24th IFIP International Information Security Conference

May 18-20, 2009 Coral Beach Hotel
Pafos, Cyprus

www.sec2009.org

Conference Program

Welcome

As General Chairs of the 24th IFIP International Information Security Conference (SEC-2009) and on behalf of the Cyprus Computer Society we would like to extend a very warm welcome to all of you who have decided to join us here in Pafos, Cyprus.

This year marks a special occasion for the Cyprus Computer Society as we celebrate twenty five years of service to the IT professional community in Cyprus. Our effort was to make this conference both an enjoyable event as well as a scientifically significant one and we believe we have succeeded in both respects.

The selection of the conference site aimed at providing the level of enjoyment that is reserved to holiday destinations. Pafos has traditionally offered a variety of places and things to experience: from *Petra tou Romiou* the mythological birthplace of the Greek goddess of love Aphrodite located at the southern part of Pafos all the way to the baths of Aphrodite at the very tip of the Akamas peninsula near the northwestern end of Cyprus. We wish that you also take this opportunity to visit the area as it offers great opportunities for sight seeing to places unique here in Cyprus.

A testament to the scientific significance is the competitiveness of the conference: out of 176 papers submitted 39 were accepted representing an acceptance rate of 22%. All of the papers were evaluated on the basis of their novelty and technical quality, and reviewed by at least two members of the conference program committee.

The conference is divided into three tracks, two being reserved for paper presentations and the third being reserved for the co-located *FIDIS - Challenges and Opportunities* event and the WG11.1/WG11.8 Panel on Common Bodies of Knowledge (CBKs) and Security Certifications.

At this point we would like to take this opportunity to thank our distinguished keynote speakers, namely Prof. Bart Preneel (Katholieke Universiteit Leuven) and Mr. Christos Ellinides (European Commission/DIGIT) for accepting our invitation and for honoring the conference with their presence and their inspired talks. We would also like to thank this year's Kristian Beckman Award winner Professor Klaus Brunnstein for accepting this award and joining us here in Pafos. We are honored.

Hosting the flagship IFIP International Security Conference is a task that requires the commitment of many people. We would like to take this opportunity to thank the PC Chairs Prof. Dimitri Gritzali of the Athens University of Economics and Business and Prof. Javier Lopez of the University of Malaga who have done a superb job of putting together the conference program and managing the conference Proceedings, the program committee and the additional reviewers for making the paper selection process a competitive one, all of the attendees who have honored us with their presence and last but not least the local organizing committee and its lead, Yiannos Aletraris for without this conference would not be possible.

Thank you, have an enjoyable stay and a fruitful conference.

