

Security of Information and Networks

Editors

Atilla Elçi

Aksaray University, Aksaray, Turkey

Alexander Chefranov

Eastern Mediterranean University, Gazimagusa, TRNC

Manoj Singh Gaur

Malaviya National Institute of Technology Jaipur, India

Mehmet A. Orgun

Macquarie University, Sydney, Australia

Oleg B. Makarevich

Southern Federal University, Taganrog, Rostov, Russia

Yasin Çelik

Aksaray University, Aksaray, Turkey

**Proceedings of the Sixth International Conference on
Security of Information and Networks (SIN 2013)
26-28 November 2013
Aksaray, Turkey**



The Association for Computing Machinery

2 Penn Plaza, Suite 701

New York, New York 10121-0701

Copyright © 2013 by the Association for Computing Machinery, Inc. (ACM). Permission to make digital or hard copies of portions of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyright for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permission to republish from: Publications Dept., ACM, Inc. Fax +1 (212) 869-0481 or <permissions@acm.org>.

For other copying of articles that carry a code at the bottom of the first or last page, copying is permitted provided that the per-copy fee indicated in the code is paid through the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923 (USA).

Notice to Past Authors of ACM-Published Articles

ACM intends to create a complete electronic archive of all articles and/or other material previously published by ACM. If you have written a work that has been previously published by ACM in any journal or conference proceedings prior to 1978, or any SIG Newsletter at any time, and you do NOT want this work to appear in the ACM Digital Library, please inform permissions@acm.org, stating the title of the work, the author(s), and where and when published.

ISBN: 978-1-4503-2498-4/13/11

Additional copies may be ordered prepaid from:

ACM Order Department

PO Box 30777

New York, NY 10087-0777, USA

Phone: 1-800-342-6626 (USA and Canada)

+1-212-626-0500 (Global)

Fax: +1-212-944-1318

E-mail: acmhelp@acm.org

Hours of Operation: 8:30 am – 4:30 pm ET

Foreword

We welcome you to *The Sixth International Conference on Security of Information and Networks (SIN 2013)*.

The SIN series of conferences aims to provide an international forum for presentation of research and applications of security in information and networks. SIN 2013 follows the successful conferences of SIN 2007 and SIN 2009 held in Gazimagusa, North Cyprus, SIN 2010 held in Rostov-on-Don, Taganrog, Russia, SIN 2011 held in Sydney, Australia, and SIN 2012 held in Jaipur, India. SIN 2013 was hosted by the Faculty of Engineering, Department of Electrical-Electronics Engineering, Aksaray University, Aksaray, Turkey. The next SIN Conference is scheduled to take place in the UK in 2014.

SIN 2013 was organized jointly by Aksaray University, Aksaray, Turkey; Malaviya National Institute of Technology, Jaipur, India; Macquarie University, Sydney, Australia; Southern Federal University, Rostov-on-Don, Taganrog, Russia; İstanbul Technical University, İstanbul, Turkey; and Ahiler Development Agency, Nevşehir, Turkey.

We thank all those involved in organizing SIN 2013; their input in bringing out a quality conference has been appreciated. First of all, we thank the authors for submitting their papers for consideration; in all there were 126 proposals coming from 34 countries. Thanks go to the program committee members for their hard work in reviewing those papers. We are greatly indebted to these fine researchers for delivering a keynote/invited talk during SIN'13: Goerges Ataya, Belgium; Ludmila Babenko, Russia; Bart Preneel, Belgium; Erkay Savaş, Turkey; Ali Aydın Selçuk, Turkey; Rudrapatna Shyamasundar, India; and Edgar Weippl, Austria. Special thanks are due to the chairs of the organization committee whose leadership made SIN 2013 possible: Program Chair Alex Chefranov, Tutorials Chair Behnam Rahnama, Workshops Chair Tuğkan Tuğlular, Posters Chair Md. Sadek Ferdous, Fast Abstracts Chair Alev Elçi, Industry Program Chair Christophe Feltus, Local Arrangements Chair Himmet Karadal, Publication Chair Yasin Çelik, Finance Chair Zeynep Duman, Registration Chair Hacı Özışık, e-Presence Chair Muhammet Saygın, Promotion Chair Yasin Çelik, Logo designs by Efe Cem Elçi, Conference poster design by Abdullah Singin and Muhammet Saygın, and volunteers from the Departments of Electrical-Electronics Engineering and Business Administration, Aksaray University, Aksaray, Turkey. 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.

