anonymity Network (Invited Talk) ........................................ 146  
  *Christopher Soghoian*
- Ethical Dilemmas in Take-Down Research ........................................... 154  
  *Tyler Moore and Richard Clayton*
- Ethical Considerations of Sharing Data for Cybersecurity Research ...... 169  
  *Darren Shou*
- Moving Forward, Building an Ethics Community (Panel Statements) ... 178  
  *Erin Kenneally, Angelos Stavrou, John McHugh, and Nicolas Christin*

## Author Index

.................................................. 185