

ENISA - FORTH
Summer School

on Network & Information Security

14-18 September 2009, Crete, Greece

Theme: Privacy and Trust in a Networked World



Privacy & Security: a fine balancing act

Privacy & Security: a fine balancing act

The European Network and Information Security Agency (ENISA) and the Institute of Computer Science (ICS) of the Foundation for Research and Technology - Hellas (FORTH) welcome you to the 2nd ENISA-FORTH Summer School on Network and Information Security (NIS'09), that they jointly organise. Following the success of NIS'08, this year's summer school will take place in the Heraklion area, Crete, Greece, on 14-18 September 2009. This year's theme is "Privacy and Trust in a Networked World". An exciting programme leverages on invited lecturers to cover a range of topics extending beyond pure technological areas to encompass economic, policy and legal issues alike.

Network and Information Security (NIS) has emerged as a fundamental aspect of Information and Communication Technologies (ICT) and its widespread adoption for improving productivity, learning and leisure. While creating new opportunities for growth in European economy and for improving quality of life for its citizens, constant advances in ICT pose new challenges to NIS, requiring a high-level of alertness, solid understanding of technology and trends, and continuous adjustment of strategic options. Therefore, raising awareness and understanding on the issues involved in NIS is of paramount importance. In this perspective ENISA and FORTH have jointly taken the initiative to set up and support this Summer School. The Summer School aims at providing a forum for experts in Information Security, policy makers from EU Member States and EU Institutions, decision makers from the industry, as well as members of the research and academic community, to interact on cutting-edge and ground breaking topics in Network and Information Security.

www.nis-summer-school.eu

about ENISA

ENISA is mandated to assist the European Commission and the Member States of the European Union in ensuring the higher levels of network and information security.



The Agency's tasks are focused on collecting and analysing data on security incidents and emerging risks, establishing public/private partnerships with industry, promoting risk assessment methods and best practices, raising awareness on network and information security and tracking the development of standards for products and services in the Network and Information Society.

ENISA - defending the future

Every day people experience the Information Society. Interconnected networks are touching our everyday lives, at home and at work. It is therefore vital that e.g. computers, mobile phones, banking, high-tech cars and the Internet function securely, as they constitute the "Digital Economy", where threats are abound. That is why ENISA is working on Network and Information Security for the EU and the Member States.

about FORTH-ICS

Research and Technology for the Information Society

The Institute of Computer Science (ICS) is one of the seven institutes of the Foundation for Research and Technology - Hellas (FORTH), a major national research centre partly funded by the General Secretariat for Research and Technology of the Hellenic Ministry of Development. The mission of FORTH-ICS is to perform high quality basic and applied research, to promote education and training, and to contribute to the development of the Information Society, at a regional, national, and European level.

Since its establishment in 1983, FORTH-ICS has had a long history and recognized tradition in conducting basic and applied research, and playing a leading role, in Greece and internationally, in the field of Information and Communication Technologies.





Dear Participants,

It is our pleasure to welcome you to the **2nd Network and Information Security (NIS) Summer School**, taking place in Crete, Greece, 14-18 September 2009. This event is jointly organised by the European Network and Information Security Agency (**ENISA**) and the Institute of Computer Science of the Foundation for Research and Technology - Hellas (**FORTH-ICS**).

This Summer School has a special "Theme" and a fresh look each year, focusing on cutting-edge topics that guide the selection of the faculty each time. The theme for the 2009 NIS Summer School is **"Privacy and Trust in a Networked World"**.

Why have we chosen this focus area?

Today, accessibility is of paramount importance for taking advantage of all the benefits offered by advances on technologies such as eID cards, wireless ubiquitous connectivity, etc. These technological advances are made to benefit both the economy of Europe and the citizens / users alike. At the same time, questions regarding privacy and security emerge, and Europe finds itself at cross roads. In the case of eID cards, presently ten national eID card schemes are already in use across the EU, and thirteen more are planned. Yet, the privacy features of these cards have been developed, implemented and tested only at national level. Thus, it appears that there is no co-ordinated strategy at European level addressing which -and how- privacy features should be implemented. This is an important obstacle for cross border eID interoperability.

ENISA is dedicated to promoting a culture of security in Europe that will impact positively on the ability of EU Member States to respond to cyber-attacks. It does so by pursuing a strategy of mitigating risks through awareness, studies, reports and Position Papers on current NIS matters. Towards this objective, ENISA and FORTH-ICS, bring together in this Summer School a distinguished faculty from around the world that will identify current trends, threats and opportunities against the background of recent advances on NIS measures and policies. Recognising the multi-dimensional facets of the Privacy and Security theme, an array of lectures will cover a variety of key aspects on policy, legal, academic and research matters. Our audience includes policy makers from EU Member States and EU Institutions, decision makers from industry, and members of the academic and research community.

We would like to thank our keynote speakers and faculty for contributing to a programme of such high quality and we are confident that the participants of the Summer School will both benefit from and enjoy the programme.

Andrea Pirotti

Executive Director of ENISA



Constantine Stephanidis

Director of FORTH-ICS



t

theme - topics

Privacy and Security in e-Citizen Services

eCitizen services span across different areas of applications regarding eGovernment, eHealth etc., mainly aiming at enhancing the quality of life of the citizens, by facilitating their interaction with the public services and modernising public administration procedures. The importance of these services and the challenges and concerns regarding information security and privacy posed by the introduction of new technologies in the provision of these services make it an important area for the NIS Summer School.

The aim of this session is thus to provide an overview of these main challenges from different viewpoints and discuss recommended solutions to address them. The four planned lectures, which will be given from speakers from different backgrounds (social, legal & data protection, IT security etc.), will cover various aspects of the discussion on eCitizen services and the information security and privacy considerations that are currently posed, so that participants may gain a better understanding of these services and challenges they pose.

Notably, new technologies are used or are expected to be introduced with a view to enhancing the provision of these services, such as Web2.0 technologies, RFID applications, mobile communications, the introduction of which is expected to improve the quality of the services offered. Therefore, an overview of these new services will be made, presenting what they really provide and the developments that are currently taking place, so that participants can have a clearer idea of what eCitizen services are all about.

There are many key requirements to these services: sound identity management, interoperable authentication mechanisms, data protection measures in place are just some of the many challenges that governments face. Addressing these concerns and meeting these requirements is a priority in our society, since it is

imperative to ensure and foster the trust of citizens in these new "enhanced" services. This session will focus on these challenges and risks, providing to participants a substantial insight on this debate. The speakers are going to talk about significant information security and privacy risks and considerations that are raised at the moment and some that may also arise in the near future. In order to do so more effectively and to provide a better understanding of these issues, certain real-world examples and use cases from EU member states will be also brought in.

Possible measures currently proposed or envisaged will be also presented and discussed at length: such as the concept of privacy and security-by-design, while also privacy impact assessments (PIA) will be presented in more detail, and its benefits and challenges will be further outlined. The topic of identity management, which is as mentioned above is very critical and plays a very significant and definitive role in this issue, is also going to be presented in more detail, specifically in relation with existing EU initiatives (e.g. STORK project: <http://www.eid-stork.eu/>). The legal aspect of privacy and data protection is equally important to consider, and thus one lecturer will focus on the legal implications and requirements.

