Preface

It is our great pleasure to welcome you to the Eighth International Conference on Information and Communications Security (ICICS 2006), held in Raleigh, North Carolina, USA, December 4–7, 2006. The ICICS conference series is an established forum that brings together researchers and scholars involved in multiple disciplines of Information and Communications Security in order to foster exchange of ideas. The past seven ICICS conferences were held in Beijing, China (ICICS 1997); Sydney, Australia (ICICS 1999); Xi’an China (ICICS 2001); Singapore (ICICS 2002); Hohhot City, China (ICICS 2003); Malaga, Spain (ICICS 2004); and Beijing, China (ICICS 2005). The conference proceedings of the past seven events have been published by Springer in the Lecture Notes in Computer Science series, in LNCS 1334, LNCS 1726, LNCS 2229, LNCS 2513, LNCS 2836, LNCS 3269, and LNCS 3783, respectively.

This year we received a total of 119 submissions on various aspects of ad-hoc and sensor network security. The Program Committee selected 22 regular papers and 17 short papers that cover a variety of topics, including security protocols, applied cryptography and cryptanalysis, access control in distributed systems, privacy, malicious code, network and systems security, and security implementations.

Putting together ICICS 2006 was a team effort. First of all, we would like to thank the authors of every paper, whether accepted or not, for submitting their papers to ICICS 2006. We would like to express our gratitude to the Program Committee members and the external reviewers, who worked very hard in reviewing the papers and providing suggestions for their improvements. We would also like to thank the Organizing Committee members, who did a wonderful job in organizing the conference. We would like to thank our sponsor, North Carolina State University (NCSU)/Duke University Center for Advanced Computing and Communications (CACC), for supporting the conference. Finally, we would like to express our gratitude to the US Army Research Office and the US National Science Foundation for the generous financial support of this conference. Their grants provided travel supports for graduate students to attend the conference.

We hope that you will find these proceedings interesting and thought-provoking.

September 2006

Peng Ning and Sihan Qing
Program Chairs, ICICS 2006
Organization

ICICS 2006 was organized by the North Carolina State University (NCSU)/Duke University Center for Advanced Computing and Communication (CACC), with support from the US Army Research Office (ARO) and the US National Science Foundation (NSF).

Organizing Committee

General Chair
Douglas S. Reeves North Carolina State University, USA

Program Chairs
Peng Ning North Carolina State University, USA
Sihan Qing Chinese Academy of Sciences, China

Publication Chair
Ninghui Li Purdue University, USA

Panel and Keynote Chair
David Evans University of Virginia, USA

Publicity Chair
Haining Wang College of William and Mary, USA

Local Arrangement Chair
Errin Fulp Wake Forest University, USA

Posters and Demos Chair
Yong Guan Iowa State University, USA

Financial Chair
Donggang Liu University of Texas at Arlington, USA

Program Committee

Mikhail Atallah Purdue University, USA
Vijay Atluri Rutgers University, USA
Tuomas Aura  
Microsoft Research, USA

