SEC 2003

**18th IFIP International
Information Security Conference**

IFIP TC11

Athens Chamber of Commerce and Industry
26-28 May 2003, Athens, Greece

http://www.sec2003.org

Preliminary Conference Programme

Monday, 26 May 2003

09:00-10:30   (Hermes Auditorium) **Opening and Keynote Address**

Opening and welcome, D. Gritzalis, Conference General Chair

Technical Programme Overview, P. Samarati and S. Katsikas, Programme Committee Chairs

The IFIP IT Security Community: Plans for the Future, L. Strous, IFIP/TC-11 Chair

K. Beckman Award presentation (winner to be announced)

Ernst & Young keynote address: The electronic citizen, T. Autret (Ernst & Young, France)

10:30-11:00   Coffee/tea

11:00-13:00   SESSION 1 (Hermes Auditorium): **Secure Networks and Distributed Systems**

Trust Mediation for Distributed Information Systems, B. Toone, M. Gertz, P. Devanbu (Univ. of California at Davis, USA)

Concerning Enterprise Network Vulnerability to HTTP Tunneling, C. Daicos, S. Knight (Royal Military College, Canada)

Providing Voice Privacy Over Public Switched Telephone Networks, M. Sharif, D. Wijesekera (George Mason University, USA)

A Multi-party Non-repudiation Protocol for Exchange of Different Messages, J.-A. Onieva, J. Zhou, (Laboratories for IT, Singapore), M. Carbonell, J. Lopez (Univ. of Malaga, Spain)

Secure Vickery Auctions without TTP: A Prototype, B. De Decker, G. Neven, F. Piessens (Catholic Univ. of Leuven, Belgium)

13:00-14:00   Lunch

14:00-15:30   SESSION 2a (Hermes Auditorium): **Content Protection**

Securing XML-based Multimedia Content, E. Damiani (Univ. of Milan, Italy), S. De Capitani di Vimercati (Univ. of Brescia, Italy)

Secure Audit Logging with Tamper-Resistant Hardware, C. N. Chong, Z. Peng, P. Hartel (INF-UT, The Netherlands)

PCMHoDC: A Scheme to Protect Copyright and Modification History of Digital Contents, H.-J. Park, J. Kim (Pohang Univ. of Science & Technology, South Korea)

SESSION 2b (Filikis Etairias Room): **R&TD Projects Presentation**

CASENET: *Computer-aided Solutions to Secure Electronic Commerce Transactions*, S. Guergens (Fraunhofer-IST, Germany), J. Lopez (Univ. of Malaga, Spain)

e-VOTE: *Electronic Voting Systems: The Impact of System Actors to the Overall Security Level*, C. Lambrinoudakis (Univ. of the Aegean, Greece), V. Tsoumas, M. Karyda, D. Gritzalis (AUEB, Greece), S. Katsikas (Univ. of the Aegean, Greece)

PISA: *Agent-based Systems and Privacy Enhancing Technologies*, L. Korba, K. El-Khalid, A. Patrick, R. Song, Y. Xu, G. Yee, J. Yu (National Research Council, Canada)

15:30-16:00   Coffee/tea

16:00-17:30   SESSION 3a (Hermes Auditorium): **Secure Multicast Communication and Secure Mobile Networks**

Using Keystroke Analysis as a Mechanism for Subscriber Authentication on Mobile Handsets, N. Clarke, S. Furnell, B.M. Lines (Univ. of Plymouth, United Kingdom), P. Reynolds (Orange Personal Communications Services, United Kingdom)

Introducing PKI to Enhance Security in Future Mobile Networks, G. Kambourakis, A. Rouskas, S. Gritzalis (Univ. of the Aegean, Greece)

A Time Driven Methodology for Key Dimensioning in Multicast Communications, R. di Pietro, L. Mancini, A. Mei (Univ. of Rome "La Sapienza", Italy)

A Flexible Category-Based Collusion-Resistant Key Management Schema for Multicast, C. Duma, N. Shahmehri, P. Lambrix (Linkoping University, Sweden)

SESSION 3b (Filikis Etairias Room): **R&TD Projects Presentation**

eCSIRT: *Efficient Cooperation Among Computer Emergency Response Teams: The eCSIRT.net Approach*, A. Helme, K.-P. Kossakowski (eCSIRT Consortium)

ASP-BP: *Application Service Provision - Best Practices*, P. Zini (ENEA, Italy), U. Kaufmann (Infoconsult, Germany)

PAIDFAIR: *Pay-per-Use: Payment standard for IP content or software use*, O. Winzenried (WIBU-SYSTEMS, Germany)

FALCONE: *Training High-Tech Crime Investigators*, S. O'Ciardhuain, A. Patel (Univ. College Dublin, Ireland), P. Gillen (An Garda Siochana, Ireland)