We sincerely thank our sponsors for their contribution to the success of this conference: gold sponsor STM Defense Technologies Engineering and Trade, Inc., Turkey; silver sponsor IGI Global Disseminator of Knowledge, USA; and supporters World Scientific, Singapore, and Bilgi Güvenliği Derneği, Turkey. We are grateful to ACM Distinguished Speakers Program for sponsoring Rudrapatna Shyamasundar's SIN'13 visit for an invited talk.

We also wish to thank Microsoft Research for providing the Conference Management Toolkit (CMT) and for hosting the SIN 2013 submission site; and EasyChair for hosting the SIN'13 Abstracts submission site.

We are proud of our association with ACM and SIGSAC, consequently greatly indebted to Elisa Bertino, the Chairperson of SIGSAC at the time the Technical In-Cooperation Agreement was concluded for ACM/SIGSAC support of SIN'13. The proceedings of SIN'13 was published by ACM and uploaded to the ACM Digital Library for perpetual online access. We thank Adrienne Griscti, Diana Brantuas and Craig Rodkin of ACM for their excellent cooperation and support.

We welcome all the participants to enjoy the conference and also what Aksaray and her vicinity have to offer in nature, culture and history.

Atilla Elçi

*General Chair
Aksaray University,
Turkey*

Manoj S. Gaur

*General Co-Chair
Malaviya National
Institute of Tech., India*

Mehmet A. Orgun

*General Co-Chair
Macquarie Univ., Australia*

Oleg Makarevich

*General Co-Chair
Southern Federal
University, Russia*

Program Chairs' Welcome

It is our great pleasure to welcome you to *The Sixth International Conference on Security of Information and Networks (SIN 2013)* organized jointly by Department of Electrical & Electronics Engineering, Aksaray University, Aksaray, Turkey; Department of Computer Engineering, Malaviya National Institute of Technology Jaipur, India; The Centre for Advanced Computing - Algorithms and Cryptography (ACAC) & The Information and Networked Systems Security (INSS) & Intelligent Systems Group (ISG), Dept. of Computing, Macquarie University, Sydney, Australia; Department of Security of Information Technologies, South-Russian Regional Scientific-Educational Center for Information Security Problems, Southern Federal University, Taganrog, Rostov, Russia; Department of Electronics and Communication Engineering, Istanbul Technical University, Istanbul, Turkey; Ahiler Development Agency, Nevşehir, Turkey. Department of Electrical & Electronics Engineering, Aksaray University, Aksaray, Turkey, hosted the event.

The main theme of the SIN 2013 conference is security of information and networks. The theme includes the following topics: Access control and intrusion detection; Cyber physical systems; Autonomous and adaptive security; Security tools and development platforms; Computational intelligence techniques in security; Security ontology, models, protocols & policies; Computer network defense; Standards, guidelines and certification; Cryptographic techniques and key management; Security-aware software engineering; Industrial applications of security; Trust and privacy; Information assurance; Cyber Warfare (attacks and defenses); Next generation network architectures; Malware analysis; Network security and protocols; Security challenges in mobile/embedded systems.

In total, there were 109 papers, 9 fast abstracts and 8 posters submitted to SIN 2013. Each paper was reviewed by at least three reviewers. In all, 30 full papers (maximum length of 8 pages), 21 short papers (maximum length of 5 pages), 19 fast abstracts and 15 posters were accepted. A rigorous review process ensured the high quality of research articles. The acceptance ratio for regular papers was ~27%.

The conference hosted the following distinguished researchers who graciously agreed to present their keynote and invited speeches:

- Information Security and Risk Governance and Management Frameworks. An Overview of COBIT 5 by Georges Ataya
- Analysis of GOST 28147-89 Security: Methods and Algorithms by Ludmila Babenko
- The SHA-3 Competition: Lessons Learned by Bart Preneel
- Attacks on Implementation of Cryptographic Algorithms: Fault and Side-Channel Attacks by Erkay Savaş
- Trusting SSL in Practice by Ali Aydın Selçuk
- Security and Protection of SCADA: A Bigdata Algorithmic Approach by Rudrapatna Shyamasundar
- Social Engineering Attacks on the Knowledge Worker and the Digital Native by Edgar Weippl.

SIN 2013 Proceedings was published by the ACM and, along with the proceedings of SIN 2009-2012, it was placed on the ACM Digital Library for perpetual online access.

We extend our thanks to all the authors for submitting articles to the conference making it a competitive event, the reviewers for comments / suggestions that improved technical quality of camera-ready submissions, the presenters for useful research inputs and the participants. We also extend our gratitude and thanks to the session chairs and to the program committee members for their continued support, guidance and mentoring.

We hope that this conference gave an excellent opportunity to researchers from both academia and industry in exchanging ideas that would bring forth better security solutions in future and inspire budding researchers in the fields of information and network security and related areas.

