3rd Applied Cryptography and Network Security Conference

(ACNS) 2005

June 7-10, 2005

Columbia University, New York, NY, USA

http://acns2005.cs.columbia.edu

Venue:

Schapiro Center for Physical Sciences Research (CEPSR), Columbia University, New York, NY

1. Davis Auditorium (4th fl.):
   Registration, invited talks, sessions tagged with a number and an A, food and refreshments.
2. Interschool Laboratory (7th fl.): Sessions tagged with a number and a B.

Sponsors:

Morgan Stanley
One client at a time.

GEMPLUS

Google

ACNS 2005 Conference Program

Tuesday, June 7th

Registration & Breakfast	8:00 – 9:00
Opening Remarks	8:45 – 9:00
Invited Talk 1:	9:00 – 10:00

Victor Shoup, NYU. "*Sequence of Games: A Technique for Taming Complexity in Security Proofs.*"

Chair: Moti Yung

Break (Coffee outside Davis Auditorium)	10:00 – 10:30
Session 1-A: Passwords & Authentication	10:30 – 12:00

Chair: Yuliang Zheng

Two-Server Password-only Authenticated Key Exchange
Jonathan Katz, Phil MacKenzie, Gelareh Taban, Virgil Gligor

Strengthening Password-Based Authentication Protocols Against Online Dictionary Attacks
Peng Wang, Yongdae Kim, Vishal Kher, Taekyoung Kwon

Cryptanalysis of an Improved Client-to-Client Password-Authenticated Key Exchange (C2C-PAKE) Scheme
Raphael C.-W. Phan, Bok-Min Goi

Session 1-B: Arithmetic & Side Channels 10:30 – 12:00
Chair: Jens Groth

Side Channel Attacks on Combined Countermeasures With Randomized Addition Chains
Tae Hyun Kim, Dong-Guk Han, Katsuyuki Okeya, Jongin Lim

Improved Chosen Message Power Analysis on XTR and a Countermeasure Suitable to Parallelism and Generalization
Dong-Guk Han, Tetsuya Izu, Jongin Lim, Kouichi Sakurai

Fixed Hamming Weight Representation for Indistinguishable Addition Formulae
Hideyo Mamiya, Atsuko Miyaji

Lunch: Carleton Cafeteria, meet at Davis Auditorium 12:00 – 1:30

Session 2-A: Multiparty Crypto 1:30 – 3:00
Chair: Feng Bao

Efficient Security Mechanisms For Overlay Multicast-based Content Distribution
Sencun Zhu, Chao Yao, Donggang Liu, Sanjeev Setia, Sushil Jajodia

A Traitor Tracing Scheme Based on RSA for Fast Decryption
John P. McGregor, Yiqun Lisa Yin, Ruby Lee

N-Party Encrypted Diffie-Hellman Key Exchange Using Different Passwords
Jin Wook Byum, Dong Hoon Lee

Session 2-B: Biometrics, Smartcards, and Voting 1:30 – 3:00
Chair: Andrew Wright

A Biometric Identity Based Signature Scheme
Fergus Byrne, Andrew Burnett, Adam Duffy, Tom Dowling

The OpenEAP Smartcard Project
Pascal Urien, Mesmin Dandjinou

ADDER: A Web-based Internet Voting System
Aggelos Kiayias, Michael Korman, David Walluck

Break (Coffee outside Davis Auditorium) 3:00 – 3:30

Session 3-A: Attacks & Countermeasures 3:30 – 5:30
Chair: Roberto Tamassia

Messin' With Texas, Deriving Mother's Maiden Names Using Public Records
Virgil Griffith, Markus Jakobsson

Mitigating Network Denial-of-Service Through Diversity-Based Traffic Management
Ashraf Matrawy, Anil Somayaji, Paul C. van Oorschot

Searching for High-Value Rare Events With Uncheatable Grid Computing
Wenliang Du, Michael Goodrich

Digital Signatures Do Not Guarantee Ownership
Thomas Pornin, Julien P. Stern

Session 3-B: Constrained Cryptography 3:30 – 5:30
Chair: John Ioannidis

Encryption-With-Redundancy For SCADA Message Authentication
Xunhua Wang, Andrew Wright

Secure Access of Medical Data With Query-Driven Encryption
Yanjiang Yang, Feng Bao, Robert H. Deng

A Management Scheme for Time-Limited Cryptographic Keys
Yuichi Kaji, Ryo Nojima

Wednesday, June 8th

Registration & Breakfast 8:30 – 9:00

Invited Talk 2: 9:00 – 10:00
Avi Rubin, Johns Hopkins. "*Security and Privacy Issues in RFID Technologies.*"
Chair: Angelos Keromytis

Break (Coffee outside Davis Auditorium) 10:00 – 10:30

Session 4-A: New Crypto Mechanisms 10:30 – 12:00
Chair: Robert Deng

Thompson's Group and Public Key Cryptography
Vladimir Shpilrain, Alexander Ushakov

Rainbow, A New Multivariable Polynomial Signature Scheme
Jintai Ding, Dieter Schmidt

Badger – A Fast and Provably Secure MAC
Martin Boesgaard, Thomas Christensen, Erik Zenner

