

ENISA Quarterly Review



Vol. 6, No. 2, June 2010

IN THIS EDITION

- | | |
|---|---|
| A Letter from the Executive Director | 2 |
| Quantum Key Distribution | 3 |
| Who will Patch my Mum's PC? | 5 |
| Towards the First Pan-European
Exercise on Critical ICT
Infrastructure Protection | 7 |
| ENISA's Country Reports | 9 |



A LETTER FROM THE EXECUTIVE DIRECTOR

Recent Landmarks for ENISA

Udo Helmbrecht



Dear reader,

There have been changes recently in the political landscape in relation to ENISA. A number of important steps have been taken which have long term, positive implications for the Agency.

Reinforced role for ENISA in the Digital Agenda

The Communication on the Digital Agenda for Europe, published on 19 May, has sent a new, decisive signal of trust in the Agency. A reinforced role for ENISA was outlined by Commissioner Kroes which includes a more active role for the Agency in Computer Emergency Response Teams (CERTs), trust and security, and in cyber-crime prevention.

Similarly, recent [Council conclusions](#) point towards closer co-operation between ENISA and cyber-crime bodies.

Finally, the Spanish EU [Presidency Grenada informal \(discussion\) 'Non Paper'](#) called for a reinforced ENISA, for example in the context of establishing a European framework for eID and authentication, to improve international co-ordination against cyber-attacks.

These consistent and strong calls for 'more ENISA' and 'more security' are also in line with citizens' expectations of the EU and the increased need for security for the economy. We are pleased to see that our work is being both appreciated and recognised.

CIIP Exercise Preparations

In line with the political signals, the Agency is preparing for the first Pan-European [CIIP exercises](#) (Critical Information Infrastructure Protection). Arrangements are well under way; ENISA recently organised a workshop, hosted by the Estonian Ministry of Economic Affairs & Communications in Tallinn. The exercise will test the efficiency of communication between different Member States during incidents affecting the normal operation of the Internet. The exercise is planned to take place in early November 2010 (see page 7 for more information).

Implementing Article 13a

We have also taken decisive steps for implementing article 13a of the 'Telecom Package'. In co-operation with the EU Spanish Presidency, we organised a workshop on the transposition of Art.13a into national law. The national authorities of the different Member States and the European Commission met and identified key issues, concluding that the biggest challenge is the harmonisation across Europe of different article 13a implementations. ENISA's facilitating role is therefore key in achieving momentum on several important issues. The Agency has also recently published a [good practice](#)

[guide](#) on national incident reporting schemes – one of the key topics of article 13a.

There are many other things which I would also like to mention including recent reports on [Flying 2.0](#) – a scenario on the Internet of Things (IoT), the [PROCENT report on EU ICT research priorities](#), the new, [updated and expanded Country reports](#) and the recent [5th CERTs workshop](#) organised by the Agency. We have also met and welcomed the new Permanent Stakeholders' Group for the first time. But space is short and there is much more for you to read in the following pages. So, to sum up, it is enough to say that the Agency is working at full throttle, 'Securing Europe's Information Society'.

With renewed political backing, we are now looking forward to the 'ENISA II' regulation, which the Commission has announced will be proposed later this year.

Enjoy reading.

Udo Helmbrecht
Executive Director, ENISA



QUANTUM KEY DISTRIBUTION

Real security or just hype?

Giles Hogben



Quantum Key Distribution (QKD) is a method for agreeing encryption keys between two parties remotely. Its most important feature is that it can be used to distribute very long secret keys in such a way that it is known that no eavesdropping has been successful.

QKD enables the encryption of data using random keys of the same length as the data being transmitted – in other words, using a true one-time-pad encryption. Encryption using a one-time-pad can only be provably unbreakable if the key generation algorithm uses a true random number generator and randomness is not lost in key agreement. As an aside, truly random key generation can also be achieved using techniques based on quantum mechanical properties [see Assche, Gilles Van. *Quantum Cryptography and Secret-Key Distillation*].

The use of one-time-pads for encryption, in combination with eavesdrop protection based on QKD, promises unconditionally secure transmission of messages – i.e., an attacker can gain no knowledge about the message. This can now be achieved at speeds which make it practical for certain real-world applications.