Michael Backes  
Saarland University, Germany

Elisa Bertino  
Purdue University, USA

Sabrina De Capitani di Vimercati  
Università degli Studi di Milano, Italy

Srdjan Capkun  
ETH Zurich, Switzerland

Hao Chen  
University of California at Davis, USA

Scott Contini  
Macquarie University, Australia

Yvo Desmedt  
University College London, UK

Wenliang (Kevin) Du  
Syracuse University, USA

David Evans  
University of Virginia, USA

Yong Guan  
Iowa State University, USA

Sushil Jajodia  
George Mason University, USA

Angelos Keromytis  
Columbia University, USA

Paris Kitsos  
Helen Open University, Greece

Christopher Kruegel  
Technical University Vienna, Austria

Yingjiu Li  
Singapore Management University, Singapore

Donggang Liu  
University of Texas at Arlington, USA

Peng Liu  
Penn State University, USA

Javier Lopez  
University of Malaga, Spain

Radha Poovendran  
University of Washington, USA

Phil Porras  
SRI International, USA

Indrajit Ray  
Colorado State University, USA

Rei Safavi-Naini  
University of Wollongong, Australia

Pierangela Samarati  
Università degli Studi di Milano, Italy

Kent Seamons  
Brigham Young University, USA

R. Sekar  
Stony Brook University, USA

Sean Smith  
Dartmouth College, USA

Tim Strayer  
BBN, USA

Wade Trappe  
Rutgers University, USA

Haining Wang  
College of William and Mary, USA

Xiaofeng Wang  
Indiana University, USA

Andreas Wespi  
IBM Zurich, Switzerland

S. Felix Wu  
University of California at Davis, USA

Jun Xu  
Google, USA

Alec Yasinsac  
Florida State University, USA

Ting Yu  
North Carolina State University, USA

Diego Zamboni  
IBM Zurich, Switzerland

Yongguang Zhang  
Microsoft Research Asia, China

Yuliang Zheng  
University of North Carolina at Charlotte, USA

Jianying Zhou  
Institute for Infocomm Research, Singapore

Sencun Zhu  
Penn State University, USA
External Reviewers

Abdulrhman Alarifi  Jeffrey Horton  Hui Song
Abdulraham Alarifi  Hungyuan Hsu  Alok Tongaonkar
Elli Androulaki  Zhengli Huang  Mercan Topkara
Joongsang Baek  Sotiris Ioannidis  Umut Topkara
Kun Bai  Pandurang Kamat  Dominique Unruh
Abhilasha  Kameswari Kotapati  Hai Wang
  Bhargav-Spantzel  Fengjun Li  Haodong Wang
Marina Blanton  Lunquan Li  Huaxiong Wang
Mike Burmester  Zhiouwei Li  Pan Wang
Matt Burnside  Anyi Liu  Ronghua Wang
Su Chang  Michael Locasto  Shuhong Wang
Shu Chen  Liang Lu  Xirnan Wang
Shuo Chen  Andreas Moser  Yawen Wei
Jong Youl Choi  Karsten Nohl  Liang Xie
Gabriela Cretu  Joseph Pamula  Mengjun Xie
Deepak Kumar Dalai  Chi-Chun Pan  Ping Xie
Kanti Das  Nathanael Paul  Yongqiang Xiong
Christophe Doche  James Riordan  Wenyuan Xu
Markus Duermuth  Sankardas Roy  Yi Yang
Yann Duponchel  Farzad Salim  Chao Yao
Sarah Edwards  Emre Sezer  Zhen Yu
Min Feng  Siamak Fayyaz  Chuan Yue
Keith Frikken  Shahandashti  Linfeng Zhang
Tim van der Horst  Nicholas Sheppard  Qinghua Zhang
Jeff Horton  Stelios Sidiroglou  Yukai Zou
Table of Contents

Security Protocols

Strong and Robust RFID Authentication Enabling Perfect Ownership Transfer .................................................. 1  
Chae Hoon Lim, Taekyoung Kwon

A Robust and Secure RFID-Based Pedigree System (Short Paper) ...... 21  
Chiu C. Tan, Qun Li

A Topological Condition for Solving Fair Exchange in Byzantine Environments .................................................. 30  
Benoît Garbinato, Ian Rickebusch

A Security Analysis of the Precise Time Protocol (Short Paper)........ 50  
Jeanette Tsang, Konstantin Beznosov

Applied Cryptography

An Identity-Based Proxy Signature Scheme from Pairings ............ 60  
Kyung-Ah Shim

Finding Compact Reliable Broadcast in Unknown Fixed-Identity Networks (Short Paper) ..................................... 72  
Huafei Zhu, Jianying Zhou

Formal Analysis and Systematic Construction of Two-Factor Authentication Scheme (Short Paper) .............................. 82  
Guomin Yang, Duncan S. Wong, Huaxiong Wang, Xiaotie Deng

Hierarchical Key Assignment for Black-Box Tracing with Efficient Ciphertext Size ............................................. 92  
Tatsuynki Matsushita, Hideki Imai

Trace-Driven Cache Attacks on AES (Short Paper) .................... 112  
Onur Acııçmez, Çetin Kaya Koç

Access Control and Systems Security

A Construction for General and Efficient Oblivious Commitment Based Envelope Protocols ........................................ 122  
Jiangtao Li, Ninghui Li
Defining and Measuring Policy Coverage in Testing Access
Control Policies

Evan Martin, Tao Xie, Ting Yu

Distributed Credential Chain Discovery in Trust Management
with Parameterized Roles and Constraints (Short Paper)