Privacy and Security in Smart Environments

The pervasiveness of wireless communications technologies in our daily lives is now commonplace. Wireless networks are starting to be used extensively for both work and leisure purposes at home. Moreover, traditional methods of communication at home, such as telephones, are starting to migrate to wireless IP technologies. This trend results in private information such as pictures, videos, conversations and private information of individuals being transmitted over more vulnerable wireless media and protocols. This session will discuss emerging threats and solutions as well as projections on applications of related technologies.



S speakers

Enhancing Citizen's Confidence on Infrastructures

Reliable communications networks and services are now critical to public welfare and economic stability. Attacks on Internet, disruptions due to physical phenomena, software and hardware failures, and human mistakes all affect the proper functioning of public eCommunications networks. Such disruptions reveal the increased dependency of our society to these networks and their services.

The experience has revealed that any country, acting independently, may face difficulties in effectively preventing and responding to these type of attacks which often originate from beyond national and European borders.

European Commission's Communications highlight the importance of network and information security and resilience. They stressed the importance of dialogue, partnership and empowerment of all stakeholders to properly address these threats and especially citizen's confidence in infrastructures.

ENISA, fully recognizing this need, devised a Multi-annual Thematic Program (MTP) with the ultimate objective to collectively evaluate and improve the resiliency of public eCommunications in Europe and therefore enhancing citizen's confidence in infrastructures.

EU Commission's recent Communication on CIIP recognises the importance of the area and confirms ENISA's role and expertise in the field.

This session will provide to the policy makers useful insights about existing good practices deployed in Member States and private sector, ideas about possible future national and/or European actions/policies, and perspectives about co-operation among Member States and/or institutional stakeholders. It will offer to participants a holistic view of the problem giving mostly emphasis to policy makers. The main questions to be answered are:

- Why resilience of public eCommunications networks is important?
- Which measures (at policy, organisational or technical) were successfully deployed the last 3-5 years and had significant impact
- Which measures (at policy, organisational or technical) could further enhance the resilience of public eCommunications networks
- How Member States and relevant stakeholders could co-operate to address problems at national, cross-border, pan European and even international level? What might be the role of an institution like ENISA?

KEYNOTE SPEAKERS

- **Dr. Jorgo Chatzimarkakis**, Member of the European Parliament, EU
- **Dr. Silvia Adriana Ticau**, Member of the European Parliament, EU
- **Prof. Ioannis Tsoukalas**, Member of the European Parliament, EU
- **Dr. Joao Da Silva**, Director of the Network & Communication Directorate, European Commission, DG INFSO, EU
- **Dr. Peter Freeman**, Emeritus Dean and Professor, Georgia Institute of Technology, USA
- **Mr. Peter Hustinx**, Supervisor, European Data Protection Supervisor, EU

Privacy and Security in e-Citizen Services

- **Mr. David Wright**, Trilateral Research & Consulting, UK
- **Prof. Antonio Lioy**, Politecnico di Torino, IT
- **Mr. David Osimo**, Tech4i2 Ltd., UK
- **Mr. Marcus Hild**, Austrian Data Protection Commission, AT

Privacy and Security in Smart Environments

- **Dr. Valtteri Niemi**, Nokia Fellow, Nokia Research Center, Lausanne, CH
- **Dr. Panos Papadimitratos**, Senior Researcher, EPFL, CH

Enhancing Citizen's Confidence on Infrastructures

- **Mr. Peter Wallstrom**, Swedish Post and Telecom Agency, SE
- **Mr. Karl F. Rauscher**, Bell Labs, Alcatel-Lucent, USA
- **Mr. John Harrison**, LanditD, UK
- **Mr. Simon van Merkom**, Ministry of Economic Affairs, NL
- **Mr. Yves Le Roux**, CISM, CISSP, ITIL Principal Consultant, FR

Privacy and Security in Social Networks and 3D Social Worlds

- **Dr. Petros Belimpasakis**, Nokia Research Center, Tampere Laboratory, FI
- **Dr. Ian Brown**, Oxford Internet Institute, UK
- **Prof. Ronald Leenes**, University of Tilburg, NL
- **Prof. Richard Bartle**, University of Essex, UK

Privacy and Security in the Internet of Things

- **Mr. Michael Vanfelteren**, Legal Adviser, European Data Protection Supervisor, EU
- **Dr. Ari Juels**, RSA Laboratories, USA



Privacy and Security in Social Networks and 3D Social Worlds

The largest number of personal data profiles on the planet is held not in a government identity registry or one of the much heralded Federated Identity Providers but in the data warehouses of Social Networking providers. Online Social Networking Sites are now among the most visited websites globally. They collect and organise huge amounts of personal data - e.g. over 30 billion images on Facebook - and provide tools for managing that data. Although there has been strong pressure to offer stronger privacy, such providers' economic models rely on exploitation of their personal data stores.

Social networking is becoming the preferred (by end-users) way to manage personal data. It is an area where people take an active interest in how their personal information is managed and displayed rather than being passive account-holders as in most identity management systems. Social engagement provides a much-needed incentive for end-users to engage in processes such as setting privacy rules and providing feedback on spammers.

ENISA's position paper on social networks paper looked at security and privacy risks in using social networks, including image based search and the growing use of automated image tagging of images with profiles without the consent of the profile owner. ENISA's submission to W3C's workshop on the future of Social Networking submission also looked at how Social networks fulfil all the main criteria to qualify as mainstream Identity Management applications and how they are starting to be used as a central point in managing identity and ways of managing the risks associated with this use.

A new trend in Social Networks is convergence with immersive 3D worlds such as Habbo, Second Life, Kaneva and There. This new breed of social environment gives users a false sense of security with respect to their privacy because their online persona is represented by an avatar, but in fact the privacy risks are every bit as important in such 3D social environments. An ENISA report identifies 12 recommendations to tackle these and other security problems in this area, including key points for awareness-raising campaigns for users eg., on child-safety and privacy risks.

The ENISA survey of 1.500 respondents in the UK, Sweden and Germany shows that most users of virtual worlds think their avatar cannot reveal anything about their real identity. But an avatar is no different from using any online persona, particularly

in so-called "social worlds", i.e. hybrids between online games and social networks. People should take just as much care of their personal data in these environments as in any other online context. Bots can be sprinkled within virtual worlds to spread spam or advertise products, for example.

This session will provide both background necessary to understand the underlying issues as well as will discuss the current state-of-the-art.

Privacy and Security in the Internet of Things

The emergence of RFID technology has given rise to a broader topic, the Internet of Things (IOT). According to the IOT vision, all objects will carry a unique identity and have the ability to communicate via wireless communication links. In this setup numerous communication links occur every second between objects exchanging information and making decisions on behalf of their users without requiring the user's intervention. Large-scale adoption of this vision is expected to have a crucial impact on the organisation of industrial processes and on the competitiveness of enterprises. This implies an increased dependency of business and citizens on the underlying ICT infrastructures and the services they support, with increased concerns for security, privacy, and possible threats to civil liberties.