QKD uses the physical property of quantum mechanical states, i.e., that they are altered by certain acts of observation. At a small scale (approximately single photons or the wavelength of light), such alterations and therefore the observation (eavesdropping) that caused them, can be reliably detected. QKD provides protocols (for example, BB84, E91) and implementations for using this property to

detect eavesdropping of secret key material. In QKD, a secret key is encoded as a set of quantum mechanical states, such that any act of observation which might lead to knowledge about the message is detected through its effect on those states. Only parts of the message which are known not to have been observed are retained.

QKD relies on physical properties rather than the intractability of a mathematical property (asymmetric cryptography, for example, relies on the intractability of certain mathematical problems, such as the factorisation of large numbers). This means that, unlike current classical cryptography techniques, the message security provided by QKD does not have a 'sell-by-date' determined by the inexorable progress in computing power. In other words, it provides 'forward security'.

What it is not

- QKD is not an encryption technique. Quantum Key Distribution is sometimes described as 'quantum cryptography' but it is not a technique for encrypting data, only for distributing keys in such a way that any eavesdropping is known. Given knowledge of eavesdropping, only key material which is known not to have been eavesdropped upon is then used to encrypt data.
- QKD is not exclusively quantum mechanical – it requires an initial secret, which must be established using a classical method (such as Public Key Infrastructure (PKI)) in order to authenticate both parties. This initial secret is then 'grown' using QKD into a secret which is suitable for one-time-pad encryption.
- QKD is not possible over unlimited distances, with current implementations. The current maximum range is of the order of 100km. This problem could be solved using repeaters, but repeaters which do not have to be trusted (i.e., do not read and re-encode the key material) are not currently available. Therefore such a repeater has to be trusted and such 'QKD networking devices' are in the early stages of development.
- QKD does not replace end-to-end security. If, for example, initial authentication of the parties is compromised, the vetting of the staff with access to the secrets is not

Key points

- The main use-case for QKD is the sharing of very long keys which may be used to provide message confidentiality using one-time-pad encryption. Due to its high cost, this means its main area of application is very high assurance applications (particularly related to national security and government use-cases).
- QKD provides future-proof secrecy – because the security of key material does not depend on the computational intractability of the algorithm used, but on physical properties which do not change over time.
- QKD relies on a security mechanism which is completely separate from traditional methods used for key exchange. It is therefore useful to develop as an alternative method which could be an essential fall-back in case other regimes become unusable (for example in case quantum computers become practical for factorisation problems, rendering traditional encryption useless).

sufficient, or, if the equipment used has back-doors, then the investment in security provided by QKD is wasted. In other words, QKD is only one link in a chain of security measures used for encrypting data and, if the other links are of unequal strength, it may not be a rational investment.

- QKD has nothing to do with Quantum Computing or Quantum Cryptanalysis – other than the encoding of information using quantum states. Quantum computing and quantum cryptanalysis use information encoded in quantum states to process information. This can be used to perform certain computing operations (such as factorisation) much more efficiently than classical computing machines.
- QKD cannot be used to transmit specific predetermined information, only to agree on a randomised secret. Since vulnerable parts of the message are routinely discarded as part of the BB84 algorithm (a process known as 'sifting'), any predetermined message would be corrupted.



Implementations and weaknesses

There are currently a number of (high cost) commercial implementations of the theory. These implementations use either:

- Discrete Variable measurements: this is typically based on the measurement of the polarisation of individual photons. This was the first type of system to be implemented and therefore may be considered more mature in terms of implementation security and robustness. However, compared with continuous variable systems, the data transmission rate is much lower, because of the need to isolate individual particles (of the order of KB/Sec).
- Continuous Variable measurements: this is typically based on the measurement of the phase and amplitude of a laser beam to encode information. This is a relatively recent development and therefore has less maturity in terms of security testing, but promises considerably higher data transmission (of the order of MB/Sec). Another advantage of continuous variable approaches is that they are possible using off-the-shelf equipment.

There are some well-documented attacks against implementations, although these generally only show a slight weakening of the unconditional security offered and not a practical attack. (For more information, see: http://arxiv.org/PS_cache/arxiv/pdf/0809/0809.3408v2.pdf and <http://spiedl.aip.org/getabs/servlet/GetabsServlet?prog=normal&id=PSISDG00671000000167100100001&idtype=cvips&gifs=yes>.)

