enisa
European Network and information Security Agency

ENISA Quarterly

IN THIS EDITION

Vol. 2, No. 4, Jan 2007

A WORD FROM THE EXECUTIVE DIRECTOR

Dear Readers,

First of all, I would like to take this opportunity to extend a warm welcome to the new EU Member States, Romania and Bulgaria. This historic, fifth round of enlargement of the European Union peacefully reunifies West and East Europe. In the words of Commissioner Olli Rehn:

"When welcoming two new Member States and 30 million people into the family, we know our debates, culture and heritage will be richer, and our mutual ties and economies will be boosted. Enlargement is not a project for the elite, but it is very much about enhancing everyday life of ordinary citizens."

Obviously, this applies also to Network and Information Security (NIS). Therefore, new representatives from Romania and Bulgaria are joining our Management Board in 2007 and I will be visiting the new Member States early in 2007 in order to establish and increase our relationship and partnership.

With the closing of 2006, I am happy to confirm that ENISA achieved all its deliverables and activities within the deadlines that were set in the Work Programme for 2006. I am impressed by the dedication of the Agency's staff, who have performed their very best for this to happen, and who travelled around Europe to present their studies to different target audiences and receive feedback.

My gratitude also goes to our stakeholders for their outstanding support. The Agency has truly established itself as a Centre of Excellence during 2006, with an increasing number of requests from EU institutions and Member States. Nevertheless, we are mutually dependent on active and close collaboration with the EU institutions and the Member States for our operations and activities. It is only by working together that we can fulfil our mission of serving the European Union and its Internal Market, the EU Member States and its citizens.

Focusing on the challenges ahead of us, we finalised the Work Programme for 2007. This year our activities will broadly be dominated by five operational themes. These themes, developed to assist in enhancing the Network and Information Security situation in Europe, are: raising awareness and building confidence, facilitating the working of the Internal Market for e-Communication, mastering emerging technologies and services, bridging security gaps in Europe, and increasing our communication and outreach activities. The full work programme for 2007 will soon be available on our website (www.enisa.europa.eu). I recommend that all of you take a closer look.

➲

ISSN1830-3609

During this month, a call will be launched for a renewed composition of the Permanent Stakeholders Group (PSG), which supports me with independent advice. The PSG has faithfully served for about two years already, producing valuable input for which we are infinitely grateful.

There is certainly space to improve, strengthen our mandate, enhance our role and tasks, as well as expand the Agency's workforce capacity. We are therefore looking forward to the independent mid-term review of ENISA, coming up during 2007. This will provide a basis for a discussion on lessons learned, what is good, where we need to improve, and how we will adapt to do better.

Being one of the EU's 28 Agencies is an honour and a big responsibility. Decentralised and spread out in Europe, we have the chance to share knowledge in each Member State. Sharing experiences on work and best practices means we can serve the European citizen at optimal level. That is exactly our intention for the years ahead.

I am looking forward to further contributions from our readers and experts so that we keep the NIS debate at the highest level.

Sincerely,

Andrea Pirotti
Executive Director, ENISA

A WORD FROM THE EDITOR

Is Network and Information Security (NIS) all about technology? Do we just need technological advancements to solve every security issue? Information and Communication Technology (ICT) today is ubiquitous; it is integral to our everyday life. The pervasiveness of these technologies makes them a significant factor in the global economy. Today, even if a business does not produce ICT products or services, it relies on them to be able to operate – and succeed – in the market. In this environment, securing ICT is not only a technological problem. It is also a social and most definitely an economic problem.

Incentive is the key word in the science of economics, and seems also to be the key word for NIS. ICT vendors need an incentive to deliver secure products. Network operators need an incentive to protect their infrastructures. Users need an incentive to learn how to choose secure products and use ICT in a safe and responsible way. Finally, governments, public bodies and policy-makers have a responsibility to ensure that all stakeholders have the right incentives to maximise overall security.