Session 4-B: Secure Networks 10:30 – 12:00
Chair: Sotiris Ioannidis

A Distributed Denial-of-Service Defense System Using Leaky-Bucket-Based Packetscore
Paulo Ayres, Huizhong Sun, H. Jonathan Chao, Wing C. Lau

Component Identification: Enabler for Secure Networks of Complex Systems
Andre Weimerskirch, Katrin Hoper, Christof Paar, Marko Wolf

Spanning Tree Protocol Management: Best Practices
Luis A. Trejo (Tecnologico de Monterrey)

Lunch: outside Davis Auditorium 12:00 – 1:30

Session 5-A: IDS & Forensics 1:30 – 3:00
Chair: Vassilis Prevelakis

IDS False Alarm Reduction Using Continuous and Discontinuous Patterns
Abdulrahman Alharby, Kideki Imai

Indexing Information for Data Forensics
Mikhail Atallah, Michael T. Goodrich, Roberto Tamassia

Model Generalization and its Implications on Intrusion Detection
Zhuowei Li, Jianying Zhou, Amitabha Das

Session 5-B: Authentication and Signatures 1:30 – 3:00
Chair: Pascal Urien

A New Transitive Signature Scheme Based on RSA-Based Security Assumptions
Dang Nguyen Duc, Zeen Kim, Kwangjo Kim

Single Password, Multiple Accounts
Mohamed G. Gouda, Alex X. Liu, Lok M. Leung, Mohamed A. Alam

Generic Fair Non-repudiation Protocols with Transparent TTP
Guilin Wang

Break (Coffee outside Davis Auditorium) 3:00 – 3:30

Session 6: Confidentiality 3:30 – 5:30
Chair: Frederic Muller

Intrusion-Resilient Secure Channels
Gene Itkis, Robert McNerney, Jr., Scott W. Rossell

Optimal Asymmetric Encryption and Signature Paddings
Benoit Chevallier-Mames, Duong Hieu Phan, David Pointcheval

Efficient And Leakage-Resilient Authenticated Key Transport Protocol Based on RSA
SeongHan Shin, Kazukuni Kobara, Hideki Imai

Identity Based Encryption Without Redundancy
Benoit Libert, Jean-Jacques Quisquater

Thursday, June 9th

Registration and Breakfast 8:30 – 9:00

Invited Talk 3: 9:00 – 10:00

Yiqun Lisa Yin, Independent Security Consultant. "*Recent Advances in Hash Function Research.*"

Chair: Moti Yung

Break (Coffee outside Davis Auditorium) 10:00 – 10:30

Session 7: Anonymity 10:30 – 12:00

Chair: Wen-Guey Tzeng

OACerts: Oblivious Attribute Certificates
Jiangtao Li, Ninghui Li

Dynamic K-Times Anonymous Authentication
Lan Nguyen, Rei Safavi-Naini

Efficient Anonymous Roaming and Its Security Analysis
Guomin Yang, Duncan S. Wong, Xiaotie Deng

Lunch: Carleton Cafeteria, meet at Davis Auditorium 12:00 – 1:30

Session 8: Collaboration Through Payments 1:30 – 3:00

Chair: Jintai Ding

Quantifying Security in Hybrid Cellular Networks
Markus Jakobsson, Liu Yang,

Off-line Karma: A Decentralized Currency for Peer-to-Peer and Grid Applications
Flavio D. Garcia, Jaap-Henk Hoepman

Building Reliable Mix Networks With Fair Exchange
Michael K. Reiter, XiaoFeng Wang, Matthew Wright

Break (Coffee outside Davis Auditorium) 3:00 – 3:30

Session 9: Symmetric Key Mechanisms 3:30 – 5:00

Chair: Jianying Zhou

SCARE of the DES
Remy Daudigny, Herve Ledig, Frederic Muller, Frederic Valette

Robust Key Extraction from Physical Uncloneable Functions
Boris Skoric, Pim Tuyls, Wil Ophey

Efficient Constructions for One-Way Hash Chains
Yih-Chun Hu, Markus Jakobsson, Adrian Perrig

Friday, June 10th

Registration and Breakfast 8:30 – 9:00

Invited Talk 4: 9:00 – 10:00

George Sherman, Morgan Stanley. "*Information Security Technologies as Enablers of Banking Systems*"

Chair: Angelos Keromytis

Break (Coffee outside Davis Auditorium) 10:00 – 10:30

Session 10: Privacy 10:30 – 12:00

Chair: Tal Malkin

Privacy-Preserving Keyword Searches on Remote Encrypted Data
Yan-Cheng Chang, Michael Mitzenmacher

An Efficient Solution to the Millionaires' Problem Based on Homorphic Encryption
Hsiao-Ying Lin, Wen-Guey Tzeng

Non-interactive Zero-knowledge Arguments for Voting
Jens Groth (UCLA)

Lunch: Carleton Cafeteria, meet at Davis Auditorium 12:00 – 1:30

Session 11: Signatures 1:30 – 3:00

Chair: Angelos Keromytis

Short Signature and Universal Designated Verifier Signature Without Random Oracles
Rui Zhang, Jun Furukawa, Hideki Imai

Efficient Identity-Based Ring Signature
Sherman S. M. Chow, S. M. Yiu, Lucas C.K. Hui

New Signature Schemes with Coupons and Tight Reduction
Benoit Chevallier-Mames