Dr. Jorgo Chatzimarkakis
Member of the European Parliament, EU

Dr. Jorgo Chatzimarkakis MEP is a member of the European Parliament Committee on Industry, Research and Energy and of the Committee on Budgetary Control. He was Rapporteur for the Competitiveness and Innovation Framework Programme. He is also a Substitute on the Committee on Agriculture and Rural Development and the Committee on Economic and Monetary Affairs. He was elected Member of the European Parliament for the German Liberal Party in 2004. Dr. Chatzimarkakis has been actively involved in developing directives on a wide range of subjects, most notably innovation issues (CIP), education and research policies (EIT), and CO2 emission reductions for the automotive industry (CARS 21).

Since 2006 Dr. Chatzimarkakis is a member of the Pharmaceutical Forum, a high level group designed to provide a political mandate for relevant public health issues. He launched the European Life Science Circle (ELSC), a platform to discuss relevant issues in the context of life sciences and pharmaceuticals.

He joined the German Young Liberals (Julis) in 1990 and the German Free Democratic Party (FDP) in 1991, of which he is a Member of the National Board. He is also Secretary General of the Regional FDP branch in Saarland.

From 1993 to 1996, Dr. Chatzimarkakis held the post of Science Policy Officer at the German Bundestag, before joining the Policy Planning Unit in the German Foreign Office. Founder of a Public Affairs Consultancy in 1999, he also lectured extensively at Duisburg University and University of Saarland on political science and information sciences. He is also President of the DHW (German-Hellenic Economic Association). Dr. Chatzimarkakis studied agriculture and political sciences in Bonn and Oxford, he holds a PhD in political science, obtained from the University of Bonn in 2000.



Dr. Silvia - Adriana Ticau
Member of the European Parliament, EU

Dr. Silvia Adriana Ticau became a Member of the European Parliament on 1 January 2007 with the accession of Romania to the European Union. She holds a Masters Degree in Business Administration (Open University Business School, UK, 1996- 2001) and a Post-graduate Degree in Security of E-Government Systems (Military Technical Academy, Bucharest, from 2002), as well as a Post-graduate Degree in Economic Benefits of Online Public Services (Paris Dauphine University, from 2004).

In 2001, she was Director-General for Information Technology and Information Society Development Strategy at the Ministry for Communications and Information Technology and, from 1999 to 2000, Director of Operations, SC Tc. Inf. SA.

From 2001 to 2004, she was State Secretary for Information Technology and then Minister of Communications and Information Technology in 2004, after which she became a Member of the Romanian Senate and, in 2006, an Observer in the European Parliament.

Dr. Ticau is Vice-President of the Social Democratic Party (Galati county branch, from 2005), a Member of the Social Democratic Party National Executive (from 2004) and of the Social Democratic County Executive (Galati, from 2001).

She is Secretary of the Committee on Equal Opportunities, Romanian Senate (from 2004), and a Member of the Committee on Economic Affairs, Industry and Services, Romanian Senate (from 2004). She is also Member of the National Order of "Serviciul Credincios" ("Faithful Service") - Cavalier, 2002.



Prof. Ioannis Tsoukalas
Member of the European Parliament, EU

Prof. Ioannis Tsoukalas was born and educated in Thessaloniki, where he also started his professional carrier, he graduated in Physics and obtained his PhD from the Aristotle University of Thessaloniki. He carried out postdoctoral research in the UK (Liverpool), France (Grenoble), Germany (TH Braunschweig), and USA (MIT, Boston). In 1986 he was elected Professor at the Department of Physics, where he served as its Head, three times.

His main research interests are in the field of solid state physics and technological materials. He has published a large number of articles in peer reviewed international journals, has written textbooks, has taught graduate and postgraduate courses, and has supervised 36 PhD theses.

From 1991 to 1993, he was responsible for the installation of the first LAN at the Aristotle University of Thessaloniki, covering 26 buildings. He was the Founder and first Head of the Department of Informatics of the Aristotle University of Thessaloniki (1995-1999). He has served as Vice-President of the Research Committee of the Aristotle University of Thessaloniki (1999-2004) and President of the International Relationships Committee and of the Ethics Committee. At national level, he has served in the Executive Committees of "Information Society S.A." and "Hellenic Data Protection Authority".

From 2004 to 2008, he was the General Secretary for Research and Technology at the Hellenic Ministry of Development. From September 2008 he is Professor Emeritus at the Aristotle University of Thessaloniki, and from June 2009 Member of the European Parliament.



Dr. Joao Da Silva

Director of the Network and Communication Directorate, European Commission, DG INFSO, EU

Dr. Joao Schwarz Da Silva is the holder of a PhD in Computing and Systems Engineering from Carleton University, Ottawa, Canada. Over the last 35 years he has successively worked for the Government of Canada and for the International Telecommunications Union in Geneva. He joined the European Commission in 1991 where he is currently Director of the Converged Networks and Services Directorate of DG-INFSO where he oversees all the R&D work relating to mobile communications, broad-band networks including satellite communications, audio-visual and home networks; software engineering and ICT for enterprise applications. He is responsible for Challenge 1 within the current ICT-FP7 programme. He is the recipient of several awards including the UMTS Forum, the IPv6 Forum and the Wireless World Research Forum.

He is the author of some 50 technical and scientific papers and numerous presentations.



Mr. Peter Hustinx

Supervisor, European Data Protection Supervisor, EU

Mr. Peter J. Hustinx (1945) has been European Data Protection Supervisor since January 2004. He was appointed by a joint decision of the European Parliament and the Council of 22 December 2003 for a term of five years. He has been closely involved in the development of data protection legislation from the start, both at the national and at the international level. Before entering his office, he was President of the Dutch Data Protection Authority for more than twelve years.

In 1970 he graduated as Master of Law (*"cum laude"*) at the University of Nijmegen (Netherlands), and in 1971 he obtained an MCL degree at the University of Michigan Law School in Ann Arbor (USA).

From 1971 to 1975 he was legal adviser at the Dutch Ministry of Justice, Division for Constitutional and Criminal Law. From 1972 to 1976 he was Deputy Secretary of the Royal Commission on Privacy and Personal Data (*"Koopmans-Commission"*). From 1975 to 1991 he was legal adviser in the Dutch Ministry of Justice, Division for Public Law Legislation. From 1979 to 1991 he was General Counsel in this Division.

From 1976 to 1991 he was member of the Council of Europe's Committee of Experts on Data Protection. From 1985 to 1988 he was Chairman of this committee.

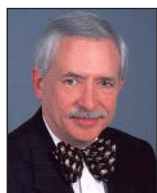
In 1991 he was appointed as President of the Dutch Data Protection Authority for a term of six years. In 1997 and 2003 he was re-appointed (*"Registratiekamer"*, since 2001 *"College bescherming persoonsgegevens"*).