Program Chairs

**Alexander
Chefranov**

*Eastern Mediterranean
University,
North Cyprus*

**Vijay
Laxmi**

*Malaviya National
Institute of Technology
Jaipur, India*

**Josef
Pieprzyk**

*Macquarie
University,
Australia*

**Lyudmila
Babenko**

*Southern Federal
University,
Russia*

**Siddika Berna
Örs Yalçın**


*İstanbul Technical
University,
Turkey*


Table of Contents


SIN 2013 Conference Organization


SIN 2013 Sponsors & Supporters


Keynote Talks


 **Information Security and Risk Governance and Management Frameworks. An Overview of COBIT 5**
Georges Ataya (*Solvay Brussels School of Economics and Management*)


 **Analysis of GOST 28147-89 Security: Methods and Algorithms**
Ludmila Babenko (*Southern Federal University*)

 **Attacks on implementation of Cryptographic Algorithms: Fault and Side-Channel Attacks**
Erkay Savaş (*Sabancı University*)


 **Trusting SSL in Practice**
Ali Aydın Selçuk (*Bilkent University*)

 **The SHA-3 Competition: Lessons Learned**
Bart Preneel (*KU Leuven ESAT/COSIC*)


 **Security and Protection of SCADA: A Bigdata Algorithmic Approach**
Rudrapatna Shyamasundar (*Tata Institute of Fundamental*)

 **Social Engineering Attacks on the Knowledge Worker and the Digital Native**
Edgar Weippl (*Security Research*)

Regular Papers


 **Conviction Model Insight for Incident Reaction Architecture Monitoring based on Automatic Sensors Alert Detection**
Christophe Feltus, Djamel Khadraoui (*CRP Henri Tudor*)

 **S-Box Construction from Non-Permutation Power Functions**
Herman Isa (*MIMOS Berhad*), Norziana Jamil (*Universiti Tenaga Nasional*), Muhammad Reza Z'aba (*MIMOS Berhad*)

 **Obligations to Enforce Prohibitions: On the Adequacy of Security Policies**
Wolter Pieters (*TU Delft/University of Twente*), Julian Padget (*University of Bath*), Francien Dechesne, Virginia Dignum, Huib Aldewereld (*Delft University of Technology*)

 **Authenticated Key Agreement in Wireless Networks with Automated Key Management**
Naïm Qachri (*Université Libre de Bruxelles*), Frédéric Lafitte, Olivier Markowitch

 **On Authentication Factors: “What You Can” and “How You Do It”**
Jérôme Dossogne (*Université Libre de Bruxelles*), Frédéric Lafitte





 **Secure and Practical Threshold RSA**
Jérôme Dossogne (*Université Libre de Bruxelles*), Frédéric Lafitte, Dirk Van Heule (*Royal Military Academy*)

