

3rd Summer School
on Network & Information Security
Jointly organised by ENISA and FORTH

NIS 2010

Privacy and Security in the Future Internet

13-17 September 2010, Crete, Greece

www.nis-summer-school.eu



Dear colleagues,

It is our pleasure to welcome you to the **3rd Network and Information Security (NIS'2010) Summer School**, taking place in Crete, Greece, 13-17 September 2010. 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**).

The 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 NIS'2010 is "**Privacy and Security in the Future Internet**".

The Future Internet promises an exciting world: new services, new infrastructures, and new capabilities at all levels. Devices that will automatically exchange information to facilitate users, services that take into account information from different and multiple sources, protocols and systems that are able to handle complex interactions. At the same time, however, concerns about privacy and security increase for individuals, organizations, and the society in general. Where should responsibility be placed and how should solutions be enforced and verified in a world of complex infrastructures and services? NIS'2010 will cover topics that address legal, technical, and policy issues in this emerging world.

ENISA is dedicated to promoting a culture of security in Europe that will improve 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, a research institute devoted to advancing the state-of-the-art in ICT, 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 and intricacies of privacy and security in the future internet, an array of lectures will cover a variety of key aspects on policy, legal, and research matters. Our audience includes policy makers from EU Member States and EU Institutions, decision makers from industry, and members of the 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 NIS'2010 will both benefit from and enjoy the programme.

Dr. Udo Helmbrecht

Executive Director of ENISA



Prof. Constantine Stephanidis

Director of FORTH-ICS



The "Future Internet" promises an exciting new world of services and capabilities: Devices that will automatically exchange information to facilitate users, services that transparently and seamlessly combine information from different and multiple sources, protocols and systems that are able to handle complex interactions. At the same time, however, concerns about privacy and security increase for individuals, organizations, and the society in general. This gives rise to a number of questions, such as where should responsibility be placed and how should solutions be enforced and verified in a world of complex infrastructures and services?

Following the success of NIS'08 and NIS'09, the 3rd edition of the Summer School on Network and Information Security (NIS'2010) will cover topics that address legal, technical, and policy issues in this emerging world. ENISA and FORTH have taken the initiative to create this Summer School following the recognition of the importance of NIS and the need for raising awareness. The Summer School aims to provide 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, for interacting on cuttingedge and interesting topics in NIS.

about ENISA

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

The Agency's tasks focus 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 Education, Lifelong Learning and Religious Affairs.

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 research and playing a leading role, in Greece and internationally, in the field of Information and Communication Technologies.





KEYNOTE ADDRESS

- **Prof. Sokratis K. Katsikas**, General Secretary for Communications, Ministry of Infrastructures, Transports & Networks, GR
 - **Dr. Silvia Adriana Țicău**, Member of the European Parliament, EU
-

KEYNOTE LECTURES

- **Mr. Peter Hustinx**, Supervisor, European Data Protection Supervisor, EU
 - **Mr. Mario Campolargo**, Director of the Emerging Technologies and Infrastructures, DG INFSO, European Commission, EU
 - **Mr. Mikko Hyppönen**, Chief Research Officer, F-Secure, FI
 - **Mr. Bruce Schneier**, Chief Security Technology Officer of BT, UK
-

DISTINGUISHED LECTURES

- **Prof. Audun Jøsang**, University of Oslo, NO
- **Mr. Caspar Bowden**, Chief Privacy Advisor, Microsoft EMEA Technology Office, UK
- **Prof. Jean-Jacques Quisquater**, Université Catholique de Louvain, BE
- **Prof. Joao Bärros**, University of Porto, PT
- **Prof. Gabi Dreo Rodosek**, Chair of Communication Systems and Internet Services, Universität der Bundeswehr Muenchen, DE
- **Dr. Jorge M. Pereira**, Principal Scientific Officer, European Commission, EU
- **Mr. Bertrand Marquet**, Acting Head of security research, Bell Labs, Alcatel-Lucent, FR
- **Mr. Jim Reavis**, Executive Director, Cloud Security Alliance
- **Prof. Reinhard Posch**, CIO for the Austrian Federal Government Republic of Austria, AT
- **Dr. Florian Kerschbaum**, CEC Karlsruhe, SAP Research, DE
- **Mr. Andreas Ebert**, Regional Technology Advisor, Microsoft EMEA, AU



Prof. Sokratis K. Katsikas

*General Secretary for Communications,
Ministry of Infrastructures, Transports &
Networks, GR*

Prof. Sokratis K. Katsikas is currently the General Secretary for Communications in the Ministry of Infrastructures, Transports & Networks, Greece. Prof. Katsikas received the Diploma in Electrical Engineering from the University of Patras, Patras, Greece in 1982, the Master of Science in Electrical & Computer Engineering degree from the University of Massachusetts at Amherst, Amherst, USA, in 1984 and the Ph.D. in Computer Engineering & Informatics from the University of Patras, Patras, Greece in 1987.