Areas of controversy and open issues

There are a number of important areas of uncertainty and debate in this area:

- Which use-cases justify the cost and complexity of implementation? Given that the security of QKD lies in its ability to exchange very large keys in a way which provides so-called 'forward security' (i.e., given that QKD only grows keys), at what point does it become worthwhile to invest in QKD equipment rather than, for example, the exchange of very large keys such as those stored on hard drives?
- The concept of 'unconditional security' – when the models used to prove unconditional security will always rely on a set of assumptions, which is necessarily incomplete. Attacks on QKD all rely on inaccurate modelling of theory in implementation because of



hidden assumptions. It is clearly impossible for any implementation to be immune to the discovery of a new assumption which was not previously considered.

- Is it worth having one link in the security chain so strong when all the other links are weaker?

Future trends and research

In the near future significant developments can be expected in QKD in the following areas:

- Range – the distance over which key agreement is possible can be expected to increase. Quantum repeaters are one way of achieving this. These are devices which can increase the range of transmission without having to be trusted. Although quantum states cannot be cloned, they can be stored and retransmitted without being observed. Quantum repeaters use this possibility, but practical commercial implementations are not yet available.

- Bandwidth – the bit-rate of transmission can be expected to increase.
- Cost – the cost of equipment can be expected to decrease.
- Quantum Random Number Generation: keys used for one-time-pads are only unconditionally secure if the process used to generate the keys is perfectly random. Measurements of quantum states can be used to create perfectly random strings.

ENISA is grateful to the following for their input and advice:

- Rainer Plaga, BSI, Germany
- Johannes Skaar, Norwegian University of Science and Technology

Dr. Giles Hogben
(Giles.Hogben@enisa.europa.eu) is an Expert in Application Security at ENISA.

WHO WILL PATCH MY MUM'S PC?

Agris Belasovs



Nowadays news articles and studies frequently refer to viruses, infected computers and botnets, and their impact on and possible consequences for critical information infrastructure. Considerable effort is expended in analysing the source of these problems, which may be criminal activity for financial gain. It is widely recognised that many of these botnets are, to a large extent, composed of infected home computers. Obviously lack of awareness and the carelessness of end-users, who are not (and should not be expected to be) experts in network and information security, do not improve the situation. Unfortunately this also goes hand in hand with deficiencies inherent in the actual technologies in use themselves.

How can we improve the level of protection of the average home computer against attacks from the network?

There are several well known factors which greatly contribute to the success of network-based attacks. Focusing on the home computer environment, these include insecure software, the widespread usage of administrative privileges, weak access controls, the running of unnecessary services and their exposure to the network, the absence of anti-malware tools and the general lack of awareness of the user. Each of these factors increases the probability of success of an attack from the network.

This article addresses just one of these weaknesses – insecure software and, more specifically, the challenges of timely software updating (patching) on home computers.

Vulnerabilities in the operating system (OS) and applications are one of the main vectors of an attack. For this reason it is very important to apply security updates issued by software vendors in a timely fashion. Although there will always remain the possibility that, where no patch is available, the vulnerability can be used for an attack, timely patching of software significantly decreases the chance of a computer being infected by mainstream malware. This applies to corporate networks as well as to home-user computers connected to the Internet. Of course, the challenges differ for these two environments. For example, in corporate networks risk assessment plays an important role in the software updating process and patches need to be properly tested for compatibility with other software used by the company because the consequences of system downtime as a result of an untested patch are usually much worse than in the average home-user environment.

Some OS distributions offer centralised package management solutions which simplify the process of keeping computer software up to date – both the operating system and applications. However, on home computers Microsoft Windows OS is dominant; according to several sources, the share of Microsoft Windows in the OS market is around 90%.

Microsoft Windows OS has an automatic updating mechanism. However, by default, Microsoft Windows uses Windows Update, which provides updates only for Windows OS and device drivers but not for other Microsoft software (such as Microsoft Office). Users need to opt in for Microsoft Update instead of Windows Update in order to obtain updates for other Microsoft software (see www.microsoft.com/windows/downloads/windowsupdate/learn/windowsxp.msp#EEF for switching to Microsoft Update in Windows XP,

www.microsoft.com/windows/downloads/windowsupdate/learn/windowsvista.msp#ESC for switching in Windows Vista and <http://windows.microsoft.com/en-XM/windows7/Change-how-Windows-installs-or-notifies-you-about-updates> for switching in Windows 7).

The responsibility for updating all the other, non-Microsoft software components is left to the specific software or the user.

