

Preface

The 3rd International Conference on Applied Cryptography and Network Security (ACNS 2005) was sponsored and organized by ICISA (the International Communications and Information Security Association). It was held at Columbia University in New York, USA, June 7–10, 2005. This conference proceedings volume contains papers presented in the academic/research track.

ACNS covers a large number of research areas that have been gaining importance in recent years due to the development of the Internet, wireless communication and the increased global exposure of computing resources. The papers in this volume are representative of the state of the art in security and cryptography research, worldwide.

The Program Committee of the conference received a total of 158 submissions from all over the world, of which 35 submissions were selected for presentation at the academic track. In addition to this track, the conference also hosted a technical/ industrial/ short papers track whose presentations were also carefully selected from among the submissions. All submissions were reviewed by experts in the relevant areas.

Many people and organizations helped in making the conference a reality. We would like to take this opportunity to thank the Program Committee members and the external experts for their invaluable help in producing the conference's program. We also wish to thank Michael E. Locasto for his help in all technical and technological aspects of running the conference and Sophie Majewski for the administrative support in organizing the conference. We wish to thank the graduate students at Columbia University's Computer Science Department who helped us as well.

We wish to acknowledge the financial support of our sponsors, and their employees who were instrumental in the sponsorship process: Morgan Stanley (Ben Fried), Gemplus (David Naccache), and Google (Niels Provos).

Finally, we would like to thank all the authors who submitted papers to the conference; the continued support of the security and cryptography research community worldwide is what really enabled us to have this conference.

May 2005

John Ioannidis
Angelos Keromytis
Moti Yung

ACNS 2005

3rd International Conference on Applied Cryptography and Network Security

New York, USA

June 7–10, 2005

Sponsored and organized by the
International Communications and Information Security Association (ICISA)

In coöperation with
Columbia University, USA

General Chair

John Ioannidis Columbia University

Program Chairs

Moti Yung Columbia University and RSA Labs
Angelos Keromytis Columbia University

Program Committee

Scott Alexander Telcordia, USA
Tuomas Aura Microsoft Research, UK
David Brumley CMU, USA
Ran Canetti IBM Research, USA
Marc Dacier Eurecom, France
Ed Dawson Queensland University of Technology, Australia
Glenn Durfee PARC, USA
Virgil Gligor University of Maryland, USA
Peter Gutman University of Auckland, New Zealand
Goichiro Hanaoka National Institute of Advanced Industrial Science
and Technology (AIST), Japan
Amir Herzberg Bar Ilan University, Israel
Russ Housley Vigilsec, USA
John Ioannidis Columbia University, USA
Sotiris Ioannidis University of Pennsylvania, USA

| | |
|---------------------|----------------------------------|
| Stas Jarecki | UC Irvine, USA |
| Ari Juels | RSA Laboratories, USA |
| Angelos Keromytis | Columbia University, USA |
| Aggelos Kiayias | University of Connecticut, USA |
| Tanja Lange | Ruhr-Universität Bochum, Germany |
| Dong Hoon Lee | Korea University, South Korea |
| Fabio Massacci | University Trento, Italy |
| Atsuko Miyaji | JAIST, Japan |
| Frederic Muller | DCSSI Crypto Lab, France |
| Kaisa Nyberg | Nokia, Finland |
| Bart Preneel | K.U.Leuven, Belgium |
| Vassilis Prevelakis | Drexel University, USA |
| Niels Provos | Google, USA |
| Pierangela Samarati | University of Milan, Italy |
| Tomas Sander | HP, USA |
| Dan Simon | Microsoft Research, USA |
| Tsuyoshi Takagi | T.U. Darmstadt, Germany |
| Wen-Guey Tzeng | NCTU, Taiwan |
| Dan Wallach | Rice University, USA |
| Susanne Wetzel | Stevens Institute, USA |
| Moti Yung | Columbia University, USA |
| Jianying Zhou | I2R, Singapore |
| Lidong Zhou | Microsoft Research, USA |

External Reviewers

Kouichiro Akiyama, Kostas Anagnostakis, Farooq Anjum, N. Asokan, Nuttapong Attrapadung, Roberto Avanzi, Dirk Balfanz, Lejla Batina, Steven Bellovin, Josh Benaloh, Enrico Blanzieri, Christophe de Canniere, Alvaro Cardenas, Roberto Cascella, Jae-Gwi Choi, Stelvio Cimato, Jared Cordasco, Giovanni di Crescenzo, Eric Cronin, Stefano Crosta, Yang Cui, Ernesto Damiani, Seiji Doi, Wenliang Du, Detlef Duehnlein, Patrick Felke, Pierre-Alain Fouque, Eiichiro Fujisaki, Abhrajit Ghosh, Philippe Golle, Michael Greenwald, Shai Halevi, Nick Howgrave-Graham, Seokhie Hong, Omer Horvitz, Tetsu Iwata, Eliane Jaulmes, Markus Kaiser, Tetsutaro Kobayashi, Sébastien Kunz-Jacques, Kaoru Kurosawa, Klaus Kursawe, Joseph Liu, Dahlia Malkhi, Gwenaëlle Martinet, Mitsuru Matsui, Breno de Medeiros, Nele Mentens, Bernd Meyer, Ulrike Meyer, Ilya Mironov, Anderson Nascimento, Francesco De Natale, Svetla Nikova, Akihito Niwa, Takeshi Okamoto, Tatsuaki Okamoto, Renaud Pacalet, Young-Ho Park, Kirthika Parmeswaran, Guillaume Poupard, Vincent Rijmen, Michael Roe, Tomas Sander, Hisayoshi Sato, Nitesh Saxena, Katja Schmidt-Samoa, Micah Sherr, Diana Smetters, Masakazu Soshi, Jessica Staddon, Martijn Stam, Maria Striki, Gelareh Taban, Rajesh Talpade, Yuuko Tamura, Simon Tsang, Guillaume Urvoy-Keller, Frederik Vercauteren, Sabrina de Capitani di Vimercati, Camille Vuillaume, Zhiguo Wan, Guilin Wang, Kai Wirt, Hongjun Wu, Bennet Yee, Rui Zhang, Sheng Zhong, Huafei Zhu

Applied Cryptography and Network Security
Third International Conference, ACNS 2005, New York,
NY, USA, June 7-10, 2005, Proceedings
Ioannidis, J.; Keromytis, A.D.; Yung, M. (Eds.)
2005, XII, 530 p., Softcover
ISBN: 978-3-540-26223-7