He has held teaching and research positions in the University of Massachusetts at Amherst, the University of Patras, the Athens University of Economics & Business, the Computer Technology Institute, the University of La Verne (Athens Campus), the Technological Educational Institute of Athens and the Technological Educational Institute of Patras.

He is currently a Professor in the University of Piraeus at the Dept. of Digital Systems. Between 1990 and 2006 he was a faculty member with the Department of Information & Communication Systems Engineering at the University of the Aegean, Greece, where he served as the University Rector between 2002 and 2006.

He has participated in more than 50 European and national R&D projects, as a researcher, scientific director or program manager, in the area of information and communication systems security. He has authored or co-authored more than 130 journal publications, book chapters and conference proceedings publications in his areas of interest.

He is a member of consultancy committees to several Ministries of the Greek Government. He served as the Chairman of the Strategic Committee for Informatics and Communications in Health and Welfare of the Ministry of Health and Welfare, the Chairman of the Strategic Committee for Informatics and Communications of the Ministry of Justice, and as a member of the Strategic Committee for Informatics and Communications in Education of the Ministry of Education and Religious Affairs.



Dr. Silvia Adriana Țicău

Member of the European Parliament, EU

Dr. Silvia Adriana Țicău 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. Țicău 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 (Galați, 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.

More effective data protection: how to face up to a digital world?

The need for data protection is increasingly relevant due to technological change, globalisation and conflicting public interests. However, as recently demonstrated, there is also a need to make data protection more effective in practice and to use more creative methods to reach this result.

Although the challenges in this field are impressive, there are also some important opportunities that should be used well. The Lisbon Treaty has provided a new and much stronger perspective for data protection in the European Union. The right to data protection has become a binding fundamental right not only for EU institutions and bodies, but also for the member states when they are implementing European law.

Other elements of the Lisbon Treaty, such as stronger roles for the Parliament, the Commission and the European Court of Justice in the former "third pillar" area of police and justice have also contributed to an increased focus on data protection in policy making. This focus is clearly visible in the new 5-year program for the area of Justice and Home affairs ("Stockholm Program") and in the activities of the new Commission, including its current Review of the existing legal framework for data protection and the Digital Agenda. Data protection is also an important part of the Transatlantic Agenda.

This presentation will look at the relevant trends and the prospects for more effective data protection in a more and more ICT dependent and globalised world, where concerns about privacy are increasing, as citizens discover how new technologies are impacting on their lives.



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.

A trustworthy Future Internet as a cornerstone of the online single market

Internet has proved to be an extraordinary catalyser of innovation which has dramatically transformed our economy and society, but the underlying networks and service infrastructures remain vulnerable to a wide range of new and evolving threats. Fraud and attacks in the cyber-space are growing in sophistication and in magnitude and are often motivated by financial or even political purposes. Addressing those threats and strengthening trust and security in the digital society is our shared responsibility.

To truly engage in future online activities, European citizens need to fully rely upon a secure and trustworthy internet infrastructure. Therefore, research and innovation endeavours related to the Future Internet cannot be decoupled from the need to foster trust in the future digital society. The Future Internet must be resilient and secure to all sorts of new threats, including new forms of cybercrime, and must be designed with legal compliance, economic and social viability in mind.

This speech will introduce the policy measures foreseen in the Digital Agenda to establish a secure and trustworthy information infrastructure in Europe and to fight against cybercrime, as well as the next R&D and innovation priorities, including the Future Internet Public Private Partnership.

State of the Net 2010

Computer security has gone several distinct eras. Attacks morph and change every few years. However, the biggest changes we've seen have not been technical. They've been social. It's all about the attackers and their motives. If we don't do the right moves now, next these attacks will move to new platforms, such as smartphones. Making money by infecting phones is actually easier than by infecting computers. Most importantly, we need to be able to convince the authorities around the world to act together on these international crimes. The situation is not getting better; it's getting worse. I do believe the very freedom of the net could be at stake here.



Mr. Mario Campolargo
Director of the Emerging Technologies and Infrastructures, DG INFSO, European Commission, EU

Mr. Mario Campolargo is the Director of the "Emerging Technologies and Infrastructures" Directorate of DG-INFSO in charge of future and emerging technologies, ICT based infrastructures for science as well as ICT trust and security, experimental facilities and experimentally driven research for future internet. Before joining the European Commission in 1990, he worked for 12 years in the R&D Center of Portugal Telecom as a researcher and manager. Mr. Campolargo has a Degree in Electrical Engineering by the University of Coimbra, a Master of Science in Computing Science by the Imperial College London, a Post graduate in Management by the Solvay Business School in Brussels and a European Studies Diploma by the Universite Catholique de Louvain-la-Neuve in Belgium.