There exist Microsoft (www.microsoft.com/downloads/details.aspx?familyid=C3D986D0-ECC3-4CE0-9C25-048EC5B52A4F&displaylang=en) and third party tools which offer centralised software management both for Microsoft and non-Microsoft client software for corporate networks with computers using Microsoft Windows. These tools are not applicable to either home-users or small networks of micro-enterprises, which do not have resources available to invest in commercial patch management solutions. This user group is left with the different kinds of software update mechanisms provided by software vendors.



Application vendors often offer built-in solutions to check for updates. However, these are difficult to deal with for the average computer user for a number of reasons: there may be decentralised and varying methods of configuration, or problems with applying updates if the user has followed best practice and has no Administrator privileges, and the user may need special skills to understand the configuration options. Some users are confused by the software update screens asking for their input. The result in such cases is that non-Microsoft software updates may not be applied at all, leaving the computer exposed to attacks which exploit the vulnerabilities in these applications.

There are several free tools available on the Internet (for example, [www.techsupportalert.com/best-free-software-](http://www.techsupportalert.com/best-free-software-update-monitor.htm)

[update-monitor.htm](http://www.techsupportalert.com/best-free-software-update-monitor.htm)), which can be installed by the end-user of a computer with a Microsoft OS and which provide help and some automation in keeping computer software up to date. However the average computer user is not aware of the necessity to apply security patches to applications and does not want to spend time searching and configuring the tools. As a result, the tools which could help to keep computers up to date are not used to provide updates for a significant share of home computers. For example, one of the vendors offering an updating tool reports that, in January 2010, there were more than 2 million users of their software (http://secunia.com/gfx/pdf/Secunia_RSA_Software_Portfolio_Security_Exposure.pdf). Another vendor reports around 4.8 million users (<http://software-informer.software.informer.com/users/>). This is not much in the light of Windows' 90% market share of the 422 million

households connected to the Internet by the end of 2009 – one in five households worldwide with a fixed broadband connection – estimated by the Gartner report of September 2009 (www.gartner.com/it/page.jsp?id=1189323).

What is needed is an 'enabled by default' solution, shipped with the OS, which would automate the application of security updates for any installed software in a very user-friendly way. While this would not fix every weakness to which computers are victim, it would greatly help the average end-user in keeping his or her computer better protected.

Agris Belasovs (agris.belasovs@enisa.europa.eu) is an Expert in Computer Incident & Response Handling at ENISA.



5-7 October 2010
Maritim Hotel
Berlin, Germany
www.isse.eu.com

Europe's only independent, interdisciplinary conference for e-security and identity management

Over the past decade, **Information Security Solutions Europe (ISSE)** has built an unrivalled reputation for its world-class, interdisciplinary approach and independent perspective on the e-security market.

On 5-7 October 2010, ISSE will join forces in Berlin with the **GI-SICHERHEIT** conference, the highly respected bi-annual security event run by the German Informatics Society (Gesellschaft für Informatik, GI).

Over four hundred ICT security professionals and industry experts will come together for a unique all-encompassing opportunity to learn, share and discuss the latest developments in e-security and identity management.

Key areas covered by our world-class programme include:

- > Identity and Access Management
- > The Economics of Security
- > Emerging Threats & Technologies
- > Securing Cloud-based Applications
- > Biometrics & Digital Signatures
- > Privacy and Data Protection
- > Network and Mobile Security
- > Hackers and Phishing Attacks
- > Cryptography Theory & Practice
- > e-Government - Governance and Policy
- > Large-scale Enterprise Security
- > Critical Infrastructure Protection
- > Dependability & Fault Tolerance
- > Cybercrime and Forensics
- > Fraud Detection & Prevention
- > Multi-media Security
- > The Future of Information Security

In collaboration with 

www.isse.eu.com

TOWARDS THE FIRST PAN-EUROPEAN EXERCISE ON CRITICAL ICT INFRASTRUCTURE PROTECTION

The Pan-European Exercise Planners



The Pan-European Exercise Planners

Exercises have long been widely used in various sectors. They are now commonly deployed by many players in the Information and Communication Technology (ICT) sector, mostly telecommunication network operators and Computer Security Incident Response Teams (CSIRTs).