-  Counterfeiting Attacks on Block-Wise Dependent Fragile Watermarking Schemes
 Hussain Nyeem, Wageeh Boles, Colin Boyd (*Queensland University of Technology*)
-  An Authentication Framework for Peer-to-Peer Cloud
 Geong Sen Poh, Mohd Amril Nurman Mohd Nazir (*MIMOS Berhad*), Syh-Yuan Tan (*Multimedia University*), Maryam Safiyah Shamsudin, Bok-Min Goi (*Universiti Tunku Abdul Rahman*), Raphael Chung-Wei Phan (*Multimedia University*)
-  Verification of OSPF Vulnerabilities by Colored Petri Net
 Saeid Tizpaz Niari, Amir Hossein Jahangir (*Sharif University of Technology*)
-  SAT Based Analysis of LTE Stream Cipher ZUC
 Frédéric Lafitte, Olivier Markowitch, Dirk Van Heule (*Royal Military Academy*)
-  Generalized Approach to Modeling User Activity Graphs for Network Security and Public Safety Monitoring
 Alexey Tselykh, Nikolay Sergeev, Alexander Tselykh (*Southern Federal University*)
-  Efficient and Robust Data Aggregation Using Untrusted Infrastructure
 Marek Klonowski, Michal Koza, Mirosław Kutylowski (*Wrocław University of Technology*)
-  Biometric Verification Using Brain Waves toward On-Demand User Management Systems - Performance Differences between Divided Regions in Alpha-Beta Wave Band
 Isao Nakanishi, Hironao Fukuda, Shigang Li (*Tottori University*)
-  Continuous Security Evaluation and Auditing of Remote Platforms by Combining Trusted Computing and Security Automation Techniques
 Mudassar Aslam, Christian Gehrmann (*SICS Swedish ICT*), Mats Björkman (*Mälardalen University*)
-  ProClick: A Framework for Testing Clickjacking Attacks in Web Applications
 Hossain Shahriar, Vamshee Devendran, Hisham Haddad (*Kennesaw State University*)
-  AndroSimilar: Robust Statistical Feature Signature for Android Malware Detection
 Parvez Faruki, Vijay Ganmoor, Vijay Laxmi, Manoj Gaur (*Malaviya National Institute of Technology*)
-  Robust Periocular Recognition by Fusing Local to Holistic Sparse Representations
 Hugo Proença, Juan Moreno (*University of Beira Interior*), Surya Prasath (*University of Missouri-Columbia*)
-  Cryptanalysis of RC4(n,m) Stream Cipher
 Mohammad Ali Orumiehchiha, Josef Pieprzyk (*Macquarie University*), Elham Shakour (*Amirkabir University*), Ron Steinfeld (*Monash University*)
-  Blinded Additively Homomorphic Encryption Schemes for Self-Tallying Voting
 Jérôme Dossogne (*Université Libre de Bruxelles*), Frédéric Lafitte
-  Analysing Attribute Aggregation Models in Federated Identity Management
 Md Sadek Ferdous, Ron Poet (*University of Glasgow*)
-  Impact Analysis of JellyFish Attack on TCP-based Mobile Ad-hoc Networks
 Vijay Laxmi, Chhagan Doot, Manoj Gaur, Parvez Faruki, Deepanshu Mehta (*Malaviya National Institute of Technology*)
-  A Flexible Framework for Detecting IPv6 Vulnerabilities
 Hosnieh Rafiee, Christoph Mueller, Lukas Niemeier, Jannik Streek, Christoph Sterz (*Hasso Plattner Institute*), Christoph Meinel
-  Exploring Attack Vectors Facilitated by Miniaturized Computers
 Casey Mortensen, Ryan Winkelmaier, Jun Zheng (*New Mexico Tech*)
-  Using Transition Systems to Model and Verify the Implementation of Security Protocol
 Fu Yulong (*University of Pau*), Kone Ousmane (*Academy of Bordeaux*)

- 🔒 Privacy and Security in IPv6 Networks: Challenges and Possible Solutions
Hosnieh Rafiee (*Hasso Plattner Institute*), Christoph Meinel
- 🔒 Designing Flexible Access Control models for the Cloud
Salim KHAMADJA (*Ecole Militaire Polytechnique*), Kamel Adi, Luigi Logrippo (*Université du Québec en Outaouais*)
- 🔒 MAIL: Malware Analysis Intermediate Language - A Step Towards Automating and Optimizing
Malware Detection
Shahid Alam, R. Nigel Horspool, Issa Traore (*University of Victoria*)
- 🔒 Anonymity and Privacy in Multicast Mobile Ad Hoc Networks
Somayeh Taheri (*Georg-August University*), Salke Hartung, Dieter Hogrefe



Short Papers

- 🔒 Metamodel for Reputation based Agents System – Case Study for Electrical Distribution SCADA
Design
Guy Guemkam (*LIP6*), Jonathna Blangenois (*University of Namur*), Christophe Feltus, Djamel Khadraoui (*CRP Henri Tudor*)
- 🔒 Countering AES Static S-Box Attack
Behnam Rahnama (*Okan University*), Yunus Kiran, Raz Dara (*European University of Lefke*)
- 🔒 Social Access Control Language (SocACL)
Edward Caprin, Yan Zhang (*University of Western Sydney*), Khaled Khan (*Qatar University*)
- 🔒 A Possibilistic Approach to Intrusion Detection under Imperfect Logging Protocol
Romdhane Ben Younes, Guy Tremblay (*UQAM*)
- 🔒 Hand Shape Recognition Using Hu and Legendre Moments
Aldjia Boucetta (*University of Batna*), K. E. Melkem (*University of Biskra*)
- 🔒 An HBAC-based Approximation for IBAC Programs
Pablo Lamilla Alvarez, Yoshiaki Takata (*Kochi University of Technology*)
- 🔒 An Access Control Framework for Hybrid Policies
Salim Khamadja (*Ecole Militaire Polytechnique*), Kamel Adi, Luigi Logrippo (*Université du Québec en Outaouais*)
- 🔒 An Empirical Study of Three Access Control Systems
Lihui Hu (*Michigan Technological University*), Jean Mayo, Charles Wallace
- 🔒 Joux Multicollisions Attack in Sponge Construction
Mohammad AlAhmad (*IUUM*), Imad Alshaikhli, Mridul Nandi
- 🔒 Digital Camera Identification System
Dmitry Rublev, Vladimir Fedorov, Oleg Makarevich (*Southern Federal University*)
- 🔒 Complexity Measurement of a Password for Keystroke Dynamics: Preliminary Study
Soumik Mondal, Patrick Bours (*GUC*), Syed Idrus Syed Zulkarnain (*ENSICAEN/ University of Caen Lower-Normandy*)
- 🔒 An Improved Fault-Tolerant Conference-Key Protocol with Forward Secrecy
Orhan Ermis (*Boğaziçi University*), Şerif Bahtiyar (*Provus Information Technologies*), Emin Anarim, Mehmet Caglayan
(*Boğaziçi University*)
- 🔒 Nature Inspired Heuristics for Attack of Simplified DES algorithm
Mekhaznia Tahar (*University of Tebessa*)
- 🔒 The Darker Side of Firefox Extension
Anil Saini, Manoj Gaur, Vijay Laxmi (*Malaviya National Institute of Technology*)

