



ENISA - FORTH
Summer School
on Network & Information Security



15-19 September 2008, Crete, Greece

Promoting a culture of security: mitigating risks through awareness.

www.nis-summer-school.eu



Promoting a culture of security: mitigating risks through awareness.

www.nis-summer-school.eu

Dear Participants,

We would like to WELCOME you to the **1st Network and Information Security Summer School** jointly organized 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**).

Internet-connected systems are subject to millions of online attacks every day. Internet users are plagued by malware, spam, phishing, and other malicious activities. Besides the constantly increasing number of security incidents, we witness a steady **rise in cyber attack sophistication**. During the last few years, there has been a decline in the number of massive easy-to-spot global epidemics, and a shift towards more targeted and evasive attacks. At the same time, cyber-criminals, motivated by the promise of financial gains and personal recognition, constantly devise new deception and exploitation methods. Finally, the unstable political situation in many countries raises the possibility of protracted **cyber wars** which can have a devastating effect to the economies and the lives of citizens in target countries. Understanding properly the issues at hand and raising awareness on good practices is of paramount importance.

ENISA is dedicated to promote the **culture of security in Europe** by pursuing a strategy of mitigating risks through awareness and enhancing the level of expertise in the European Union. Towards this objective, through the NIS Summer School we aim to bring together a distinguished faculty from around the world and an audience of policy makers from EU Member States and EU Institutions, decision makers from industry, as well as members of the academic and research community, for the purpose of identifying current threats and opportunities against the background of recent advances on NIS measures and policies. This will raise the level of expertise of attendees and impact positively on, **the ability of European Union Member States to respond to cyber-attacks**.

This Summer School will have 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 2008 Summer School is on "**Network Security**".

Recognizing the multi-dimensional facet of this theme, we have an array of very interesting lectures covering a variety of aspects such as policy, legal, academic and research. We would like to take this opportunity to thank our **keynote speakers** and faculty for helping us offer a program of such high quality.

We hope that you will enjoy the program of the School and your stay in Crete!

Andrea Pirotti
Executive Director of ENISA

Constantine Stephanidis
Director of FORTH-ICS



LECTURERS

- **Dr. Janet Beattie**, Glen Abbot Ltd, UK
"Business Continuity Planning"
- **Prof. Steven Bellovin**, Columbia Univ., USA
"Newspeak: A Paradigm for Architectural Security"
- **Prof. Levente Buttyan**, Budapest Univ. of Technology & Economics, HU
"Security in wireless sensor and mesh networks"
- **Mr. Ilias Chantzou**, SYMANTEC, BE
"Policy Issues related to Network Security"
- **Dr. Richard Clayton**, Cambridge Univ., UK
"Security Economics and Network Security"
- **Dr. Myriam Dunn**, ETH Zurich, CH
"Critical (Information) Infrastructure Protection: History, Trends, and Concepts"
- **Ms. Anne-Marie Eklund-Löwinder**, .SE, SE
"DNSSEC the .SE way: Overview, deployment and lessons learned"
- **Prof. Mike Fairhurst**, Univ. of Kent, UK
"Biometrics & the citizen: a case study of the future of cooperative planning for security in modern society"
- **Prof. Giusella Finocchiaro**, University of Bologna, IT,
"Main Legal Issues Concerning Information Security"
- **Prof. Angelos Keromytis**, Columbia Univ., USA
"Denial of Service Attacks and Resilient Overlay Networks"
- **Mr. Achim Klabunde**, European Commission
DG-INFSO, EU
"Security in the Regulatory Framework for Electronic Communications"
- **Prof. Evangelos Markatos**, FORTH-ICS, GR
"Emerging Risks in Network and Information Systems Security"
- **Mr. Jose Marcos Muela**
& **Dr. Dimosthenis Ikononou**, ENISA, EU
"Open Doors to Technologies Enhancing Network Resilience"
- **Prof. Bart Preneel**, Katholieke Universiteit Leuven, BE
"Cryptographic algorithms and protocols for network security"
- **Prof. Vassilis Prevelakis**, Technische Universität Braunschweig, DE
"Lessons Learned from the Vodafone Wiretapping Incident"
- **Dr. Wietse Venema**, IBM, USA
"Forensic discovery of hosts and networks"
- **Prof. Paulo Verissimo**, Univ. of Lisbon, PT
"Challenges of Architecting Resilient Critical Information Infrastructures"
- **Dr. Claire Vishik**, Intel, UK
"Building Secure E-commerce Systems"
- **SSA David West**, FBI Cyber Division / Computer Intrusion Unit, USA
"Overview of Cyber Crime in Networked Environments"
- **Mr. Ken Van Wyk**, Outbreak Security, LLC, Board Member at FIRST and FIRST.org, Inc., & Carnegie Mellon University, USA
"The essential role of incident response in secure software development"

WELCOME ADDRESS

- **Mrs. Androulla Vassiliou***, Commissioner for "Health and Consumers", EU

KEYNOTE SPEAKERS

- **Dr. Jorgo Chatzimarkakis**, Member of the European Parliament, EU
"Network and Information Security - Challenges for EU Policymakers"
- **Lord Toby Harris**, House of Lords, UK
"Public Confidence is Endangered unless Information Security is Central to Risk Management"
- **Mr. Mikko H. Hyppönen**, Chief Research Officer, F-Secure, FI
"Fighting Organized Online Crime"

*Invited



Ms. Androulla Vassiliou
*Commissioner for
"Health and Consumers"*

Androulla Vassiliou studied Law at Middle Temple Inn of Court, London (1961-1964) and International affairs at the London Institute of World Affairs, (1964-1966).

She practiced Law in Cyprus for twenty years (1968-1988). During this period she acted as Legal Advisor to The Standard Chartered Bank and later, to the Bank of Cyprus. She had also been on the Board of many public and private companies.

Married to Dr. George Vassiliou, former President of the Republic of Cyprus (1988-1993) and Chief Negotiator for Cyprus' accession to the EU she gave up her legal practice in 1988, upon her husband's election to the Presidency of the Republic of Cyprus.

In 1991, she was elected President of the World Federation of United Nations Associations and she was re-elected to this position for two terms. On the occasion of the 50th Anniversary of the U.N. she had been appointed member of the select international group for the world wide celebrations of this important anniversary, by the Secretary General Boutros Boutros Ghali.

Upon the expiration of her Presidency of WFUNA she was unanimously elected Honorary President of the Federation.

In 1996 she was elected President of the Cyprus Federation of Business and Professional Women and she was re-elected to this position for two terms.

In the year 1996 she was elected Member of the Cyprus House of Representatives representing the Movement of United Democrats, and in 2001 she was re-elected for a second term of five years. During this period she was also a member of the Joint Parliamentary Committee of Cyprus and the EU.

She has been Vice President of the European Liberal Democrats and Reform Party (ELDR) (2001-2006) and as such she was the chairperson of the European Liberal Women's Network.