Exercises ensure that participants are fully prepared and capable of responding to incidents by efficiently following existing preparedness measures, such as business continuity and disaster recovery procedures. Increasingly Member States (MS) of the European Union (EU) and businesses with an understanding of infrastructure protection and disaster management are viewing exercises as an essential means to demonstrate and gain greater knowledge of security and gaps in their preparedness.

Policy context

In the European Commission's Communication on Critical Information Infrastructure Protection (CIIP) ('Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience', COM(2009)149), the importance of running cyber-security exercises is highlighted. The Communication especially refers to pan-European exercises and sets the target for conducting exercises clearly: "The Commission invites Member States to

organize regular exercises for large scale networks security incident response and disaster recovery...".

The EU institutions have gradually mapped out their initiatives to protect critical information infrastructure, and specifically to conduct pan-European exercises to help in this effort. It is important that these initiatives are embraced and developed by the Member States as well.

The Commission's Communication was discussed at the EU Ministerial Conference on CIIP in Tallinn, Estonia, in April 2009. Member States and the Commissioner for Information Society agreed on the 'Tallinn process', i.e. to proceed with the objectives set out in the Commission's Communication, including conducting a pan-European exercise in 2010: "A joint EU exercise on Critical Information Infrastructure Protection should be organised and staged by 2010, in line with the Commission's action plan..."

As a final ratification of the importance of exercising, at national but also at a pan-European level, the Council Resolution published in December 2009 mentions that: "Member States should organise national exercises and/or participate in regular European exercises in the area of Network and Information Security..." and that "...ENISA could, upon request, assist Member States (on exercises)...".

Pan-European Exercise Planners

Country	Name
DK	John Michael Foley
FI	Ojala Kari Sami Vesterinen
FR	Adrien Ogee
HU	Ferenc Suba
IT	Tommaso Palumbo Luisa Franchina Marcellino Ferrazza Giorgio Maria Tosi Beleffi Anna Passeggia Rita Forsi
PT	Manuel Barros
SE	Peter Wallström
UK	Andrew Powell Reeves Alice (IE)
JRC	Christos Siaterlis Marcelo Masera Petteri Ihalainen
ENISA	Panagiotis Trimintzios Evangelos Ouzounis Panagiotis Saragiotis

The first exercise on CIIP on a pan-European scale is planned to take place in November 2010 within this policy context.

First pan-European Exercise

Initial steps towards the first pan-European scale Exercise were taken in December 2009, when ENISA created a core group of interested Member States, as outlined in its Work Programme 2010 and the Network Resilience thematic programme. A series of workshops followed. The first event was held in January 2010, with the aim of establishing the interest and dedication of the Member States as well as of obtaining agreement upon the objectives of the exercise and a list of basic principles and roles. It was confirmed that the Member States should take responsibility for the exercise themselves, with ENISA as a facilitator and organiser, and that the European Commission's Joint Research Centre (JRC) would offer scientific and technical support.

Having confirmed the overall objectives, at the second and third workshops (March and May 2010) the delegates agreed on the planning of the exercise, both at the higher level and the more detailed scenario, the setting up of the exercise and policies on observers and the media. In the meantime,

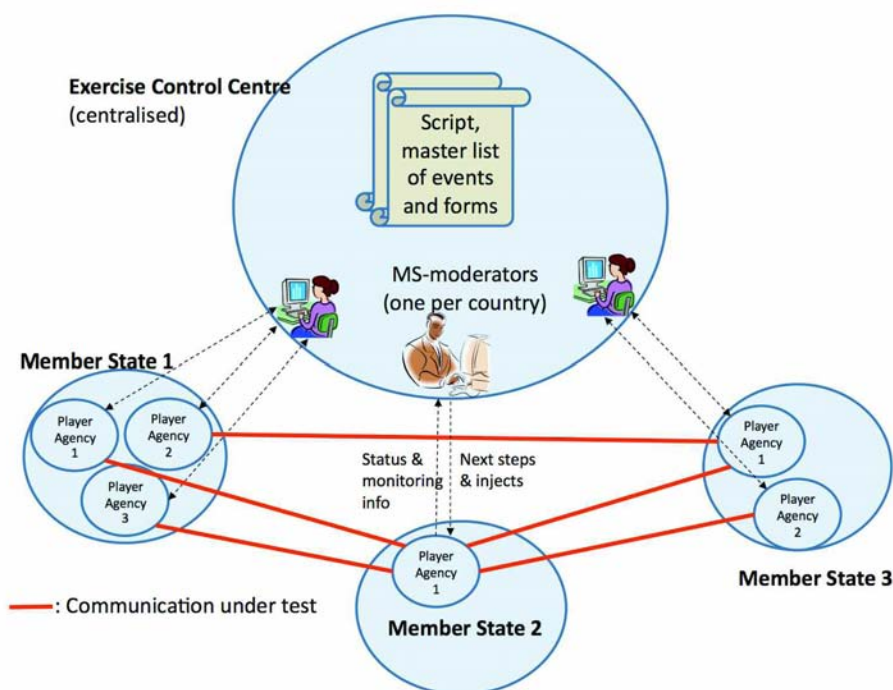
a core group of individuals from participating Member States, ENISA and the JRC was established – the exercise planners – who were tasked to work on all aspects related to the planning and organisation of the first Exercise. The workshop at the end of June was planned to enable the exercise participants to get to know each other better by presenting their national approaches and procedures for handling large-scale ICT incidents.

