SEC2005: Programme

Call for Participation

Call for participation is available.
TEXT version PDF version
Early-bird registration deadline is 25th May 2005.

Time Table

PDF file is here.

TIME	30th May (Mon)		31st May (Tue)		1st June (Wed)	
9:30-11:00	Opening *5 (International Conference Room)		WS for WG11.2 *4 (7)R302	Trusted Computing Systems (8)R303	Internet and Web Security (13)R302	Digital Signature Schemes (14)R303
11:00-11:30	Break *6		Break		Break	
11:30-13:00	Privacy and Anonymity *2 *7 (1)R302	Special Session 1 *8 (2)R303	WS for WG11.2 (9)R302	Secure Commercial Systems (10)R303	Internet Security to DoS Attack (15)R302	Key Management *3 (16)R303
13:00-14:30	Lunch *9		Lunch		Lunch	
14:30-16:00	Security Management (3)R302	Special Session 2 (4)R303	WS for WG11.2 *1 (11)R302	Mobility and Ubiquitous Security *1 (12)R303	Intrusion Detection (17)R302	Security for Multimedia (18)R303
16:00-16:30	Break		Social Event and Dinner(departure: 16:00 to Tokyo Central Area: Asakusa etc.)		Break	
16:30-18:00	Security Architecture (5)R302	Panel (6)R303			Closing *10 (Room 201)	
19:00-21:00	Simple Welcome Reception					

Special Session 1: Security management and IT governance
Special Session 2: Security Education in Asia
Panel: Security in Ubiquitous Computing
*1: WS (11) and Session "Mobility and Ubiquitous Security" start at 14:20.
*2, *3: Sessions "Privacy and Anonymity" and "Key Management" each takes only an hour.
*4: WS (7) starts at 10:00.
*5: Opening session ends at 11:20.
*6: Break starts at 11:20 and ends at 11:40.
*7: Session "Privacy and Anonymity" starts at 11:40 and ends at 12:40.
*8: Special Session 1 (2) starts at 11:40 and ends at 13:10.
*9: Lunch starts at 13:10 and ends at 14:30.

*10: Closing session starts at 16:20 and ends at 17:20.

Conference Programme

Opening Session

09:30-11:20, 30th May in International Conference Room

Session Chair: Yuko Murayama

- General Chair Address
  Ryoichi Sasaki
- Programme Chair Address
  Eiji Okamoto
- TC 11 Chair Address
  Leon Strous
- KB Award Winner Address
- 20th Anniversary Report "Information Security Research: 20 years of SEC conferences"
  Prof. Reinhardt A. Botha
- Keynote Address "The Future of Cybersecurity: Working Backward, Thinking Forward"
  Dr. Carl E. Landwehr (US National Science Foundation)

Privacy and Anonymity

11:40-12:40, 30th May in Room 302

Chair: Kai Rannenberg

- Accountable Anonymous E-Mail
  V. Naessens, L. Demuynck, B. D. Decker
- Protecting Consumer Data in Composite Web Services
  C. Pearce, P. Bertok, R. V. Schyndel

Security Management

14:30-16:00, 30th May in Room 302

Chair: Rossouw Von Solms

- A Decision Matrix Approach to Prioritize Holistic Security Requirements in E-Commerce
  A. Zuccato
- Assignment of Security Clearances in an Organization
  L. J. Janczewski, V. Portougal
- Tool Supported Management of Information Security Culture
  T. Schlienger, S. Teufel

Special Session 1 : Security Management and IT Governance

11:40-13:10, 30th May in Room 303

Co-Chair: Leon Strous
Co-Chair: Masakatsu Nishigaki

- ISMS in Action - an innovative approach
  William List, Partner, Wm. List & Co, UK
- Practices and Experiments of Information Security Management
  Koji Nakao, Director, KDDI Corp., Japan