Dr Philippos Peleties and **Panikos Masuras**
SEC2009 General Chairs

Organization

General Chairs

Philippos Peleties, *Cyprus Computer Society, Cyprus*

Panikos Masouras, *Cyprus Computer Society, Cyprus*

Program Chairs

Dimitris Gritzalis, *Athens University of Economics & Business, Greece*

Javier Lopez, *University of Malaga, Spain*

Program Committee

Vijay Atluri, *Rutgers University, USA*

Lujo Bauer, *Carnegie Mellon University, USA*

Joachim Biskup, *Technical University of Dortmund, Germany*

Jan Camenisch, *IBM Research, Switzerland*

Bart de Decker, *Katholieke Universiteit Leuven, Belgium*

Yves Deswarte, *LAAS-CNRS, France*

Ed Dawson, *Queensland University of Technology, Australia*

Jan Eloff, *University of Pretoria, South Africa*

Simone Fischer-Huebner, *Karlstad University, Sweden*

Debora Frincke, *Pacific Northwest National Laboratory, USA*

Steven Furnell, *University of Plymouth, United Kingdom*

Sushil Jajodia, *George Mason University, USA*

Lech Janczewski, *University of Auckland, New Zealand*

Sokratis Katsikas, *University of Piraeus, Greece*

Costas Lambrinoudakis, *University of the Aegean, Greece*

Fabio Martinelli, *National Research Council, Italy*

Natalia Miloslavskaya, *MEPHI, Russia*

Refic Molva, *Institut Eurecom, France*

Kostas Moulinos, *ENISA, European Union*

Yuko Murayama, *Iwate Prefectural University, Japan*

Eiji Okamoto, *University of Tsukuba, Japan*

Rolf Oppliger, *eSecurity, Switzerland*

George Pangalos, *Aristotle University of Thessaloniki, Greece*

Jong-Hyuk Park, *Kyungnam University, South Korea*

Gunther Pernul, *University of Regensburg, Germany*

Bart Preneel, *Katholieke Universiteit Leuven, Belgium*

Sihan Qing, *Chinese Academy of Sciences, China*

Kai Rannenberg, *Goethe University Frankfurt, Germany*

Rodrigo Roman, *University of Malaga, Spain*

Pierangela Samarati, *University of Milan (Bicocca), Italy*

Sujeet Shenoi, *University of Tulsa, USA*

Miguel Soriano, *Technical University of Catalonia, Spain*
Willy Susilo, *University of Wollongong, Australia*
Stefanie Teufel, *University of Freiburg, Switzerland*
Bill Tsoumas, *Ernst & Young, Greece*
Gene Tsudik, *University of California (Irvine), USA*
Rossouw von Solms, *Nelson Mandela Metropolitan University, South Africa*
Tatjana Welzer, *University of Maribor, Slovenia*
Stephen Wolthusen, *Gjovik University College, Norway*
Louise Yngstrom, *University of Stockholm, Sweden*
Jianying Zhou, *I2R, Singapore*

Local Organizing Committee
Yiannos Aletraris, *Cyprus Computer Society*
Michalis Georgiou, *Cyprus Computer Society*
George Beitis, *Cyprus Computer Society*
Elena Stylianou, *Cyprus Computer Society*

FIDIS Summit Committee
Kai Rannenberg, *Goethe University Frankfurt, Germany*
Denis Royer, *Goethe University Frankfurt, Germany*
André Deuker, *Goethe University Frankfurt, Germany*

