Foreword

With great pleasure, we welcome you to The Fourth International Conference on Security of Information and Networks (SIN 2011). SIN 2011 was held at the Macquarie Graduate School of Management (MGSM), CBD Campus, in Sydney, Australia on 14-19 November, 2011. The SIN series of conferences aims to provide an international forum for presentation of research and applications of security in information and networks. SIN 2011 follows the successful conferences of SIN 2007 and SIN 2009 held in Gazimagusa, North Cyprus, and SIN 2010 held in Rostov-on-Don, Taganrog, Russia. The next SIN Conference is scheduled to take place in Germany in 2012.

SIN 2011 was organized jointly by Macquarie University, Sydney, Australia; Süleyman Demirel University, Turkey; Southern Federal University, Rostov-on-Don, Taganrog, Russia; and Technical University of Darmstadt, Germany. SIN 2011 was hosted by the Centre for Advanced Computing - Algorithms and Cryptography (ACAC), the Information and Networked Systems Security (INSS) and the Intelligent Systems Group (ISG) of the Department of Computing, Macquarie University, Sydney, Australia.

Organizing SIN 2011 was a great team effort. First of all, we thank the authors for submitting their papers for consideration, and the program committee members for their hard work in reviewing those papers. Special thanks are due to the chairs of the organization committee whose leadership made SIN 2011 possible: Program Chair Josef Pieprzyk, Tutorials Chair Christophe Doche, Workshops Chair Ron Steinfeld, Publication Chair Behnam Rahnama, Finance Chair Michael Hitchens, Local Arrangements Chair Rajan Shankaran, Registration Chair Yan Wang, e-Presence Chair Wanli Ma, Promotion Chair Yi Mu. The full list of all the members of the organization committee is available as part of the front matter of the Proceedings; again, we thank them all. Special thanks go to Michelle Kang for supporting the Committees so effectively.

We wish to thank the Air Force Office of Scientific Research (AFOSR), Asian Office of Aerospace Research and Development (AOARD), Army International Technology Center-Pacific (ITC-PAC), and Office of Naval Research-Global (ONRG) for their contribution to the success of this conference.

We also wish to thank Microsoft Research for providing the Conference Management Toolkit (CMT) and for hosting the SIN 2011 submission site.

We are greatly indebted to the ACM Press / Sheridan Printing Company for producing this proceedings book. We also thank Lisa Tolles of Sheridan Printing Company for her excellent cooperation and support.

We welcome all the participants to enjoy the conference and also what Sydney has to offer.

Mehmet A. Orgun
General Chair
Macquarie University
Australia

Atilla Elçi
General Co-Chair
Süleyman Demirel University, Turkey

Oleg Makarevich
General Co-Chair
Southern Federal University, Russia

Sorin Huss
General Co-Chair
Technical University of Darmstadt, Germany
Program Chairs’ Welcome

It is our great pleasure to welcome you to The Fourth International Conference on Security of Information and Networks (SIN 2011) organized jointly by Macquarie University, Sydney, Australia; Süleyman Demirel University, Turkey; Southern Federal University, Rostov-on-Don, Taganrog, Russia; and Technical University of Darmstadt, Germany.

The main theme of the SIN 2011 conference is security of information and networks. The theme includes the following topics: next generation network architectures, protocols, theory, systems and applications; the development and the realization of cryptographic solutions, security schemes; critical analysis of, and/or experimenting with, existing approaches; secure information systems, especially distributed control and processing applications, and security in networks; interoperability, service levels and quality issues in such systems; information assurance, security, and public policy; detection and prevention of cyber-crimes such as fraud and phishing.

In total, there were 78 papers submitted to SIN 2011. Each paper was assigned at least 3 reviewers. There were 27 full papers accepted to the conference (~35%) with the maximum length of 8 pages. There were 3 student papers accepted with a smaller paper length of 6 pages. There were also 3 position and 9 short papers accepted with the maximum length of 4 pages.

The conference hosted two distinguished researchers who graciously agreed to present their keynote speeches:

- Vijay Varadharajan – Microsoft Chair of Innovation in Computing, Macquarie University, Sydney, NSW, Australia.
- Kevin Kwiat – Principal Computer Engineer, The Cyber Science Branch of the U.S. Air Force Research Laboratory (AFRL), Rome, New York, USA

SIN 2011 Proceedings was published as part of the International Conference Proceedings Series by the ACM and, along with the proceedings of SIN 2009 and SIN 2010, it was placed on the ACM Digital Library for perpetual online access.

