INTRUST 2011 – Accepted Papers

- Michał Koza, Przemyslaw Kubiak, Lukasz Krzywiecki and Miroslaw Kutylowski. Restricted Identification Scheme and Diffie-Hellman Linking Problem
- Gina Kounga and Liqun Chen. Enforcing Sticky Policies with TPM and Virtualization Technologies
- Jan-Erik Ekberg and Sandeep Tamrakar. Mass transit ticketing with NFC mobile phones
- Dong Hao, Avishek Adhikari and Kouichi Sakurai. Mixed-Strategy Game Based Trust Management for Clustered Wireless Sensor Networks
- Wei Li, Dawu Gu, Zhiqiang Liu, Ya Liu and Xiaohu Huang. Fault Detection of the MacGuffin Cipher against Differential Fault Attack
- Chunhua Chen, Chris J. Mitchell and Shaohua Tang. Building general purpose security services on trusted computing
- Shin'Ichiro Matsuo, Daisuke Moriyama and Moti Yung. Multifactor Authenticated Key Renewal
- Yasaman Rabiee Kenari and Reza Azmi. Reputation Based Trust Modeling Using Dynamic Neuro-Fuzzy Model in P2P Networks
- Patrick Koeberl, Jiangtao Li, Roel Maes, Anand Rajan, Claire Vishik and Marcin Wojcik. Evaluation of a PUF Device Authentication Scheme on a Discrete 0.13um SRAM
- Ernie Brickell, Liqun Chen and Jiangtao Li. A (Corrected) DAA Scheme Using Batch Proof and Verification
- Yiyuan Luo, Xuejia Lai and Zheng Gong. Indifferentiability of Domain Extension Modes for Hash Functions
- Johannes Winter, Paul Wiegele, Martin Pirker and Ronald Tögl. A flexible software development and emulation framework for ARM TrustZone
- Danilo Gligoroski, Rune Steinsmo Oedegaard, Rune Erlend Jensen, Ludovic Perret, Jean-Charles Faugere, Svein Johan Knapskog and Smile Markovski. MQQ-SIG, An Ultra-fast and Provably CMA Resistant Digital Signature Scheme
- David Derler, Klaus Potzmader, Johannes Winter and Kurt Dietrich. Anonymous Ticketing for NFC-enabled Mobile Phones
- Christopher Jämthagen, Martin Hell and Ben Smeets. A technique for remote detection of certain virtual machine monitors
- Kimmo Halunen. Multicollisions and graph-based hash functions
- Qinggang Yue, Feng Liu and Rui Xue. Some Improvements to the Cost-Based Framework for Analyzing Denial of Service Attacks
- Pengqi Cheng, Yan Gu, Zihong Lv, Jianfei Wang, Wenlei Zhu, Zhen Chen and Jiwei Huang. A Performance Analysis of Identity-Based Encryption Schemes
- Thouraya Bouabana-Tebibel. A trust protocol to secure ad hoc networks
- Zijian Zhang, Hongyuan Wang and Cong Guo. Computationally Sound Symbolic Analysis of EAP-TNC Protocol
- Kun Peng. A Simple and Efficient Exclusion Proof Scheme
- Yu Qin. DAA Protocol Analysis and Verification