Mr. Mikko Hyppönen
Chief Research Officer, F-Secure, FI

Mr. Mikko Hyppönen is the Chief Research Officer for F-Secure. He has worked with F-Secure since 1991. Mr. Hyppönen led the team that took down the world-wide network used by the Sobig.F worm in 2003, was the first to warn the world about the Sasser outbreak in 2004 and named the infamous Storm Worm in 2007. Mr. Hyppönen has assisted law enforcement in USA, Europe and Asia on cybercrime cases. He has written for magazines such as Scientific American, Foreign Policy and Virus Bulletin. Mr. Hyppönen has addressed the most important security-related conferences worldwide. He is also an inventor for several patents, including US patent 6,577,920 "Computer virus screening". He has been the subject of dozens of interviews in global TV and print media, including a 9-page profile in Vanity Fair. Mr. Hyppönen, born in 1969, was selected among the 50 most important people on the web in March 2007 by the PC World magazine. Apart from computer security issues, Mr. Hyppönen enjoys collecting and restoring classic arcade video games and pinball machines from past decades. He lives with his family, and a small deer community, in an island near Helsinki.

The Future of Privacy, and the Generation Gap

The Internet is the greatest generation gap since rock and roll. The older of us need to be prepared for a younger generation that lives life on the Internet, doesn't understand where their computer or smart phone ends and the Internet begins, shares passwords with their friends as a sign of trust, and deliberately lies when registering for services. At the same time, both technological and business trends point to less user control (both security and privacy), and laws are leaving these trends alone. What will security and privacy look like in this new world? Someone needs to figure it out.



Mr. Bruce Schneier

Chief Security Technology Officer of BT, UK

Bruce Schneier is an internationally renowned security technologist and author. Described by *The Economist* as a "security guru", he is best known as a refreshingly candid and lucid security critic and commentator. When people want to know how security really works, they turn to Schneier.

His first bestseller, *Applied Cryptography*, explained how the arcane science of secret codes actually works, and was described by *Wired* as "the book the National Security Agency wanted never to be published". His book on computer and network security, *Secrets and Lies*, was called by *Fortune* "[a] jewel box of little surprises you can actually use". *Beyond Fear* tackles the problems of security from the small to the large: personal safety, crime, corporate security, national security. His current book, *Schneier on Security*, offers insight into everything from the risk of identity theft (vastly overrated) to the long-range security threat of unchecked presidential power and the surprisingly simple way to tamper-proof elections.

Regularly quoted in the media, he has testified on security before the United States Congress on several occasions and has written articles and op eds for many major publications, including *The New York Times*, *The Guardian*, *Forbes*, *Wired*, *Nature*, *The Bulletin of the Atomic Scientists*, *The Sydney Morning Herald*, *The Boston Globe*, *The San Francisco Chronicle*, and *The Washington Post*.

Schneier also publishes a free monthly newsletter, *Crypto-Gram*, with over 150,000 readers. In its ten years of regular publication, *Crypto-Gram* has become one of the most widely read forums for free-wheeling discussions, pointed critiques, and serious debate about security. As head curmudgeon at the table, Schneier explains, debunks, and draws lessons from security stories that make the news.

There's no information self-determination without information self-awareness, or - why you should have a right to access all your data all the time

The EU Data Protection Directive 95/46 embodies the principle that a person may access data which exists about them, but encumbered with exemptions which mean it is not useful in the age of cloud computing and behavioural advertising. Theoretical considerations suggest that being able to access "all your data, all the time" is an indispensable 21st century human right, but it may also eliminate malignant externalities in economic competition for online services, by correcting the market failure of innovation in privacy enhancing technologies. Traditional exceptions and exemptions to subject access are largely obsolete if we look beyond "Privacy by Design" to embrace "Transparency by Design" for the data subject. In particular, user-centric identity management can provide strong mutual authentication between data controller and subject, however some architectures claimed to be "user-centric" may actually exacerbate privacy risks. However the possibility of systematic surveillance over the exercise of transparency rights creates a human rights antinomy, and should categorically be prohibited.

Identity Management

This lecture provides an introduction to identity management. Attendees will get a deep understanding of the concepts of identity and the problems related to managing identities to support security in online applications. The tutorial will present the most prominent methods and models for identity management, will understand identity management can be integrated with security systems and applications, will appreciate their limitations and will have a good overview of standardisation activities and research challenges in this area.



Mr. Caspar Bowden
*Chief Privacy Advisor, Microsoft EMEA
Technology Office, UK*

Caspar Bowden is Chief Privacy Adviser for Microsoft in Europe, Middle-East and Africa. His goal is to ensure that users of Microsoft products and services are in control of their personal data and that fair information practices are respected. He is a specialist in data protection policy, privacy enhancing technology research, identity management and authentication. He was formerly director of the Foundation for Information Policy Research, an independent think-tank that studies the interaction between computers and society, and promotes public understanding and dialogue between UK and European civil society and policy-makers in the fields of e-commerce, copyright, law enforcement and national security, e-government, cryptography and digital signatures. He was appointed expert adviser to the UK parliament for the passage of three bills concerning privacy issues, and was co-organizer of the influential Scrambling for Safety public conferences on UK encryption and surveillance policy. His previous career over two decades ranged from investment banking (proprietary trading risk-management for option arbitrage), to software engineering (graphics engines and cryptography), including work for Goldman Sachs, Microsoft Consulting Services, Acorn, Research Machines, and IBM.