Ziqing Mao, Ninghui Li, William H. Winsborough

An Operating System Design for the Security Architecture
for Microprocessors

Jörg Platte, Raúl Durán Díaz, Edwin Naroska

Privacy and Malicious Code

Point-Based Trust: Define How Much Privacy Is Worth

Danfeng Yao, Keith B. Frikken, Mikhail J. Atallah,
Roberto Tamassia

Efficient Protocols for Privacy Preserving Matching Against
Distributed Datasets

Yingpeng Sang, Hong Shen, Yasuo Tan, Naixue Xiong

Quantifying Information Leakage in Tree-Based Hash Protocols
(Short Paper)

Karsten Nohl, David Evans

An Anonymous Authentication Scheme for Identification Card

He Ge

A Wireless Covert Channel on Smart Cards (Short Paper)

Geir Olav Dyrkolbotn, Einar Snøkkernes

Network Security

From Proxy Encryption Primitives to a Deployable
Secure-Mailing-List Solution

Himanshu Khurana, Jin Heo, Meenal Pant

Mathematical Foundations for the Design of a Low-Rate DoS Attack
to Iterative Servers (Short Paper)

Gabriel Maciá-Fernández, Jesús E. Díaz-Verdejo,
Pedro García-Teodoro

An Independent Function-Parallel Firewall Architecture
for High-Speed Networks (Short Paper)

Errin W. Fulp
Estimating Accuracy of Mobile-Masquerader Detection Using Worst-Case and Best-Case Scenario ........................................ 302
Oleksiy Mazhelis, Seppo Puuronen, Mika Raento

An Enhanced N-Way Exchange-Based Incentive Scheme for P2P File Sharing (Short Paper) ........................................ 322
Lingli Deng, Yeping He, Ziyao Xu, Chunyang Yuan

Systems Security

Provably Correct Runtime Enforcement of Non-interference Properties ................................................................. 332
V.N. Venkatakrishnan, Wei Xu, Daniel C. DuVarney, R. Sekar

An Attack on SMC-Based Software Protection ........................................ 352
Yongdong Wu, Zhigang Zhao, Tian Wei Chui

Modular Behavior Profiles in Systems with Shared Libraries (Short Paper) ................................................................. 369
Carla Marceau, Matt Stillerman

Efficient Protection Against Heap-Based Buffer Overflows Without Resorting to Magic ........................................ 379
Yves Younan, Wouter Joosen, Frank Piessens

Cryptanalysis

Cryptanalysis of Timestamp-Based Password Authentication Schemes Using Smart Cards ........................................ 399
Guilin Wang, Feng Bao

Cryptanalysis of ID-Based Authenticated Key Agreement Protocols from Bilinear Pairings (Short Paper) ........................................ 410
Kyung-Ah Shim, Seung-Hyun Seo

Seifert’s RSA Fault Attack: Simplified Analysis and Generalizations ..... 420
James A. Muir

The Fairness of Perfect Concurrent Signatures ........................................ 435
Guilin Wang, Feng Bao, Jianying Zhou

Applied Cryptography and Network Security

Secure Set Membership Using 3Sat (Extended Abstract) .............. 452
Michael de Mare, Rebecca N. Wright
Left-to-Right Signed-Bit $\tau$-Adic Representations of $n$ Integers
(Short Paper) ................................................. 469

*Billy Bob Brumley*

Universal Designated Verifier Signature Without Delegatability ....... 479
*Xinyi Huang, Willy Susilo, Yi Mu, Wei Wu*

Tracing HTTP Activity Through Non-cooperating HTTP Proxies
(Short Paper) .................................................. 499

*Richard J. Edell, Peter Kruus, Uri Meth*

**Security Implementations**

A Fast RSA Implementation on Itanium 2 Processor ..................... 507
*Kazuyoshi Furukawa, Masahiko Takenaka, Kouichi Itoh*

Efficient Implementation of Public Key Cryptosystems
on Mote Sensors (Short Paper) ..................................... 519
*Haodong Wang, Qun Li*

Threshold Implementations Against Side-Channel Attacks
and Glitches ....................................................... 529
*Svetla Nikova, Christian Rechberger, Vincent Rijmen*

Hardware-and-Software-Based Security Architecture for Broadband
Router (Short Paper). ............................................. 546
*Xiaozhuo Gu, Yufeng Li, Jianzu Yang, Julong Lan*

**Author Index** .................................................. 557