The first pan-European Exercise on CIIP – the main elements

Objectives of the Exercise – As a first step towards raising the level of joint preparedness against large-scale attacks and disruptions, the exercise will focus on the communication links and procedures between different Member States.

The exercise is designed to highlight the pan-European dimension of co-operation and collaboration, activities which are essential as cyber-space defies national boundaries. This will complement and build upon the experience gained with national exercises.

The first exercise will focus on the co-operation between public authorities in Member States of the EU and the European Free Trade Association (EFTA).



The objectives of the exercise include building and reinforcing trust relationships between participants, increasing understanding of how cyber-incidents are handled in cross-border scenarios, testing communication points and procedures between participating Member State authorities, highlighting interdependencies between key actors within each Member State, and finally promoting mutual support.

High level scenario – The exercise scenario of the first pan-European Exercise on CIIP will concern incidents affecting the Internet's normal operation. The scenario will cover incidents that involve the resilience of the Internet – of the type which could affect all participating countries.

Co-operation and communication will be necessary in order to understand and solve the problem.

Set up – The exercise will require that public authorities in one Member State make contact with participating public authorities, also called players, in other Member States.

Exercise control will be centralised, while participating public authorities will play from their sites. One representative, called the MS-moderator, from each participating Member State has to be present at the

exercise control in order to moderate this country's participation. Other observers would be allowed in the exercise control.

The organisation and evaluation of the national part of the exercise will be done by each Member State separately.

Current status and next steps – Building upon the lessons derived from the first pan-European Exercise on CIIP, the next step will be to identify the gaps and needs in terms of interaction among public authorities. For example, procedures may need to be set up and the minimum requirements for establishing effective communications may be determined, based on the need for common resources etc.

For the future...

This exercise could be the beginning in a series of pan-European Exercises on CIIP that will raise the joint level of preparedness and resilience in Europe. Future pan-European level exercises in CIIP will certainly benefit from the experience gained from the first attempt, and would try to improve in terms of scale, coverage etc.

For further information please contact:
Dr. Panagiotis Trimintzios
(panagiotis.trimintzios@enisa.europa.eu).

ENISA'S COUNTRY REPORTS

Putting together the pieces of the NIS puzzle in Europe

Ulrike Lechner and Silvia Portesi



ENISA's 'Country Reports' provide a useful tool for all policy-makers in the European Union (EU) working in the field of Network and Information Security (NIS).

The first edition was compiled in 2008 and published in 2009. It covered the 27 EU Member States and the three European Economic Area (EEA) countries (Iceland, Liechtenstein and Norway). While keeping the same geographical scope, the latest edition (now available on the ENISA website at www.enisa.europa.eu/act/sr/country-reports) offers an updated and extended overview of the state of play in key NIS thematic areas.

These updated Country Reports have been compiled for ENISA by Deloitte and are based on invaluable input from ENISA's National Liaison Officer (NLO) contacts in the Member States (www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office). The network of NLOs serves as an essential point of reference for ENISA within Member States on specific issues, and the Country Reports provide evidence of excellent collaborative work between the Agency and the NLOs.

The updated Country Reports have been compiled following an in-depth review of the previous years' reports and extensive desktop research into various information sources, and have been streamlined to complement ENISA's 'Who-is-Who

Directory on Network and Information Security'. Additional primary input was provided by ENISA's own Experts. A steering committee of ENISA experts gave guidance and support to enhance the integration of the Country Reports with the content of the ENISA Work Programme.

