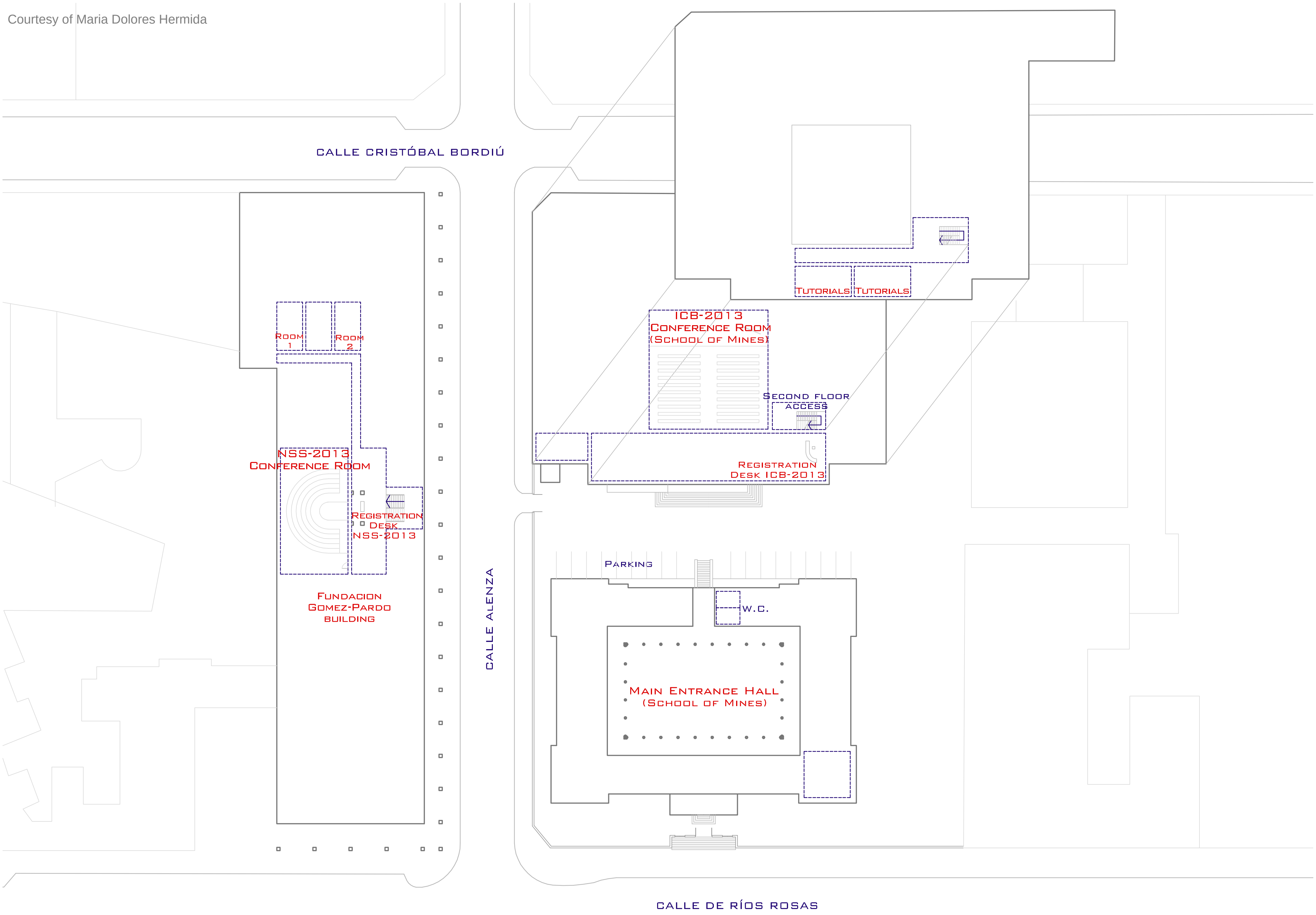
Courtesy of Maria Dolores Hermida

NSS 2013 All-in-One Program (41 Full Papers*25mins + 30 Short Papers* 20mins)