From 1996 to 2000 he was Chairman of the Article 29 Data Protection Working Party (established under Directive 95/46/EC).

From 1998 to 2001 he was Chairman of the Appeals Committee of the Supervisory Body for Europol (established under Article 24 Europol Convention).

In 2002 he was elected Chairman of the Commission for the Control of Interpol's Files for a term of three years. In 2005 he was elected for a second term.

Since 1986 he has also been deputy judge at the Court of Appeal in Amsterdam.



Dr. Peter Freeman
*Emeritus Dean and Professor, Georgia
 Institute of Technology, USA*

Dr. Peter A. Freeman is Dean Emeritus and was Founding Dean of the College of Computing from 1990 to 2002. He continues to work with Georgia Tech on specific projects and is a Director with the Washington Advisory Group.

From 2002 to 2007, he was Assistant Director of NSF, heading the Computer & Information Science & Engineering Directorate. He previously held positions at George Mason University, NSF, the University of California, Irvine, and Carnegie-Mellon University. He is a resident of Washington, DC.

He has focused his attention for the past twenty years on national policy and local action intended to advance science and engineering research and education. For more than thirty years, he has been active internationally teaching, lecturing, and consulting overseas for extensive periods.

As a Director at the Washington Advisory Group, he advises on university and R&D strategy and management, especially in information technology, cyber-infrastructure, research networks, and software development. The Washington Advisory Group provides strategic counsel and management consulting to the leaders of companies, universities, governments and non-profit organizations. It was founded in 1996 by a group of leaders in national science policy and research funding, including Erich Bloch, Frank Press, and Bob White.

Dr. Freeman held the first endowed dean's chair at Georgia Tech. Under his leadership, the College of Computing became one of the strongest and largest computing research and education groups in the country. In 1998, he chaired the Sam Nunn NationsBank Policy Forum on information security, which led to the creation of the Georgia Tech Information Security Center, a comprehensive center focused on information security. From 1992 to 1995, he also acted as the university's Chief Information Officer and was a key part of the team that prepared the campus to host the 1996 Olympics.

As an Assistant Director of NSF he was part of the senior management team that helped formulate national science policy and that operated the NSF. As AD/CISE, he oversaw a staff of approximately 100 and a funding budget of over \$500M/year. CISE is responsible for over 85% of the Federal funding for fundamental computer science research in academia. As the senior computing research official in the U.S. Government, he led the inter-agency NITRD Subcommittee that coordinates all Federal Networking and IT R&D. At NSF, he was also responsible for insuring that the U.S. computing research community was well connected internationally. During his time as AD/CISE, Dr. Freeman was responsible for a number of activities that have had a major impact on computing, including: leading the Information Technology

Research Program, overseeing a comprehensive reorganization of the CISE Directorate, leading the elevation of cyberinfrastructure to a major activity across NSF, initiating the GENI Internet Research project, coordinating homeland security research across NSF, and starting several key CISE programs including Broadening Participation in Computing, Science of Design, and the Computing Community Consortium. As a division director at NSF in the 1980's he was part of a small team that drafted the Government's influential High-Performance Computing Initiative.

Dr. Freeman is widely recognised for his technical and educational activities in software systems and software engineering, and computer science and information technology more generally. In addition to his academic and research activities, he is an experienced university and government executive and manager, and a seasoned lecturer and consultant to corporations, governments, and universities in more than a dozen countries.

His research and technical expertise is focused on software systems and software engineering, and computer science more broadly. He co-authored *"The Supply of Information Technology Workers in the United States"* and authored *"Software Perspectives: The System is the Message"*, *"Software Systems Principles"*, and numerous technical papers. In addition, he edited or co-edited four books including, *"Software Reusability"* and *"Software Design Techniques"*.

Security and Virtual Worlds

Virtual worlds are massively multiplayer online spaces through which and with which players interact. Whether they are game worlds (such as World of Warcraft) or social worlds (such as Second Life), they face not only the usual security issues, but also a number of problems particular to them. This talk identifies the main dangers faced by developers and players, and describes the solutions that have been adopted to mitigate their effects.

From Social Networks and Web Mash-ups towards Mixed Reality

As social networking sites are being widely adopted and used, by people of all market segments, the amount of information shared there is constantly growing. We first present different privacy practices and policies in online social networks, with some example stories of things that “turned bad”, when personal information was not used as originally intended. Further more, as mash-ups allow information to flow among different services and sites, in a loosely coupled manner, we will analyse the typically associated security and privacy threads, along with state-of-the-art solutions. Finally, as the Internet is moving outside the standard personal computers and mobile devices, basic elements will be presented about the next generation Internet services, where the real and the digital world fuse, towards mixed reality.

Privacy and security by design

A plague of malware, Denial of Service attacks and data breaches is causing ongoing damage to Europe’s digital economy and to citizens’ trust in the online world. How could information systems be better designed in order to significantly reduce this damage? What should policymakers do to incentivise government agencies, companies and users to improve Internet security? And how we can provide a more stable and resilient technological infrastructure to underpin our information societies?



Prof. Richard Bartle
University of Essex, UK

Prof. Richard A. Bartle co-wrote the first virtual world, MUD, in 1978; he has thus been at the forefront of the industry from its very inception. He divides his time equally between being an industry consultant and an academic specialising in virtual worlds. His 2003 book, "Designing Virtual Worlds", is the standard text on the subject, and he is an influential writer on all aspects of virtual world design and development.



Dr. Petros Belimpasakis
Nokia Research Center, Tampere Laboratory, FI

Dr. Petros Belimpasakis joined Nokia Research Center in 2000 where he has been working in the area of home networking, ubiquitous computing and Internet mash-ups, in many different internal and external collaboration projects. Since the beginning of 2009 his work has been focused in Mixed Reality, namely life-logging, mobile augmented reality and mirror worlds. He is currently a Principal Researcher, located in Tampere, Finland. Dr. Belimpasakis received his B.Sc. in Mathematics from Aristotle University of Thessaloniki, Greece and his M.Sc & Dr.Tech degrees in Information Technology, from Tampere University of Technology, Finland. He has authored numerous papers on refereed conferences and journals and he is an inventor in more than 15 patent applications.



Dr. Ian Brown
Oxford Internet Institute, UK

Dr. Ian Brown is a senior research fellow at the Oxford Internet Institute, where he leads research on public policy issues around information and the Internet, particularly privacy, copyright and e-democracy. He also works in the more technical fields of information security, networked systems and healthcare informatics. He is leading studies for the European Commission on the Future Internet and on technological challenges to data protection; and for the UK Research Councils on various privacy and security issues. Dr. Brown is a Fellow of the Royal Society of Arts, the International University of Japan and the British Computer Society, a senior member of the ACM, and has consulted for the US Department of Homeland Security, JP Morgan, Credit Suisse, Allianz, McAfee, BT, the BBC, the Cabinet Office, Ofcom, the National Audit Office and the Information Commissioner’s Office. He has variously been a trustee of Privacy International, the Open Rights Group and the Foundation for Information Policy Research and an adviser to Greenpeace, the Refugee Council, Amnesty International and Creative Commons UK.