Network and Information Security - Challenges for EU Policymakers

One of the key challenges for national and European Policymakers, in support of the proper functioning of the Internal Market, is to address the Network and Information Security (NIS) issues under a holistic perspective. Achieving a holistic approach entails, as essential elements of success, the accurate recognition and coordination of the respective roles of the various stakeholders.

The contribution of ENISA towards this goal has been critically important, both in its role as a center of excellence for information sharing and cooperation amongst stakeholders, as well as for the exchange of best practices within Europe and around the world.

European economic integration is in need of an influx of new technologies in pursue of efficiency, effectiveness, increase of productivity and increased profit margins. However, the use of new technologies comes also with potential risks that need to be addressed proactively, by engaging the Industry as well as the target user population. In particular, European Industry should be encouraged to break away from the prevailing mental model that NIS is an additional, and largely unnecessary, cost in doing business. Instead, NIS should be treated as an asset that increases the competitive advantage, as well as the reliability of a partner.

The role that EU Policymakers are called upon to play towards achieving the above objectives is crucially important.

Fighting Organized Online Crime

The virus writers as we used to know them have disappeared. They have almost completely been replaced by professional for-profit virus writers.

How does the underground economy work?

How do the criminals turn malware into money?

How do they move their funds from the cyberworld into real world?

And why have we been unable to fix these problems?



Dr. Jorgo Chatzimarkakis
Member of the European Parliament

Jorgo Chatzimarkakis, MEP, elected as Member of the European Parliament for the German Liberal Party in 2004, is member of the 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.

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, as member of the Pharmaceutical Forum, 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 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).

Jorgo Chatzimarkakis studied agriculture and political sciences in Bonn and Oxford, and holds a PhD in political science, obtained from the University of Bonn in 2000.



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

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.

Public Confidence is Endangered unless Information Security is Central to Risk Management

Too many enterprises give insufficient priority to information security.

There is a real risk that public confidence in using the internet and in conducting transactions electronically could be jeopardised.

Similarly, many government agencies have had major failures in information security and the consequences may affect not just public confidence but also public safety.

Information security must be central to risk management in all organisations.



Lord Toby Harris
House of Lords, UK

Lord Toby Harris of Haringey was made a Life Peer in June 1998. He is Chair of the All-Party Parliamentary Group on Policing and Treasurer of the Parliamentary Information Technology Committee (PITCOM). He was also a member of the House of Lords Select Committee that recently reported on Personal Internet Security.

He was born in 1953 and graduated from Cambridge University in 1975, having studied Natural Sciences and Economics. His professional career began with four years in the Economics Division of the Bank of England. He then spent seven years at the Electricity Consumers' Council, becoming Deputy Director in 1983. In 1987, he became Director of the Association of Community Health Councils for England and Wales (the national statutory body representing patients' interests).

He remained there until October 1998, when he established his own public affairs consultancy, Toby Harris

Associates. Organisations he advises or has advised include KPMG, the National Grid, Unisys, the Anite Group, Airwave Solutions, Sunrise Group, Transport for London, Wyeth Laboratories and the Commission for Patient and Public Involvement in Health.

He was a member of the London Assembly from May 2000 to June 2004, on which he led the Labour Group. He was the first Chair of the Metropolitan Police Authority (MPA), during that period and a member of the Executive of the Association of Police Authorities from 2000 to 2006. He continues to sit on the MPA as the representative of the Home Secretary with a remit to oversee the national and international functions of the Metropolitan Police - primarily its role in counter-terrorism and security.

He was a member of Haringey Council from 1978 to 2002 and was its Leader from 1987 to 1999, having previously spent five years as Chair of Social Services. He was Chair of the Association of London Government, representing the 33 local authorities in London, from its formation in 1995 until 2000, having previously chaired the Association of London Authorities.

From 1986 to 1993, he was Chair of the Association of Metropolitan Authorities' Social Services Committee and led for local government in negotiations about the introduction of Community Care and the Children Act. He is Vice-President of and was formerly a member of the Executive of the Local Government Association.

He is the first Chair of the Institute of Commissioning Professionals, has been a non-executive director of the London Ambulance Service, a Senior Associate of the Kings Fund, and a member of the Committee on the Medical Effects of Air Pollutants.

He is a former member of the Committee of the Regions of the European Union.

Business Continuity Planning

Business Continuity Planning is often seen as a black art rather than a science and there are many standards, handbooks, guidelines, regulatory requirements and codes of practice around the world each presenting varied approaches to business continuity and using different terminology.

This talk presents a methodology which is based on the best elements from the various worldwide methods and links business continuity to risk management, corporate governance and information security. Each of the methods are reviewed for their relevance, depth of content and ease of use.

Newspeak: A Paradigm for Architectural Security

Most computer security problems arise from buggy code. It seems clear that writing large, bug-free programs is and will remain beyond our abilities.

We propose a different goal: protecting what really matters. On e-commerce sites, the web server is primarily a front end for a database.

Protecting the latter is much more important than protecting the former. Doing this properly requires a different approach to overall system architecture.



Ms Janet Beattie
Glen Abbot Ltd., UK

Janet Beattie is the Operations Director of Glen Abbot and started the company with David in 1998.

During her years with Glen Abbot she has worked with a large number of blue chip companies in various sectors including banking, oil, medical, and manufacturing as well as public sector organisations such as local councils, the NHS, museums and art galleries. This work has covered all stages of Business Continuity from project management and analysis to writing plans and testing and training. Janet is also responsible internally for developing methodologies, HR, HSE and Quality Assurance.

One of her recent projects has been the delivery of a report for ENISA on Business and IT Continuity Planning. This report presented a methodology which was compiled from a combination of author's experience and the most well known continuity planning methods from around the world.

In the past, Janet was a research scientist and later moved into Finance and IT, before specialising in the newly emerging discipline of Business Continuity.

Janet is the Administrator for the Scottish Business Continuity Institute (BCI) Forum which involves organising quarterly meetings for Business Continuity professionals in Scotland. She is also a member of the Worldwide BCI Forum and of the Scottish Continuity Group.



Prof. Steven Bellovin
Columbia University, USA

Steven M. Bellovin is a professor of computer science at Columbia University, where he carries out research on networks, security, and especially why the two don't get along. He joined the faculty in 2005 after many years at Bell Labs and AT&T Labs Research, where he was an AT&T Fellow. He received a BA degree from Columbia University, and an MS and PhD in Computer Science from the University of North Carolina at Chapel Hill. While a graduate student, he helped create Netnews; for this, he and the other perpetrators were given the 1995 Usenix Lifetime Achievement Award. He is a member of the National Academy of Engineering and is serving on the Department of Homeland Security's Science and Technology Advisory Board; he has also received the 2007 NIST/NSA National Computer Systems Security Award.