2013-06-03 (Day 1)	**1 keynote + 25 Full Papers +2 Short Papers:** “Fundacion Gomez-Pardo Building” (1 calle Alenza)		
8:00:-8:40	Registration and Conference Kit Collection		
8:40-9:00	Opening (Ravi Sandhu and Javier Ortega-Garcia): Conference Room		
9:00-10:00	Keynote: *Biometrics: The Future Beckons* by Prof. Arun Ross (Chair: Ravi Sandhu): Conference Room		
10:00-10:30	Coffee Break: Main Entrance Hall of the School of Mines building (21 calle Rios Rosas)		
	Conference Room (4F+1S)	**ROOM 2 (4F+1S)**	
10:30-12:30	S1: Malware and Intrusions	S7: Security Protocols and Practice	
12:30-13:45	Lunch @ Main Entrance Hall of the School of Mines building (21 calle Rios Rosas)		
	Conference Room (8F)	**ROOM2 (9F)**	
13:50-15:30	S2: Applications Security	S8: Applications Security	
15:30-16:00	Coffee Break: Main Entrance Hall of the School of Mines building (21 calle Rios Rosas)		
16:00-18:05	S3: Security Algorithms and Systems	S9: Modeling and Evaluation	
20:30	Banquet Dinner: VP Jardin Metropolitano Hotel (12 Avenida Reina Victoria)		
2013-06-04 (Day 2)	**1 keynote + 16 Full Papers + 28 Short Papers:** “Fundacion Gomez-Pardo Building” (1 calle Alenza)		
8:00-9:00	Registration and Conference Kit Collection		
9:00-10:00	Keynote: Authentication, Privacy and Ownership Transfer in Mobile RFID Systems by Prof. Wanlei Zhou (Chair: Jiankun Hu): Conference Room		
10:00-10:30	Coffee Break: Main Entrance Hall of the School of Mines building (21 calle Rios Rosas)		
	Conference Room (4F+1S)	**ROOM 2 (4F+1S)**	
10:30-12:30	S4: Cryptographic Algorithms I	S10: Privacy	
12:30-13:45	Lunch @ Main Entrance Hall of the School of Mines building (21 calle Rios Rosas)		
	Conference Room (4F + 7S)	**ROOM 2 (4F+7S)**	**ROOM1 (12 S)**
13:50-15:30	S5: Cryptographic Algorithms II	S11: Key Agreement and Distribution	S13: Industrial Track I
15:30-16:00	Coffee Break @ Main Entrance Hall of the School of Mines building (21 calle Rios Rosas)		
16:00-18:20	S6: Shot Papers I	S12: Shot Papers II	S14: Industrial Track II

NSS 2013 Program @ Conference Room, Fundacion Gomez-Pardo Building (1 calle Alenza)

2013-06-03 (Day 1)	
S1: Malware and Intrusions (Chair: José M. Fernandez)	
10:30-10:55	MADS: Malicious Android Applications Detection through String Analysis *Borja Sanz, Igor Santos, Javier Nieves, Carlos Laorden, Iñigo Alonso-González and Pablo García Bringas*
10:55-11:20	X-TIER: Kernel Module Injection *Sebastian Vogl, Fatih Kilic, Christian Schneider and Claudia Eckert*
11:20-11:45	Leveraging String Kernels for Malware Detection *Jonas Pfoh, Christian Schneider and Claudia Eckert*
11:45-12:10	Insiders Trapped in the Mirror Reveal Themselves in Social Media *Miltiadis Kandias, Konstantina Galbogini, Lilian Mitrou and Dimitris Gritzalis*
12:10-12:30	Combing Dynamic Passive Analysis and Active Fingerprinting for Effective Bot Malware Detection in Virtualized Environments (short paper) *Shun-Wen Hsiao, Yi-Ning Chen, Yeali Sun and Meng Chang Chen*
Lunch 12:30-13:45: Main Entrance Hall of the School of Mines building (21 calle Rios Rosas)	
S2: Applications Security (Chair: Wanlei Zhou)	
13:50-14:15	On Business Logic Vulnerabilities Hunting: The APP_LogGIC Framework *George Stergiopoulos, Bill Tsoumas and Dimitris Gritzalis*
14:15-14:40	Using the Smart Card Web Server in Secure Branchless Banking *Sheila Cobourne, Keith Mayes and Konstantinos Markantonakis*
14:40-15:05	Liability for data breaches: a proposal for a revenue-based sanctioning approach *Maurizio Naldi, Marta Flamini and Giuseppe D'Acquisto*
15:05-15:30	Efficient and Private Three-Party Publish/Subscribe *Giovanni Di Crescenzo, Jim Burns, Brian Coan, John Schultz, Jonathan Stanton, Simon Tsang and Rebecca N. Wright*
Coffee Break: 15:30-16:00: Main Entrance Hall of the School of Mines building (21 calle Rios Rosas)	
S3: Security Algorithms and Systems (Chair: Qiang Tang)	
16:00-16:25	Marlin: A fine grained randomization approach to defend against ROP attacks *Aditi Gupta, Sam Kerr, Michael Kirkpatrick and Elisa Bertino*