Trusted Information Sharing

The recent 2009 Communication from the European Commission on Critical Information Infrastructure Protection [COM(2009)149 - "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"] reported that the World Economic Forum estimated in 2008 that there is a 10-20% probability of a major critical information infrastructure breakdown in the next 10 years, with a potential global economic cost of 250 billion US\$. The Communication went on to say that in addressing the problem "cooperation and information sharing between Member States of reliable and actionable data on security incidents appears underdeveloped". The action plan in the Communication includes many references to the need for effective information sharing and exchange, all of which it is argued must start by building trust between those taking part in both the public and private sectors. This session looks at the background to trusted information sharing as a means to help protect Critical Information Infrastructures and to help build citizens confidence in these infrastructures. The session looks at the different information sharing models in common use together with some case studies of real life examples. Particular attention will be focussed on building trust where research from the WARP programme in the UK (www.warp.gov.uk) and the EC project MS3i (www.ms3i.eu) will be presented. The concluding part of this session will look at the recent ENISA Guide on building "Trusted Information Exchanges" which was created from an analysis of good practice in a number of European countries and the US.

The ePrivacy System in the Austrian Government

This lecture will describe the electronic identity system used in the Austrian E-Government applications and focus on the legal and practical background of the applications that are currently in use. It will detail how the challenge of making a both reliable and privacy friendly system has been resolved. Examples of the successful use like the register based census or the secure transfer of medical data will be presented. General data protection principles will be seen in the context of E-Government tools and their specific requirements for accuracy and security. Examples of legal and practical problems encountered by the Austrian E-Government Register Authority in its role as operator of the system and in its role as data protection authority will be discussed.



Mr. John Harrison
LanditD, UK

Mr. John Harrison is an independent consultant and engineer with over 30 years experience in the telecommunications industry working for BT. Since 1996 he has worked in the field of Critical Information Infrastructure Protection and for the last six years supported the UK's CPNI and their trusted information sharing WARP programme www.warp.gov.uk, as well as a number of projects on infrastructure resilience. Mr. Harrison and his team at landitD have recently completed work on the EC funded project "messaging standard for sharing security information (MS3i)" (www.ms3i.eu) as well as the ENISA guide on "trusted information Exchanges". John is currently working on the 2 year EC funded project "National and European Information Sharing and Alerting System (NEISAS)", as well as continuing to support the WARP programme.



Mr. Marcus Hild
Austrian Data Protection Commission, AT

Mr. Marcus Hild works for the Austrian Data Protection Commission (DSK) and is responsible for the Austrian E-Government Register Authority. This authority is a part of the independent national data protection authority (DPA) in Austria and is not only in charge of dealing with the legal and practical privacy issues arising in this sector but also of running the electronic identity system on which the Austrian E-Government applications and the Citizen card system is based upon.

On international level Mr. Hild is a member of the Traveller Data subgroup of the Article 29 Data Protection Working Party which is the independent EU Advisory Body on Data Protection and Privacy.

Actions to promote resilience and confidence in e-communication infrastructures

Nations and businesses are highly dependent on well functioning and resilient e-communications. The competition among e-communication operators is high and increasing as are the vulnerabilities. Not all compete with quality and resilience. We have learnt that there are needs to take complementary actions to assure robust and secure networks. Actions in place are e.g. policies, privat-public partnership projects, exercises, CERT co-op, monitoring and supervision/oversight of operators, awareness raising among users. Lessons learned, especially in Sweden, will be discussed.

RFID Security and Privacy: A Primer

Variouly called "spychips," "next-generation barcodes," and enablers of "The Internet of Things," RFID (Radio-Frequency Identification) tags are microchips that communicate via radio. In common use today, they may ultimately proliferate into a pervasive labelling infrastructure for most everything under the sun--- consumer products, machine parts, documents, animals, and people. Given this promise, RFID tags call for well conceived anti-counterfeiting and data-privacy support. As cheap, constrained devices, though, they often cannot rely on time-tested data-security tools such as cryptography. Practical demands are likely to call for new approaches and expectations. This talk will be a general overview of the security and privacy problems posed by RFID and some of the solutions proposed by the research community.



Mr. Peter Wallstrom
Swedish Post and Telecom Agency, SE

Mr. Peter Wallstrom is a senior advisor at the network security department of the Swedish Post and Telecom Agency, the agency in charge of regulating security in electronic communications. His recent tasks have been to develop the agency's crisis management system, heading the agency's participation in the bi-annual national electronic communications exercise, and managing the upcoming international conference "Resilient Electronic Communications - A Multistakeholder Challenge", in association with the Swedish Presidency of the EU. Prior to his current position, Mr. Wallstrom was the deputy head of the Swedish IT Incident Centre, the national computer emergency response team. Before joining the agency in 2002, Mr. Wallstrom was for three years with the consultancy-group Mandator, where he was addressing issues concerning IT-related national security on behalf of clients like the Ministry of Defence, the Armed Forces and the European Commission. Mr. Wallstrom has a background from the Swedish Defence Research Agency in projects analyzing national policies for information operations and critical infrastructure protection.



Dr. Ari Juels
RSA Laboratories, USA

Dr. Ari Juels is Chief Scientist and Director of RSA Laboratories, where he works to bring sparks of invention and insight from RSA's scientists and affiliates to the company as a whole. He joined RSA after receiving his Ph.D. in Computer Science from U.C. Berkeley in 1996. In 2004, MIT's Technology Review Magazine named Dr. Juels one of the world's top 100 technology innovators under the age of 35. Computerworld honored him in its "40 Under 40" list in 2007.

Where the rubber meets the road: Privacy and Sociability in social network sites

SNSs pose a plethora of privacy issues that are reasonably well understood (see ENISA study, art 29 wp report etc). These studies contain all sorts of recommendations, but most prominently call for raising awareness of the SNS users as well as implementing security measures. This advice is not very helpful because it underestimates the innate social aspects of SNSs and how these platforms meet the social needs of their users. In order to be more effective we need to understand the social dynamics of social networks. I will briefly discuss why teens have no choice but to be on SNSs and on SNSs, data disclosure is the norm. Next I will focus on a couple of approaches to reconcile privacy and sociability in SNS. I will discuss two kinds of attackers in more detail: snoopers (parents, teachers, employers) and platform providers who harvest the data as part of their business model, and discuss remedies for their attacks.

Electronic ID at work: issues and perspective

Electronic IDs have come of age, at least in Europe where every citizen possesses several of them. This poses several challenges, mainly related to control of personal data, interoperability, and compatibility with applications. The dualism between IDs provided by the government and by the private sector further adds to the complexity. All these issues will be discussed in this talk, with reference to current initiatives in the field.