This issue of ENISA Quarterly (EQ) opens with an article by Bruce Schneier, CEO of BT Counterpane, on the network and information security externalities inherent in the problems of securing software products. Mr. Schneier argues that we are paying to mitigate the risk rather than to fix the problem. The latter, of course, can only be done properly if software vendors have an incentive to do so. Andrew Cormack, a member of the Permanent Stakeholders Group (PSG) established by ENISA, looks at another angle of the problem, that of enabling user confidence by drawing a comparison between confidence in online services and travelling services (aeroplanes, cars, trains). Mr. Cormack maintains that users should take greater control of their own safety online. Jaak Akker, chairman of the Malicious Code Committee of SIG Security, looks at the business of electronic crime and the changes in incentives and methods of cyber attackers. The professionalism of electronic crime is exemplified by trends and statistics related to malware, particularly computer viruses. Among other key research areas, the role of user-centric security and the empowerment of stakeholders are listed in the article by Stephan Lechner, a member of ENISA's PSG, and James Clarke, programme manager at TSSG/WIT. This article presents a strategic research agenda and key research areas for Security and Dependability over the next years, drawn from the results of the European Commission supported SecurIST co-ordination action.

Carsten Casper, one of our own experts in NIS Policies, presents the main findings from ENISA's Workshop on Information Security Certifications that was organised in November. Jani Arnell, an expert in ENISA's Risk Management unit, introduces his unit's activities and future action plan in the context of the recently produced Roadmap for Contemporary and Emerging Risks. Giles Hogben, also an ENISA expert in NIS Policies, reports from ENISA's Workshop on creating a common authentication language and introduces the new Interest Group on the subject.

From the Member States we have two very interesting contributions. Anders Rafting, an expert within PTS in Sweden, introduces Sweden's strategy for improving Internet security, including efforts to secure inter-domain routing and the domain name system. Finally, Krzysztof Silicki, a member of ENISA's Management Board, and Miroslaw Maj, a member of ENISA's Network of Liaison Officers, present the results of the discussion and e-polling on the evolution and future of NIS that took place in Poland at SECURE 2006, the conference co-organised by ENISA.

Finally, I would like to invite readers to submit an article for publication in ENISA Quarterly. EQ is open to contributions in all NIS-related areas but, for the next issue in particular, we would like to encourage contributions in the area of 'early warning and emergency preparedness systems'. EQ provides a great opportunity to reach out to a wide audience in Europe and beyond. The more we receive from you and your colleagues, the better this publication becomes for you. Please pass this message on to all your peers and do not hesitate to send us any ideas or suggestions for improvement.

I hope you enjoy reading this issue, and may I wish you a healthy, productive and secure 2007!

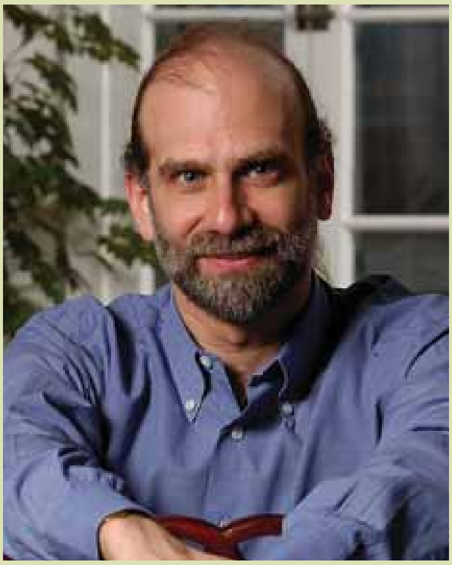
Sincerely,

Panos Trimintzios,
Editor-in-Chief, ENISA Quarterly

Dr. Panagiotis Trimintzios is an Expert at ENISA responsible for Relations with Industry, Academia and International Organisations

Information Security and Externalities

Bruce Schneier



Information insecurity is costing us billions. There are many different ways in which we pay for information insecurity. We pay for it in *theft*, such as information theft, financial theft and theft of service. We pay for it in *productivity loss*, both when networks stop functioning and in the dozens of minor security inconveniences we all have to endure on a daily basis. We pay for it when we have to *buy security products and services* to reduce those other two losses. We pay for the lack of security, year after year.

> "The only way to fix the problem is for vendors to improve their software. They need to design security in their products from the start and not as an add-on feature. "

Fundamentally, the issue is insecure software. It is a result of bad design, poorly implemented features, inadequate testing and security vulnerabilities from software bugs. The money we spend on security is to deal with the myriad effects of insecure software. Unfortunately, the money spent does not improve the security of that software. *We are paying to mitigate the risk rather than fix the problem.*

The only way to fix the problem is for vendors to improve their software. They need to design security in their products from the start and not as an add-on feature. Software vendors need also to institute good security practices and improve the overall quality of their products. But they will not do this until it is in their financial best interests to do so. And so far, it is not.