Each Country Report provides information on the different countries' national NIS strategies, the regulatory framework and key policy measures, and offers an overview of the NIS governance model at country level, including key stakeholders, their mandates, roles and responsibilities, their main activities in NIS and interaction with other stakeholders.

In addition, each Country Report identifies specific NIS facts, trends, good practices and case studies in areas such as incident management and reporting, risk management and emerging risks, network resilience, privacy and trust, and awareness raising. They serve as inspiration for other countries or other areas of NIS.

The Country Reports do not represent a benchmarking or ranking of the NIS-specific elements of the Member States; in many cases practices are still new and not standardised across the EU, which makes comparison difficult. It is also hard to say what could be compared, since policies, data collection etc. vary considerably across the Member States. However, this year's Reports have used a more comparative methodology, since the same things have been examined in all of the Member States.

A key finding is that there is no particular pattern with respect to the existence of national NIS strategies. The national NIS strategy of some countries, though, might be a useful source of inspiration for the development and improvement of an NIS strategy in other countries.



In the countries observed, a common co-operation mechanism has also been noted, via Ministries or Ministerial Committees responsible for NIS in each country. Many countries do not have a single institution recognised among NIS stakeholders as the NIS-related agency or authority, so co-operation is a prerequisite for establishing an NIS strategy. In countries where a national/governmental CERT is present, it generally acts as a key catalyst for NIS co-operation. CERTs in general serve as a central contact point in case of security incidents and are a source of important security information.

The Country Reports are available for download at: www.enisa.europa.eu/act/sr/country-reports.

The Country Reports are complemented by an updated 'Who-is-Who Directory on Network and Information Security', which serves as a 'yellow pages' of NIS in Europe. The latter contains contacts, websites and short descriptions of national and European authorities, CERTs and private sector and academic organisations active in NIS, as well as of international and pan-European organisations working in the area. The Who-is-Who Directory is available in printed format and downloadable from ENISA's website at: www.enisa.europa.eu/act/sr/files/deliverables/who-is-who-directory-nis-2010.

Ulrike Lechner (ulrike.lechner@enisa.europa.eu) is an Expert in Stakeholder Relations at ENISA.

Silvia Portesi (silvia.portesi@enisa.europa.eu) is an Expert in Stakeholder Relations at ENISA.



28-29 October 2010
FIL, the Parque das Nações,
Lisbon, Portugal

The GRC Meeting 2010 in Lisbon, Portugal, aims to present the main challenges for managers involved in Governance, Risk and Compliance.

The programme includes lectures and workshops, with major keynote addresses from world-recognised speakers including Bruce Schneier, John P. Pironti, Geraint Price, John Howie, Samuel Sadek, Danny Lieberman and Anderson Ramos.

Get more at www.grc-meeting.com!
For more information contact us at contact@grc-meeting.com



RSA® CONFERENCE EUROPE 2010

12-14 OCTOBER | HILTON LONDON METROPOLE | U.K.



Dear Members of ENISA Standing Bodies

Stay ahead of information security threats.

Three days of answers.

Threats, insights and practical solutions. Attend RSA® Conference Europe 2010 and benefit from cutting-edge education right across the information security spectrum.

RSA® Conference Europe gives you the knowledge you need to secure your organisation. Come and learn about the latest trends and technologies. Bring clarity and substance to the daily decisions that you and your team make.

Education for you. Vital insight for your company.

Attend RSA Conference Europe 2010. Here's why:

- **Extensive agenda, exclusive content.** Choose from 70 educational sessions spanning 10 tracks.
- **Intensive 3-day programme, affordable cost.** 14 hours of educational sessions, 4 hours of keynote insight from industry leaders and over 7 hours to meet your peers.
- **Practical solutions, instant payback.** Learn from real-world experts. Put new knowledge and contacts to work the moment you return.
- **Dedicated professionals, unparalleled networking.** Mix with Europe's premier security players. Build valuable new contacts, talk and mix with colleagues and peers.
- **Leading vendors, 1 to 1 access.** Meet with sponsors and vendors. Get 1 to 1 access and see demos. See Technology Showcase Theatre sessions and participate in discussion groups and special events.