Prof. Ronald Leenes
University of Tilburg, NL

Prof. Ronald Leenes is associate professor in IT, law and new technologies at TILT, the Tilburg Institute for Law, Technology, and Society (Tilburg University). His primary research interests are privacy and identity management, regulation of, and by, technology. He is also involved in research in ID fraud, biometrics and Online Dispute Resolution. Leenes (1964) studied Public Administration and Public Policy at the University of Twente. He received his PhD for a study on hard cases in law and Artificial Intelligence and Law from the same university. Prof. Leenes was work package leader on socio-cultural aspects of privacy-enhancing IDM in the EU FP6 PRIME project. Currently he leads a work package on social software in the FP7 PrimeLife project. He has contributed to and edited various deliverables for the EU FP6 Network of Excellence "Future of IDentity in the Information Society" (FIDIS).



Prof. Antonio Liroy
Politecnico di Torino, IT

Prof. Antonio Liroy holds a M.Sc. degree in Electronic Engineering and a Ph.D. in Computer Engineering. Currently he is Full Professor at the Politecnico di Torino and leads the TORSEC research group active in ICT security. This group has taken part to several international security projects, the most recent ones being Positif, Deserec, Open-TC, and Stork. Prof. Liroy often acts as a consultant and reviewer for public and private bodies. His current research interests are in the fields of network security, PKI, and policy-based system protection. He has published nearly 100 scientific papers. Since September 2007, Prof. Liroy is a member of the PSG (Permanent Stakeholders' Group) of ENISA.

E-citizen services, databases and privacy impact assessments; To gather or not to gather, is that resilience?

Over the years electronic communications services and infrastructures and IT, to which we nowadays refer as ICT, have become critical to the functioning of society. If disrupted, impact can be huge. Prevention of disturbances is a major issue in the ICT sector as well as in the dependent sectors. In The Netherlands this issue was recognized towards the end of the 90's. Several projects were carried out to cover different aspects of the issue. Awareness raising at end-user level was taken up and implemented through e.g. media campaigns and certificates in primary school and via SME discussion fora. Resilience of services and infrastructures was covered in a PPP approach: government and providers started to cooperate on resilience issues like continuity planning and crisis management. Interesting detail of this approach is that it is situated on the borderline between public and private interest.

With the upcoming Internet cyber security also became of importance. A few years ago an information exchange on cybercrime was installed. This was also a PPP based operation, which has grown towards a group of linked exchanges for several sectors. Alongside these projects the Strategy on National Security was developed, which now covers in a structured way many sectoral and cross sector activities like analysis on risks, impact and dependencies, scenario development, capacity planning, crisis management, etc. The new challenge we are facing is, since ICT services are not bound to national borders, to connect the national approach to international activities. All these projects started at a low profile, but after some time all became a big success. Major factor for our success is the way PPP was implemented, with regulation regarded as only necessary as a last resort. Will this also be possible in an international environment?



Mr. Simon van Merkom
Ministry of Economic Affairs, NL

Mr. Simon van Merkom works with the Ministry of Economic Affairs in The Netherlands.

He is senior policy advisor in the section ICT Security since 2001 and coordinating the national policy regarding resilience of public telecommunications. He is involved in several projects covering national and international activities on critical infrastructure protection, crisis management structures and national security.

He received a MSc degree in electrical engineering at the Delft University of Technology in 1983. Then he joined the Ministry of Transport and worked on experiments and innovative projects related to the usage of IT in public transport systems. Followed by a few years of implementing ICT and office automation systems in several departments of the Ministry he moved to the telecommunications department of the Ministry to work on standardization and international relations. Keywords were telecommunications equipment, EU common market and enforcement. After implementing the EC R&TTE Directive in The Netherlands he joined the ICT Security section of the Ministry of Economic Affairs.

Privacy and identity in context-aware services

There is a rapidly growing trend towards mobile services that utilize context of the user. This context could be in the physical dimension (e.g. space and time) or in social dimension (e.g. friendship or collegial relationship). These kinds of services tend to be privacy-sensitive. New ways of combining physical and digital worlds also call for new types of identities. Technologies that help in managing the interplay between privacy and identity (but also security and trust) are presented. Areas covered vary from identification of radio devices to usage control of the privacy-sensitive context data.

Wireless System Security

Wireless devices are becoming pervasive and increasingly versatile, and they enable a multitude of applications closely knitted with the physical world. However, our increasing dependence on wireless systems is a double-edged sword: The nature of wireless communications and the applications of these systems create new vulnerabilities, and attacks can create new dangers for the system users.

This lecture will focus on the unique characteristics and security requirements of wireless systems, covering building blocks and fundamental aspects of wireless system security, as well as methods to reason rigorously on the correctness of wireless security protocols. Topics will include secure neighbourhood discovery, secure communication, and secure localization.



Dr. Valtteri Niemi

Nokia Fellow, Nokia Research Center, Lausanne, CH

Dr. Valtteri Niemi received a PhD degree from the University of Turku, Finland, Mathematics Department, in 1989. After serving in various positions in Univ of Turku, he was an Associate Professor in the Mathematics and Statistics Department of the University of Vaasa, Finland, during 1993-97. He joined Nokia Research Center (NRC), Helsinki in 1997 and in 1999 he was nominated as a Research Fellow. During 2004-2006, he was responsible for Nokia research in wireless security area as a Senior Research Manager. During 2007-2008, Dr. Niemi lead the Trustworthy Communications and Identities team in the Internet laboratory of NRC, Helsinki. He recently moved to the new NRC laboratory in Lausanne, Switzerland, where his main focus is on privacy-enhancing technologies. He was also nominated as a Nokia Fellow in 2009. Dr. Niemi's work has been on security issues of future mobile networks and terminals, the main emphasis being on cryptological aspects. He has participated 3GPP SA3 (security) standardization group from the beginning. Starting from 2003, he has been the chairman of the group. Before 3GPP, Dr. Niemi took part in ETSI SMG 10 for GSM security work. In addition to cryptology and security, Dr. Niemi has done research on the area of formal languages. He has published more than 40 scientific articles and he is a co-author of three books.



Dr. Panos Papadimitratos

Senior Researcher, EPFL, CH

Dr. Panos Papadimitratos is a senior researcher at the EPFL Institute of Communication Systems, Switzerland and the LCA-1 unit led by Prof. Hubaux. Prior to joining EPFL, he spent a year as a postdoctoral fellow at Virginia Tech. In January 2005, Dr. Papadimitratos received his PhD from Cornell University, Ithaca, NY, where he worked with Prof. Haas since 2000.

His research is concerned primarily with:

- Security for vehicular communication systems
- Formal verification of wireless security protocols
- Security for mobile ad hoc networks
- Sensor network security
- Ad hoc (mobile, sensor, and vehicular) networking
- Spectrum-agile systems

He has authored more than 65 technical publications on these topics. He is an Area Editor for ACM MC2R journal and he has served in several technical program committees, including ACM WiSec, ASIACCS, and MobiHoc, and IEEE INFOCOM.

Government 2.0: open and safe?

The new wave of collaborative, crowd-sourced government applications bring new opportunities and new challenges. Among the challenges, most important is how to ensure safe citizen participation, balancing ease of use and anonymity preservation with security and representativity, as described in the FP7 ICT workprogramme 2009-2010 (priority 7.3). This presentation will look and compare existing practice in government 2.0 applications in terms of privacy, identity, trust, security, reputation and differences with more traditional government applications.