The reason is easy to explain. In a capitalist society, businesses are profit-making ventures, so they make decisions based on both short- and long-term profitability. This holds true for decisions about product features and sale prices, but it also holds true for software. Vendors try to balance the costs of more secure software – extra developers, fewer features, longer time to market – against the costs of insecure software: expense to patch, occasional bad press, potential loss of sales.

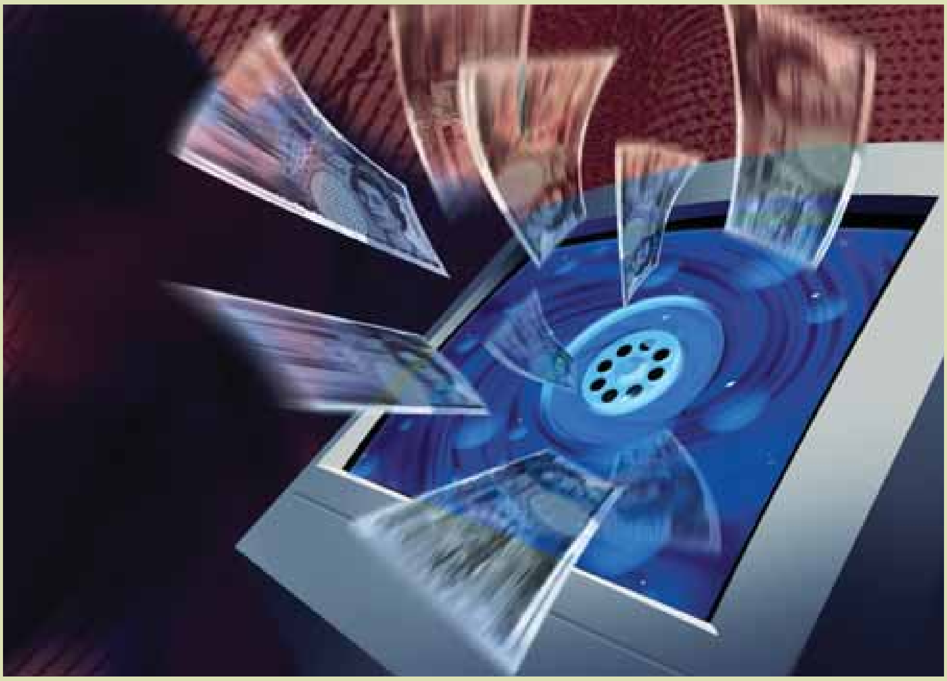
So far, so good. But what the vendors do not look at is the *total* costs of insecure software; they only look at what insecure software costs *them*. And because of that, they miss a lot of the costs: all the money we, the software product buyers, are spending on security. In economics, this is known as an *externality*: the cost of a decision that is borne by people other than those taking the decision.

Normally, you would expect users to respond by favouring secure products over insecure products – after all, users are also making their buying decisions based on the same capitalist model. Unfortunately, that is not generally possible. In some cases software monopolies limit the available product choice; in other cases, the 'lock-in effect' created by proprietary file formats or existing infrastructure or compatibility requirements makes it harder to switch; and in still other cases, none of the competing companies have made security a differentiating characteristic. In all cases, it is hard for an average buyer to distinguish a truly secure product from an insecure product with a 'trust us' marketing campaign.

Because of all these factors, there are no real consequences to the vendors for having insecure or low-quality software. Even worse, the marketplace often rewards low quality. More precisely, it rewards additional features and timely release dates, even if they come at the expense of quality. The result is what we have all witnessed: insecure software. Companies find that it is cheaper to weather the occasional press storm, spend money on PR campaigns touting good security and fix public problems after the fact, than to design security in from the beginning.

And so the externality remains...

➲



If we expect software vendors to reduce features, lengthen development cycles and invest in secure software development processes, it needs to be in their financial best interests to do so. If we expect corporations to spend significant resources on their own network security – especially the security of their customers – it also needs to be in their financial best interests.

Liability law is one way to make it in those organisations' best interests. If end users could sue software manufacturers for product defects, then the cost of those defects to the software manufacturers would rise. Manufacturers would then pay the true economic cost for poor software, and not just a piece of it. So when they balance the cost of making their software secure versus the cost of leaving their software insecure, there would be more costs on the latter side. This would provide an incentive for them to make their software more secure.