16:25-16:50	Mobile Trusted Agent (MTA): Build user-based trust for general-purpose computer platform *Wei Feng, Yu Qin, Dengguo Feng, Ge Wei, Lihui Xue and Dexian Chang*
16:50-17:15	Anomaly Detection for Ephemeral Cloud IaaS Virtual Machines *Suaad Alarifi and Stephen Wolthusen*
17:15-17:40	JShadObf: A JavaScript Obfuscator based on Multi-objective Optimization Algorithms *Benoit Bertholon, Sebastien Varrette and Pascal Bouvry*
20:30 Banquet Dinner: VP Jardin Metropolitano Hotel (12 Avenida Reina Victoria)	
2013-06-04 (Day 2)	
S4: Cryptographic Algorithms I (Jiankun Hu)	
10:30-10:55	Forward Secure Certificateless Proxy Signature Scheme *Jiguo Li, Yanqiong Li and Yichen Zhang*
10:55-11:20	Leakage-Resilient Zero-Knowledge Proofs of Knowledge for NP *Hongda Li, Qihua Niu and Bei Liang*
11:20-11:45	On the Security of an Efficient Attribute-Based Signature *Yan Zhang, Dengguo Feng and Zhenfeng Zhang*
11:45-12:10	Factoring RSA Modulus with Known Bits from Both p and q: A Lattice Method *Yao Lu, Rui Zhang and Dongdai Lin*
12:10-12:30	Enhancing Passive Side-Channel Attack Resilience through Schedulability Analysis of Data-dependency Graphs *Giovanni Agosta, Alessandro Barenghi, Gerardo Pelosi and Michele Scandale*
Lunch: 12:30-13:45: Main Entrance Hall of the School of Mines building (21 calle Rios Rosas)	
S5: Cryptographic Algorithms II (Qiang Tang)	
13:50-14:15	Performance Prediction Model for Block Ciphers on GPU Architectures *Naoki Nishikawa, Keisuke Iwai, Hidema Tanaka and Takakazu Kurokawa*
14:15-14:40	Threshold-Oriented Optimistic Fair Exchange *Yang Wang, Man Ho Au, Joseph Liu, Tsz Hon Yuen and Willy Susilo*
14:40-15:05	Secure Storage and Fuzzy Query over Encrypted Databases *Zheli Liu, Haoyu Ma, Jin Li, Chunfu Jia, Jingwei Li and Ke Yuan*
15:05-15:30	A Highly Efficient RFID Distance Bounding Protocol Without Real-time PRF Evaluation *Yunhui Zhuang, Anjia Yang, Duncan S. Wong, Guomin Yang and Qi Xie*
Coffee Break: 15:30-16:00: Main Entrance Hall of the School of Mines building (21 calle Rios Rosas)	

S6: Shot Papers I (Chair: Brian Coan)	
16:00-16:20	Building Better Unsupervised Anomaly Detector with S-Transform *Sirikarn Pukkawanna*
16:20-16:40	Fault-Tolerant Topology Control Based on Artificial Immune in WMNs *Jing Chen and Yang Xiang*
16:40-17:00	Virtually Reconfigurable Secure Wireless Networks using Broadcast Tokens *Kannan Karthik*
17:00-17:20	On the Use of Key Assignment Schemes in Authentication Protocols *James Alderman and Jason Crampton*
17:20-17:40	On the Interactions Between Privacy-Preserving, Incentive, and Inference Mechanisms in Participatory Sensing Systems *Idalides Vergara, Diego Mendez-Chavez and Miguel Labrador*
17:40-18:00	Security Authentication of AODV Protocols in MANETs *Ahmad Alomari*
18:00-18:20	Architecture for Trapping Toll Fraud Attacks Using a VoIP Honeynet Approach *Markus Gruber, Christian Schanes, Florian Fankhauser, Martin Moutran and Thomas Grechenig*