- 
 A Review on Cloud Security
 Duygu Sinanc (*Gazi University*), Seref Sagiroglu (*Purdue University*)
- 
 CGA integration into IPsec/IKEv2 Authentication
 Ahmad Alsadeh (*HPI*), Christoph Meinel
- 
 Secure True Random Number Generator in WLAN/LAN
 Alexander Chefranov, Seyed Masoud Alavi Abhari, Hooman Alavizadeh, Maryam Farajzadeh (*Eastern Mediterranean University*)
- 
 Public Key Infrastructure for UAE: A Case Study
 Eman Hableel, Young-ji Byon, Joon Sang Baek (*Khalifa University*)

Extended Abstracts



- 
 Information Protection Systems based on Universal Knapsack Problem
 Valeriy Osipyany (*Kuban State University*)
- 
 Expert Key Selection Impact on the MANETs' Performance Using Probabilistic Key Management Algorithm
 Mohammed Gharib, Mohsen Minaei, Morteza Golkari, Ali Movaghar (*Sharif University of Technology*)
- 
 Influence of S-Boxes to the Resistance of GOST Algorithm against Linear Cryptanalysis
 Evgeniya Ishchukova, Lyudmila Babenko (*Southern Federal University*)
- 
 Security Policy Verification in Grid Systems
 Artem Konoplev, Maxim Kalinin (*SPbSTU*)
- 
 Visual Steganalysis of LSB-encoded Audio Data based on Frequency Domain Characteristics
 Yuksel Arslan (*Mikes A.Ş.*), Yıldray Yalman (*Turgut Özal University*)
- 
 Authorized! Access Denied, Unauthorized! Access Granted
 Abdulaziz Almeahmadi, Khalil El-Khatib (*University of Ontario Institute of Technology*)
- 
 A Finite Transition Model for Security Protocol Verification
 Fu Yulong (*University of Pau*), Kone Ousmane (*Academy of Bordeaux*)
- 
 Development of a Secure Cluster Wireless Sensor Network Model
 Evgeny ABRAMOV, Elena Basan, Oleg Makarevich (*Southern Federal University*)
- 
 A Key Management Scheme for Content Centric Networks
 Sarmadullah Khan (*CECOS University*), Rafiullah Khan
- 
 About Responsibilities Distribution for Information Security
 Anthon Pyatkov, Vyacheslav Zolotarev (*Siberian State Aerospace University*)
- 
 A Clique-Based Method for Mining Fuzzy Graph Patterns in Anti-Money Laundering Systems
 Alexey Tselykh, Leonid Bershtein (*Southern Federal University*)
- 
 A Novel Approach for Dynamic Authorisation Planning in Constrained Workflow Systems
 Meriam Jemel, Nadia Ben Azzouna, Khaled Ghedira (*University of Tunisia*)
- 
 Features Extraction of Fingerprint by using Firefly Algorithm
 Omar Younis (*Univercities*)
- 
 Performance Analysis of the Developed Mandatory Access Control System in the DBMS
 Lyudmila Babenko, Alexandr Basan, Oleg Makarevich (*Southern Federal University*)


-  A Protocol for Simultaneous use of Confidentiality and Integrity in Large-scale Storage Systems
 Zahra Khani (OSSL), Reza Azmi
-  Using Quadcopter as a Pentest Tool
 Maxim Kobilev, Evgeny Abramov, Oleg Makarevich (Southern Federal University)