We extend our thanks to all the authors (of all the papers – both accepted and rejected), the participants, the presenters and the session chairs for their effort and support. We would like to express our gratitude to the program committee members, who worked very hard in reviewing papers and providing suggestions for their improvements.

We hope that the conference gave an excellent opportunity to air thought-provoking views and to benefit from sharing ideas with other researchers and practitioners from both academia and industry.

Josef Pieprzyk  
Program Chair  
Macquarie University, Australia

Lyudmila Babenko  
Program Co-Chair  
Southern Federal University, Russia

Alexander Chefranov  
Program Co-Chair  
Eastern Mediterranean University, North Cyprus

Rajan Shankaran  
Program Co-Chair  
Macquarie University, Australia
Table of Contents

SIN 2011 Conference Organization

SIN 2011 Sponsors & Supporters

Keynote Talks

- **Fault Tolerance for Fight-Through: A Basis for Strategic Survival** ................................................................. 1
  Kevin A. Kwiat *(Air Force Research Laboratory)*

- **Rethinking Cyber Security** .......................................................................................................................... 3
  Vijay Varadharajan *(Macquarie University)*

Regular Papers

- **Collusion Resistant Fingerprinting of Digital Audio** ................................................................. 5
  Andrew Z. Tirkel *(Scientific Technology)*,
  Thomas E. Hall, Charles F. Osborne, Nicholas Meinhold *(Monash University)*,
  Oscar Moreno *(Gauss Research Laboratory)*

- **Using Decision Trees for Generating Adaptive SPIT Signatures** ............................................. 13
  Mohamed Nassar *(INRIA Research Center Nancy, Grand Est)*, Sylvain Martin, Guy Leduc *(University of Liège)*,
  Olivier Fester *(INRIA Research Center, Nancy, Grand-Est)*

- **Cryptanalysis of the Stream Cipher BEAN** .............................................................................. 21
  Martin Ågren, Martin Hell *(Lund University)*

- **Corporate Networks Security Evaluation Based on Attack Graphs** ........................................ 29
  Evgeny Abramov, Artem Andreev, Oleg Makarevich, Denis Mordvin *(Southern Federal University)*

- **Echo Hiding Based Stereo Audio Watermarking Against Pitch-Scaling Attacks** .............. 37
  Iynkaran Natgunanathan, Yong Xiang *(Deakin University)*

- **The Optimal Linear Multi-Secret Sharing Scheme for Non-Threshold Access Structure**
  *(Student Contribution)* ......................................................................................................................... 43
  Shu-guang Dai *(Guangzhou University)*,
  Chun-ming Tang *(Guangzhou University & Chinese Academy of Sciences)*,
  Yue-nai Chen *(Guangzhou University)*

- **Rational Distance-Bounding Protocols Over Noisy Channel** .................................................. 49
  Long Hoang Nguyen *(Oxford University)*

- **Algebraic Analysis of GOST Encryption Algorithm** ................................................................. 57
  Ludmila Babenko, Evgeniya Ishchukova, Ekaterina Maro *(Southern Federal University)*

- **Fault Attack to the Elliptic Curve Digital Signature Algorithm with Multiple Bit Faults** .... 63
  Alessandro Barenghi *(Politecnico di Milano)*, Guido M. Bertoni *(STMicroelectronics)*,
  Luca Breveglieri, Andrea Palomba, Gerardo Pelosi *(Politecnico di Milano)*

- **Trust Based Fusion Over Noisy Channels Through Anomaly Detection**
  *in Cognitive Radio Networks* ........................................................................................................ 73
  Shamieck Bhattacharjee, Saptarshi Debroy, Mainak Chatterjee *(University of Central Florida)*,
  Kevin Kwiat *(Air Force Research Laboratory)*

- **On Automatic Detection of SQL Injection Attacks by the Feature Extraction**
  *of the Single Character* .................................................................................................................. 81
  Michio Sonoda, Takeshi Matsuda, Daiki Koizumi, Shigeichi Hirasawa *(Cyber University)*

- **Logic Based Authorization Program and Its Implementation** ............................................. 87
  Chun Ruan, Seyed Shahrestani *(University of Western Sydney)*

