MONDAY, 31 AUGUST 1998

13.30 - 15.00

OPENING
by the program committee co-chairs **INVITED SPEAKER**
Joseph N. Pato, HP Labs Cambridge, USA:
"**Securing the Extended Enterprise in an Electronic World**"

15.30 - 17.00

SECURITY AND THE INTERNET Iliadis, Technological Educational Institute, Athens, GR:
"Security issues surrounding the JavaTM Programming Language: A state-of-the-art review" Prof. Roberto Gorrieri, Dipartimento di Scienze dell Informazione, I:
"Applet Watch-Dog: A Monitor Controlling the Execution of Java Applets" J. Dittmann, M. Stabenau, GMD - Darmstadt, D:
"Robust MPEG Video Copyright Protection Technology"

17.15 - 18.15

SHORT PAPERS

ELECTRONIC COMMERCE

Emilia Rosti, Univ. Milano, I: "A prepaid offline payment system for electronic money distribution" Susan B. Pancho, Royal Holloway, GB: "Policing the Global Information Infrastructure" Srividhya Subramanian and Mukesh Singhal, The Ohio State Univ., USA: "Detecting violation of real-time constraints in secure electronic commerce transactions"

MODELLING AND MANAGEMENT

R. Baskerville, Georgia St. Univ., USA, J. Pries-Heje, Copenhagen Business School, DK: "Packaging Information Security Safeguards" E. Franz, A. Graubner, A. Jerichow, A. Pfitzmann, Techn. Univ. Dresden, D: "Modelling mix-mediated anonymous communication and preventing pool-mode attacks" Eugene Kozik, Malvern, USA: "Telecommunication and Networking Security Activities of the People s Republic of China" T.K. Apostolopoulos, C. D. Moulinos, Univ. of Econ. and Bus., Athens, GR: "Security Management Using a Security Related MIB

CRYPTOGRAPHY AND INFRASTRUCTURE

Martin Stanek, Daniel Olejar, Comenius University, Bratislava, SK: "The methodology for symmetric encryption algorithms evaluation" H. Chang, Electronic Commerce Group, Ottawa, CDN: "A prototype implementation of a system to support multiple certification authorities" Tomaz Klobucar, Borka Jerman-Blazic, Jozef Stefan Institute, Ljubljana, SI: "Certificate policies formalisation and evaluation"

Approach"

TUESDAY, 1 SEPTEMBER 1998

10.00 - 10.30

KRISTIAN BECKMAN AWARD

Mr Sizer was proposed by the British Computer Society.

Mr Sizer is an independant Consultant in Risk Analysis and IT Security. Mr Sizer has a long and acknowledged career involving IT Security,starting in the early sixties. Richard also has a long involvement with IFIP, having been the UK's representative on TC 9 since its formation. He is also the foundingChairman of WG 9.6. On behalf of TC 11, and IFIP, Mr Sizer is congratulated on this very prestigous award, which will formally be awarded to him during the IFIP/Sec 98 Conference in Viennna/Budapest at the end of August.

11.00 - 12.30

INVITED SPEAKER
Tim Moses, Advanced Security Technology Entrust Technologies, CDN:
"**Building the Global PKI**" **HUMAN FACTORS**
Louise Yngström, Pateep Methakunavudhi, Unversity of Stockholm, S:
"A Methodology for Comparative Studies of Ethical Opinions related to IT-security issues"

13.30 - 15.00

SECURITY ARCHITECTURE

Pierangela Samarati, SRI International, USA:
"Secure Interoperation of Heterogeneous Systems: - A Mediator-Based Approach" X. Yi, X. F. Wang, K. Y. Lam, National University of Singapore, SGP:
"An Intelligent Agent Architecture for Securing Internet Trading" Mikko T Siponen, Jorma Kajava, University of Oulu, SF:
"The Dimensions and Categories of Information Security Awareness"

15.30 - 17.00

SESSION A	**SESSION B**
ACCESS CONTROL Mark Burge, Wilhelm	**DIGITAL SIGNATURES** Yuliang Zheng,

Burger, Johannes Kepler University Linz, A: **"Automating covert identification using ear biometrics and computer vision"** L. J. Janczewski, B. Lo, The University of Auckland, NZ: **"Reference monitor for hypermedia-based hospital information systems"** Ralph Holbein, Othmar Morger, Ulrich Nitsche, StephanieTeufel, University of Zurich, CH: **"Realization of a Context-Dependent Access Control Mechanism on a Commercial Platform"**

Monash University Melbourne, AUS: "Efficient Signcryption Schemes On Elliptic Curves" Chang. N. Zhang, University of Regina, CDN: **"An Integrated Approach for Fault Tolerance and Digital Signature in RSA"** Hideki Imai, Miodrag Mihaljevic, Yuliang Zheng, The University of Tokyo, J: **"A Fast Cryptographic Hash Function Based on Linear Cellular Automata over GF(q)"**

17.15 - 18.15

SESSION A

NETWORK SECURITY Sebastian Staamann, EPFL-DI-LSE, CH: **"Security in TINA"** Arun Iyengar, Robert Cahn, Juan A. Garay, Charanjit Jutla, IBM T. J. Watson Research Center, USA: **"Design and Implementation of a Secure Distributed Data Repository"**

SESSION B

SECURITY DEVICES Wolfgang Mayerwieser, Karl C. Posch, Reinhard Posch, Graz Univ. of Technology, A: **"Design flow and modeling for cryptographic macro cells"** Tibor Nemetz, KriptoHun Datasec. Consult., Pal Papp, HunGuard, H: **"Hybrid Random Byte Generators"**