NSS 2013 Program @ ROOM 2, Fundacion Gomez-Pardo Building (1 calle Alenza)	
2013-06-03 (Day 1)	
S7: Security Protocols and Practice (Chair: Xu Huang)	
10:30-10:55	A Novel Security Protocol for Resolving Addresses in the Location/ID Split architecture *Mahdi Aiash*
10:55-11:20	The OffPAD: Requirements and Usage *Kent Are Varmedal, Henning Klevjer, Joakim Hovlandsvåg, Audun Jøsang, Johann Vincent and Laurent Miralabé*
11:20-11:45	Information-oriented Trustworthiness Evaluation in Vehicular Ad-hoc Networks *Sashi Gurung, Dan Lin, Anna Squicciarini and Elisa Bertino*
11:45-12:10	Using Trusted Platform Modules for Location Assurance in Cloud Networking *Christoph Krauß and Volker Fusenig*
12:10-12:30	Human Identification with Electroencephalogram (EEG) for the Future Network Security (short paper) *Xu Huang, Salahiddin Altahat, Dat Tran and Shutao Li*
Lunch 12:30-13:45: Main Entrance Hall of the School of Mines building (21 calle Rios Rosas)	
S8: Applications Security (Chair: Christoph Krauß)	
13:50-14:15	Tracing sources of anonymous slow suspicious activities *Harsha Kalutarage, Siraj A. Shaikh, Qin Zhou and Anne E. James*
14:15-14:40	Static Analysis for Regular Expression Denial-of-Service Attacks *Asiri Rathnayake, Hayo Thielecke and James Kirrage*
14:40-15:05	Next-Generation DoS at the Higher Layers: a Study of SMTP Flooding *Gabriel Cartier, Jean-Francois Cartier and José M. Fernandez*
15:05-15:30	Towards Hybrid Honeynets Via Virtual Machine Introspection and Cloning *Tamas Lengyel, Justin Neumann, Steve Maresca and Aggelos Kiayias*
Coffee Break: 15:30-16:00: Main Entrance Hall of the School of Mines building (21 calle Rios Rosas)	
S9: Modeling and Evaluation (Chair: Gabriel Macia-Fernandez)	
16:00-16:25	Stochastic Traffic Identification for Security Management: eDonkey Protocol as a Case Study *Rafael A. Rodríguez-Gómez, Gabriel Macia-Fernandez and Pedro García-Teodoro*

16:25-16:50	A Technology Independent Security Gateway for Real-Time Multimedia Communication *Fudong Li, Nathan Clarke and Steven Furnell*
16:50-17:15	Efficient Attribute Based Access Control Mechanism for Vehicular Ad Hoc Network *Y.Sreenivasa Rao and Ratna Dutta*
17:15-17:40	Evaluation of Detecting Malicious Nodes Using Bayesian Model in Wireless Intrusion Detection *Yuxin Meng, Wenjuan Li and Lam-For Kwok*
17:40-18:05	Model the Influence of Sybil Nodes in P2P Botnets *Wang Tianzuo, Wang Huaimin, Liu Bo and Shi Peichang*
20:30 Banquet Dinner: VP Jardin Metropolitano Hotel (12 Avenida Reina Victoria)	
2013-06-04 (Day 2)	
S10: Privacy (Chair: Qianhong Wu)	
10:30-10:55	Privacy Preserving Context Aware Publish Subscribe Systems *Mohamed Nabeel, Stefan Appel, Elisa Bertino and Alejandro Buchmann*
10:55-11:20	A New Unpredictability-Based RFID Privacy Model *Anjia Yang, Yunhui Zhuang, Duncan S. Wong and Guomin Yang*
11:20-11:45	Privacy-Preserving Multi-Party Reconciliation using Fully Homomorphic Encryption *Florian Weingarten, Georg Neugebauer, Ulrike Meyer and Susanne Wetzel*
11:45-12:10	Privacy-Preserving Password-based Authenticated Key Exchange in the Three-party Setting *Weijia Wang, Lei Hu and Yong Li*
12:10-12:30	Towards a Privacy-Preserving Solution for OSNs *Qiang Tang*
Lunch: 12:30-13:45: Main Entrance Hall of the School of Mines building (21 calle Rios Rosas)	
S11: Key Agreement and Distribution (Chair: Jia Hu)	
13:50-14:15	Light Weight Network Coding Based Key Distribution Scheme for MANETs *Jianwei Liu, Abdur Rashid Sangi, Ruiying Du and Qianhong Wu*
14:15-14:40	Identity-based Dynamic Authenticated Group Key Agreement Protocol for Space Information Network *Chao Wang, Kefei Mao, Jianwei Liu andf Jianhua Liu*
14:40-15:05	Authentication and Key Agreement based on Hyper-Sphere using Smart Cards *Shaohua Tang and Lingling Xu*
15:05-15:30	An Efficient Constant Round ID-based Group Key Agreement Protocol for Ad hoc Networks