Bellovin is the co-author of "Firewalls and Internet Security: Repelling the Wily Hacker", and holds several patents on cryptographic and network protocols. He has served on many National Research Council study committees, including those on information systems trustworthiness, the privacy implications of authentication technologies, and cybersecurity research needs; he was also a member of the information technology subcommittee of an NRC study group on science versus terrorism. He was a member of the Internet Architecture Board from 1996-2002; he was co-director of the Security Area of the IETF from 2002 through 2004.

Security in wireless sensor and mesh networks

We have entered the era of wireless networks. By now, the number of wireless phones has superseded that of wired ones. Wireless LANs are routinely used by millions of nomadic users and various wireless devices have become commonplace. Moreover, technologists promise us a world of ubiquitous computing, in which myriads of tiny, untethered sensors and actuators will communicate with each other, promptly taking care of our various needs and wishes.

In addition to this pervasiveness, we are witnessing a change of paradigm: initially, wireless devices had limited or no programmability and were managed (and secured) in a highly centralized fashion. Today, high-tier wireless end-systems are full-fledged computers and take an increasingly active role in the networking mechanisms. In the extreme case of multi-hop ad hoc networks, the end systems are the network.

Unfortunately, this evolution is creating new vulnerabilities. Even existing wireless networks (and especially wireless LANs) exhibit a number of security weaknesses, some of which have been painstakingly fixed a posteriori. It is now clear that the security solutions devised for wired networks cannot be used as such to protect the wireless ones. An additional problem is that the frenzy to commercialize quickly new products and new services is in contradiction with the design of a well-thought (and possibly standardized) security architecture.

In this lecture, we will give an overview of the security problems and challenges arising in wireless sensor and mesh networks, and we will present a selected set of security solutions specific to these kinds of wireless networks.



Prof. Levente Buttyan

Budapest University of Technology and Economics, HU

Levente Buttyan received the MSc degree in Computer Science from the Budapest University of Technology and Economics (BME) in 1995, and the Ph.D. degree from the Ecole Polytechnique Federale de Lausanne (EPFL) in 2002. In 2003, he joined the Department of Telecommunications at BME, where he currently holds a position as an Associate Professor and works in the Laboratory of Cryptography and Systems Security (CrySyS).

His research interests are in the design and analysis of security protocols and privacy enhancing mechanisms for wireless networked embedded systems, including wireless sensor networks, vehicular communications, RFID systems, wireless mesh networks, and opportunistic ad hoc networks. Levente Buttyan has numerous peer-reviewed publications in the field of security and privacy in wireless embedded systems. He also served on the Technical Program Committee of several conferences and workshops in this field. He was a steering committee member of ESAS (European Workshop on Security and Privacy in Ad hoc and Sensor Networks), and he was co-chair of the TPC of ESAS in 2006. Currently, he is a Steering Committee member of ACM WiSec (ACM Conference on Wireless Security).

Policy Issues related to Network Security

Ilias Chantzios will speak about the overall regulatory policy approach on network and information security.

He will discuss the question of leadership on IT security policy across the world and will address specifically the EU data protection legislation as a model discussing some of its strong points as well as the challenges that Europe is facing when applying the existing framework.

He will discuss the challenges arising from the links between data protection, data retention and cybercrime legislation and the evolution towards a critical information infrastructure policy touching as well on the growing defense aspects of information security.

He will also propose some suggestion as to where he believes future developments of EU policy will materialize.

Security Economics and Network Security

Back in the 1990s, when people began to notice that the Internet isn't terribly secure, they tried to fix it with more technology, more cryptography, more authentication, more firewalls, more filtering, and to their disappointment, the Internet often didn't get any safer.

We can now explain many of these failures by considering the economics behind the issue - and in particular, do the people who can fix the problems have any incentive to do so?

This talk will provide an introduction to this way of thinking about the world, and will consider the recommendations for the EU and member states made in the ENISA-commissioned report: "Security Economics and the Internal Market", Ross Anderson, Rainer Bohme, Richard Clayton and Tyler Moore, January 2008.



Mr. Ilias Chantzios
SYMANTEC, BE

Ilias Chantzios is in charge of Symantec's Government Relations and Public Affairs programmes for Europe, Middle East, Africa as well as the Asia, Pacific and Japan Regions. He is based in Brussels.

Chantzios represents Symantec before government bodies, national authorities and international organisations advising on public policy issues with particular regard to IT security and availability issues.

Chantzios is a member of the Executive Board of AeA Europe. He was also recently appointed member of the Permanent Stakeholders Group of the European Network and Information Security Agency (ENISA). He was chair of the European Policy Council of Business Software Alliance for two consecutive terms. Chantzios is regularly invited as a speaker to conferences and events on public policy, information security and privacy.

Before joining Symantec in 2004, Chantzios worked as legal and policy officer in the Directorate General Information Society of the European Commission. His tasks were mainly focused around information security policy. He covered the Council of Europe Cybercrime Convention and the Framework Decision on Attacks against Information Systems. Furthermore he worked on a number of EU legislative initiatives relevant to information society and information security, including the directives on Privacy on Electronic Communications and the European Network and Information Security Agency. Chantzios represented the European Commission in various international forums and conferences.

Chantzios holds a law degree from the University of Thessaloniki and a Masters degree in computers and communications law from the University of London. He is fluent in Greek, English and German.



Dr. Richard Clayton
Cambridge University, UK

Dr Richard Clayton ran the team that developed one of the earliest Internet access packages for Windows. In 1995 his company was bought by Demon Internet, then the largest UK ISP and he worked for Demon until 2000. He then went back to the University of Cambridge and obtained a PhD on "Anonymity and Traceability in Cyberspace". Since then he stayed on as an academic; his recent work being a series of papers that study the econometrics of phishing.

He was one of the authors of "Security Economics and the Internal Market", the ENISA-commissioned report that was published in January 2008. This sets out a series of recommendations for the EU and member states on information security issues. It is based on the principles of "security economics" - a powerful way of thinking about security, which is more concerned with the economic incentives of participants than in specifying particular hardware or software solutions.

Critical (Information) Infrastructure Protection: History, Trends, and Concepts

Cyber-threats are a "new" kind of threat to national security and to the very foundations of developed societies. The worst possible consequences of risks created by information and communication technologies manifest themselves in the possible failure of so-called critical infrastructures, which are systems and assets whose incapacity or destruction would have a debilitating impact on the national security and the economic and social well-being of a state.

Driven by a growing concern for the potential vulnerability of networked societies and by the increasing number of disruptions in the cyber-domain, many countries have taken steps to better understand the vulnerabilities and threats that their (information) infrastructure is subject to, and have proposed measures for the protection of these assets.

This presentation will talk about the beginnings of the cyber-threat story and then discuss how the issue has evolved over the years and what the trends seem to be.

Further, it will examine the threat spectrum in terms of actors, technologies, and tools. It will further look at state responses and discuss the differences between them. This will help to characterize the cyber-threat and talk about the consequences for state and non-state actors.