19:00-21:30   **Gala Dinner: The known-to-few ancient Greek Cuisine**

Tuesday, 27 May 2003

09:00-10:30   SESSION-11.1.A (Hermes Auditorium): **Workshop on Information Security Management, Part I**
World Framework for Security Benchmark Changes, L. Janczewski, A.M. Colarik (Univ. of Auckland, New Zealand)
Information Security: Auditing the Behavior of the Employee, C. Vroom, R. von Solms (Port Elizabeth Technicon, South Africa)
Priorities in the Deployment of Network Intrusion Detection Systems, M. Dobrucki, T. Virtanen (Helsinki University of Technology, Finland)

SESSION 11.4.A (Filikis Etairias Room): **Workshop on Privacy and Anonymity in Networked & Distributed Systems (INet '03)**
Statistical Disclosure Attacks: Traffic Confirmation in Open Environments, G. Danezis (Univ. of Cambridge, United Kingdom)
On the Anonymity of Timed Pool Mixes, A. Serjantov (Univ. of Cambridge, United Kingdom), R.E. Newman (Univ. of Florida, USA)
Privacy in Content Networks Distribution: A Framework Description, R. Hulsebosch (Telematica Institute, The Netherlands)

10:30-11:00   Coffee/tea

11:00-13:00   SESSION 11.1.B (Hermes Auditorium): **Workshop on Information Security Management, Part II**
Bridging the Gap between Risk Analysis and Security Policies, P. Gaunard, E. Dubois (IT Innovation Center, Luxemburg)
Framework and Architecture for Secure Mobile Business Applications, J. Haller, P. Robins (SAP, Germany), T. Walter (DoCoMo, Germany), R. Killian-Kehr (SAP, Germany)
ISO 17799 and Australian Healthcare Organizations, W. Brooks, M. Warren, (Deakin University, Australia), W. Hutchinson (Edith Cowan University, Australia)

SESSION 11.2.A (Filikis Etairias Room): **Workshop on Small Systems Security, Part I**
Security, Fault-Tolerance and their Verification for Ambient Systems, J.-H. Hoepman (Univ. of Nijmegen, The Netherlands)

Hidden Layer Authentication Using Smart Card for Web-based WLANS, J. Pikrammenos, G. Sarkis, J. Soldatos, V. Anagnostopoulos (National Technical Univ. of Athens, Greece)

13:00-14:00   Lunch

14:00-15:30   SESSION 11.7.A (Hermes Auditorium): **Workshop on Security and Control of IT in Society (SCITS-III), Part I**
Invited talk: L. Yngstrom (Univ. of Stockholm, Sweden) (title to be announced)
Lawful Cyber Decoy Policy, J. B. Michael (Naval Postgraduate School, USA), T. Wingfield (Aegis Research Corp., USA)
Electronic Signature as a part of Information Society Infrastructure: Legal and Technological Situation in Finland, the Republic of Croatia and the Czech Republic, J. Paavilainen (Tampere University, Finland), S. Stojakovic-Celustka (UZI VRH, Croatia), D. Brechlerova (CUA, Czech Republic)

SESSION 11.2.B (Filikis Etairias Room): **Workshop on Small Systems Security, Part II**
PINPAS: a Tool for Power Analysis of Smartcards, J. den Hartog (Eindhoven Univ. of Technology), J. Verschuren (TNO-EIB), E. de Vink (Eindhoven Univ. of Technology and LIACS), J. de Vos (TNO-EIB), W. Wiersma (Eindhoven Univ. of Technology), The Netherlands
Assessing Security in Energy-efficient Sensor Networks, Y. W. Law, S. Etalle, P. Hartel (Univ. of Twente, The Netherlands)
From Finite State Machines to Provably Correct Java Card Applets, E. Hubbers, M. Oostdijk, E. Poll (Univ. of Nijmegen, The Netherlands)

15:30-16:00   Coffee/tea

16:00-17:30   SESSION 11.7.B (Hermes Auditorium): **Workshop on Security and Control of IT in Society (SCITS-III), Part II**
Panel debate: Topic: *Data Retention Policy – Cyber Security and Privacy Considerations.* Panelists: K. Rannenberg (Goethe Univ. Frankfurt, Germany), G. Wenngren (Swedish Defence Research Agency, Sweden), B. Michael (Naval Postgraduate School, USA), G. Danezis (Cambridge University, UK), A. Serjantov (Cambridge University, UK).