Basically, we have to tweak the risk equation in such a way that the Chief Executive Officer (CEO) of a company cares about actually fixing the problem – and putting pressure on the balance sheet is the best way to do that. Security is risk management; liability fiddles with the risk equation.

Clearly, liability is not all or nothing. There are many parties involved in a typical software attack. The list includes:

- the company that sold the software with the vulnerability in the first place
- the person who wrote the attack tool
- the attacker himself, who used the tool to break into a network

- and finally, the owner of the network, who was entrusted with defending that network.

100% of the liability should not fall on the shoulders of the software vendor, just as 100% should not fall on the attacker or the network owner. But today, 100% of the cost falls directly on the network owner, and that just has to stop.

Certainly, making software more secure will cost money, and manufacturers will have to pass those costs on to users in the form of higher prices. But users are already paying extra costs for insecure software: costs of third-party security products, costs of consultants and security services companies, direct and indirect costs of losses. But as long as one is going to pay anyway, it would be better to pay to fix the problem. Forcing the software vendor to pay to fix the problem and then passing those costs on to users means that the actual problem might get fixed.

Liability changes everything. Currently, there is no reason for a software company not to offer feature after feature after feature, without any regard to security. Liability forces software companies to think twice before changing something. Liability forces companies to protect the data they are entrusted with. Liability means that those in the best position to fix the problem are actually responsible for the problem.

Information security is not a technological problem. It is an economics problem. And the way to improve information security is to fix the economics problem. If this is done, companies will come up with the right technological solutions that vendors will happily implement. Fail to solve the economics problem, and vendors will not bother implementing or researching any security technologies, regardless of how effective they are.

Bruce Schneier (schneier@counterpane.com) is the CTO of BT Counterpane and the author of 'Beyond Fear: Thinking Sensibly About Security in an Uncertain World' and the popular 'Schneier on Security' blog. You can read more of his writing at www.schneier.com.

Enabling User Confidence

Andrew Cormack

All services need users. Anyone investing money or effort in developing an on-line service needs to know that users will be comfortable accessing it across the Internet. So long as users are liable to panic that the Internet is unsafe for them, their data or their computers, then investment in Internet services will be limited. User confidence is therefore critical to the development of all major on-line applications, from e-commerce to e-government and e-health.

Unfortunately user confidence in the Internet still appears to be fragile. Reports suggest that significant numbers of people are stopping using the Internet, or only using it for recreation, because of concerns about safety. In the first stages of public adoption of a new technology, when the safety risks really are unknown, this sort of behaviour is to be expected. However the Internet and PCs are now familiar technology to most people in Europe, and are an everyday part of life for many of us. This should have resulted in a more mature appreciation of the risks and benefits.

Part of the problem may be the way that computer and Internet security is sometimes presented, as something technical, too hard for the average user, that is best done for them by service providers and governments. This is not only inaccurate – basic Internet safety measures are simple and well within the capability of anyone who can send or receive an e-mail – but it can mean that users leave it to others to take care of their safety and act as if there is nothing they themselves can do to change their security status. The likely results of such an approach can be seen by comparing users' attitudes to other infrastructures: those we use to travel around.

On trains and aeroplanes, we are encouraged to place our safety in the hands of others: train drivers, airline pilots and the many people and technologies involved in airport security. All we have to do as passengers is turn up at an appointed place with our bags packed in a particular way and trust the system to keep us safe. Unfortunately this means that, whenever safety systems do fail (or even when they succeed in detecting and preventing a threat), passengers conclude that the whole system is flawed and unsafe to use. Where possible, many will move to another means of transport, often one where the risks are actually much higher!

Travelling by road is, statistically, much more dangerous than either plane or train. Yet it seems always to be the alternative favoured by those frightened off railways or aeroplanes. The reason for this illogical behaviour must be that when travelling by car we feel, whether correctly or not, that we are in control of our own safety. On average, ten people a day are killed on the roads in the UK alone but headlines are very rare and panics about road dangers almost unheard of. The vast majority of us carry on using our cars regardless. On-line service providers must envy such a phlegmatic attitude, as must managers at British Airways where a potential security incident, successfully prevented, was reported to have cost the airline £100 million in one month.