	Elisavet Konstantinou
Coffee Break: 15:30-16:00: Main Entrance Hall of the School of Mines building (21 calle Rios Rosas)	
S12: Shot Papers II (Chair: Shaohua Tang)	
16:00-16:20	Collusion-Resistant Domain-Specific Pseudonymous Signatures *Julien Bringer, Herve Chabanne and Alain Patey*
16:20-16:40	On the Applicability of Time-Driven Cache Attacks on Mobile Devices *Raphael Spreitzer and Thomas Plos*
16:40-17:00	Ancestor Excludable Hierarchical ID-based Encryption Revisited *Fan Zhang, Hua Guo and Zhoujun Li*
17:00-17:20	Think Twice before You Share: Analyzing Privacy Leakage under Privacy Control in Online Social Networks *Yan Li, Yingjiu Li, Qiang Yan and Robert Deng*
17:20-17:40	A Dynamic and Multi-Layer Reputation Computation Model for Multi-Hop Wireless Networks *Jia Hu, Hui Lin and Li Xu*
17:40-18:00	Distributed and Anonymous Publish-Subscribe *Jörg Daubert, Mathias Fischer, Stefan Schiffner and Max Mühlhäuser*
18:00-18:20	Measuring and Comparing the Protection Quality in Different Operating Systems *Zhihui Han, Liang Cheng, Yang Zhang and Dengguo Feng*

NSS 2013 Program @ ROOM 1, Fundacion Gomez-Pardo Building (1 calle Alenza)	
2013-06-04 (Day 2) 13:50-18:20	
S13: Industrial Track I (Chair: Waleed Alsalih)	
13:50-14:10	Filtering Trolling Comments through Collective Classication *Jorge De-La-Peña-Sordo, Igor Santos, Iker Pastor-López and Pablo G. Bringas*
14:10-14:30	Security Analysis of Touch Inputted Passwords - A Preliminary Study Based on the Resistance against Brute Force Attacks *Nelson Uto, Emílio Tissato Nakamura and Bruno Alves Pereira Botelho*
14:30-14:50	A Pairing-free Identity Based Authentication Framework for Cloud Computing *Dheerendra Mishra, Vinod Kumar and Sourav Mukhopadhyay*
14:50-15:10	Formal Modeling and Automatic Security Analysis of Two-Factor and Two-Channel Authentication Protocols *Alessandro Armando, Roberto Carbone and Luca Zanetti*
15:10-15:30	Towards a More Secure Apache Hadoop HDFS Infrastructure Anatomy of a Targeted Advanced Persistent Threat against HDFS and analysis of Trusted Computing based Countermeasures *Jason Cohen and Dr. Subatra Acharya*
Coffee Break: 15:30-16:00: Main Entrance Hall of the School of Mines building (21 calle Rios Rosas)	
S14: Industrial Track II (Chair: Jiankun Hu)	
16:00-16:20	A Formally Verified Initial Authentication and Key Agreement Protocol in Heterogeneous Environments using Casper/FDR *Mahdi Aiash*
16:20-16:40	A Comprehensive Access Control System for Scientific Applications *Muhammad Ihsanulhaq Sarfraz, Peter Baker, Jia Xu and Elisa Bertino*
16:40-17:00	Partial Fingerprint Reconstruction With Improved Smooth Extension *Wei Zhou, Jiankun Hu, Ian Petersen and Mohammed Bennamoun*
17:00-17:20	Modeling and Analysis for Thwarting Worm Propagation in Email Networks *Sheng Wen, Yang Xiang and Wanlei Zhou*
17:20-17:40	On Secure and Power-efficient RFID-based Wireless Body Area Network *Sana Ullah and Waleed Alsalih*
17:40-18:00	Towards Authenticated Objects

	Daniele Midi, Ashish Kundu and Elisa Bertino
18:00-18:20	A Finger-vein based Cancellable Bio-cryptosystem *Wencheng Yang, Jiankun Hu and Song Wang*