May 21, 2007

08.00 - 09.00	Keynote		
Session 1A	**Cryptographic algorithms**		
09.10 - 9.35	Fast and Efficient Implementation of AES Via Instruction Set Extensions	1	Adam Elbirt
09.35 - 10.00	Reducing the Complexity in the Distributed Multiplication Protocol of Two Polynomially Shared Values	24	Peter Lory
10.00 - 10.25	Efficient Conjunctive Keyword-Searchable Encryption	38	Eun-Kyung Ryu, Tsuyoshi Takagi
10.25 - 10.45	*Coeffe/Tea Break*		
Session 1B	**Distributed access control and firewalls**		
10.45 - 11.10	Advanced Packet Filter Placement Strategies for Carrier-Grade IP-Networks	58	Birger Tödtmann, Erwin Rathgeb
11.10 - 11.35	Obligations for Role based Access Control	28	Gansen Zhao, David Chadwick, Sassa Otenko
11.35 - 12.00	Effective Storage Security In Incompletely Trusted Environment	27	Chunming Rong, Won-Chol Kim
12.00 - 13.20	*Lunch*		
Session 1C	**Wireless ad hoc and sensor network security**		
13.20 - 13.45	An Efficient Scheme for User Authentication in Wireless Sensor Networks	11	Canming Jiang, Bao Li
13.45 - 14.10	Using Social Network Theory Towards Development Of Wireless Ad hoc Network Trust	15	Sameer Pai, Tanya Roosta, Shankar Sastry, Stephen Wicker
14.10 - 14.35	Detecting Anomaly Node Behavior in Wireless Sensor Networks	20	Qinghua Wang, Tingting Zhang
14.35 - 15.00	Mobile Jamming Attack and its Countermeasure in Wireless Sensor Networks	49	Hung-Min Sun, Shih-Pu Hsu, Chien-Ming Chan
15.00 - 15.20	*Coeffe/Tea Break*		
Session 1D	**Network security issues and protocols**		
15.20 - 15.45	Random Oracle Instantiation in Distributed Protocols Using Trusted Platform Modules	50	Vandana Gunupudi, Stephen R. Tate
15.45 - 16.10	Information security threats and access control practices in Norwegian businesses	57	Janne Merete Hagen, Tormod Kalberg Sivertsen, Chunming Rong
16.10 - 16.35	Context-Aware Security Policy for the Service Discovery	71	Slim Trabelsi, Laurent Gomez, Yves Roudier
16.35 - 17.00	Adapting the UCONABC Usage Control Policies on CORBASec Infrastructure	80	Lau Lung, Marcelo Higashiyama, Rafael Obelheiro, Joni Fraga

May 22, 2007

08.00 - 09.00	Keynote		
Session 2A	**Authorization schemes**		
09.10 - 9.35	Enforcing Fine-grained Authorization Policies for Java Mobile Agents	48	Giovanni Russello, Changyu Dong, Naranker Dulay
09.35 - 10.00	A Decentralized Authorization Architecture	65	Feike Dillema, Simone Lupetti, Tage Stabell-Kulø
10.00 - 10.25	Conflict Detection and Resolution in Context-Aware Authorization	74	Amir Reza Masoumzadeh, Morteza Amini, Rasool Jalili
10.25 - 10.45	*Coeffe/Tea Break*		
Session 2B	**Authentication and access control**		
10.45 - 11.10	Authenticated Broadcast Encryption Scheme	25	Chik How Tan, Joseph Chee Ming Teo, Jens-Are Amundsen
11.10 - 11.35	Leveraging Identity-based Cryptography for Node ID Assignment in Structured P2P Systems	51	Sunam Ryu, Kevin Butler, Patrick Traynor, Patrick McDaniel
11.35 - 12.00	A Certified Email Protocol using Key Chains	63	Jan Cederquist, Mohammad Torabi Dashti, Sjouke Mauw
12.00 - 13.20	*Lunch*		
Session 2C	**Key management**		
13.20 - 13.45	Heuristics for Improving Cryptographic Key Assignment in a Hierarchy	40	Anne Kayem, Patrick Martin, Selim Akl
13.45 - 14.10	An identity-based key management framework for personal networks	60	Khaled Masmoudi, Hossam Afifi
14.10 - 14.35	Identity-Based and Inter-Domain Password Authenticated Key Exchange for Lightweight Clients	64	Hoon Wei Lim, Ford Long Wong
14.35 - 15.00	Efficient Key Management for Content Access Control within Tree Hierarchies	88	H. Ragab Hassen, A Bouabdallah, H Bettaha
15.00 - 15.20	*Coeffe/Tea Break*		
Session 2D	**Distributed intrusion detection and protection systems**		
15.20 - 15.45	Detecting Coordinated Distributed Multiple Attacks	87	Srinivas Mukkamala
15.45 - 16.10	Finding Logically Consistent Resource-Deception Plans for Defense in Cyberspace	10	Neil Rowe
16.10 - 16.35	Intrusion Detection for Encrypted Web Accesses	17	Akira Yamada, Miyake Yutaka, Keisuke Takemori, Adrian Perrig, Ahren Studer
16.35 - 17.00	Relative Entropy-Based Filtering of Internet Worms by Inspecting TCP SYN Retry Packets	26	Byungseung Kim, Saewoong Bahk

May 23, 2007

08.00 - 09.00	Keynote	
Session 3A	**Software security**	
09.10 - 9.35	Kernel and Application Integrity Assurance: Ensuring Freedom from Rootkits and Malware in a Computer System	16 Lifu Wang, Partha Dasgupta
09.35 - 10.00	HTTPS Hacking Protection	61 Thawatchai Chomsiri
10.00 - 10.25	Towards an Aspect Oriented Approach for the Security Hardening of Code	75 Azzam Mourad, Marc-Andre Laverdiere, Mourad Debbabi
10.25 - 10.45	*Coeffe/Tea Break*	
Session 3B	**PKI and Digital signatures**	
10.45 - 11.10	An Online/Offline Signature Scheme Based on the Strong RSA Assumption	53 Ping Yu, Stephen Tate
11.10 - 11.35	Authenticating Feedback in Multicast Applications Using a Novel Multisignature Scheme Based on Cubic LFSR Sequences	82 Saikat Chakrabarti, Santosh Chandrasekhar, Mukesh Singhal, Kenneth Calvert
11.35 - 12.00	A Robust and Efficient Mechanism to Distribute Certificate Revocation Information Using the Grid Monitoring Architecture	69 Daniel Kouril, Ludek Matyska, Michal Prochazka
12.00 - 13.20	*Lunch*	
Session 3C	**Privacy and trust**	
13.20 - 13.45	Privacy Rights Management for Privacy Compliance Systems	2 Ronggong Song, Larry Korba, George Yee
13.45 - 14.10	The All-Or-Nothing Anti-Theft Policy—Theft Protection for Pervasive Computing	30 Jakob Illeborg Pagter, Michael Østergaard Pedersen
14.10 - 14.35	On the Contribution of Preamble to Information Hiding in Mimicry Attacks	46 Gunes Kayacik, Nur Zincir-Heywood
14.35 - 15.00	**Conclusion**	
15.00 - 15.20	*Coeffe/Tea Break*	
Session 3D		
15.20 - 15.45		
15.45 - 16.10		
16.10 - 16.35		
16.35 - 17.00		