Find out more.

www.rsaconference.com/2010/europe

Dates: 12th – 14th October
Venue: Hilton London
Metropole Hotel, UK

Special Offer for ENISA Members

Receive a **£100 discount**
when you register.
Use code: **ENISAMEM10**

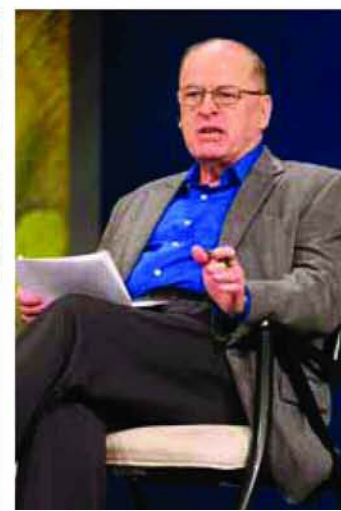
Register Early and Save!

Early Bird Registration
May - 16th July:
£650 + VAT (with discount)

Discount Registration
17th July - 10th September:
£750 + VAT (with discount)

Standard Registration
11th September - Event:
£875 + VAT (with discount)

©2010 RSA Security LLC. All rights reserved. RSA, the RSA logo and RSA Conferences are either registered trademarks or trademarks of RSA Security LLC, in the United States and/or other countries. All other products and services mentioned are trademarks of their respective companies. RSA Security UK Limited, Incorporated on June 6, 1996. Company Number: 3208788. Registered Office: 1 Carnegie Road, Newbury, Berkshire, RG14 5DJ, England



3rd Summer School on Network & Information Security Privacy and Security in the Future Internet

Jointly organised by ENISA and FORTH

NIS 2010

CALL FOR PARTICIPATION

The European Network and Information Security Agency (ENISA) and the Institute of Computer Science (ICS) of the Foundation for Research and Technology - Hellas (FORTH) invite you to the jointly organised 3rd ENISA-FORTH Summer School on Network and Information Security (NIS'10).

Following the success of NIS'08 and NIS'09, NIS'10 will take place in Crete, Greece, between the 13th and the 17th of September 2010, with the special theme **Privacy and Security in the Future Internet**. An exciting programme is being prepared, in the context of which invited lecturers will cover a range of topics extending beyond pure technological areas towards economic, policy, and legal issues.

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? The 3rd Summer School on Network and Information Security (NIS'10) 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 cutting-edge and interesting topics in NIS.

CONTACT Email: admin@nis-summer-school.eu



13-17 September 2010 • Heraklion, Crete, Greece

KEYNOTE ADDRESS *

- Mr. Mario Campolargo
Director of the Emerging Technologies and Infrastructures, DG INFSO, European Commission, EU
- Dr. Jorgo Chatzimarkakis
Member of the European Parliament, EU
- Dr. Silvia Adriana Țicău, Member of the European Parliament, EU

KEYNOTE LECTURES *

- Dr. Didier Bourse
Director, European Research Cooperation, Alcatel-Lucent, FR
- Dr. José Fernandes
Microsoft Portugal, PT
- Mr. Peter Hustinx
Supervisor, European Data Protection Supervisor, EU
- Mr. Mikko Hyppönen
Chief Research Officer, F-Secure, FI
- Mr. Bruce Schneier
Chief Security Technology Officer of BT, UK

STEERING COMMITTEE

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

PROGRAMME CO-CHAIRS

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

VENUE

NIS'10 will take place in Hersonissos, a small town close to Heraklion city, Crete, Greece.

REGISTRATION INFORMATION

Information about registration will soon become available through the summer school web page <http://www.nis-summer-school.eu>

* On the basis of the confirmations received as of 29 March 2010. For the latest information on the NIS'2010 program please refer to <http://www.nis-summer-school.eu>

The ENISA Quarterly Review is published once each quarter. You can find information about the ENISA Quarterly Review, including back issues and subscription information, on the EQR pages on the ENISA website: www.enisa.europa.eu/publications/eqr.

Contact: eq-editor@enisa.europa.eu

More about ENISA

For the latest information about ENISA, check out our website at: www.enisa.europa.eu.

Subscribe to RSS feeds of ENISA news items:

www.enisa.europa.eu/media/news-items/news-wires/RSS

and for press releases:

www.enisa.europa.eu/media/press-releases/press-releases/RSS

ENISA, 2010

Reproduction is authorised provided the source is acknowledged.

ENISA assumes no responsibility for any damages that may result from use of the publication contents or from errors therein.

