

SEC 2004

19th IFIP International
Information Security
Conference

TC11 — Security and Protection in Information Processing Systems

Security is probably the most critical factor for the development of the “Information Society”. E-government, e-commerce, e-healthcare and all other e-activities present challenging security requirements that cannot be satisfied with current technology, except maybe if the citizens accept to waive their privacy, which is unacceptable ethically and socially. New progress is needed in security and privacy preserving technologies.

The IFIP/Sec conference has been established from the eighties as one of the most important forum for presenting new scientific research results as well as best professional practice to improve the security of information systems. This balance between future technology improvements and day-to-day security management has contributed to better understanding between researchers, solution providers and practitioners, making this forum lively and fruitful.

IFIP/Sec 2004 will continue this tradition with sessions dedicated to risk management, malicious code analysis, identity management, intrusion detection, security architectures and protocols, home security, authentication, data protection, etc. A panel will present current approaches and new developments in security incident response management. For Sec 2004, 35 presentations have been selected from more than 160 full paper submissions, which represents a record for all Sec conferences. This severe selection is a guarantee that all the presentations will deserve a great interest.

Dedicated workshops, embedded within Sec 2004 will present new achievements in Information Security Education (**ISE**, the WG11.8 Workshop), in Information Security Management (**ISM**, the 10th IFIP WG 11.1 Working Conference), and in Privacy and Anonymity in Networked and Distributed Systems (**I-NetSec'04**, the 3rd IFIP 11.4 Working Conference).

With all these features, there is no doubt that Sec 2004 will be a memorable success.

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 - Lam For Kwok (City U. of Hong-Kong, Hong-Kong), Dennis Longley (Queensland U. Technology, Australia)

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), Andre Pohl, Heiko Krum (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 Smart Censors? — 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 - S.H. von Solms, Manfred P. Hertenberger (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) - Yvo Desmedt, Mike Burmester (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 (Supélec, 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 Rannenber (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 - Aleksey Kurchuk, Angelos D. Keromytis (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

**Embedded Workshop
Information Security Management (ISM)
Tuesday 24 August 2004**

10h30 – 12h

Corporate ISM

Corporate Information Security Education: Is Outcomes Based Education the Solution? - Joahn Van Niekerk, Rossouw Von Solms (Port Elizabeth Technikon, South Africa)

Towards Corporate Information Security Obedience - Kerry-Lynn Thomson, Rossouw von Solms (Port Elizabeth Technikon, South Africa)

13h30 – 15h

ISM - Risk Analysis Methods and Frameworks

CIIP-RAM - A Security Risk Analysis Methodology for Critical Information Infrastructure Protection - Tyrone Busutiil, Matthew Warren (Deakin U., Australia)

A Framework for role-based monitoring of Insider Misuse - Aung Htike Phy, Steven M. Furnell, Francisco Portilla (U. Plymouth, UK)

15h30 – 17h30

ISM & Technology

Update/Patch Management Systems: a protocol taxonomy with security implications - Andrew Colarik, Clark Thomborson, Lech Janczewski (U. Auckland, New Zealand)

Investigating a smart Technology - Kevin O'Sullivan, Karen Neville, Ciara Heavin (U. College Cork, Ireland)

Discussion on what are the future issues of Information Security.

Panel: to-be-announced

Embedded Workshop Information Security Education (ISE)

Wednesday 25 August 2004

10h30-12h

Welcome - Aims of workshop, Helen Armstrong (Curtin U., Australia)

Doctoral Programmes – Breadth and Depth

Chair: Helen Armstrong (Curtin U., Australia)

Laboratory Support for Information Security Education - Natalia Miloslavskaya, Alexander Tolstoy, Dmitry Ushakov (Moscow Engineering Physics Institute, Russia)

An holistic approach to an international doctoral program in information security - Louise Yngström, (U. Stockholm DSV, Sweden)

A new paradigm for information security education at doctoral level - Nimal Jayaratna (Curtin Business School, Australia)

13h30-15h

Doctoral Programmes – from East to West

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

Highly qualified information security personnel training in Russia – Victor Gorbatov, Anatoly Maluk, Natalia Miloslavskaya, Alexander Tolstoy (Moscow Engineering Physics Institute, Russia)

Doctor of Philosophy: IT Security - Jill Slay (U. South Australia, Australia)

Doctoral Programme on Information and Communication Systems Security at the University of the Aegean - Socratis Katsikas, (U. the Aegean, Greece)

An international security perspective - Gerald Quirchmayr (U. Vienna, Austria)

15h30-16h30

Doctoral Programme - Strategy and Cooperation

Chair: Gerald Quirchmayr (U. of Vienna, Austria)

Academic content and structure required by the military for an international doctoral program - Ronald Dodge (US Military Academy West Point, USA)

Doctoral Program with Specialization in Information Security: A High Assurance Constructive Security Approach - Cynthia Irvine & Timothy Levin (Naval Postgraduate School, Monterey, USA)

16h30-17h30

Building an International Doctorate Programme

General content standards and core body of knowledge requirements - Corey Schou (Idaho State U., USA)

Panel: *Minimum requirements for international doctorate*

Moderators: Helen Armstrong (Curtin U., Australia) and Gerald Quirchmayr (U. Vienna, Austria)

Embedded Workshop
Privacy and Anonymity in Networked and Distributed Systems
(I-NetSec'04)

Thursday 26 August 2004

10h30 – 12h

Privacy Enhancing Technologies

A Security Model for Anonymous Credential Systems - Andreas Pashalidis, Chris J. Mitchell (Royal Holloway, UK)

Private Information Storage with Logarithmic-Space Secure Hardware - Alexander Iliev, Sean Smith (Dartmouth College, USA)

Taxonomy of Mixes and Dummy Traffic - Claudia Diaz, Bart Preneel (K.U.Leuven, Belgium)

13h30 – 15h

Design for Privacy and Identity Management

Identity Management for Self-Portrayal - Toby Baier, Christian P. Kunze (U. Hamburg, Germany)

Privacy Preserving Online Reputation Systems - Marco Voss (Darmstadt U. of Technology, Germany)

A Risk Driven Approach to Designing Privacy Enhanced Secure Applications - Els Van Herreweghen (IBM Research, Zurich, Switzerland)

15h30 – 17h

Privacy Threats and Trusted Computing

Privacy-Invasive Software in File-Sharing Tools - Andreas Jacobsson, Martin Boldt, Bengt Carlsson (Blekinge Institute of Technology, Sweden)

Infusing Privacy Norms in DRM --Incentives and Perspectives from Law - Alex Cameron (U. Ottawa, Canada)

Panel: Trusted Computing and Privacy –

Moderator: Bart De Decker (K. U. Leuven, Belgium)

Participants: Yves Deswarte (LAAS-CNRS, France)

Dirk Kuhlmann (HP Labs, UK)

Kai Rannenbergh (Goethe U. Frankfurt, Germany)

Els Van Herreweghen (IBM Research, Zurich, Switzerland)