



The 10<sup>th</sup> IFIP TC6 and TC11 Open Conference on  
**Communications and Multimedia Security**  
19 - 21 October 2006, Heraklion, Greece

---

## CALL FOR PARTICIPATION TENTATIVE PROGRAMME

---

### COMMITTEES

#### **Programme Co-Chairs**

Herbert Leitold  
A-SIT

Prof. Evangelos P. Markatos  
FORTH & University of Crete

#### **Programme Committee**

See the conference website  
<http://www.ics.forth.gr/cms06/>

#### **Organizing Committee Chair**

Prof. Angelos Bilas  
FORTH & University of Crete

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 10<sup>th</sup> 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*

<b><u>DAY ONE</u></b>	Thursday 19. October 2006
08:00-08:45	<u>Registration</u>
08:45-09:00	<u>Welcome</u> <i>Evangelos Markatos, FORTH ICS</i>
09:00-10:00	<u>Keynote One</u> <i>Andrea Pirotti, ENISA</i>
10:00-10:30	<u>Coffee</u>
10:30-12:00	<u>Applied Network and Information Security</u>  Computing of Trust in Ad-hoc Networks <i>Huafei Zhu, Feng Bao and Jianwei Liu</i>  TAO: Protecting against Hitlist Worms using Transparent Address Obfuscation <i>Spiros Antonatos and Kostas Anagnostakis</i>  On The Privacy Risks of Publishing Anonymized IP Network Traces <i>Dimitris Koukis, Spiros Antonatos and Kostas Anagnostakis</i>
12:00-13:30	<u>Lunch</u>
13:30-15:00	<u>Identification and Authentication</u>  Secure Mobile Notifications of Civilians in Case of a Disaster <i>Heiko Rossnagel and Tobias Scherner</i>  A Fair Anonymous Submission and Review System <i>Vincent Naessens, Liesje Demuyne and Bart De Decker</i>  Attributes Delegation Based on Ontologies and Context Information <i>Isaac Agudo, Javier Lopez and Jose A. Montenegro</i>
15:00-15:30	<u>Coffee</u>
15:30-16:30	<u>DRM and Multimedia Security (Part One)</u>  Compression of Encrypted Visual Data <i>Michael Gschwandtner, Andreas Uhl and Peter Wild</i>  Equivalence Analysis among DIH, SPA and RS Steganalysis Methods <i>Luo Xiangyang, Yang Chunfang and Liu Fenlin</i>
16:30-17:30	<u>Keynote Two</u> <i>Herbert Bos, Vrije Universiteit Amsterdam</i>
20:00-	<u>Conference Dinner</u>

### **Organized and supported by:**



<http://www.ics.forth.gr>



<http://www.enisa.eu.int>



<http://www.a-sit.at>



### CONFERENCE VENUE

CMS2006 will take place in Hersonissos, Crete, Greece. Hersonissos is a small town ca. 30km from Heraklion and its airport.

The venue of the conference is Aldemar Knossos Royal Village hotel, a magnificent resort place located on the north coast of the island

Special, low rates are offered to CMS2006 participants:

Proceed to the conference site for the hotel reservation form

<http://www.ics.forth.gr/cms06/>

### CONFERENCE REGISTRATION

Online via conference website

<http://www.ics.forth.gr/cms06/>

#### Early Registration

(before 31 August 2006)

Students	€ 350
Standard	€ 450

#### Late Registration

(from 1 September 2006)

Students	€ 420
Standard	€ 520

CMS registration fees include conference sessions, coffee breaks, two lunches, two dinners, proceedings.

### CONFERENCE PROCEEDINGS

The conference proceedings will be available at the conference.

The proceedings will be published by Springer, Lecture Notes in Computer Science (LNCS)

## DAY TWO Friday 20. October 2006

9:00- 10:00 Keynote Three  
*European Commission (to be confirmed)*

10:00-10:30 Coffee

10:30-12:00 Web and XML Security  
*Parallel Session*

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

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

13:30-15:00 Privacy and Data Protection  
*Parallel Session*

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

Attack Graph based Evaluation of Network Security  
*Igor Kottenko 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

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

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

## DAY THREE Saturday 21. October 2006

9:00- 13:00 Co-located E-Government Workshop on secure communication of certificates among European Universities  
see <http://www.ics.forth.gr/cms06/workshops.html> for details