On-line service providers have an opportunity that airlines do not: *they can involve their customers in protecting themselves.* Service providers should, of course, continue to offer the safest systems they can, but combining this with educating users in safe computing practice and, in particular, getting users accustomed to the idea that they can control whether or not they are safe offers a double benefit. Not only will users behave more safely on-line, but they will also develop the lasting confidence that comes from feeling in control. These users should be able to recognise and avoid risks, and will take a much more pragmatic approach when security failures do occur or new threats are discovered. On-line service providers need this kind of user, so user education should be seen as a key part of ensuring the viability of every on-line service.

Andrew Cormack (A.Cormack@ukerna.ac.uk) is Chief Regulatory Adviser at UKERNA, operator of JANET, the UK's National Research and Education Network, and a member of the Permanent Stakeholders Group (PSG) established by ENISA.

Computer Viruses – from Electronic Graffiti to a Crime Business

Jaak Akker

This article is intended to shed light on recent developments in computer viruses ('malicious software – malware'). To create trust in electronic commerce one has to tackle the threats presented by malware. Trust is not a limitless asset. If the number of Internet attacks rises, it will have a detrimental effect on electronic commerce. Recent polls have shown that fear of criminal abuse is an important factor in making the average citizen reluctant to conduct e-business. By educating ourselves in the relevant components of e-crime, the citizens of Europe will gain a more realistic perception of the risks involved. It will also be easier to promote effective technical countermeasures.

The scope of this article is deliberately narrow, in order to be as comprehensive as possible. All kinds of phishing, common credit card number theft and the new emerging threats, such as malicious code in websites etc, are not discussed.

As the Internet has changed within the last ten years from an IT specialist's tool to everyone's handy helper, cyber criminals have found it a profitable target. Though there is awareness that the Internet is used by cyber criminals, it is not obvious to everybody that some of today's attacks are committed with the help of malware. Another term often used for software which is used for cyber crime is 'crimeware'. By crime we mean behaviour that is punishable in a court of law in the country where the activity is undertaken. It should also be pointed out that the crime may not be conducted by malware, but malware may provide the necessary information to commit the crime. A very obvious example is criminal interception of passwords and user identity for bank accounts, to promote cyber theft from those accounts. Another example is disclosure of company proprietary trade secrets, which is a punishable crime in several countries. 'Spyware' is the term often used to denote malware that gathers a user's information from a computer.

"Trust is not a limitless asset. If the number of Internet attacks rises, it will have a detrimental effect on electronic commerce. "

In this article we refer to statistics and trends found in widely referenced reports such as those prepared by companies like MessageLabs and Symantec. Their findings are generally accurate because of the large volume of incident information with which they are dealing. We chose 2005 as a reference year to ensure accurate cross referencing between different consolidated reporting sources.

Statistics and trends

Statistical analyses are also available from some law enforcement agencies. These, however, contain interpretations of statistical data and analysis that is based on reported crimes. These statistics may therefore be influenced by several factors, for example the willingness, or otherwise, of citizens to report a crime. Crime investigation may also be further complicated by the fact that it is not always obvious how the crime was committed. How was the information about access to a bank account stolen? It cannot always be verified that malware was involved. So the scope of this analysis is restricted to statistics of *intercepted* crimeware.

MessageLabs provides an interesting overall statistic for the malware scene. The input data were collected from countries on four continents, where the collectors currently scan almost one billion e-mails per week. The report shows that several EU countries were the targets of e-mails with attachments containing malware. In 2005, 2.8% of all e-mails contained some kind of malware. This is a significant decrease compared with the situation several years ago. But even though this is a positive result, it may have the negative effect of decreasing the end user's awareness of the existence of malware, and thus may decrease awareness of the need for protection.

➲

According to MessageLabs, in 2005 there were 2-3 malware attacks every week targeting specific companies, whereas the figure for this sort of targeted attack was almost negligible in 2004. Most traditional malware protection measures are designed to recognise previously known malicious software code, so some of these targeted attacks remain unnoticed for long periods. According to MessageLabs, antivirus signatures for this narrowly spread malware appear only 1-3 months after their spreading. This is obviously a long time. Only very few such incidents are brought to a court of law: many may remain unnoticed. The aim behind these attacks cannot therefore always be determined. Sometimes it may be industrial espionage; sometimes the attackers may just be searching for a victim host to launch further cybercrime activities.