DAY 1

Monday, May 18, 2009

8:30 AM	9:00 AM	Registration Room: Akamas		
9:00 AM	9:30 AM	Welcome Room: Akamas A		
9:30 AM	10:30 AM	Keynote speech: Prof. Bart Preneel, Katholieke Universiteit Leuven, Belgium *Research Challenges In Applied Cryptology* Room: Akamas A		
10:30 AM	11:00 AM	Coffee/Tea		
		Session 1A: Identification and Authentication I **Room: Akamas A**	**Session 2A: Threats and Attacks** **Room: Akamas B**	**Session 3A (FIDIS): Introduction - What is Identity?** **Room: Akamas C**
11:00 AM	11:30 AM	Flexible and Transparent User Authentication for Mobile Devices N. Clarke, S. Furnell, S. Karatzouni	Roving Bugnet: Distributed Surveillance Threat and Mitigation R. Farley, X. Wang	The Future of Identity in the Information Society (FIDIS) - Challenges and Opportunities Details: www.fidis.net
11:30 AM	12:00 AM	Combining Authentication, Reputation and Classification to make Phishing Unprofitable A. Herzberg	On Robust Covert Channels Inside DNS L. Nussbaum, P. Neyron, O. Richard	
12:00 AM	12:30 AM	Audio CAPTCHA for SIP-based VoIP Y. Soupionis, G. Tountas, D. Gritzalis	Discovering Application-level Insider Attacks using Symbolic Execution K. Pattabiraman, N. Nakka, Z. Kalbarczyk, R. Iyer	
12:30 PM	2:00 PM	Lunch		
		Session 1B: Identification and Authentication II **Room: Akamas A**	**Session 2B: Applications of Cryptography and Information Hiding** **Room: Akamas B**	**Session 3B (FIDIS): Identity in a High-Tech World** **Room: Akamas C**
2:00 PM	2:30 PM	Custom JPEG Quantization for Improved Iris Recognition Accuracy A. Uhl, G. S. Kostmajer, H. Stögner	Media-break resistant eSignatures in eGovernment - An Austrian Experience H. Leitold, R. Posch, T. Roessler	The Future of Identity in the Information Society (FIDIS) - Challenges and Opportunities Details: www.fidis.net
2:30 PM	3:00 PM	On the IPP Properties of Reed-Solomon Codes M. Fernandez, J. Cotrina, M. Soriano, N. Domingo	How to Bootstrap Security for Ad-hoc Network: Revisited W. Shin, C. Gunter, S. Kiyomoto, K. Fukushima, T. Tanaka	
3:00 PM	3:30 PM	A Generic Authentication LOA Derivation Model L. Yao, N. Zhang	Steganalysis of Hydan J. Blasco, J. C. Hernandez, J. Estevez-Tapiador, A. Ribagorda, M. Orellana-Quiros	
3:30 PM	4:00 PM	Coffee/Tea		
		Session 1C: Trusted Computing **Room: Akamas A**	**Session 2C: Security Policies** **Room: Akamas B**	**Session 3C (FIDIS): Profiling & Forensics** **Room: Akamas C**
4:00 PM	4:30 PM	On the Impossibility of Detecting Virtual Machine Monitors J.-P. Seifert, S. Gueron	A Policy-based Approach for the Management of Web Browser Resources to Prevent Anonymity Attacks in Tor G. Navarro-Arribas, J. Garcia-Alfaro	The Future of Identity in the Information Society (FIDIS) - Challenges and Opportunities Details: www.fidis.net
4:30 PM	5:00 PM	Implementation of a Trusted Ticket System A. Schmidt, N. Kuntze, A. Leicher	A Policy Language for Modeling Recommendations A. Abou El Kalam, P. Balbiani	
7:30 PM	09:30 PM	Reception O' Solomon's Irish Pub		