THURSDAY, 3 SEPTEMBER 1998

13.30 - 15.00

INVITED SPEAKER
Mark Rotenberg, Electronic Privacy Information Center, USA:
"Privacy Protection and the Future of Electronic Commerce"

BEST STUDENT PAPER

Rodolphe Ortalo, Yves Deswarte, LAAS-CNRS & INRIA, Toulouse, F:
"Quantitative Evaluation of Information System Security"

15.30 - 17.00

SESSION A

PUBLIC KEY INFRASTRUCTURES Patrick Horster, Peter Schartner, Petra

SESSION B

HUNGARIAN IT SECURITY to be announced

Wohlmacher, University of Klagenfurt, A:
"Keymanagement" Peter Lipp, Andreas Sterbenz, Graz University of Technology, A, Reinhard Kuch, Post und Telekom Austria, A:
"Setting up a Public Certification Authority" Antonio Lioy, Fabio Maino, Politecnico di Torino, I:
"Providing X.509-based user access control to web servers"

17.15 - 18.15

SHORT PAPERS

SECURITY AND THE INTERNET

Klaus Keus, German Information Security Agency (GISA), D:
"A Model for a European Digital Signature Approach"

P. Kirsch, H. Weidner, K. Bauknecht, Univ. of Zurich, CH:
"Secure Conception of Internet Services" Anja Hartmann, German Information Security Agency (GISA), D:
"Security Culture in the Global Information Society"

MANAGEMENT AND RISK

J. Leiwo, Monash Univ., AUS:
"An Object Oriented Modeling Approach into the Management of Information Security "

J.-M. Kabasele-Tenday, Univ. Catholique de Louvain, B:
"Toward an Object Based Access Control model" D. Gregory, Qi Shi, M. Merabti, Liverpool John Moores Univ., GB:
"An Intrusion Detection System Based upon Autonomous Mobile Agents" E. Smith, J.H.P. Eloff, Rand Afrikaans University, ZA:
"A framework for determining the factors involved in calculating the information technology risk value of a health-care institution"

NETWORKS AND MODELLING

M.Laurent, ENSTB, F:
"A guide to help develop solutions for securing communications over networks"

G. Mohay, Queensland Univ. of Tech., AUS:
"A Model for Access Control and Intrusion Detection in Distributed Systems" W. Prentner, Digital Signum, Vienna, A:
"Predicting development cost of security in distributed software" A. Jøsang, S. Knapskog, Norwegian Univ. of Science and Technology, Trondheim, N:
"A Metric for Trusted Systems"

FRIDAY, 4 SEPTEMBER 1998

10.00 - 10.30

SESSION A

PROTOCOLS

Dr. Mahmoud T. El-Hadidi, Cairo University, Dr. Nadia H. Hegazi, Eng. Heba K. Aslan, Electronic Research Institute, ET:
"Logic-Based Analysis of a New Hybrid Encryption Protocol for Authentication and Key Distribution"

SESSION B

HUMAN FACTORS Marcel E.M. Spruit, Delft University of Technology, nl:
"Information security, the human factor"

11.00 - 12.30

MODELLING FOR SECURITY Kathrin Schier, University of Hamburg, D:
"A Role and Task Based Security Model for Multifunctional Smartcard Applications in the Area of Electronic Commerce" Masashi Yasuda, Takayuki Tachikawa, Makoto Takizawa, Tokyo Denki University, J:
"A Purpose-Oriented Access Control Model for Information Flow Management" C. P. Louwrens and S.H. von Solms, Rand Afrikaans University, ZA
"Can computerized immunity be achieved, based on a biological model?"

13.30 - 15.00

SESSION A

MODELLING FOR SECURITY Paloma Diaz, Ignacio Aedo, Arturo Ribagorda, Universidad Carlos III de Madrid, E
Fivos Panetsos, Universidad Nacional de Educacion a Distancia (UNED), Madrid, E:
"A security model for the design of hypermedia systems" Peter Trommler, IBM Research Division Zurich, CH:
"The Application Profile Security Model for Downloaded Executable Content"
Jussipekka Leiwo, Monash University, AUS:
"A group - enhanced ISSI model for secure interconnection of information systems"

SESSION B

MALICIOUS SOFTWARE Hervé Debar, Marc Dacier, Andreas Wespi, IBM Zurich Research Rueschlikon, CH:
"Reference Audit Information Generation for Intrusion Detection Systems" Jose Mauricio Bonifacio Junior, Instituto de Ciencias Matematicas de Sao Carlos, BR
Adriano Mauro Cansian, Universidade Estadual Paulista, BR:
"An Adaptive Intrusion Detection System Using Neural Networks" M. J. Warren, Deakin University, AUS:
"Cyber Terrorism"

15.30 - 17.00

SESSION A

SECURITY MANAGEMENT

J. Großschädl, Graz University of Technology, Austria:

SESSION B

PROTOCOLS

Claudia Eckert, Munich University of Technology, D:

"Breaking the 1 Mbit/s barrier in RSA encryption"

J. P. Bekmann, P. de Goede, A.C.M. Hutchison, University of Cape Town, ZA:
"Concurrancy and Synchronisation Issues in Security Implementaitons"

Severine Dusollier, Facutés Universitaires de Namur, B:
"Legal Aspects of Electronic Rights Management Systems"

"Tool-Supported Verification of Cryptographic Protocols"

Qi He, Carnegie Mellon University, USA:
"A New Practical Secure e-Voting Scheme"

Andreu Riera, Joan Borrell, Josep Rifa, Universitat Autonoma de Bercelona, E:
"An Uncoercible Verifiable Electronic Voting"

17.00 - 17.15

CLOSING
by the program committee co-chairs