Prof. Audun Jøsang
University of Oslo, NO

Audun Jøsang works at Oslo University and UNIK Graduate Center where he teaches and conducts research on trust management and information security. In particular Prof. Jøsang is well known for his work on user-centric identity management and on computational trust based on subjective logic. Prior to joining Oslo University he was Associate Professor at QUT, research leader of the Security Unit at DSTC in Brisbane, worked in the telecommunications industry for Alcatel in Belgium and for Telenor in Norway. He was also Associate Professor at the Norwegian University of Science and Technology (NTNU). Prof. Jøsang has a Masters degree in Information Security from Royal Holloway College London, and a PhD from NTNU in Norway.

Sensors, Vehicles and Things: Can We Secure the New Species on the Internet Landscape?

As the Internet evolves into an immense jungle of people, computers, mobile devices, sensors, vehicles and networked infrastructures, bringing forward unexpected technologies, applications, products and services, the proposed security sub-systems seem strangely "d  j   vu", relying on variations of established techniques such as hashing, symmetric encryption, public-key cryptography or access control policies. But is this really all that it takes to secure the internet of things, smart grids or intelligent transportation systems, to name just a few of the envisioned future internet environments? In this lecture, we shall address this question from various angles by looking at case studies such as vehicular networking, distributed sensing, network coding and physical-layer security. Our ultimate goal is to point at ways to ensure that such technologies can be well integrated in the (hopefully) secure internet of the future.

Challenges of Cyber Defense in the Future Internet

Whether the Future Internet will be evolutionary or clean slate, assuring security and privacy will be among the most challenging tasks. State-of-the-art cyber defense systems and algorithms for intrusion detection and early warning based on data provided by sensors in the networks are not able to cope with the upcoming challenges such as trillions of fixed as well as mobile devices, huge amounts of data, encrypted payloads, ad-hoc interactions between devices and complex security strategies. A discussion about the upcoming challenges of cyber defense, an overview of existing work, and possible directions how to approach them are aspects targeted in the presentation.



Prof. Jo  o Barros

University of Porto / MIT, Director of the Carnegie Mellon Portugal Program

Jo  o Barros is an Associate Professor at the Department of Electrical and Computer Engineering of the School of Engineering of the University of Porto and the coordinator of the Porto Laboratory of the Instituto de Telecomunicac  es. He is also a Research Affiliate with the Massachusetts Institute of Technology (MIT). In February 2009, Dr. Barros was appointed National Director of the CMU-Portugal Program, a five-year international partnership between Carnegie Mellon University and 12 Portuguese Universities and Research Institutions, with a total budget of 56M Euros. He received his undergraduate education in Electrical and Computer Engineering from the Universidade do Porto (UP), Portugal and Universitaet Karlsruhe, Germany, until 1999, and the Ph.D. degree in Electrical Engineering and Information Technology from the Technische Universitaet Muenchen (TUM), Germany, in 2004. From 2005 to 2008, Jo  o Barros was an assistant professor at the Department of Computer Science of the School of Sciences of the University of Porto. The focus of his research lies in the general areas of information theory, communication networks and data security. Dr. Barros received a Best Teaching Award from the Bavarian State Ministry of Sciences, Research and the Arts, as well as scholarships from several institutions, including the Fulbright Commission and the Luso-American Foundation. He held visiting positions at Cornell University and the Massachusetts Institute of Technology, where he spent a sabbatical in 2008. Beyond his duties as Secretary of the Board of Governors of the IEEE Information Theory Society, his service included co-chairing the 2008 IEEE Information Theory Workshop in Porto, Portugal, and participating in several Technical Program Committees, including ITW 2009, WiOpt (2008 and 2009), ISIT 2007, IS 2007, and IEEE Globecom (2007 and 2008).



Prof. Gabi Dreo Rodosek,

Chair of Communication Systems and Internet Services, Universitaet der Bundeswehr Muenchen, DE

Gabi Dreo Rodosek holds the Chair of Communication Systems and Internet Services at the Universitaet der Bundeswehr Munich in Germany since 2004. She received her M.Sc. degree from the University of Maribor, Slovenia, and her doctoral degree from the University of Munich, Germany. She is the member of the executive committee of the EU FP6 NoE EMANICS project, and the chairwoman of the IT security research group at the University. She was general co-chair of the 10th IFIP/IEEE Integrated Management Symposium (IM 2007), she is member of the Editorial Advisory Board of the International Journal of Network Management, co-chair of the IFIP/IEEE workshop series on Management of the Future Internet (<http://www.manfi.org>) and TPC co-chair of the DFN-Forum series "Communication Technologies".

Privacy, social networks and archives

Human memory is not perfect and with time forgets many facts and information. Internet memory is too perfect for human people with some sense of privacy. What are the facts, the problems, the solutions? With special attention to social networks and archives. I'll also speak about the role of cryptography and some recent results.



Prof. Jean-Jacques Quisquater
Universite catholique de Louvain, BE

Jean-Jacques Quisquater is an engineer in applied mathematics from UCL and holds a PhD in computer science from the university of Orsay (LRI, France). He was working as a scientist for Philips (MBLE-PRLB) from 1970 to 1991. There his main contributions were the design of the first smart card with cryptographic capabilities (going to the Proton card), the first smart card with a cryptographic coprocessor (still in use for many applications including identity cards and most of the electronic passports in the world) and the beginning of internet in Belgium together with Michel Lacroix. From 1991, he is a professor of cryptography at UCL, head of the UCL Crypto Group, together with ENS (rue d'Ulm, Paris, ending 2002) and at many other universities (Lille, MIT, Bordeaux, Namur, Brussels, Limoges, Toulouse...). He published about 200 papers and holds 20 patents. He is an IACR fellow. In 2010 he was a general chair of CHES 2010 in Santa Barbara and a program chair for EVT-WOTE in Washington.

Global Efforts to Secure Cloud Computing

In this session, Jim Reavis will present the key security problems of Cloud Computing that need to be solved. He will provide information about activities in the public and private sector around the world to develop standards and guidelines for cloud security. He will also provide an overview of key innovations being made by global IT solution providers and small entrepreneurs that will "change the game" of cloud security.

Operational Security Assurance: Requirements for a trusted future internet and privacy

The situation is somewhat simple: we have most of the technology to secure ICT infrastructures and services but we are most of the time uncertain about how efficient if the deployed security within such infrastructures.

One key topic to address by all actors is operational security assurance i.e. the capacity to measure and maintain a certain level of security where investments are correctly balanced with risks.

Operational security assurance is an enabling factor of confidence that risk are correctly mastered and at the same time that at the end side of the infrastructure, the user experience is protected and therefore giving guaranties that privacy is enforced.



Mr. Jim Reavis

Executive Director, Cloud Security Alliance

Jim is helping shape the future of information security as co-founder, executive director and driving force of the Cloud Security Alliance. For many years, Jim Reavis has worked in the information security industry as an entrepreneur, writer, speaker, technologist and business strategist. Jim's innovative thinking about emerging security trends have been published and presented widely throughout the industry and have influenced many. Jim is the President of Reavis Consulting Group, LLC, where he advises security companies, large enterprises and other organizations on the implications of new trends such as Cloud and how to take advantage of them. Jim has previously been an international board member of the ISSA, a global not for profit association of information security professionals and formerly served as the association's Executive Director. Jim was a co-founder of the Alliance for Enterprise Security Risk Management, a partnership between the ISSA, ISACA and ASIS, formed to address the enterprise risk issues associated with the convergence of logical and traditional security. Jim currently serves in an advisory capacity for many of the industry's most successful companies. Jim is also a partner with the MetroSITE Group. Jim founded SecurityPortal in 1998 and has been an advisor on the launch of many industry ventures. Jim is widely quoted in the press and has worked with hundreds of corporations on their information security strategy and technology roadmap. Jim has a background in networking technologies, marketing, product management and systems integration. Jim received a B.A. in Business Administration / Computer Science from Western Washington University in 1987 and serves on WWU's alumni board.



Mr. Bertrand Marquet

Acting Head of security research, Bell Labs, Alcatel-Lucent, FR

Bertrand Marquet is working for Alcatel-Lucent for more than 10 years. Previously, he has been working within the French Network and Information Security Agency helping industrials to achieve security certifications. Bertrand built and coordinated an Awarded European funded research project of operational security assurance. He is now acting Head of security research head of Bell Labs, the corporate research entity of Alcatel-Lucent.

IT and Internet Security from a Government Service Viewpoint

The lecture focusses on the experiences and results Austria has achieved when implementing its new Strategy eAustria since 2001. Describing a citizen centric approach the lecture starts with the citizen dimension taking a view on trust and trustworthiness on data protection and privacy and on the ease of use given the constraints mentioned afore. The next viewpoint is taken from a government agencies point of view efficiency and effectiveness. This is done on the background of a federal setup given by the Austrian constitution. This viewpoint includes also interoperability cross border which can be seen as a further layer of federation. Here both national legal and technical provisions as well as approaches seen in the CIP large scale pilots are discussed. Special attention is paid to ease of use as a precondition for take-up. The lecture is complemented with a practical view and discussion on the results which are mostly available on the Open Source E-Government program in Austria.



Prof. Reinhard Posch

*CIO for the Austrian Federal
Government Republic of Austria, AT*

Reinhard Posch is member of many professional societies: IEEE, ACM, OCG (member of the board of the Austrian Computer Society), OGI (Oesterreichische Gesellschaft fur Informatik), ACONET, OeMG (Oesterreichische Mathematische Gesellschaft), GME (Microelectronic society) etc. He was the Austrian representative in IFIP TC6 (Communication) as well as IFIP TC11 (Computer Security). Besides this Reinhard Posch is member of the Working group on Security of payment systems with chip cards of the Austrian National Bank. He worked with the OECD group of experts on cryptography in preparing the OECD guidelines for cryptographic policies. At the national level he was consulting the Federal Chancellery, the Ministry of the Interior and other public institutions on matters of security and cryptography. He was participating in the negotiations for the "Directive on a common framework for electronic signatures" of the European Union. Reinhard Posch is also participating in the Working Party on the authenticity of legal data and electronic signature in the justice sector of the Council of Europe. Within the i2010 framework Reinhard Posch participated in the eGovernment subgroup taking the lead in identities and interoperability of electronic documents. Reinhard Posch acts as the Austrian member of the ENISA Management Board. At the 10th meeting on 23rd of March 2007 he got elected Chairmen of the management board. Reinhard Posch was appointed coordinator for the electronic citizen card, a signature based smart card, by the Austrian government. As Chief Information Officer Reinhard Posch is heading the platform "Digital Austria", the coordination body for ICT in public administration and E-Government in Austria. Reinhard Posch has received several awards among those the IFIP Silver Core, and the ID Peoples Award 2006.

Trust Gates for the Future Internet

One of the latest megatrends of the internet is the establishment of "application islands" like eBay, Amazon, iTunes, Google and more. These "islands" represent a platform operator and a wider ecosystem of suppliers and prosumers and have led to what some call "private fragmentation" of the internet. What are the concepts and technologies for the next generation of "internet trust gates" and how can these approaches be applied to the internet of services, the internet of things and the internet of energy?

Will security issues hinder cloud computing adoption?

Much of current Enterprise IT systems will migrate to the cloud over the next few years and this migration needs to include appropriate security. Cloud computing is not a new concept, but is gaining traction rapidly in large part because of potential cost savings and scalability. However, like any new product or service, cloud computing requires careful consideration in order to ensure that security, privacy, legal and compliance issues are properly handled.

The intent of this lecture is to give the audience a broad introduction into the security issues facing cloud based systems and provide an understanding of the differences between traditional enterprise security and the issues facing systems that are deployed into the cloud.



Dr. Florian Kerschbaum
CEC Karlsruhe, SAP Research, DE

Dr. Florian Kerschbaum is a senior researcher and project lead at SAP Research in Karlsruhe, Germany. Before SAP he has worked for Siemens, the San Francisco-based startup Arxan, Intel and Digital Equipment in the job functions of project manager, software architect, and developer. He holds a Ph.D. in computer science from the Karlsruhe Institute of Technology, a master's degree from Purdue University, and a bachelor's degree from Berufshochschule Mannheim. His research focuses on improving the efficiency of cryptographic mechanisms in order to make them suitable for business software problems. At SAP Research he coordinates the EC funded research project SecureSCM which builds confidentiality-preserving collaborative supply chain planning based on secure multi-party computation. He has more than ten years of experience in computer security and contributed to 40 scientific, peer-reviewed publications and 30 patent applications. He served on the program committees of international conferences and workshops.



Dr. Andreas Ebert
Regional Technology Advisor, Microsoft EMEA, AU

Dr. Andreas Ebert joined Microsoft in 1991. His current focus and interest is on the economic impact of technological developments, software ecosystems and technology policy. Mr. Ebert has more than 25 years of experience in the IT industry ranging from software development, raising and establishing a consulting organization to general manager for Microsoft Austria. Since 2004, Mr. Ebert increasingly focused his work on the broader applicability of interoperability, standardization, security and privacy.

Panel on "Reporting Serious Security Incidents"

According to the revised Telecom Package (agreed on 25 November 2009) all EU Member States are obliged to implement within 18 Months a notification scheme for security incidents. Commission, taking the utmost opinion of ENISA, would propose guidelines to harmonise MS efforts. At the end of 2009 ENISA published a good practice guide on this topic. In 2010, ENISA together with EU MS and private stakeholders will continue its work on the topic with the objective to build momentum among MS. The goal of this panel is to help both policy makers and private sector to better understand the complexities of the problem, exchange views on important parameters of it aiming towards reaching agreement on a number of good practices (e.g. partially deploying ENISA's Good Practice Guide).

Panel on "Risk and Innovation"

Current developments in the area of finance put innovation and risks in new a light and make the debate on their coexistence as interesting as ever before. In this session, we will discuss experiences from innovation activities of "high-tech" organisations from different sizes and sectors. Possible courses of action that have supported innovation will be presented and discussed, especially in areas where ICT deployment plays a fundamental role. Positive and negative aspects from the coexistence of risk posture, innovation and entrepreneurship will be main elements to be addressed during the presentations.

Main focus will be on the relevant risk areas, particular risks and mitigation techniques to surface them. Very important will be to refer on the size, nature and management techniques of residual risks that have been accepted during the innovation process.

Given the context of the Summer School, information security risks will be the main concern of the presentations. This perspective underlines the fact, that good security is an essential component of innovation. In other words, due to their inherent risk exposure, implementations of innovative ideas that do not incorporate reasonable security models will probably not survive in the long term.

Moderator:

Dr. Evangelos Ouzounis

Senior Expert - Network Security Policies, ENISA, EU

Panelists:

- **Scott Algeier**, *US ISAC, US (industry)*
- **Lauri Almann**, *Estonia Ministry of Economy (public)*
- **Kauto Huopio**, *FICORA, Finland (public)*
- **Rick Krock**, *Alcatel Lucent, US*

Moderator:

Dr. Louis Marinos

Senior Expert - Risk Management, ENISA, EU

Panelists:

- **Patrick Crasson**, *Associate Partner CEINOO, The Chief Executive and Innovation Officers - Board and Advisory services*
- **Jeremy Ward**, *Partner at ExecIA LLP*
- **Julien Touzeau**, *Aircraft Security, Head of Innovation and Strategic Projects*

Panel on "Priorities for Research on Current and Emerging Network Technologies"

The past decade has seen a revolution in the way we communicate. An increasing number of services are offered online, along with vast quantities of rich, multimedia content. The Digital Society that derived from this revolution is accompanied by a shift in terms of expectations. All part of this value chain, consumers, service providers, government expect that the underlying communications infrastructure will support the demands the Digital Society will place on it. They expect services to provide the required functionality, to be available at all times and in all places and to process and store data securely. Moreover, the service and infrastructure components will need to actively cooperate to provide the most reliable environment while at the same time services become increasingly complex, interdependent and mashed-up. In this context, it is the subject of availability that is of concern to us as well as of the required R&D into the technologies that improve the resilience of data networks and, therefore, the availability of online services.

In March 2010 the European Commission launched the EU2020 strategy and, within its frame, a flagship initiative of preparing 'A digital agenda for Europe'. It is the continuation of earlier Lisbon Strategy and its i2010 initiative which highlighted the importance of network and information security for the creation of a single European information space.

In its proposal for European Digital Agenda

(<http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/132&format=HTML&aged=0&language=EN&guiLanguage=en>) the European commission aims to maximise the potential of Information and Communications Technologies (ICTs) to drive of job creation, sustainability and social inclusion, and so contribute to the overall goals of the Europe 2020 strategy (http://ec.europa.eu/eu2020/index_en.htm). In this light, the European Commission is aiming towards "building people's trust in using the Internet" creating this way the right conditions for ICTs and the internet ecosystem to flourish.

ENISA's activities recently focused on, among other matters, the suitability of backbone Internet technologies regarding the integrity and stability of networks as currently deployed. As a further step in this direction, in 2009 the Agency proceeded with an assessment of the impact of new technologies on the security and resilience of network resources

(<http://www.enisa.europa.eu/act/it/library/deliverables/procent>).

This panel will become an excellent opportunity to review and discuss research priorities in the areas of networking resilience and in network and information security.

Moderator:

Dr. Demosthenes Ikonou

Technical Competence Department, ENISA, EU

Panelists:

- **Slawomir Gorniak**, *ENISA*
- **Fabrizio Sestini**, *DG INFSO, European Commission*
- **Claire Vishik**, *Intel*
- **Matt Broda**, *Microsoft*
- **Daniel Gidoin**, *Thales Communications*

SUNDAY, 12 SEPTEMBER

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

21:30 Welcome Cocktail at the Platform Area

MONDAY, 13 SEPTEMBER

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

09:00 - 09:25 Welcome:Dr. Udo Helmbrecht, *Executive Director of ENISA, EU*Prof. Constantine Stephanidis, *Director of FORTH-ICS, GR*09:25 - 09:50 Keynote AddressProf. Sokratis K. Katsikas, *General Secretary for Communications, Ministry of Infrastructures, Transports & Networks, GR*09:50 - 10:15 Keynote AddressDr. Silvia Adriana Țicău, *Member of the European Parliament, EU*

10:15 - 10:45 Coffee Break

10:45 - 12:00

Keynote Lecture: **A trustworthy Future Internet as a cornerstone of the online single market**Mr. Mario Campolargo, *Director of the Emerging Technologies and Infrastructures DG INFSO, European Commission, EU*

12:00 - 14:00 Lunch

14:00 - 15:15

Keynote Lecture: **More effective data protection: how to face up to a digital world?**Mr. Peter Hustinx, *Supervisor, European Data Protection Supervisor, EU*

15:15 - 15:45 Coffee Break

15:45 - 17:00

Keynote Lecture: **State of the Net 2010**Mr. Mikko Hyppönen, *Chief Research Officer, F-Secure, FI*

17:00 - 20:00 Free Time

20:00

Gala Dinner**TUESDAY, 14 SEPTEMBER**

09:00 - 10:15

Keynote Lecture: **The Future of Privacy, and the Generation Gap**Mr. Bruce Schneier, *Chief Security Technology Officer of BT, UK*

10:15 - 10:45 Coffee Break

10:45 - 12:00

There's no information self-determination without information self-awareness, or - why you should have a right to access all your data all the timeMr. Caspar Bowden, *Chief Privacy Advisor, Microsoft EMEA Technology Office, UK*

12:00 - 14:00 Lunch

14:00 - 15:15

Sensors, Vehicles and Things: Can We Secure the New Species on the Internet Landscape?Prof. João Barros, *University of Porto / MIT, Director of the Carnegie Mellon Portugal Program*

15:15 - 15:45 Coffee Break

15:45 - 17:00

Panel 1***Reporting Serious Security Incidents***Moderator: Dr. Evangelos Ouzounis, *Senior Expert - Network Security Policies, ENISA, EU*

17:00 - 19:30 Free Time

19:30

Dinner

WEDNESDAY, 15 SEPTEMBER

09:00 - 10:15

Identity ManagementProf. Audun Jøsang, *University of Oslo, NO*

10:15 - 10:45

Coffee Break

10:45 - 12:00

Challenges of Cyber Defense in the Future InternetProf. Gabi Dreo Rodosek, *Chair of Communication Systems and Internet Services, Universitat der Bundeswehr Muenchen, DE*

12:00 - 14:00

Lunch

14:00 - 15:15

Privacy, social networks and archivesProf. Jean-Jacques Quisquater, *Universite catholique de Louvain, BE*

16:30 - 19:30

Visit to the archaeological site of Knossos

19:30

Dinner

THURSDAY, 16 SEPTEMBER

09:00 - 10:15

Operational Security Assurance: Requirements for a trusted future internet and privacyMr. Bertrand Marquet, *Acting Head of security research, Bell Labs, Alcatel-Lucent, FR*

10:15 - 10:45

Coffee Break

10:45 - 12:00

Global Efforts to Secure Cloud ComputingMr. Jim Reavis, *Executive Director, Cloud Security Alliance, USA*

12:00 - 14:00

Lunch

14:00 - 15:15

IT and Internet Security from a Government Service ViewpointProf. Reinhard Posch, *CIO for the Austrian Federal Government Republic of Austria, AT*

15:15 - 15:45

Coffee Break

15:45 - 17:00

Panel 2**Risk and Innovation**Moderator: Dr. Louis Marinos, *Senior Expert on Risk Management, ENISA, EU*

17:00 - 19:30

Free Time

19:30

Dinner

FRIDAY, 17 SEPTEMBER

09:00 - 10:15

Trust Gates for the Future InternetDr. Florian Kerschbaum, *CEC Karlsruhe, SAP Research, DE*

10:15 - 10:45

Coffee Break

10:45 - 12:00

Will security issues hinder cloud computing adoption?Dr. Andreas Ebert, *Regional Technology Advisor, Microsoft EMEA, AU*

12:00 - 14:00

Lunch

15:15 - 15:45

Coffee Break

15:45 - 17:00

Panel 3**Priorities for Research on Current and Emerging Network Technologies**Moderator: Dr. Demosthenes Ikonomidou, *Technical Competence Department, ENISA, EU*

17:00 - 19:30

Free Time

19:30

Dinner

committees

STEERING COMMITTEE

- **Dr. Udo Helmbrecht**, Executive Director of ENISA, EU
 - **Prof. Constantine Stephanidis**, Director of FORTH-ICS, GR
-

PROGRAMME COMMITTEE

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

ADVISORY COMMITTEE

- **Prof. Javier Lopez**, University of Malaga, ES
- **Dr. Stephan Lechner**, Director of the Institute for the Protection and Security of the Citizen (IPSC), European Commission Joint Research Centre (JRC), EU
- **Dr. Nigel Jefferies**, Head of Academic Relationships for Vodafone Group R&D, UK
- **Prof. Antonio Lioy**, Politecnico di Torino, IT
- **Dr. Aljosa Pasic**, ATOS, ES
- **Prof. Reinhard Posch**, CIO for the Austrian Federal Government Republic of Austria, AT
- **Prof. Radu Popescu-Zeletin**, Technical University Berlin and director of the Fraunhofer Institute for Open communication Systems (GMD/FOKUS), DE
- **Dr. Alain MERLE**, Technical manager of CESTI LETI, FR
- **Dr. Claude Castelluccia**, Senior Researcher, INRIA, FR
- **Prof. Jean Jacques Quisquater**, UCL, Crypto Group, BE
- **Prof. Evangelos Markatos**, FORTH-ICS, GR
- **Dr. Steve Purser**, ENISA, EU
- **Dr. Karl F. Rauscher**, Executive Director, Bell Labs Network Reliability & Security Office, USA
- **Prof. Kai Rannenber**, Johann Wolfgang Goethe -Frankfurt University, DE
- **Prof. Pierangela Samarati**, Universita degli Studi di Milano, IT
- **Prof. Fred Piper**, Royal Holloway, UK
- **Dr. Nikos Pronios**, Intracom Defense Electronics, GR

ORGANISING COMMITTEE

- **Mr. Ioannis Askoxylakis**, FORTH-ICS, GR
- **Ms. Theodosia Bitzou**, FORTH-ICS, GR
- **Ms. Alison Manganas**, FORTH-ICS, GR

contact NIS'2010



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>