Special Session 2 : Security Education in Asia

14:30-16:00, 30th May in Room 303

Chair: Ryoichi Sasaki

- Security Education in Japan
  Katsuya Uchida, Associate Professor, Institute of Information Security
- Security Education in Korea
  Min Kyoung-sik, Project Manager, Korea Information Security Agency
  Won Soon-Jae (presenter)
- Security Education in Singapole
  Leong Peng Chor, Associated Professor, Nanyang Technological University

Security Architecture

16:30-18:00, 30th May in Room 302

Chair: Javier Lopez

- ERPSEC - A Reference Framework to Enhance Security in ERP Systems
  M. Hertenberger, S. V. Solms
- A New Architecture for User Authentication and Key Exchange Using Password for Federated Enterprises
  Y. Yang, F. Bao, R. H. Deng
- A Secure Quantum Communication Protocol Using Insecure Public Channels
  I. Tsai, C. Yu, W. Tu, S. Kuo

Trusted Computing Systems

09:30-11:00, 31st May in Room 303

Chair: Yves Deswarte

- Trusted Component Sharing by Runtime Test and Immunization for Survivable Distributed Systems
  J. S. Park, P. Chandramohan, G. Devarajan
- Design and Implementation a TPM Chip SUP320 by SOC
  R. Jiang-chun, D. Kui, W. Zhi-ying, Z. Xue-mi, T. Yuan-man
- Mathematical Models of IP Traceback Methods and Their Verification
  K. Ohmori, R. Matsushima, A. Suzuki, M. Kawabata, M. Ohmuro, T. Kai, S. Nishiyama

Secure Commercial Systems

11:30-13:00, 31st May in Room 303

Chair: William List

- Transferable E-Cash Revisit
  J. Liu, S. Wong, D. Wong
- A License Transfer System for Supporting Content Portability in Digital Rights Management
  Q. Liu, R. Safavi-Naini, N. P. Sheppard
- Secure Person-To-Person Communications Based on Biometrics Signals
  Y. Wu, F. Bao, R. H. Deng

Mobility and Ubiquitous Security

14:20-15:50, 31st May in Room 303

Chair: Bart de Decker

- Distance-Bounding Proof of Knowledge to Avoid Real-Time Attacks
  L. Bussard, W. Bagga
- Adaptive Multicast Polling Scheme for IEEE 802.11 Wireless LAN
  K. Kim, S. Lee, K. Han
- The Pairing Problem with User Interaction
  T. Peyrin, S. Vaudenay

Internet and Web Security

09:30-11:00, 1st June in Room 302

Chair: Carl Landwehr

- Protection Against Spam Using Pre-Challenges
  R. Roman, J. Zhou, J. Lopez
- Network Smart Card: A New Paradigm of Secure Online Transactions
  A. Ali, K. Lu, M. Montgomery
- Automatically Hardening Web Applications Using Precise Tainting
  A. Nguyen-Tuong, S. Guarnieri, D. Greene, J. Shirley, D. Evans

Internet Security to DoS Attack

11:30-13:00, 1st June in Room 302

Chair: Masato Terada

- Traffic Redirection Attack Protection System (TRAPS) - A Full-Fledged Adaptive DoS/DDoS Attack Mitigation Scheme
  V. L. L. Thing, H. C. J. Lee
- Statistical Signatures for Early Detection of Flooding Denial-Of-Service Attacks
  J. Haggerty, Q. Shi, M. Merabti

- Design, Implementation, and Evaluation of "FRiTrace"
  W. Huang, J. Cong, C. Wu, S. F. Wu

Intrusion Detection

14:30-16:00, 1st June in Room 302

Chair: Eiji Okamoto

- Design and Implementation of a High-Performance Network Intrusion Prevention System
  K. Xinidis, K. Anagnostakis, E. Markatos
- STRIDE: Polymorphic Sled Detection through Instruction Sequence Analysis
  P. Akritidis, E. P. Markatos, M. Polychronakis, K. Anagnostakis
- Piranha: Fast and Memory-Efficient Pattern Matching for Intrusion Detection
  S. Antonatos, M. Polychronakis, P. Akritidis, K. G. Anagnostakis, E. P. Markatos