Posters


-  EndNote vs Zotero in Searching Library Catalog via Z39.50 of Academic Libraries in Thailand
 Aurathai Wareesa-ard (Srinakharinwirot University)
-  Improved Face Recognition At A Distance Using Light Field Camera & Super Resolution Schemes
 R. Raghavendra, Kiran Bylappa Raja, Bian Yang, Christoph Busch (Gjøvik University College)
-  Building of Mathematical Model of Flow Data Processing System based on Given Selection of Elements of the Set
 Zhuck Arseniy, Valeriy Osipyany (Kuban State University)
-  D0M-WLAN: A Traffic Analysis based Approach for Detecting Malicious Activities on Wireless Networks
 Rohan Nanda, P. Venkata Krishna (VIT University)
-  Securing the Virtual Machine Images in Cloud Computing
 Muhammad Kazim, Rahat Masood, Muhammad Awais Shibli (NUST SEecs)
-  Implementing Real-Time Transactional Security Property using Timed Edit Automata
 N. Rajamanickam, R. Nadarajan (PSG College of Technology)
-  Development the Method of Detection the Malicious Pages Interconnection in the Internet
 Ksenia Tsyganok, Evgeny Tumoyan, Lyudmila Babenko (Southern Federal University)
-  A Novel Threshold-based Scan Detection Method Using Genetic Algorithm
 Morteza Barati, Karim Faez, Zahra Hakimi
-  Towards A Dynamic Authorisation Planning Satisfying Intra-instance and Inter-Instance Constraints
 Meriam Jemel, Nadia Ben Azzouna, Khaled Ghedira (University of Tunisia)
-  On Designing Automatic Reaction Strategy for Critical Infrastructure SCADA System
 Christophe Feltus, Djamel Khadraoui (CRP Henri Tudor)
-  The Method of the Information Security Risk Assessment in Cloud Computing Systems
 Oleg Makarevich (Southern Federal University), Irina Mashkina, Alina Sentsova (Ufa State Aviation University)
-  Preventing Malicious Data Harvesting from Deallocated Memory Areas
 Maxim Anikeev (Southern Federal University), Felix Freiling

Tutorials

-  Linking Business Goals to Information Security Plans and Activities
 Georges Ataya (Solvay Brussels School of Economics and Management)
-  Addressing Security Challenges in WiMAX Environment
 Arif Sari (European University of Lefke), Behnam Rahnama (Okan University)


 **Improbable Differential Cryptanalysis**
Cihangir Tezcan (*Middle East Technical University*)


 **Insecurities within the Browsers: Issues and Challenges**
M.S. Gaur (*MNIT Jaipur*), Vijay Laxmi (*MNIT Jaipur*), Dhiren Patel (*NIT Surat*), Anil Saini (*MNIT Jaipur*)

 **Security Vulnerabilities and Mitigation Techniques of Web Applications**
Hossain Shahriar (*Kennesaw State University*)

Panels

 **Security through human-factors and biometrics**
Tugkan Tuglular (*Softin Technology*), Sambit Bakshi (*NIT Rourkela*)

 **Multidisciplinary Perspectives in Cryptology**
Sattar B. Sadkhan, Nidaa A. Abbas (*University of Babylon*)

 **Industry Program Panel**
Christophe Feltus (*CRP Henri Tudor*)

Author Index

SIN 2013 Conference Organization

Honorary Chairs: Mustafa ACAR (*Rector of Aksaray University, Turkey*)
Prof. I.K.BHAT (*Director, MNIT Jaipur, India*)
Marina BOROVSKEYA (*Rector of Southern Federal University, Russia*)
Kadir YILDIZ (*Dean of Engineering, Aksaray University, Turkey*)

Advisory Committee: Bart PRENEEL (*Katholieke Universiteit Leuven, Belgium*)
Bülent ÖRENCİK (*Beykent University, Turkey*)
Çetin Kaya KOÇ (*University of California Santa Barbara, USA*)
Edward DAWSON (*Queensland University of Technology, Australia*)
Elisa BERTINO (*Purdue University, USA*)
Gene SPAFFORD (*Purdue University CERIAS, USA*)
N. BALAKRISHNAN (*IISc Bangalore, India*)
Willy SUSILO (*University of Wollongong, Australia*)