DNSSEC the .SE way: Overview, deployment and lessons learned

DNS Security Extensions (DNSSEC) is a more secure way of doing look-ups of Internet addresses for e.g. web and e-mail.

In contrast to the usual domain name system (DNS), look-ups with DNSSEC are signed cryptographically, which makes it possible to ensure that they originate from the right nameserver and that the content has not been altered or tampered with during transmission.

.SE-DNSSEC is a supplemental service to .SE's domain name service. The objective of the service is for the domain name registrant to be able to secure his/her domains with DNSSEC.

.SE started the deployment 2005, and we've learned a lot during the time.



Dr. Myriam Dunn Cavelty
ETH Zurich, CH

Dr. Myriam Dunn Cavelty is lecturer and head of the new risks research unit at the Center for Security Studies (CSS), ETH Zurich. Dunn Cavelty holds a degree in political science, modern history, and international law from the University of Zurich.

She specializes in security studies and the impact of the information revolution on security policy issues in particular (other topics: information operations, cyber-terrorism, critical infrastructure protection). Along with various articles and book chapters on the topic, she is the author of *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (Routledge, 2008) as well as co-editor of three recent volumes:

The Resurgence of the State: Trend and Processes in Cyberspace Governance (Asghate: 2007); *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace* (Asghate: 2007); and *Securing the Homeland: Critical Infrastructure, Risk, and (In) Security* (Routledge 2008).



Ms. Anne-Marie Eklund Löwinder
.SE, SE

Quality & Security Manager responsible for the security, stability and robustness of the implementation, planning and long-term strategic management of the Swedish ccTLD, .SE. Specialist running projects such as DNSSEC and other security efforts aiming at developing and advancing the security of the Internet infrastructure in Sweden. Member of the boards of the Swedish ISOC Chapter, ISOC-SE, and the Swedish Network Users' Society, SNUS.

SUNDAY, 14 SEPTEMBER

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

21:30 Welcome cocktail at the Platform Area

MONDAY, 15 SEPTEMBER

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

09:00 - 10:00 Welcome Address
Ms. Androulla Vassiliou*, *Commissioner for "Health and Consumers"*10:00 - 11:00 Keynote Address 1
Network and Information Security - Challenges for EU Policymakers
Dr. Jorgo Chatzimarkakis, *Member of the European Parliament*

11:00 - 11:30 Coffee Break

11:30 - 12:30 Keynote Address 2
Public Confidence is Endangered unless Information Security is Central to Risk Management
Lord Toby Harris, *House of Lords*

12:30 - 14:00 Lunch

14:00 - 16:00 **Newspeak: A Paradigm for Architectural Security**
Prof. Steven Bellovin, *Columbia University*

16:00 - 16:30 Coffee Break

16:30 - 18:30 **Critical (Information) Infrastructure Protection: History, Trends, and Concepts**
Dr. Myriam Dunn Cavelty, *ETH Zurich*21:00 **Gala Dinner****TUESDAY, 16 SEPTEMBER**09:00 - 10:00 Keynote Address 3
Fighting Organized Online Crime
Mr. Mikko H. Hyppönen, *Chief Research Officer, F-Secure*10:00 - 11:00 **Policy Issues related to Network Security**
Mr. Ilias Chantzou, *SYMANTEC*

11:00 - 11:30 Coffee Break

11:30 - 12:30 **DNSSEC the .SE way: Overview, deployment and lessons learned**
Ms. Anne-Marie Eklund-Löwinder, *.SE*

12:30 - 14:00 Lunch

14:00 - 16:00 **Cryptographic algorithms and protocols for network security**
Prof. Bart Preneel, *Katholieke Universiteit Leuven*

16:00 - 16:30 Coffee Break

16:30 - 18:30 **Main Legal Issues Concerning Information Security**
Prof. Giusella Finocchiaro, *University of Bologna*18:30 - 19:30 **Open Doors to Technologies Enhancing Network Resilience**
Mr. Jose Marcos Muela & Dr. Demosthenes Ikonomou, *ENISA*

21:00 Dinner

* Invited

WEDNESDAY, 17 SEPTEMBER

09:00 - 11:00	Overview of Cyber Crime in Networked Environments SSA David West, <i>FBI Cyber Division / Computer Intrusion Section</i>
11:00 - 11:30	Coffee Break
11:30 - 12:30	Lessons Learned from the Vodafone Wiretapping Incident Prof. Vassilis Prevelakis, <i>Technische Universität Braunschweig</i>
12:30 - 14:00	Lunch
14:00 - 16:00	"The essential role of incident response in secure software development" Mr. Kenneth R. van Wyk, <i>Outbreak Security, LLC, Board Member at FIRST and FIRST.org, Inc., Carnegie Mellon University</i>
19:30	Social Event: Cretan Cuisine Dinner in Archanes

THURSDAY, 18 SEPTEMBER

09:00 - 11:00	Biometrics and the citizen: a case study of the future of cooperative planning for security in modern society Prof. Mike Fairhurst, <i>University of Kent</i>
11:00 - 11:30	Coffee Break
11:30 - 12:30	Denial Of Service Attacks and Resilient Overlay Networks Prof. Angelos Keromytis, <i>Columbia University</i>
12:30 - 14:00	Lunch
14:00 - 16:00	Forensic discovery of hosts and networks Dr. Wietse Venema, <i>IBM</i>
16:00 - 16:30	Coffee Break
16:30 - 18:30	Challenges of Architecting Resilient Critical Information Infrastructures Prof. Paulo Verissimo, <i>University of Lisbon</i>
18:30 - 19:30	Security in wireless sensor and mesh networks Prof. Levente Buttyan, <i>Budapest Univ. of Technology & Economics</i>
21:00	Dinner

FRIDAY, 19 SEPTEMBER

09:00 - 11:00	Security Economics and Network Security Dr. Richard Clayton, <i>Cambridge University</i>
11:00 - 11:30	Coffee Break
11:30 - 12:30	Building Secure E-commerce Systems Dr. Claire Vishik, <i>Intel</i>
12:30 - 14:00	Lunch
14:00 - 16:00	Business Continuity Planning Dr. Janet Beattie, <i>Glen Abbot Ltd.</i>
16:00 - 16:30	Coffee Break
16:30 - 17:30	Security in the Regulatory Framework for Electronic Communications Mr. Achim Klabunde, <i>European Commission DG-INFOS</i>
17:30 - 18:30	"Emerging Risks in Network and Information Systems Security" Prof. Evangelos Markatos, <i>FORTH-ICS</i>
18:30 - 19:30	Closing remarks
21:00	Dinner

Biometrics and the citizen: a case study of the future of cooperative planning for security in modern society

Security for all its citizens must be one of the priorities for any state. Unsurprisingly, therefore, steps towards security are often Government-led, and the inevitable tensions which always perceived between enhancing security and diminishing the freedom of the individual therefore often become projected into a confrontation, real or imagined, between the state and the citizen. This may be both a misrepresentation and an unnecessary limitation of where a legitimate and important debate should be focused. The citizen should be at the heart of such a debate, not part of just one side of an argument, and should be seen as the facilitator of informed decision making, and as the ultimate principal beneficiary of its outcome. This is a primary principle embraced, for example, in the recent Crosby Report in the UK in connection with progress towards a national Identity Card Scheme.