- **Security Analysis of a Femtocell Device** ............................................................................. 95
  Ravishankar Borgaonkar, Kevin Redon, Jean-Pierre Seifert *(Technical University of Berlin & Deutsche Telekom Laboratories)*
• A Model-Based Attack Injection Approach for Security Validation .......................................................... 103
  Anderson Moraes, Ana Cavalli (Télécom SudParis), Eliane Martins (University of Campinas)

• Detection of Neighbor Solicitation and Advertisement Spoofing in IPv6 Neighbor
  Discovery Protocol ................................................................................................................................. 111
  Ferdous A. Barbhuiya, Santosh Biswas, Sukumar Nandi (IIT Guwahati)

• Counteracting DDoS Attacks in WLAN .................................................................................................. 119
  Udaya Tupakula, Vijay Varadarajan (Macquarie University), Sunil Kumar Vuppala (Infosys Labs)

• A Secure and Anonymous Cooperative Sensing Protocol for Cognitive Radio
  Networks .................................................................................................................................................. 127
  Helena Rifa-Pous, Carles Garrigues (Universitat Oberta de Catalunya)

• A HTTP Cookie Covert Channel ........................................................................................................ 133
  William Huba, Bo Yuan, Daryl Johnson, Peter Lutz (Rochester Institute of Technology)

• Detour Attack in OLSR ......................................................................................................................... 137
  Manoj S. Gaur, Vijay Laxmi, Manish Kumar, Rajbir Kaur (Malaviya National Institute of Technology)

• Exploration of a Hand-Based Graphical Password Scheme ................................................................. 143
  Haichang Gao, Licheng Ma, Jinhua Qiu, Xiyang Liu (Xidian University)

• A Sybil Attack Detection Approach Using Neighboring Vehicles in VANET ...................................... 151
  Jyoti Grover, Manoj Singh Gaur, Vijay Laxmi, Nitesh Kumar Prajapati (Malaviya National Institute of Technology)

• Model Checking Security Policy Model Using Both UML Static and Dynamic Diagrams ................ 159
  Liang Cheng, Yang Zhang (Chinese Academy of Sciences)

• TW-KEAP: An Efficient Four-Party Key Exchange Protocol for End-to-End Communications ........ 167
  Wei-Kuo Chiang, Jian-Hao Chen (National Chung Cheng University)

• Secure Random Number Generation in Wireless Sensor Networks .................................................. 175
  Giuseppe Lo Re, Fabrizio Milazzo, Marco Ortolani (University of Palermo)

• Improving Operation Time Bounded Mission Critical Systems’ Attack-Survivability
  Through Controlled Source-Code Transformation .................................................................................. 183
  Alban Vignaux, Arnaud Auguste, Bogdan Korel, Shangpin Ren (Illinois Institute of Technology),
  Kevin Kwiat (Air Force Research Laboratory)

• A Different Algebraic Analysis of the ZUC Stream Cipher ................................................................. 191
  Mufeed AlMashrafi (Queensland University of Technology)

Student Papers

• Algebraic Analysis of the SSS Stream Cipher ......................................................................................... 199
  Mufeed AlMashrafi, Kenneth Koon-Ho Wong, Leonie Simpson, Harry Bartlett
  (Queensland University of Technology), Ed Dawson (Information Security Institute)

• An Approach to Enhance the Security of Remote Health Monitoring Systems .............................. 205
  Mahmoud Elkhodr, Seyed Shahrestani, Hon Cheung (University of Western Sydney)

• On the Impacts of Join and Leave on the Propagation Ratio of Topology-Aware Active Worms ....... 209
  Ahmad Jafarabadi, Mohammad Abdollahi Azgomi (Iran University of Science & Technology)

Position Papers

• Different Models of Information Protection System, Based on the Functional Knapsack .................. 215
  Valeriy O. Osipyan (Kuban State University)

• Obscurity of Network Security Course Curriculum .............................................................................. 219
  Suleyman Kondakci (Izmir University of Economics)

• Counterfactually Reasoning About Security .......................................................................................... 223
  Manuel Peralta, Supratik Mukhopadhyay (Louisiana State University),
  Ramesh Bharadwaj (Naval Research Laboratory)
Short Papers

- **Acceleration of Packet Filtering Using GPGPU** ................................................................. 227
  Lakshminarayan V, Kamal Chandra, Manoj S. Gaur, Vijay Laxmi (Malaviya National Institute of Technology), Mark Zwolinski (University of Southampton)