Program Committee: Ahmet ÜNVEREN (*Eastern Mediterranean University, North Cyprus*)
Albert LEVİ (*Sabancı University, Turkey*)
Alexander CHEFRANOV (*Eastern Mediterranean University, North Cyprus*)
Alfonso RODRIGUEZ (*Universidad del Bio-Bio, Chile*)
Ali Aydın SELÇUK (*Bilkent University, Turkey*)
Alwyn Pais (*NITK Surathkal, India*)
Ana Isabel FERRERES (*Universidad Carlos III de Madrid, Spain*)
Anil SAINI (*MNIT Jaipur, India*)
Anton CHUVAKIN (*Security Warrior Consulting, Russia*)
Arif SARI (*European University of Lefke, North Cyprus*)
Ashutosh SAXENA (*Infosys Technologies, India*)
Atilla ELÇİ (*Aksaray University, Turkey*)
Attila ÖZGİT (*Middle East Technical University, Turkey*)
Babak SOKOUTI (*Tabriz University of Medical Sciences, Iran*)
Basant AGARWAL (*MNIT Jaipur, India*)
Behnam RAHNAMA (*European Univ. of Lefke, North Cyprus*)
Berna ÖRS YALÇIN (*Istanbul Technical University, Turkey*)
Bernardi PRANGGONO (*Glasgow Caledonian University, UK*)
Bruhadeshwar BEZAWADA (*IIT Hyderabad, India*)
Bok-Min GOI (*Universiti Tunku Abdul Rahman, Malaysia*)
Bülent ÖRENCİK (*Beykent University, Turkey*)
Cecelia BROWN (*University of Baltimore, USA*)
Christophe FELTUS (*CRP Henri Tudor, Luxembourg*)
Cihangir TEZCAN (*Middle East Technical University, Turkey*)
Dai WATANABE (*Hitachi, Japan*)
Dhiren PATEL (*NIT Surat, India*)
Dmitry RUBLEV (*TTI SFU, Russia*)
Dushyant SINGH (*MNIT Jaipur, India*)
Duygu ÇELİK (*İstanbul Aydın University, Turkey*)
Edgar WEIPPL (*Security Research, Austria*)
Ekaterina MARO (*Southern Federal University, Russia*)
Ekaterina PAKULOVA (*Southern Federal University, Russia*)

Emin ANARIM (*Boğazici University, Turkey*)
Erkay SAVAŞ (*Sabancı University, Turkey*)
Evgeniya ISHCHUKOVA (*Southern Federal University, Russia*)
Evgeny ABRAMOV (*Southern Federal University, Russia*)
Fedor NOVIKOV (*St.Petersburg Inst. for Informatics and Autom., Russia*)
Georges ATAYA (*Solvay Brussels School of Economics & Mngment, Belgium*)
Gerardo PELOSI (*Politecnico di Milano, Italy*)
Guangzhi QU (*Oakland University, USA*)
Hossain SHAHRIAR (*Kennesaw State University, USA*)
Huaxiong WANG (*Nanyang Technological University, Singapore*)
Ion TUTANESCU (*University of Pitesti, Romania*)
Jiankun HU (*UNSW Canberra at ADFA, Australia*)
John ZIC (*CSIRO, Australia*)
Joon Sang BAEK (*Khalifa University of Science, Tech. & Research, UAE*)
Jose ONIEVA (*Universidad de Malaga, Spain*)
Josef PIEPRZYK (*Macquarie University, Australia*)
Jyoti GROVER (*MNIT Jaipur, India*)
Khaled SALAH (*KFUPM, Saudi Arabia*)
Khalil ABUSBA (*University of Ontario Inst. of Tech. (UOIT), Canada*)
Kubilay ATASU (*IBM Zurich Research Lab, Switzerland*)
Liangfu LU (*Tianjin University, China*)
Ludmila FEDORCHENKO (*St.Petersburg Inst. for Inform. & Autom., Russia*)
Luigi LOGRIPPO (*Université du Quebec en Outaouais, Canada*)
Lyudmila BABENKO (*Southern Federal University, Russia*)
Manoj BOHRA (*MNIT Jaipur, India*)
Manoj GAUR (*MNIT Jaipur, India*)
Maryna KROTOFIL (*Tech. Univ. Harburg, Germany*)
Maxim ANIKEEV (*Southern Federal University, Russia*)
Md Sadek FERDOUS (*University of Glasgow, UK*)
Mehmet ORGUN (*Macquarie University, Australia*)
Mehmet Ufuk ÇAĞLAYAN (*Bogazici University, Turkey*)
Mert ÖZARAR (*Middle East Technical University, Turkey*)
Michael HITCHENS (*Macquarie University, Australia*)
Mushtaq AHMED (*MNIT Jaipur, India*)
Namita MITTAL (*MNIT Jaipur, India*)
Nele MENTENS (*Katholieke Universiteit Leuven, Belgium*)
Oleg MAKAREVICH (*Southern Federal University, Russia*)
Parvez FARUKI (*MNIT Jaipur, India*)
Piyi YANG (*University of Shanghai for Science and Technology, China*)
Preety SINGH (*LNMIIT, Jaipur, India*)
Qiong HUANG (*City University of Hong Kong, Hong Kong SAR*)
Rajan SHANKARAN (*Macquarie University, Australia*)
Rajbir KAUR (*LNMIIT, Jaipur, India*)
Ramesh Babu BATTULA (*K L University, India*)
Rimpy BISHNOI (*MNIT Jaipur, India*)
Sambit BAKSHI (*National Institute of Technology Rourkela, India*)
Sattar ALMALIKY (*University of Babylon, Iraq*)
Seyed SHAHRESTANI (*University of Western Sydney, Australia*)
Shaoquan JIANG (*University of Electronic Science and Tech., China*)
Shashikala TAPASWI (*IITM, India*)
Smita NAVAL (*MNIT Jaipur, India*)