The ISACA Business Model for Information Security

In this session, we will:

- Consider the business challenges that organizational leaders and security managers need to confront;
- Evaluate traditional approaches to protection used to address these challenges;
- Introduce systemic thinking as a better way of addressing the business needs for information protection;
- Review the concepts contained within the Systemic Security Management Model as a suitable Business Model for Information Security Management; and
- Have a mutually beneficial exchange of ideas.

A data protection view on the Internet of Things

The lecture will discuss about the growing evolution of Internet of things and its impact on data protection. Based on this, I will present the different aspects relating to EDPS' tasks towards the development of IoT, via his supervision, consultation and cooperation tasks. The implementation of privacy and data protection safeguards will also be touched upon.



Mr. David Osimo
Tech4i2 Ltd., UK

Mr. David Osimo joined in 2008 Tech4i2 Ltd as director and partner, after 15 years working on EU innovation policies and projects. Up to 2005 he worked in the Institute for Prospective Technological Studies, based in Sevilla and part of Joint Research Centre of the European Commission, where he was coordinating research activities on eGovernment. Previously, he worked as advisor and project manager on public policies for innovation and information society in Milan (I), Brussels (B) and Bologna (I). His current interests cover the role of government in the innovation system, the impact of technology on future models of government, and in particular the impact of web 2.0 on public services.



Mr. Yves Le Roux
CISM, CISSP, ITIL Principal Consultant, FR

As the EMEA Subject Matter Expert on Governance, Risk and Compliance, Mr. Yves LE ROUX is responsible for presenting the CA vision and positions on these matters. After his graduation from Paris University in 1970, he worked in the Rothschild Group where, among others tasks, he was in charge of the network security and other security related issues. In 1981, he joined the French Ministry of Industry where he was in charge of the Open Systems Standardization programs. In 1986, he took the position of European Information Security Manager at Digital Equipment. Then, he joined the security research and development team. In 1999, he went to Entrust Technologies, PKI software editor. In 2003, Yves joined Computer Associates Int. He has co-authored three books on security. He was a lecturer at Paris University and spoke in many conferences (e.g. ISSE 2007, ISMC USA 2008, ISMF 2008, ISMC Europe 2008). He is member of the European Network and Information Security Agency (ENISA) Permanent Stakeholders' Group (PSG). He is member of the ISACA Security Management Committee. He is also a member of the (ISC)2® European Advisory Board (EAB), the (ISC)2® CBK Review Committee, the (ISC)2® Journal Editorial Board and a (ISC)2® authorized Instructor for the CISSP CBK Review Seminar.



Mr. Michael Vanfleteren
Legal Adviser, European Data Protection Supervisor, EU

Mr. Michael Vanfleteren has a degree in law from the Universite Catholique de Louvain and a post-graduate degree in law (LLM) from University College London. He previously worked as trainee in the data protection unit of the European Commission and as legal researcher at the Katholieke Universiteit Leuven. He is currently working as legal adviser at the secretariat of the European Data Protection Supervisor.

Resilience of Critical Infrastructure

Controlled improvement in the reliability and security of any system requires a comprehensive analysis. This requires the systematic identification of the fundamental underlying components of the system using a rigorous discipline. If successful, this process will illuminate areas for concern and identify areas for potential system enhancements. Such comprehensive analysis can be conducted for communications infrastructure using a framework of eight ingredients. This paper will explore these eight ingredients and identify their usage in vulnerability analysis and best practice identification for enhancing the reliability and security of communications infrastructure.

Should privacy impact assessments be mandatory

This presentation concerns privacy impact assessments. It argues that the creation of large databases of personal data poses significant risks of privacy intrusion, breaches and losses of personal data as well as the attendant risk of loss of public confidence in our political leaders, governments and industry, which in turn undermines the development of e-government and e-commerce. One way of instilling more trust and optimising the configuration, safety and security of projects or services using personal data is to undertake a privacy impact assessment, which can be regarded as a specialised tool of risk management. A few countries have been using privacy impact assessments in recent years. The paper examines the UK and Canadian approaches to privacy impact assessment. While there are similarities, the UK model is voluntary, whereas the Canadian approach is mandatory. The paper asks: should PIAs be mandatory and, if so, should they be mandatory for government and industry? Are there lessons to be learned from the Canadian experience?



Mr. Richard E. Krock
Alcatel-Lucent, USA

Mr. Richard E. Krock is a member of technical staff in the Services Technology department at Alcatel-Lucent Worldwide Services in Lisle, Illinois. His responsibilities include the analysis of network outages and the identification and implementation of countermeasures. He has been an active member of the past two Network Reliability and Interpretability Councils and has led various sub-teams related to power. He has provided consulting services on emergency preparedness/disaster recovery both domestically and internationally, and also represents Lucent at the Telecom Information Sharing and Analysis Center, part of the National Coordinating Center for Telecommunications. Mr. Krock holds a B.S. degree in electrical engineering from Valparaiso University in Indiana and an M.B.A in telecommunications from Illinois Institute of Technology in Chicago. He is also a licensed professional engineer.



Mr. David Wright
Trilateral Research & Consulting, UK

Mr. David Wright is managing partner of Trilateral Research & Consulting, based in London. He has organised and participated in several successful consortia in FP6 and FP7. He was a partner in the SWAMI and STARC projects in FP6 and SENIOR project in FP7. He was principal author and editor of a report on privacy and trust for DG INFOS, delivered in early 2009. He is on the International Advisory Board of iNTeg-RISK, an integrated project on risks in new technologies. He is a member of working group 2 of the FP7 ThinkTrust project, the Living in a Surveillance Society COST action and the European Foresight Monitoring Network. He is the principal author and editor of Safeguards in a World of Ambient Intelligence, a book published by Springer in 2008, and author of many articles in many different peer-reviewed journals. He is also a free-lance researcher on the faculty of the Free University of Brussels (Vrije Universiteit Brussel, VUB).