- **Formal Analysis of Usage Control Policies** ............................................................ 231
  Boulares Ouchenne, Ousmane Koné (University of Pau)

- **Extending the Scope of CardSpace** .............................................................................. 235
  Haitham S. Al-Sinani, Chris J. Mitchell (University of London)

- **Towards Hiding Federated Digital Identity: Stop-Dissemination Mechanism in Content-Centric Networking** ................................................................. 239
  Amine Elabidi (University of Manouba), Ghazi Ben Ayed (University of Lausanne), Sonia Mettal Gammar, Farouk Kamoun (University of Manouba)

- **WinSEND: Windows SECure Neighbor Discovery** ......................................................... 243
  Hosnieh Rafiee, Ahmad AlSa’deh, Christoph Meinel (University of Potsdam)

- **Research on Survivability Metrics Based on Survivable Process of Network System** ..... 247
  Ming Liang, Huang Minhuan, Wang Dongxia, Kuang Xiaohui (National Key Laboratory of Science & Technology on Information System Security), Wang Chunlei (National Key Laboratory of Science & Technology on Information System Security and Tsinghua University), Feng Xuewei (National Key Laboratory of Science & Technology on Information System Security)

- **On the Security and Practicality of a Buyer Seller Watermarking Protocol for DRM** .... 251
  Geong Sen Poh, Muhammad Reza Z’aba (MIMOS Berhad)

- **Proposal and Implementation of Enhanced HDD Authentication that Enables Self-Wipe** .................................................................................................................. 255
  Zhaogong Guo, Kouichi Yasaki, Yousuke Nakamura, Kazuaki Nimura, Isamu Yamada (Fujitsu Laboratories Ltd.)

- **Microcontroller-Based Implementation of parseKey+ for Limited Resources Embedded Applications** ................................................................. 259
  Atilla Elci (Suleyman Demirel University), Behnam Rahnama (European University of Lefke), Reza Makvandi (Eastern Mediterranean University)

**Author Index** .................................................................................................................... 263
SIN 2011 Conference Organization

**General Chairs:** Mehmet A. Orgun *(Macquarie University, Australia)*
Atilla Elçi *(Süleyman Demirel University, Turkey)*
Oleg Makarevich *(Southern Federal University, Russia)*
Sorin Huss *(Technische Universität Darmstadt, Germany)*

**Program Chairs:** Josef Pieprzyk *(Macquarie University, Australia)*
Lyudmila Babenko *(Southern Federal University, Russia)*
Alexander Chefranov *(Eastern Mediterranean University, North Cyprus)*
Rajan Shankaran *(Macquarie University, Australia)*

**Publication Chairs:** Behnam Rahnama *(European University of Lefke, North Cyprus)*
Ekaterina Maro *(Southern Federal University, Russia)*
Kaile Su *(Griffith University, Australia & Peking University, PRC)*

**Local Arrangements Chairs:** Rajan Shankaran *(Macquarie University, Australia)*
Dat Tran *(University of Canberra, Australia)*
Kalyan Janakiraman *(Macquarie University, Australia)*

**Promotion Chairs:** Yi Mu *(University of Wollongong, Australia)*
Maxim Anikeev *(Southern Federal University, Russia)*
Deniz Özdemir *(Toros University, Turkey)*

**Tutorials Chairs:** Christophe Doche *(Macquarie University, Australia)*
Olga Peskova *(Southern Federal University, Russia)*
Duygu Çelik *(İstanbul Aydın University, Turkey)*

**Workshops Chairs:** Ron Steinfeld *(Macquarie University, Australia)*
Evgeny Tumoian *(Southern Federal University, Russia)*
Luc Rolland *(Toros University, Turkey)*