Indeed, the deployment of biometrics (the measurement of physical or behavioural characteristics such as facial features, fingerprints, iris patterns, etc) for establishing or verifying the identity of individuals represents a good illustrative domain typifying the problems referred to, and this presentation will focus on this technology as a case study. Biometrics is a field around which there is a remarkable circulation of misinformation, where opportunities are in danger of being missed, and where system deployment might be in danger of becoming marginalised, relevant only to specific Government programmes or, at worst, a controlling tool of the state.

The talk will summarise the current focus of the debate and will argue that a more informed discussion is required if society is both to avoid inappropriate adoption of technology which merely restricts rather than liberates, and also to avoid missing out on opportunities to benefit from greater security (and therefore freedom of action) in an increasingly dangerous world.

A primary element of this argument is that the notions of integration and inclusiveness, embracing rather than confronting the citizen, hold the key to balancing security and liberty, and that these notions should be played out on several fronts, including promotion of national partnerships, integration of different strands of technology, better connecting citizens and government, carefully integrating people and information systems, and so on.

The talk will explore these ideas and will show how diversification in application, research and technological development, and enlightened policy-making can provide the foundations on which a more productive and visionary future strategy can be built. It is vital that partnerships between all stakeholders in the security enterprise are nurtured and developed if we are to become the masters rather the servants of security technologies.



Prof. Mike Fairhurst
University of Kent, UK

Professor Michael Fairhurst is Head of the Department of Electronics at Kent. Research interests focus on computational architectures for image analysis and classification, and applications including handwritten text reading and document processing, medical image analysis and, especially, security and biometrics.

Current projects include work on multimodal biometrics, on quantifying the vulnerability of biometric identification techniques, and on the analysis of handwriting, both for identification purposes, and to improve the effectiveness of automated processing for forensic applications. Biometric processing also underpins work which is investigating document encryption linked to biometric data. In related work, he is further developing work he pioneered at Kent which established novel techniques for the assessment and monitoring of neurological conditions (following a stroke, for example) through the analysis of patients' writing and drawing abilities.

Professor Fairhurst sits on numerous Conference, Workshop, and other Committees, and on the Editorial Boards of several international Journals. He has undertaken several international Technology Watch Missions, he was an invited speaker at a recent US/UK Joint Workshop on Homeland Security and is a member of the Steering Committee for the Knowledge Transfer Network in Cyber Security.

He played a leading role in the EU-funded BioSecure Network of Excellence, has participated in and led many UK-based initiatives in this area, and is currently an organiser of a forthcoming European Workshop on Biometrics.

He sits on the UK's Biometrics Assurance Group, a small group of international experts advising UK Government on all aspects of their national biometrics-related programmes.

He is a member of the UK Engineering and Physical Sciences Research Council Peer Review College and has sat on many of their Committees.

He has published some 350 papers in the scientific literature.

He is an elected Fellow of the International Association for Pattern Recognition in recognition of his international contributions to the field.

Main Legal Issues Concerning Information Security

Information security raises many legal issues: provider's liability, intellectual property rights, applicable law. Among them, two subjects will be dealt with in this talk: electronic signatures and data protection.

Both the subjects will be analyzed in the framework of the European legislation.

The European regulation on electronic signatures is constituted by Directive 1999/93/EC on electronic signatures. It aims to increase trust on information network and to develop electronic commerce. The European legislator has adopted a technologically neutral approach, articulated on two levels of electronic signature: the electronic signature and the advanced electronic signature.

The European regulation on data protection is constituted by the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data and by the Directive 2002/58/EC on privacy and electronic communications.

The European regulation can be regarded as concerning the use of information: not limited to defining rules for confidential data, it deals also with the circulation of data in general. Data protection is granted in a broad sense and with a high level of protection, not limited to sensitive data. Information is an asset to be aware of for companies and public administrations: it is a valuable resource to protect and defend having recourse to the instruments provided by the law.

Denial Of Service Attacks and Resilient Overlay Networks

Denial of service (DoS) attacks have been the subject of considerable research in the past few years, with interest remaining high due to their increasing use in fraud and extortion schemes against online businesses. Many of the proposed mechanisms to date require extensive re-engineering of the Internet, in terms of protocols, endpoint software, and the routing infrastructure.

In this talk, I will discuss the Secure Overlay Services (SOS) architecture, which provides service to hosts targeted by DDoS attacks by using a combination of overlay networking, distributed firewalling, and simple packet filtering. I will describe the original architecture as well as three extensions, WebSOS, MOVE and SpreadSpectrum, that address different deployment and use strategies of the basic approach.



Prof. Giusella Finocchiaro
University of Bologna, IT

Giusella Finocchiaro is Full Professor of Internet Law and of Private Law at the University of Bologna, and owner of the Finocchiaro legal firm specializing in internet law. She has been appointed as an Italian correspondent for various projects by the EU Commission and private IT Law Firms. She is also consultant for some legal firms in Brussels. She is a past member of the Tacis Project on Electronic Commerce in Russia. Since 2003 she has been the Scientific Director of the Master's programme: "Information Security" at the Alma Graduate School of the University of Bologna. She is a past member of the UNCITRAL Expert Group on Legal Issues of Digital Signatures. She is a Professor of Information Technology Law, Management School, at the "Luigi Bocconi" University in Milan. She is a contributor for "Il Sole - 24 Ore".

She is the author of several books in the field of internet law including Internet law, Zanichelli, 2001, and Digital signature and electronic signatures - Civil law aspects, Giuffrè, 2003 and has been published in many international books, including Concise European IT Law, ed. Alfred Bullesbach, Yves Pouillet, Corien Prins, Kluwer Law International, 2006; Personal data protection in the workplace in Reasonable expectations of privacy?, ed. Corien Prins, Berend de Vries, Sjaak Nouwt, T.M.C. Asser Press, 2005. She has been published in many international journals including: European Law and Consumer Protection in the Information Age, in Information & Communication Technology Law, vol. 12, n. 2, 2003; Digital Signature and Electronic Signatures: the Italian Regulatory Framework after the D.Lgs. 10/2002, in Electronic Communication Law Review, 2002, vol.9. She has been a speaker in international conferences among which ILPF Conference 2002, "Security v. Privacy".

Finally she is member of (i) the Scientific Committee of many legal reviews, (ii) the Scientific Committee of the Institute of Advanced Studies-University of Bologna, (iii) the Scientific Advisory Committee of the European Privacy Institute, (iv) ENISA Permanent Stakeholders Group, (v) ENISA Working Group on "Privacy e Technology", (vi) the Commission on Technology and Copyright, for the reform of the Copyright Law, by the Italian Minister of Culture.



Prof. Angelos Keromytis
Columbia University, USA

Angelos Keromytis is an Associate Professor at the Department of Computer Science at Columbia University, and director of the Network Security Laboratory. He received his B.Sc. in Computer Science from the University of Crete, Greece, and his M.Sc. and Ph.D. from the Computer and Information Science (CIS) Department, University of Pennsylvania. He is the author and co-author of more than 130 papers on refereed conferences and journals, and has served on over 60 conference program committees. He is an associate editor of the ACM Transactions on Information and Systems Security (TISSEC). He recently co-authored a book on using graphics cards for security, and is a co-founder of StackSafe Inc. His current research interests revolve around systems and network security, and cryptography.

Security in the Regulatory Framework for Electronic Communications

One of the central goals of the reform of the EU regulatory framework for electronic communications is to promote the interests of EU citizens by ensuring a high level of protection of personal data and privacy and ensuring that the integrity and security of public communications networks are maintained. The growing number of new electronic threats in recent years such as viruses, spam, spyware and phishing has further increased the importance of these objectives. Furthermore, the proposed changes to the framework are designed to strengthen the resilience of current networks and systems, complementing other legislation that criminalises certain activities, and to enhance the security of personal data in the electronic communications sector.

The legislative proposals address a range of issues, including: (i) Ensuring that consumers are informed if their personal data have been compromised as a result of a breach of network security; (ii) Giving operators and NRAs more responsibility with respect to the security and integrity of all electronic communications networks and services; (iii) Strengthening implementation and enforcement powers for competent authorities, in particular in the fight against 'spam'.

Emerging Risks in Network and Information Systems Security

Network and Information Systems Security is becoming increasingly important as our society depends more and more on the seamless operation of our cyber-infrastructure. New security risks are emerging, and our society must anticipate them if it is to face future successfully.

In this process we need to identify (i) sources of current and emerging vulnerabilities, and (ii) sources of emerging risks. In this talk, we outline sources of the above information and provide examples of emerging risks.

We survey earlier work which has been done in the area, and we show several different sources of information. We then present a list of current, emerging, and future risks, commenting on the likelihood of their eventual appearance. To put these emerging risks in their appropriate context, we also present some possible usage scenarios, as well as a methodology on systematically creating such security-related scenarios. We finally summarize our findings and provide an outlook for the future.



Mr. Achim Klabunde

European Commission, DG-INFO, EU

Achim Klabunde leads the team for privacy and trust at the European Commission's Directorate General for Information Society and Media. His responsibilities include the privacy and security regulation in the domain of electronic communications and the information society, in particular within the EU regulatory framework for electronic communications. Achim holds a computer science degree from the University of Bonn. Before his post at the Commission, he worked for several ICT and telecommunications companies in Western and Central Europe, as project manager and systems architect. His experience also includes university teaching and consulting in IT security and data protection.



Prof. Evangelos Markatos

FORTH-ICS, GR

Prof. Evangelos Markatos received his diploma in Computer Engineering from the University of Patras in 1988, and the M.S and Ph.D. degrees in Computer Science from the University of Rochester, NY in 1990 and 1993 respectively.

Since 1992 he has collaborated with FORTH-ICS, where he is currently the founder and head of the Distributed Computing Systems Laboratory. He conducts research in several areas including distributed and parallel systems, the World-Wide Web, Internet Systems and Technologies, as well as Computer and Communication Systems Security. He is currently the project manager of the LOBSTER and NoAH projects, both funded in part by the European Union and focusing on developing novel approaches to network monitoring and network security.

Since 1992, he has also been affiliated with the Computer Science Department of the University of Crete, where he is currently a full Professor. Since 2001 Professor Markatos has been the head of the W3C (World Wide Web Consortium) Office in Greece, one of only 17 such offices around the world. Since 2005, he has served as a member of the Permanent Stakeholders Group of ENISA, the European Network and Information Security Agency.

Prof. Markatos, has co-authored more than 80 conference/journal papers and book chapters, has served as a reviewer in for several prestigious Journals, Conferences, and IT projects, and has headed several projects funded by the European Commission, by the Greek Government, and by private Organizations.

Open Doors to Technologies Enhancing Network Resilience

The aim of this lecture is to provide with an insight on the subject of communication networks resilience and the activities of ENISA in this area in the context of the Agency's Work Program 2008. In the context of the lecture, a range of technologies expected to enhance end-to-end network resilience, such as IPv6, DNSSec and MPLS, will be presented.

Cryptographic algorithms and protocols for network security

This talk presents an overview of the state of the art of cryptographic algorithms and protocols for network security.

While creating a "secure pipe" and authenticating the entities is the easy part of network security, we can't escape the observation that very often security problems are identified in algorithms, protocols and their implementations.

We will explore the reasons for these problems and discuss which approaches can help us to avoid some of these problems in the future.



Mr. Marcos Muela
ENISA, EU

Mr. Marcos Muela, holds over 13 years of progressive responsible experience in ICT including overseeing and developing distributed and centralized ICT infrastructure and mission-critical systems in international controlled environments. Mr Muela has 7 years of experience as a professional trainer of ICT professionals. He holds a PhD in IT, a Masters Degree in ICT and holds a Bachelor Degree in Computer Networks, more than 3.000 hours in additional ICT training and 24 Professional Certifications. He joined the ENISA last February as Expert in Security Technologies and is currently working on identifying the current and emerging technologies used by Service Providers around Europe to improve Network Resilience.



Dr. Demosthenes Ikonomou
ENISA, EU

Demosthenes Ikonomou received his Masters of Science in Electronics and Computer Sciences and his Ph.D. in applied sciences from the University of Southampton, United Kingdom, in 1992 and the Université catholique de Louvain-la-Neuve (UCL), Belgium, in 2002 respectively. Between 1996-2008 he worked for DG Information Society & Media (INFOS) of the European Commission mainly involved in the management of R&D projects in the fields of wireless and personal communications as well as networked media. In 2008 he joined the Technical Department of the European Network and Information Security Agency (ENISA) as a Senior Expert in the section of Security Tools and Architecture



Prof. Bart Preneel
Katholieke Universiteit Leuven, BE

Bart Preneel received the Doctorate in Applied Sciences from the Katholieke Universiteit Leuven (Belgium) where he is currently a full professor. He was visiting professor at several universities in Europe and research fellow at the University of California at Berkeley. His main research interests are cryptography and information security. He has authored and co-authored more than 200 scientific publications. He is president of the IACR (International Association for Cryptologic Research) and a member of the Editorial Board of the Journal of Cryptology and of the IEEE Transactions on Forensics and Information Security.

He has participated to 25 research projects sponsored by the European Commission, for five of these as project manager. He has been program chair of ten international conferences and he has been an invited speaker at more than 30 conferences. In 2003, he has received the European Information Security Award in the area of academic research.

He is president of L-SEC vzw. (Leuven Security Excellence Consortium), an association of 60 companies and research institutions in the area of e-security. He is cofounder and conductor of the jazz ensemble of the K.U.Leuven.

Lessons Learned from the Vodafone Wiretapping Incident

In the run up to the 2004 Olympics an unknown group infiltrated the network of a Greek mobile operator (Vodafone) and carried out extensive wiretaps of various highly placed individuals in Greek government, security forces and industry. A cell phone used by the Greek Prime Minister himself was also tapped.

We analyse the incident, the methods used by the infiltrators, the response of the company, law enforcement and regulatory authorities and attempt to draw lessons on how to reduce the possibility of a recurrence, and various response strategies that can be employed if a similar infiltration is detected in the future.

Forensic discovery of hosts and networks

Wietse will present lessons learned about the persistence of information in file systems and in main memory of modern computers - not only how long information persists, but also why this happens, and what the limitations of that information are. Many examples are from UNIX/Linux systems, but some examples cover Windows as well (and illustrate that Windows and *NIX aren't fundamentally different).



Prof. Vassilis Prevelakis
Technische Universität Braunschweig, DE

Vassilis Prevelakis is visiting Professor at the Technische Universität Braunschweig in Germany. He has worked in various areas of security in Systems and Networks both in his current academic capacity and as a free-lance consultant.

Prevelakis' current research involves issues related to automation network security, secure software design, autoconfiguration issues in secure VPNs, etc. He has published numerous papers in these areas and is actively involved in standards bodies such as the IETF.

He has received research funding from DARPA (CHATS) and from NSF (CAREER). Prevelakis received his Ph.D. from the University of Geneva in Switzerland and his M.Sc. and B.Sc. from the University of Kent in the U.K.



Dr. Wietse Venema
IBM, USA

Wietse Venema is known for his software such as the TCP Wrapper and the Postfix open source mail system. He co-authored the SATAN network scanner and the Coroner's Toolkit (TCT) for forensic analysis, as well as a book on Forensic Discovery. Wietse received awards from the System Administrator's Guild (SAGE), the Netherlands UNIX User Group, Sendmail, and IBM (outstanding technical achievement).

He served a two-year term as chair of the international Forum of Incident Response and Security Teams (FIRST). Wietse is currently a research staff member at the IBM T. J. Watson research center. After completing his Ph.D. in physics he changed career to computer science and never looked back.

Challenges of Architecting Resilient Critical Information Infrastructures

This lecture will focus on innovative concepts related to achieving trustworthiness of control system cyber architectures such as used in modern critical information infrastructures. Power grids will be used as example, since they are an excellent case study on the challenges of future control systems. Over the past few decades, utility infrastructures have become largely computerized, remotely/automatically controlled, and interconnected. Such a web of critical information infrastructures became susceptible to digital accidental faults and computer-borne malicious cyber attacks, and understanding the problems related with resilience is a complex task, due to their hybrid composition (SCADA, corporate intranets and Internet). However, these infrastructures must be architected and managed having in mind even better security and dependability goals than classical IT systems, in order to present very high levels of resilience. The need for a new architecture is explained by the fact that cyber architectures for process control, despite being basically physical processes controlled by computers interconnected by networks, exhibit a potentially huge cost of failure in socio-economic terms, thus bringing extremely demanding requirements, which have not been previously found together in a same class of computer-based systems.

The lecture will discuss some recent advances in this area, based on concepts that help realize the innovative vision of automatic security. We present a reference architecture for advanced critical infrastructures featuring a combination of: aprioristic prevention of known attack and vulnerability combinations; middleware devices that achieve automatic security, through tolerance of remaining faults and intrusions; use of trusted-trustworthy components and architectural hybridization; perpetual unattended operation through proactive and reactive recovery mechanisms for self-healing.

Secure E-commerce Systems

Internet-based electronic commerce is ubiquitous in developed countries, with purchases, bill payment, and other online interactions becoming routine for many people. Although concerns about security and privacy exist, clearly there is enough trust in digital economy to ensure that electronic commerce continues to grow. But what does it take to build secure electronic commerce systems?

The talk will start with the history of electronic commerce, outline main areas of security that need to be addressed when discussing secure e-commerce, evaluate privacy issues associated with e-commerce applications, explain common security features in standard transport and application protocols as well as security features in user-facing and back-end electronic commerce systems, address issues of usability and usage patterns, and conclude with implementation examples for various types of e-commerce systems.



Prof. Paulo Verissimo

University of Lisbon, PT

Paulo Verissimo is currently a professor of the Department of Informatics (DI) of the University of Lisboa Faculty of Sciences and Director of LASIGE, a research laboratory of the DI.

He is Fellow of the IEEE. He is also associate editor of the Elsevier Int'l Journal on Critical Infrastructure Protection, and past associate editor of the IEEE Tacs. on Dependable and Secure Computing.

He belonged to the European Security & Dependability Advisory Board. He is past Chair of the IEEE Technical Committee on Fault Tolerant Computing and of the Steering Committee of the DSN conference, and belonged to the Executive Board of the CaberNet European Network of Excellence.

He was coordinator of the CORTEX IST/FET project (<http://cortex.di.fc.ul.pt>). Paulo Verissimo leads the Navigators research group of LASIGE, and is currently interested in: architecture, middleware and protocols for distributed, pervasive and embedded systems, in the facets of real-time adaptability and fault/intrusion tolerance.

He is author of more than 130 refereed publications in international scientific conferences and journals in the area, and co-author of five books.



Dr. Claire Vishik

Intel, UK

Dr. Claire Vishik works at Intel Corporation UK. Her work focuses on hardware security, trusted computing, privacy enhancing

technologies, some aspects of encryption and related policy issues. Claire is a member of the Permanent Stakeholders Group of ENISA, the European Network and Information Security Agency. She is active in standards development and is on the Board of Directors of TCG, the Trusted Computing Group.

Claire received her PhD from the University of Texas at Austin. Prior to joining Intel, Claire worked at Schlumberger Laboratory for Computer Science and AT&T (SBC) Laboratories studying security and other aspects of Internet technologies, from electronic commerce and communication protocols to software systems and applications. Claire is the author of many papers and reports and 23 pending and granted US patents.

Overview of Cyber Crime in Networked Environments

Introduction

FBI Mission / Priorities / Location /
History/People/Motto & Core Values
What We Investigate - Priorities
(National Security & Criminal)
Cyber Investigative Priorities /
Organization / Objectives

The Problem

Threat / Forecast / Critical Infrastructure /
Growing Trends

Cyber Crime

Computer Intrusions, Online Predators,
Piracy / Intellectual Property, Internet
Fraud

SSA David West

FBI Cyber Division/Computer Intrusion Section

Supervisory Special Agent David West is the Program Manager for the Cyber Division / Computer Intrusion Section. SSA West is currently assigned to FBI Headquarters in Washington, DC and has Cyber Program Management responsibilities for various field offices throughout the United States as well as Legal Attaches Offices (Legats) throughout the World.

SSA West has worked Counter Terrorism/Counter Intelligence and Criminal Cyber investigations in both the Philadelphia and Washington Field Offices. Additionally, SSA West has worked investigations related to White House Background Investigations, Child Pornography, Interstate Transportation of Obscene Material, Intellectual Property Rights, and Theft of Trade Secret cases. SSA West is also a member of the FBI's National Recruiting Team.

Prior to joining the FBI, SSA West had worked for over 15 years in the private sector as a Systems Integrator and Project Manager. SSA West has an Engineering Degree from North Carolina A&T State University and continuing education certificates from the Pennsylvania State University as well as other organizations. SSA West has held membership in professional organizations including the National Society of Professional Engineers (NSPE) and the National Association of Radio and Telecommunications Engineers (NARTE).

The rapid evolution of computer technology, coupled with ever-creative techniques used by foreign intelligence actors, terrorists, and criminals, requires FBI investigators and professionals to have highly specialized computer-based skills. The FBI Cyber Program uses a centrally-coordinated strategy to support crucial counter terrorism, counterintelligence, and criminal investigations. The Cyber Program also targets major criminal violators with a cyber nexus.

Pursuant to the National Strategy to Secure Cyberspace signed by the President of the United States in February 2003, the Department of Justice and the Federal Bureau of Investigation (FBI) lead the national effort to investigate and prosecute cyber crime.

The essential role of incident response in secure software development

Incident response as we know it has come a long way since its inception in the late 1980s. In today's digital environment, it is vital that incident response teams are able to rise to increasing demands. Today's demands range from ensuring regulatory compliance through working with software development teams to help adequately build security in to our business software.

In his talk, Ken will discuss the changing incident response environment and what sorts of technical skill sets it will take for a CSIRT to be able to succeed in the future.



Mr. Kenneth R. van Wyk

Outbreak Security, LLC, Board Member at FIRST and FIRST.org, Inc., and Carnegie Mellon University, USA

Kenneth R. van Wyk is an internationally recognized information security expert and author of the O'Reilly and Associates books, *Incident Response* and *Secure Coding*. In addition to providing consulting and training services through his company, KRvW Associates, LLC, (<http://www.KRvW.com>), he currently holds numerous positions: Founder and moderator of the "Secure Coding" mailing list, SC-L@SecureCoding.org, Member of the Board of Directors and Steering Committee for non-profit organization, FIRST.org, Inc. (<http://www.first.org>), monthly columnist for on-line security portal, eSecurityPlanet and a Visiting Scientist at Carnegie Mellon University's Software Engineering Institute.

Ken has 20+ years experience as an IT Security practitioner in the academic, military, and commercial sectors. He has held senior and executive technologist positions at Tekmark, Para-Protect, Science Applications International Corporation (SAIC), in addition to the U.S. Department of Defense and Carnegie Mellon and Lehigh Universities.

Ken also served a two-year elected position as a member of the Steering Committee, and a one-year elected position as the Chairman of the Steering Committee, for the Forum of Incident Response and Security Teams (FIRST) organization. At Carnegie Mellon University's Software Engineering Institute, Ken was one of the founders of the Computer Emergency Response Team (CERT®). He holds an engineering degree from Lehigh University and is a frequent speaker at technical conferences, and has presented tutorials and technical sessions CSI, ISF, USENIX, FIRST, AusCERT, and others. Ken is also a CERT® Certified Computer Security Incident Handler.

COMMITTEES

STEERING COMMITTEE

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

SCIENTIFIC COMMITTEE

- **Dr. Sotiris Ioannidis**, FORTH-ICS, co-chair, GR
- **Dr. Panagiotis Trimintzios**, ENISA, co-chair, EU

ADVISORY COMMITTEE

- **Prof. Ross Anderson**, Cambridge Univ., UK
- **Prof. Angelos Bilas**, FORTH-ICS, GR
- **Prof. Matt Bishop**, University of California, Davis, USA
- **Dr. Alain Esterle**, ENISA, EU
- **Prof. Giusella Finocchiaro**, University of Bologna, IT
- **Prof. Theodoulos Garefalakis**, FORTH-IACM, GR
- **Dr. Jaap-Henk Hoepman**, Radboud University Nijmegen, NL
- **Prof. Manolis Katevenis**, FORTH-ICS, GR
- **Prof. Antonio Lioy**, Politecnico di Torino, IT
- **Prof. Evangelos Markatos**, FORTH-ICS, GR
- **Dr. Evangelos Ouzounis**, ENISA, EU
- **Prof. Sachar Paulus**, SAP AG, DE
- **Prof. Norbert Pohlmann**, Univ. of Applied Sciences Gelsenkirchen, DE
- **Prof. Reinhard Posch**, TU Graz, IAIK, AT
- **Prof. Jacques Stern**, ENS/DI, FR
- **Prof. Apostolos Traganitis**, FORTH-ICS, GR
- **Prof. Louise Yngstrom**, Stockholm Univ., SE

LOCAL ARRANGEMENTS COMMITTEE

- **Mr. Ioannis Askoxylakis**, FORTH-ICS, chair, GR
- **Ms. Anna Doxastaki**, FORTH-ICS, GR
- **Ms. Maria Mastoraki**, FORTH-ICS, GR
- **Ms. Eleni Orphanoudaki**, FORTH-ICS, GR

PUBLICITY COMMITTEE

- **Ms. Theodosia Bitzou**, FORTH-ICS, GR
- **Mr. Tim Mertens**, ENISA, EU
- **Ms. Eleni Orphanoudaki**, FORTH-ICS, GR
- **Dr. Panagiotis Trimintzios**, ENISA, EU

ENISA - FORTH
Summer School
on Network & Information Security



15-19 September 2008, Crete, Greece

Theme: Network Security



about ENISA

<http://enisa.europa.eu>

ENISA is mandated to assist the European Union and its Member States 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 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 are functioning, as they constitute the "Digital Economy." That is why ENISA is working with Network and Information Security for the EU and the Member States.

about FORTH-ICS

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

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.



ENISA - FORTH
Summer School
on Network & Information Security



15-19 September 2008, Crete, Greece

Theme: Network Security

www.nis-summer-school.eu

ENISA
European Network and Information Security Agency

Science and Technology Park of Crete
Vassilika Vouton, GR-70013 Heraklion
Crete, Greece
Tel: +30 2810391280
Fax: +30 2810391410
Email: info@enisa.europa.eu



<http://enisa.europa.eu>

FORTH - ICS
Foundation for Research and Technology - Hellas
Institute of Computer Science

N. Plastira 100
Vassilika Vouton, GR-70013 Heraklion
Crete, Greece
Tel.: +30 2810391600
Fax: +30 2810391601
Email: ics@ics.forth.gr



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