SUNDAY, 13 SEPTEMBER

18:00 - 21:00 Registration at the Conference Hall

21:30 Welcome Cocktail at the Platform Area

MONDAY, 14 SEPTEMBER

08:00 - 09:00 Registration at the Conference Hall

09:00 - 09:30 Welcome:Mr. Andrea Pirotti, *Executive Director of ENISA, EU*Prof. Constantine Stephanidis, *Director of FORTH-ICS, GR*09:30 - 09:45 Keynote AddressDr. Jorgo Chatzimarkakis, *Member of the European Parliament, EU*09:45 - 10:45 Keynote AddressDr. Joao da Silva, *Director of the Network and Communication Directorate, European Commission, DG INFSO, EU*

10:45 - 11:15 Coffee Break

11:15-11:30 Keynote AddressProf. Ioannis Tsoukalas, *Member of the European Parliament, EU*11:30-12:30 Keynote AddressDr. Peter Freeman, *Emeritus Dean and Professor, Georgia Institute of Technology, USA*

12:30 - 14:00 Lunch

14:30 - 15:00 Keynote AddressDr. Silvia-Adriana Ticau, *Member of the European Parliament, EU*

15:00 - 16:00

The ePrivacy System in the Austrian GovernmentMr. Marcus Hild, *Austrian Data Protection Commission, AT*

16:00 - 16:30 Coffee Break

16:30 - 17:30 ***Government 2.0: open and safe?***Mr. David Osimo, *Tech4i2 Ltd., UK*19:30 **Gala Dinner****TUESDAY, 15 SEPTEMBER**09:00 - 10:00 ***Actions to promote resilience and confidence in e-communication infrastructures***Mr. Peter Wallstrom, *Swedish Post and Telecom Agency, SE*10:00 - 11:00 ***Policy Issues related to Network Security***Mr. Simon van Merkom, *Ministry of Economic Affairs, NL*

11:00 - 11:30 Coffee Break

11:30 - 12:30 ***Resilience of Critical Infrastructures***Mr. Richard E. Krock, *Alcatel-Lucent, USA*

12:30 - 14:00 Lunch

14:00 - 15:00 ***Trusted Information Sharing***Mr. John Harrison, *LanditD, UK*

15:00 - 15:30 Coffee Break

15:30 - 16:30 ***The ISACA Business Model for Information Security***Mr. Yves Le Roux, *CISM, CISSP, ITIL Principal Consultant, FR*16:30 - 17:30 ***RFID Security and Privacy: A Primer***Dr. Ari Juels, *RSA Laboratories, USA*

19:30 Dinner

WEDNESDAY, 16 SEPTEMBER (Special event: Visit to ENISA-FORTH campus)

08:30	Departure for ENISA-FORTH campus
09:15 - 09:30	<u>Welcome:</u> Mr. Andrea Pirotti, <i>Executive Director of ENISA, EU</i> Prof. Constantine Stephanidis, <i>Director of FORTH-ICS, GR</i>
09:30 - 10:30	<u>Keynote Address</u> Mr. Peter Hustinx, <i>Supervisor, European Data Protection Supervisor, EU</i>
10:30 - 11:00	<u>Keynote Address</u> Dr. Klaus Birkenbihl, <i>W3C Offices Coordinator, DE</i>
11:00 - 11:30	Coffee Break
11:30 - 12:00	ENISA Strategy for the Future Dr. Steve Purser, <i>ENISA, EU</i>
12:00-12:30	ENISA and the EC community on CIIP Dr. Evangelos Ouzounis and Mr. Marco ThobruEGge, <i>ENISA, EU</i>
12:30-13:00	Emerging and Future Risks (EFR) Dr. Louis Marinos, <i>ENISA, EU</i>
13:30	Lunch at a traditional cretan restaurant
16:00	Return to the hotel
19:30	Dinner (Beach Buffet)

THURSDAY, 17 SEPTEMBER

09:00 - 10:00	Where the rubber meets the road: Privacy and Sociability in social network sites Prof. Ronald Leenes, <i>University of Tilburg, NL</i>
10:00 - 11:00	Privacy and security by design Dr. Ian Brown, <i>Oxford Internet Institute, UK</i>
11:00 - 11:30	Coffee Break
11:30 - 12:30	Should privacy impact assessments be mandatory? Mr. David Wright, <i>Trilateral Research & Consulting, UK</i>
12:30 - 14:00	Lunch
14:00 - 15:00	Security and Virtual Worlds Prof. Richard Bartle, <i>University of Essex, UK</i>
15:00 - 15:30	Coffee Break
15:30 - 16:30	From Social Networks and Web Mash-ups towards Mixed Reality Dr. Petros Belimpasakis, <i>Nokia Research Center, Tampere Laboratory, FI</i>
16:30 - 17:30	A data protection view on the Internet of Things Mr. Michael Vanfleteren, <i>Legal Adviser, European Data Protection Supervisor, EU</i>
19:30	Dinner

FRIDAY, 18 SEPTEMBER

09:00 - 10:00	Privacy and identity in context-aware services Dr. Valtteri Niemi, <i>Nokia Fellow, Nokia Research Center, Lausanne, CH</i>
10:00 - 11:00	Wireless System Security Dr. Panos Papadimitratos, <i>Senior Researcher, EPFL, CH</i>
11:00 - 11:30	Coffee Break
11:30 - 12:30	Electronic ID at work: issues and perspective Prof. Antonio Lioy, <i>Politecnico di Torino, IT</i>
12:30 - 13:00	Closing remarks
13:00	Lunch

committees

STEERING COMMITTEE

- **Mr. Andrea Pirotti**, Executive Director of ENISA, EU
 - **Prof. Constantine Stephanidis**, Director of FORTH-ICS, GR,
Member of ENISA Management Board
-

PROGRAMME COMMITTEE

- **Prof. Angelos Bilas**, FORTH-ICS, GR
 - **Dr. Demosthenes Ikonou**, ENISA, EU
-

ADVISORY COMMITTEE

- **Prof. Matt Bishop**, Univ. of California, Davis, USA
- **Prof. Giusella Finocchiaro**, University of Bologna, IT, Member of ENISA PSG
- **Dr. Nigel Jefferies**, Vodafone Group Research & Development, UK
- **Prof. Jaap-Henk Hoepman**, Radboud University Nijmegen, NL, Member of ENISA PSG
- **Mr. Erkki Kataja**, Nokia Corporation, FI
- **Prof. Antonio Lioy**, Politecnico di Torino, IT, Member of ENISA PSG
- **Prof. Evangelos Markatos**, FORTH-ICS, GR, Member of ENISA PSG
- **Dr. Fabio Martinelli**, ERCIM/CNR-IIT, IT
- **Prof. Sachar Paulus**, Paulus Consult, DE
- **Prof. Fred Piper**, Royal Holloway, UK
- **Prof. Norbert Pohlmann**, Univ. of Applied Sciences Gelsenkirchen, DE
- **Dr. Nikos Pronios**, Intracom Defense Electronics, GR
- **Dr. Steve Purser**, ENISA, EU
- **Prof. Kai Rannenberg**, Johann Wolfgang Goethe - Frankfurt University, DE,
Member of ENISA Management Board
- **Dr. Joao da Silva**, European Commission, EU
- **Prof. Jacques Stern**, ENS/DI, FR
- **Prof. Apostolos Traganitis**, FORTH-ICS, GR

contact NIS'09



ENISA-FORTH Summer School on Network and Information Security
email: admin@nis-summer-school.eu • <http://www.nis-summer-school.eu>

European Network and Information Security Agency (ENISA)

Science and Technology Park of Crete • Vassilika Vouton • GR-70013 Heraklion, Crete, Greece
email: info@enisa.europa.eu • <http://enisa.europa.eu>

Foundation for Research & Technology - Hellas (FORTH) • Institute of Computer Science

N. Plastira 100 • GR-70013 Heraklion, Crete, Greece
email: ics@ics.forth.gr • <http://www.ics.forth.gr>