**Finance Chair:** Michael Hitchens *(Macquarie University, Australia)*

**e-Presence Chair:** Wanli Ma *(University of Canberra, Australia)*

**Liaison for Americas:** Carlos Becker Westphall *(Federal University of Santa Catarina, Brazil)*

**Liaison for Asia-Pacific:** Huaxiong Wang *(Nanyang Technological University, Singapore)*

**Registration Chairs:** Yan Wang *(Macquarie University, Australia)*
Ekaterina Pakulova *(Southern Federal University, Russia)*
D. Tayyar Şen *(Toros University, Turkey)*
Program Committee:
Evgeny Abramov (Southern Federal University, Russia)
Kamel Adi (Université du Québec en Outaouais, Canada)
Sheikh Iqbal Ahamed (Marquette University, USA)
Maxim Anikeev (Southern Federal University, Russia)
Kubilay Atasu (IBM Zürich Research Laboratory, Switzerland)
Lyudmila Babenko (Southern Federal University, Russia)
Joonsang Baek (Khalifa University of Science, Technology & Research, UAE)
Tagir Bakirov (Universität Karlsruhe, Germany)
Ayşe Bener (Boğaziçi University, Turkey)
Mehmet Ufuk Çağlayan (Boğaziçi University, Turkey)
Duygu Çelik (Eastern Mediterranean University, North Cyprus)
Alexander Chefranov (Eastern Mediterranean University & ITRC, North Cyprus)
Atilla Elçi (Süleyman Demirel University, Turkey)
Gengfa Fang (Macquarie University, Australia)
Ana Isabel González-tablas-ferreres (Universidad Carlos III de Madrid, Spain)
Johann Großschädl (University of Luxembourg, Luxembourg)
Song Han (Curtin University of Technology, Australia)
Qiong Huang (City University of Hong Kong, Hong Kong SAR)
Zhenjie Huang (Zhangzhou Normal University, PRC)
Sorin Huss (Technische Universität Darmstadt, Germany)
Shaoquan Jiang (University of Electronic Science and Technology of China, PRC)
Zhen Jiang (West Chester University of Pennsylvania, USA)
Hai Jin (Huazhong University of Science and Technology, PRC)
Salil Kanhere (University of New South Wales, Australia)
Vijay Laxmi (Malaviya National Institute of Technology, India)
Vincent Lee (Monash University, Australia)
Tiberiu S. Letia (Technical University of Cluj-Napoca, Romania)
Albert Levi (Sabancı University, Turkey)
Luigi Logrippo (Université du Québec en Outaouais, Canada)
Liangfu Lu (Tianjin University, PRC)
Ji Ma (Johannes-Kepler-University Linz, Austria)
Nele Mentens (Katholieke Universiteit Leuven, Belgium)
Surya Nepal (CSIRO, Australia)
Jose Antonio Onieva (University de Málaga, Spain)
Bülent Örencik (TUBITAK MAM, Turkey)
Mehmet A. Orgun (Macquarie University, Australia)
Valery Osipyan (Kuban State University, Russia)
Ekaterina Pakulova (Southern Federal University, Russia)
Josef Pieprzyk (Macquarie University, Australia)
Guangzhi Qu (Oakland University, USA)
Behnam Rahnama (European University of Lefke, North Cyprus)
Yonglin Ren (University of Ottawa, Canada)
Alfonso Rodríguez Rios (Universidad del Bio-Bio, Chile)
Yakov Romm (Taganrog State Pedagogical Institute, Russia)
Seref Sağroğlu (Gazi University, Turkey)
Program Committee
(continued):
Khaled Salah (Khalifa University, UAE)
Saji Sathiyan (CSIRO, Australia)
Erkay Savaş (Sabancı University, Turkey)
Ashutosh Saxena (Infosys Technologies, India)
Siraj Shaikh (Coventry University, UK)
Rajan Shankaran (Macquarie University, Australia)
Abdulhadi Shoufan (CASED, Germany)
Dave Singelee (Katholieke University Leuven, Belgium)
Jaipal Singh (Curtin University of Technology, Australia)
Chunming Tang (Guangzhou University, PRC)
Tuğkan Tuğlular (İzmir Institute of Technology, Turkey)
Ion Tutanescu (University of Pitesti, Romania)
Ahmet Ünveren (Eastern Mediterranean University, North Cyprus)
Huaxiong Wang (Nanyang Technological University, Singapore)
Dai Watanabe (Hitachi, Japan)
Edgar Weippl (Security Research, Austria)
Carlos Becker Westphall (Federal University of Santa Catarina, Brazil)
Brecht Wyseur (NagraVision S.A., Switzerland)
Ming Xu (National University of Defense Technology, PRC)
Yaping Zhang (Tianjin University, PRC)
John Zic (CSIRO, Australia)
SIN 2011 Sponsors & Supporters

Sponsors:

Organizers:

Host: