CALL FOR PARTICIPATION

Along the lines of encouraging and catalyzing research in the area of Communications and Multimedia Security, it is our great pleasure to invite you to participate in the 10th IFIP TC-6 and TC-11 Conference on Communications and Multimedia Security (CMS 2006), which will be held in Crete on October 19-21, 2006.

Continuing the tradition of previous CMS conferences, we sought a balanced program containing presentations on various aspects of secure communication and multimedia systems. In a competitive process 22 full papers were selected for presentation out of a total of 76 submissions.

We are convinced that CMS’2006 will be a great opportunity for discussing novel ideas in information security amongst academia, industry, and authorities.

Herbert Leitold and Evangelos Markatos
Program co-Chairs CMS2006

DAY ONE

Thursday 19. October 2006

08:30-09:15 Registration – Aldemar Knossos Royal Village hotel, Conference Hall 2

09:15-09:30 Welcome
Evangelos Markatos, FORTH ICS

09:30-10:00 Keynote One
Communication, Networks and Multimedia security-what lies ahead?
Andrea Pirotti, ENISA

10:00-10:30 Coffee - Conference Hall 2

10:30-12:00 Applied Network and Information Security (session chair: Wolfgang Schneider)

Computing of Trust in Ad-hoc Networks
Huafei Zhu, Feng Bao and Jianwei Liu

TAO: Protecting against Hitlist Worms using Transparent Address Obfuscation
Spiros Antonatos and Kostas Anagnostakis

On The Privacy Risks of Publishing Anonymized IP Network Traces
Dimitris Koukis, Spiros Antonatos and Kostas Anagnostakis

12:00-13:30 Lunch – main restaurant (Aldemar Knossos Royal Village hotel)

13:30-15:00 Identification and Authentication (session chair: David Chadwick)

Secure Mobile Notifications of Civilians in Case of a Disaster
Heiko Rossnagel and Tobias Scherner

A Fair Anonymous Submission and Review System
Vincent Naessens, Liesje Demuynck and Bart De Decker

Attributes Delegation Based on Ontologies and Context Information
Isaac Agudo, Javier Lopez and Jose A. Montenegro

15:00-15:30 Coffee - Conference Hall 2

15:30-16:30 DRM and Multimedia Security (Part One) (session chair: Herbert Leitold)

Compression of Encrypted Visual Data
Michael Gschwandtner, Andreas Uhl and Peter Wild

Equivalence Analysis among DIH, SPA and RS Steganalysis Methods
Luo Xiangyang, Yang Chunfang and Liu Fenlin

16:30-17:30 Keynote Two: Between (Little) Hope and (Much) Fear: Security Measures and Future Threats; Herbert Bos, Vrije Universiteit Amsterdam

20:00 Conference Dinner – Fontana Amorosa (Aldemar Knossos Royal Village hotel)
DAY TWO  
Friday 20. October 2006

9:00-10:00  Keynote Three: FP7: Status of the ICT Work programme  
Antonis Galetsas, European Commission

10:00-10:30  Coffee - Conference Hall 2

10:30-12:00  Web and XML Security  
(special chair: Peter Lipp)
Adding Support to XACML for Dynamic Delegation of Authority in Multiple Domains,  
David W Chadwick, Sassa Otenko and Tuan Anh Nguyen

One-Round Protocol for Two-Party Verifier-Based Password-Authenticated Key Exchange,  
Jeong Ok Kwon, Kouichi Sakurai and Dong Hoon Lee

Enhanced CAPTCHAs: Using Animation To Tell Humans And Computers Apart  
Elias Athanasopoulos and Spiros Antonatos

Cryptography  
(special chair: Howard Chivers)

Perturbing and Protecting a Traceable Block Cipher  
Julien Bringer, Hervé Chabanne and Emmanuelle Dottax

A new Encryption and Hashing Scheme for the Security Architecture for Microprocessors,  
Jörg Platte, Raúl Durán Díaz and Edwin Naroska

Timed Release Cryptography from Bilinear Pairings using Hash Chains  
Konstantinos Chalkias and George Stephanides

12:00-13:30  Lunch - main restaurant (Aldemar Knossos Royal Village hotel)

13:30-15:00  Privacy and Data Protection  
(special chair: Bart De Decker)

PPINA - A Forensic Investigation Protocol for Privacy Enhancing Technologies  
Giannakis Antoniou, Campbell Wilson and Dimitris Geneiatakis

A Privacy Agent in Context-Aware Ubiquitous Computing Environments  
Ni (Jenny) Zhang and Chris Todd

Ensuring Privacy in Smartcard-based Payment Systems: A Case Study of Public Metro Transit Systems,  
Seng-Phil Hong and Sungmin Kang

Network and Information Security Analysis and Modelling  
(Evangelos Markatos)

Attack Graph based Evaluation of Network Security  
Igor Kotenko and Mikhail Stepashkin

Information Modeling for Automated Risk Analysis  
Howard Chivers

Towards Practical Attacker Classification for Risk Analysis in Anonymous Communication,  
Andriy Panchenko and Lexi Pimenidis

15:00-15:30  Coffee - Conference Hall 2

15:30-16:30  DRM and Multimedia Security (Part Two)  
(Angelos Bilas)

Selective Encryption of Hierarchical MPEG  
Heinz Hofbauer, Thomas Stütz and Andreas Uhl

A Flexible and Open DRM framework  
Kristof Verslype and Bart De Decker

16:30-17:30  Keynote Four: Cryptographic hash functions: dead or alive?  
Bart Preneel, KU Leuven

20:00-  Dinner – Villas restaurant (Aldemar Knossos Royal Village hotel)
DAY THREE  Saturday 21. October 2006

Secure Communication of certificates and transcripts between European Universities in the spirit of the Bologna process

9:00-13:00  Workshop - Conference Hall 2

Talks:

Problem description:
e-archive and e-communication of University academic transcripts and testamurs (diplomas). Standardized interfaces for the Inter-University workflow. Access and protection, availability and trust.
Rüdiger Grimm Koblenz, Germany

Trust relationships and interfaces for transcripts; discussion of digitally signed transcripts.
Scott Rea and/or Registrar’s office, Dartmouth, USA

E-application to the Bachelor and Master courses at ETH.
Bernhard Plattner and/or registrar’s office, Zürich, Switzerland

POLITO approach to e-transcripts in Universities.
Certification of e-documents in public administration, including acceptance of University transcripts.
Antonio Lioy, Torino, Italy

Models and an Architecture for secure and legally correct Process Communication for Students and Universities according to the Bologna Process Infrastructure based on the eGovernment Standard OSCI.
Hermann Strack, Harz, Germany

Suggestion for a technical solution by X.509 attribute certificates and SAML
David Chadwick, Kent, UK

A pk certificate creation software as a basic technology, developed by TU Graz and possibly available to all Universities for research.
Peter Lipp, Graz, Austria