DAY 2

Tuesday, May 19, 2009

9:00 AM	9:30 AM	Registration Room: Akamas		
9:30 AM	10:30 AM	Keynote speech: Christos Ellinides, European Commission (DIGIT) *E-Signatures: Vision and Orientation of the European Commission* Room: Akamas A		
10:30 AM	11:00 AM	Coffee/Tea		
		Session 1A: Validation, Verification, Evaluation **Room: Akamas A**	**Session 2A: Privacy Protection, Security Assessment** **Room: Akamas B**	**Session 3A (FIDIS): Privacy & Mobility** **Room: Akamas C**
11:00 AM	11:30 AM	On the Security Validation of Integrated Security Solutions S. Guergens, A. Fuchs, C. Rudolph	Collaborative Privacy - A Community-based Privacy Infrastructure J. Kolter, T. Kernchen, G. Pernul	The Future of Identity in the Information Society (FIDIS) - Challenges and Opportunities Details: www.fidis.net
11:30 AM	12:00 AM	Verification of Security Policy Enforcement in Enterprise Systems P. Gupta, S. Stoller	Security and Privacy Improvements for the Belgian eID Technology P. Verhaeghe, J. Lapon, B. De Decker, V. Naessens, K. Verslype	
12:00 AM	12:30 AM	Optimization of the Controlled Evaluation of Closed Relational Queries J.-H. Lochner, J. Biskup, S. Sonntag	A Structured Security Assessment Methodology for Manufacturers of Critical Infrastructure Components T. Brandstetter, K. Knorr, U. Rosenbaum	
12:30 PM	2:00 PM	Lunch		
		Session 1B: Role Mining and Content Protection **Room: Akamas A**	**Session 2B: Security Protocols** **Room: Akamas B**	**Session 3B (FIDIS): Interoperability & eGovernment** **Room: Akamas C**
2:00 PM	2:30 PM	Mining Stable Roles in RBAC N. V. Verde, A. Colantonio, R. Di Pietro, A. Ocello	NGBPA - Next Generation BotNet Protocol Analysis Felix Leder and Peter Martini	The Future of Identity in the Information Society (FIDIS) - Challenges and Opportunities Details: www.fidis.net
2:30 PM	3:00 PM	Privacy-Preserving Content-Based Publish/Subscribe Networks A. Shikfa, M. Onen, R. Molva	Non-Repudiation Analysis with LySa A. Cortesi, M. Bruso	
3:00 PM	3:30 PM	Broadcast Encryption for Differently Privileged H. Jin, J. Lotspiech	A Provably Secure Secret Handshake with Dynamic Controlled Matching A. Sorniotti, R. Molva	
3:30 PM	4:00 PM	Ontology-based Secure XML Content Distribution M. A. Rahaman, Y. Roudier, P. Miseldine, A. Schaad	Towards a Theory of White-Box Security A. Herzberg, H. Shulman, A. Saxena, B. Crispo	
4:00 PM	4:30 PM	Coffee/Tea		
4:30 PM	5:30 PM	Panel discussion / Round table *Trust and security initiatives: The role of the academic and industry Sectors* Room: Akamas A Moderator: Dimitris Gritzalis, Professor, Athens University of Economics & Business Panelists: Christos Ellinides, Director, Corporate IT Solutions and Services (DIGIT/A), European Commission Jacques Bus, Head, Trust and Security (INFSO/D/F5), European Commission Kyriakos Kokkinos, Managing Director, IBM Italia (Cyprus) Ltd		
7:30 PM	10:30 PM	Gala Dinner Metohi Tavern – Polemi Village		

DAY 3

Wednesday, May 20, 2009

8:30 AM	9:00 AM	Registration Room: Akamas		
9:00 AM	9:30 AM	Best Paper Award Session Room: Akamas A		
9:30 AM	10:30 AM	Kristian Beckman Award Session Professor Klaus Brunnstein *About ICT Security and Safety in the Banking Industry* Room: Akamas A		
10:30 AM	11:00 AM	Coffee/Tea		
		Session 1A: Access Control **Room: Akamas A**	**Session 2A: Internet and Web Applications Security** **Room: Akamas B**	**Session 3A** **Room: Akamas C**
11:00 AM	11:30 AM	On a Taxonomy of Delegation Q. Pham, J. Reid, A. McCullagh, E. Dawson	In Law we Trust? Trusted Computing and Legal Responsibility for Internet Y. Danidou, B. Schafer	WG11.1/WG11.8 Panel: Common Bodies of Knowledge (CBKs) and Security Certifications - do they meet the need?
11:30 AM	12:00 AM	Efficient Key Management for Enforcing Access Control in Outsourced Scenarios C. Blundo, S. Cimato, S. De Capitani di Vimercati, A. De Santis, S. Foresti, S. Paraboschi, P. Samarati	Persona: Network Layer Anonymity and Accountability for Next Generation Internet Y. Mallios, S. Modi, A. Agarwala, C. Johns	
12:00 AM	12:30 PM	A Probabilistic Bound on the Basic Role Mining Problem and its Applications N. V. Verde, A. Colantonio, R. Di Pietro, A. Ocello	Jason: A Scalable Reputation System for the Semantic Web S. Steinbrecher, S. Groß, M. Meichau	
12:30 PM	1:00 PM	Automating Access Control Logics in Simple Type Theory with LEO-II C. Benzmueller	Which Web Browsers Process SSL Certificates in a Standardized Way? A. S. Wazan, R. Laborde, D. Chadwick, F. Barrere Abdelmalek Benzekri	
1:00 PM	1:30 PM	Closing Plenary Room: Akamas A		


1960-2010
50
ifip


Cyprus
Computer
Society
25