

SEC 2004 PROGRAMME

Monday 23 August 2004

13h30 - 15h

Risk management

Chair: Sushil Jajodia (George Mason U., USA)

An Abstract Reduction Model for Computer Security Risk- Mohamed Hamdi, Nouredine Boudriga
(U. Carthage, Tunisia)

Remediation Graphs for Security Patch Management- Vipin Swarup, (The MITRE Corporation, USA)

Security Modelling for Risk Analysis- Dennis Longley (Queensland U. Technology, Australia), Lam For Kwok (City U. of Hong-Kong, Hong-Kong)

13h30 - 15h

Malicious code analysis

Chair: Frédéric Cuppens (ENST-Bretagne, France)

Contrasting Malicious Java Applets by Modifying the Java Virtual Machine- Vincenzo Ciaschini (INFN-CNAF, Italy), Roberto Gorrieri (U. Bologna, Italy)

Analyzing Network Management Effects with SPIN and cTLA- Gerrit Rothmaier (Materna GmbH, Germany), Heiko Krum, Andre Pohl (U. Dortmund, Germany)

Formal Reasoning of Various Categories of Widely Exploited Security Vulnerabilities by Pointer Taintedness Semantics- Shuo Chen, Karthik Pattabiraman, Zbigniew Kalbarczyk and Ravi K. Iyer (UIUC, USA)

15h30 - 17h

Panel

Meeting the Global Challenges of Security Incident Response

Chair: Vijay M. Masurkar (Sun Microsystems, Inc., U.S.A.)

Participants:

Simone Fischer-Hübner, Karlstad University, Sweden
Morton Swimmer, IBM Zurich Research Laboratory, Switzerland
Kai Rannenberg, Goethe University of Frankfurt, Germany
Albin Zuccato, Karlstad University, Sweden
Gunnar Wenngren, Swedish Defence Research Agency, Sweden

17h - 17h30

Kristian Beckman Award

Chair: Louise Yngström (U. of Stockholm DSV, Sweden)

Recipient: Jean-Jacques Quisquater (U.Catholique de Louvain, Belgium)

Talk: *Secure Sensors for Smarts Sensors? -- Moore's law for Fahrenheit 1984?*

Tuesday 24 August 2004

10h30 - 12h

Information Flow

Chair: William List (Wm. List & Co, UK)

Security in Globally Distributed Industrial Information Systems- Petri Saloma, Ronja Addams-Moring, Teemupekka M. Virtanen (Helsinki U. Technology, Finland)

A Case for Information Ownership in ERP systems- Manfred P. Hertenberger, S.H. von Solms (Rand Afrikaans U., South Africa)

Interactive Access Control for Web Services- Hristo Koshutanski, Fabio Massacci (U. Trento, Italy)

13h30 - 15h

Security and Control of IT in Society: Identity Management

Chair: Teemupekka M. Virtanen (Helsinki U. Technology, Finland)

Identity-based Key Infrastructures (IKIs)- Mike Burmester, Yvo Desmedt (Florida State U., USA)

ModInt: Compact Modular Arithmetic Class Library Available on Cellular Phone and its Application to Secure Electronic Voting System- Hiroaki Kikuchi, Junji Nakazato (Tokai U., Japan)

Dependable Security by Twisted Secret Sharing- Semir Daskapan (Delft U. Technology, Netherlands)

15h30 - 17h30

Intrusion Detection

Chair: Hervé Debar (France-Telecom R&D, France)

A Language Driven IDS for Event and Alert Correlation- Eric Totel, Bernard Vivinis, Ludovic Mé (Supelec, France)

Install-time Vaccination of Windows Executables to Defend Against Stack Smashing Attacks- Avishai Wool, Danny Nebenzahl (Tel Aviv U., Israel)

Eigenconnections to Intrusion Detection - Yacine Bouzida, Sylvain Gombault (ENST Bretagne, France)

Visualising Intrusions: Watching the Webserver- Stefan Axelsson (Chalmers U., Sweden)

Wednesday 25 August 2004

10h30 - 12h

Security Architecture

Chair: Sushil Jajodia (George Mason U., USA)

MASKS: Managing Anonymity while Sharing Knowledge to Servers- Robert Pinto, Lucila Ishitani, Virgílio Almeida, Wagner Meira Júnior, Fabiano A. Fonseca, Fernando D. Castro (U. Federal Minas Gerais, Brazil)

Security and Differentiated Hotspot Services Through Policy-based Management Architecture- Idir Fodil, Vincent Jardin (6WIND, France)

Key Management for Secure Multicast in Hybrid Satellite Networks- Ayan Roy-Chowdhury, John S. Baras (U. Maryland, USA)

13h30 - 15h

Security Protocols

Chair: Dr. Indrajit Ray (Colorado State U., USA)

Supporting End-to-end Security across Proxies with Multiple-Channel SSL- Yong Song, Victor

Leung, Konstantin Beznosov (U. British Columbia, Canada)

A Content-Protection Scheme for Multi-Layered Reselling Structures- Pei-Ling Yu, Pan-Lung Tsai, Chin-Laung Lei (National Taiwan U., Taiwan)

An Asymmetric Cryptography Secure Channel Protocol for Smart cards- Konstantinos Markantonakis, Konstantinos Rantos (Royal Holloway, UK)

15h30 - 17h

Security Protocols and Home Security

Chair: Kai Rannenbergh (Goethe U. Frankfurt, Germany)

IPsec clustering- Antti Nuopponen (Emic Networks, Finland), Sami Vaarala (Stinghorn, Finland), Teemupekka Virtanen (Helsinki U. Technology, Finland)

Improving secure device insertion in home ad-hoc networks- Olivier Heen, Jean-Pierre Andreaux (Thomson R&D; France, France)

Spam Filter Analysis- Flavio D. Garcia, Jaap-Henk Hoepman (U. Nijmegen, The Netherlands), Jeroen van Nieuwenhuizen (U. Twente, The Netherlands)

Thursday 26 August 2004

10h30 - 12h

Database management

Chair: Frédéric Cuppens (ENST-Bretagne, France)

Collective Signature for Efficient Authentication of XML Documents- Indrajit Ray, Eunjong Kim (Colorado State U., USA)

Updating Encrypted XML Documents on Untrusted Machines- Prakash D. Reddy, Robert N. Mayo, Eamonn O'Brien-Strain, Jim Rowson, Yuhong Xiong (Hewlett Packard Labs, USA)

Efficient Simultaneous Contract Signing- Martin Stanek (Comenius U., Slovakia), Lubica Liskova (Slovak U. Technology, Slovakia)

13h30 - 15h

Access Control and Data Protection

Chair: Yves Deswarte (LAAS-CNRS, France)

DHCP Authentication Using Certificates- Jacques Demerjian, Ahmed Serhrouchni (ENST, France)

Recursive Sandboxes: Extending Systrace To Empower Applications- Angelos D. Keromytis, Aleksey Kurchuk (Columbia U., USA)

Fast Digital Certificate Revocation- Vipul Goyal, (Banaras Hindu U., India)

15h30 - 17h

Authentication

Chair: Éric Totel (Supélec, France)

A Long-term Trial of Keystroke Profiling using Digraph, Trigraph and Keyword Latencies- Paul S. Dowland, Steven M. Furnell (U. Plymouth, UK)

Trusted Computing, Trusted Third Parties, and Verified Communications- Martín Abadi (U. California at Santa Cruz, USA)

Maille Authentication- A Novel Protocol for Distributed Authentication- Andrew A. Fritz, (U. Houston, USA)

17h - 17h30

Closing: Best Student Paper Award and Presentation of Sec 2005