SESSION 11.2.C (Filikis Etairias Room): **Workshop on Small Systems Security, Part III**
Security Characteristics of E-collaborating Environments, B. Hulsebosch, E.-J. Goedvolk, W. Janssen (Telematica Institute, The Netherlands)
Roadmap for Securing Handheld Devices: System Integrity and Confidentiality, P. Vinayakray-Jani (Nokia Research Center, Finland)

18:00-22:30   **Cultural event - Excursion** (details to be announced)

Wednesday, 28 May 2003

09:00-10:30   SESSION 4 (Hermes Auditorium): **Panel discussion: Cybersecurity Education**

Moderator: D. Gritzalis (Athens Univ. of Economics & Business, Greece)

Panelists: S. Katsikas (Univ. of the Aegean, Greece), J. Lopez (Univ. of Malaga, Spain), Y. Maghiros (JRC Seville, Spain), L. Yngstrom (Stockholm University, Sweden)

10:30-11:00   Coffee/tea

11:00-13:00   SESSION 5a (Hermes Auditorium): **Security Management**

A User Friendly Guard with Mobile Post-release Access Control Policy, D. Williams, A. Fayad, S. Jajodia, D. Calle (The MITRE Corp., USA)

Context, Content, Process Analysis of IS Security Policy Formation, M. Karyda (AUEB, Greece), S. Kokolakis (Univ. of the Aegean, Greece), E. Kiountouzis (AUEB, Greece)

Integrating Security into Systems Development, U. Evertsson, U. Orthberg, L. Yngstrom (Stockholm University, Sweden)

Building an Enterprise IT Security Management System, M. Belsis, L. Smalov (Coventry University, United Kingdom)

Information Security Management System: Processes and Products, M. Eloff (Univ. of South Africa, South Africa), J. Eloff (Univ. of Pretoria, South Africa)

SESSION 5b (Filikis Etairias Room): **Intrusion Prevention and Detection**

Detecting Malicious Use With Unlabelled Data Using Clustering and Outlier Analysis, S. Knight, L. Carosielli (Royal Military College, Canada)

E^2xB: A Domain-Specific String Matching Algorithm for Intrusion Detection, K. Anagnostakis, S. Antonatos, E. Markatos, M. Polychronakis (Institute of Computer Science, Greece)

Intrusion Masking for Distributed Atomic Operations, M. Yu, P. Liu, W. Zang (Pennsylvania State University, USA)

Using Fuzzy System to Manage False Alarms in Intrusion Detection, M. Shajari (National Research Council, Canada), A. Ghorbani (Univ. of New Bunswick, Canada)

An Experiment in Software Decoy Design: Intrusion Detection and Countermeasures via System Call Instrumentation, J. Michael (Naval Postgraduate School, USA), G. Fragkos (Hellenic Army, Greece), M. Auguston (New Mexico State University, USA)

13:00-14:00   Lunch

14:00-15:30   SESSION 6a (Hermes Auditorium): **Access Control Policies and Models**

Integrating Information Security into Corporate Governance, K.-L. Thomson, R. von Solms (Port Elizabeth Technicon, South Africa)

Security Model for Health Care Computing and Communication Systems, A. A. el-Kalam, Y. Deswarte (LAAS/CNRS, France)

Constrained Role-based Delegation, L. Zhang, G.-J. Ahn (Univ. of Northern Carolina at Charlotte, USA)

SESSION 6b (Filikis Etairias Room): **R&TD Projects Presentation**

NESSIE, STORK: *Past and Future of Cryptographic Research in Europe*, B. Preneel (Catholic Univ. of Leuven, Belgium)

La Mer: *Smart Card Based PKI for Chambers of Commerce Services*, N. Polemi (National Technical Univ. of Athens, Greece)

USB: *Attribute Certificates in e-Health Privilege Management Infrastructure*, O. Ferrer-Roca, J. Collings, J. Gomez, M. Suarez (Univ. of La Laguna, Spain), J. de Leon (Servizio Canario de Salud, Spain)

15:30-16:00   Coffee/tea

16:00-17:30   SESSION 7a (Hermes Auditorium): **Secure Information Systems**

CSAP - An Adaptable Security Module for the e-Government System Webocrat, F. Dridi, M. Fischer (Univ. of Essen, Germany), G. Pernul (Univ. of Regensburg, Germany)

Perceptions of Security Contributing to the Implementation of Secure Information Systems, T. Tryfonas, E. Kiountouzis (AUEB, Greece)

New Directions on Information System Security Methods, M. Siponen (Univ. of Oulu, Finland)

Establishing Chain of Evidence as a Base for Non-repudiation Services, J.-J. Hwang, M.-H. Shao, S. Wu (Chang Gung University)

SESSION 7b (Filikis Etairias Room): **Security Protocols**

Integrating Logics and Process Calculi for Cryptographic Protocol Analysis, M. Papa, O. Bremer, J. Hale, S. Shenoi (Univ. of Tulsa, USA)

Flexible Delegation Security for Improved Distribution in Ubiquitous Environments, G. Kalogridis, C. Y. Yeun, G. Clemo (Toshiba Telecommunications Research Lab., United Kingdom)

Cooperative Defense Firewall Protocol, M. El-Soudani, M. Eissa (Cairo University, Egypt)

How to turn a PIN into an Iron Beam: A Patent-Free Practical Protocol for Secure Communication using a Weak Common Secret, S. Lucks (Univ. of Manheim, Germany), R. Weis (Free University, The Netherlands)

17:30-18:30   CLOSING SESSION (Hermes Auditorium)
Best Student Paper Award (winner to be announced during the session)
IFIP/SEC-2004 Announcement
Conference Closing