Sonal YADAV (*MNIT Jaipur, India*)
Surya NEPAL (*CSIRO, Australia*)
Tang QIANG (*University of Luxembourg, Luxembourg*)
Tiberiu S. LETIA (*Technology University of Cluj-Napoca, Romania*)
Tuğkan TUĞLULAR (*Izmir Institute of Technology, Turkey*)
Valeriy OSIPYAN (*Kuban State University, Russia*)
Vijay LAXMI (*MNIT Jaipur, India*)
Vinod P. (*MNIT Jaipur, India*)
Vladimir VASILYEV (*Ural State Aviation Tech. University, Russia*)
Wen-Jung HSIN (*Park University, USA*)
Zeki BAYRAM (*Eastern Mediterranean University, North Cyprus*)
Zhen JIANG (*West Chester University of Pennsylvania, USA*)

Additional reviewers: Murat AK (*Bilkent University, Turkey*)
Wun-She YAP (*Universiti Tunku Abdul Rahman, Malaysia*)
Nickolay MOLDOVYAN (*SPIIRAS, Russia*)
Atiskov ALEXEY (*St.Petersburg Inst. for Informatics and Autom., Russia*)

Organization Committee

General Chairs: Atilla Elçi (*Aksaray University, Turkey*)
Manoj Singh Gaur (*Malaviya National Institute of Technology Jaipur, India*)
Mehmet A. Orgun (*Macquarie University, Australia*)
Oleg Makarevich (*Southern Federal University, Russia*)

Program Chairs: Alexander Chefranov (*Eastern Mediterranean University, North Cyprus*)
Vijay Laxmi (*Malaviya National Institute of Technology, India*)
Josef Pieprzyk (*Macquarie University, Australia*)
Ludmila Babenko (*Southern Federal University, Russia*)
Sıddıka Berna Örs Yalçın (*İstanbul Technical University, Turkey*)

Tutorials Chairs: Behnam Rahnama (*European University of Lefke, North Cyprus*)
Olga Peskova (*Southern Federal University, Russia*)
B.Bazewada (*IIT, Hyderabad, India*)
Dr. Virendra Singh (*IIT, Bombay, India*)

Workshops Chairs: Tuğkan Tuğlular (*İzmir Institute of Technology, Turkey*)
Evgeny Tumoyan (*Southern Federal University, Russia*)
Parvez Faruki (*Malaviya National Institute of Technology, India*)

Posters Chair: Md. Sadek Ferdous (*University of Glasgow, UK*)

Fast Abstracts Chair: Alev Elçi (*Aksaray University, Turkey*)

Industry Program Chair: Christophe Feltus (*CRP Henri Tudor, Luxembourg*)

Local Arrangements Chairs: Himmet Karadal (*Aksaray University, Turkey*)
Mehmet Reşit Tolun (*Aksaray University, Turkey*)
Celal Karaca (*Aksaray University, Turkey*)

Publication Chairs: Yasin Çelik (*Aksaray University, Turkey*)

Alexey Nekrasov (*Southern Federal University, Russia*)
Sonal Yadav (*Malaviya National Institute of Technology, India*)

Finance Chair: Zeynep Duman (*Aksaray University, Turkey*)

Registration Chairs: Hacı Özışık (*Aksaray University, Turkey*)
Ekaterina Pakulova (*Southern Federal University, Russia*)
Smita Naval (*Malaviya National Institute of Technology, India*)

E-presence Chair: Muhammet Saygın (*Aksaray University, Turkey*)

Promotion Chairs: Yasin Çelik (*Aksaray University, Turkey*)
Muhammet Saygın (*Aksaray University, Turkey*)
Maxim Anikeev (*Southern Federal University, Russia*)
Vinod P. (*SSET, Cochin, India*)

**Logo, Cover &
Certificates Designs:** Efe Cem Elçi (*Turkish Airlines*)

Conference Poster Design: Abdullah Singin (*Aksaray University, Turkey*)
Muhammet Saygın (*Aksaray University, Turkey*)

Volunteers Team: Celal Karaca (*Aksaray University, Turkey*)
Students of Department of Electrical-Electronics Engineering, Aksaray
University