Digital Signature Schemes

09:30-11:00, 1st June in Room 303

Chair: Kanta Matsuura

- Designated-Verifier Proxy Signature Schemes
  G. Wang
- Tripartite Concurrent Signatures
  W. Susilo, Y. Mu
- Signcryption in Hierarchical Identity Based Cryptosystem
  S. Chow, T. H. Yuen, L. C. K. Hui, S. M. Yiu

Key Management

11:30-12:30, 1st June in Room 303

Chair: Mi Rang Park

- Protecting Membership Dynamic Information in Large Scale Multicast Groups
  Y. Wu, T. Li, R. H. Deng
- Secure Group Communication with Distributed Generation of Private Keys in Ad-hoc Networks
  S. Sundaram, P. Bertok, B. Burton

Security for Multimedia

14:30-16:00, 1st June in Room 303

Chair: Hiroshi Yoshiura

- Ensuring Media Integrity on Third-Party Infrastructures
  J. Dittmann, S. Katzenbeisser, C. Schallhart, H. Veith
- A New Fragile Mesh Watermarking Algorithm for Authentication
  H. Wu, Y. Cheung

- New Paradigm in Graph-Based Visual Secret Sharing Scheme by Accepting Reversal in Black-White Images
  Y. Suga

Closing Session

16:20-17:20, 1st June in Room 201

Session Chair: Yuko Murayama

- Best Student Paper Award
- Presentation of SEC 2006
- TC 11 Chair Address
- Closing Address by SEC 2005 General Chair

Workshop on Small Systems Security and Smart Cards

Workshop Chair: Jan Verschuren

Keynote Address

10:00-11:00, 31st May in Room 302

Chair: Leon Strous

- Appropriate Security: dealing with the limitations of smart cards
  Mike Paterson (Security and System Applications Engineering Manager, Mobile Security Business Group, Renesas Technology Europe Ltd.)

JavaCards

11:30-13:00, 31st May in Room 302

Chair: Bill Caelli

- Overcoming Channel Bandwidth Constraints in Secure SIM Applications
  John A. MacDonald, William Sirett and Chris J. Mitchell
- On the Performance of Certificate Revocation Protocols Based on a Java Card Certificate Client Implementation
  K. Papapanagiotou, K. Markantonakis, Q. Zhang, W.G. Sirett and K. Mayes
- On-the-Fly Formal Testing of a Smart Card Applet
  Arjen van Weelden, Martijn Oostdijk, Lars Frantzen, Pieter Koopman and Jan Tretmans

Side Channel Analysis, Fault Injection and Applications

14:20-15:50, 31st May in Room 302

Chair: Martijn Oostdijk

- A Computationally Feasible SPA Attack on AES via Optimized Search

Joel VanLaven, Mark Brehob and Kevin J. Compton

- The Proof by 2^M-1: a Low-Cost Method to Check Arithmetic Computations
  Sylvain Guilley and Philippe Hoogvorst
- StreamTo: Streaming Content using a Tamper-Resistant Token
  Jieyin Cheng, Cheun Ngen Chong, Jeroen M. Doumen, Sandro Etalle, Pieter H. Hartel and Stefan Nikolaus

Panel

Security in Ubiquitous Computing

16:30-18:00, 30th May in Room 303

Moderator: Hiroaki Kikuchi (Tokai University)

- From a community of ubiquitous computing
  Prof. Hideyuki Tokuda (Keio University)
- From Mobile computing research
  Prof. Kai Rannenberg (Goethe University Frankfurt)
- From Network security and Cryptographic research
  Prof. Bart De Decker (Katholieke Universiteit Leuven)
- From Japanese industries
  Mr. Naoki Endo (General Manager of SI Technology Center, Toshiba Solutions Corp.)