Similar results are given in other reports. For example, in the second half of 2005 Symantec identified an average of around 9000 'bot' infected computers per day. A 'bot' is defined as a piece of malware that can be controlled remotely. This is an 11% decrease compared with the first half of 2005. The proportion of malicious code threatening confidential information however rose from 74% to 80% from the first to the second half of 2005, as compared with only 54% in the same period during the previous year. Out of the top ten most prevalent malware, six allow remote access, with the potential to perform *any* operation requested by their controller.

What are the common denominators in these two reports? Both state that the technical design of malware has changed. Years ago one only distinguished between Trojans (that do not replicate) and viruses (that do), and worms. Today's malware are small software programs – usually composed of one code block for the replication and disabling of antivirus software, another component for update and others for change of functionality, sometimes amounting to up to ten components within a malware software system.

Today's malware is a multipurpose tool. It can be used for sending spam, which may include replicating the malware to new hosts to perform Distributed Denial of Service (DDoS) attacks for a fee, but also to collect information from the host computer, in which case it is also acting as spyware. A large number of the same malware instance, managed remotely, is called a 'botnet'. Malware has changed from electronic graffiti to criminal big business.

Possible countermeasures

What is the cure? One thing is certain: most of the time malware-writers rely on known vulnerabilities. The need for speedy and effective patching is constantly demonstrated. Some security companies offer 'virtual patching' software, which involves techniques to neutralise the threat until a real patch is applied. It is too early to assess whether this technique is state of the art, but it is definitely something to watch.

Another issue to consider is the time it takes for the detection of previously unknown malware. Detecting and thwarting by antivirus signatures may sometimes take weeks for antivirus companies. This trend is also highlighted in the more recent report by Symantec, published in the first half of 2006.

Traditional antivirus software is based on the principle of blacklisting; previously detected menaces are prevented from future execution. But the evolution of malware that has not already been seen, and therefore not blacklisted within a short time, calls for another solution, such as the so called 'whitelisting'. With whitelisting, only software that is known not to be malicious can execute, while any other program is prohibited. Some work in this area has already started. There are separate security products based on this idea, but sometimes similar logic can be integrated into existing products, such as client firewalls.

Last, but by no means least, there are countermeasures that neutralise the effect of spyware. By making the stolen information useless, damage can be avoided. There may still be a few banks that rely on user ID and password as authentication mechanisms but, given the changes in the cybercrime scene as outlined above, this is no longer sufficient. For example, communication may be intercepted before entering an encrypted session with a bank.

Two-factor authentication is a key solution to avoid this situation. Electronic one-time password generators, where the password is a function of transaction content, can provide unique passwords to ensure the integrity of all the steps of a banking session. There are other solutions to this access control problem that are debated among professionals and researchers. In the future some of these may receive wider acceptance from the business community.

To conclude, it is important that security professionals study core statistics and trends to obtain a true picture of current and upcoming threats. This will strengthen our fight for an increased level of security. When doing battle, the first step on the path to victory is always "Know your enemy"!

Jaak Akker (jaak.akker@ekelow.se) is a senior security consultant working in Ekelow Infosecurity and co-founder and Chairman of the Security Malicious Code Committee of SIG Security, Sweden's largest organisation of security professionals.

Security and Dependability – Strategic Research Agenda for Europe

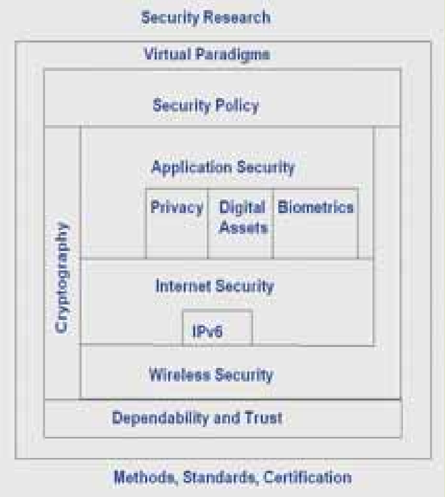
Stephan Lechner and James Clarke

The Internet and other digital networks have now become an integral part of both our economy and society. But as we are rapidly introducing more information and communication technologies (ICT) to enable services and commerce, private information is at increasing risk, and security and reliability problems have become prevalent. Indeed, today people are becoming more and more concerned about the increasing complexity of information and communication systems and the proliferation of privacy-invasive information gathering sources and techniques. In their online daily interactions, they often find themselves faced with high-profile losses of their personal information and with viruses, spam, phishing and other crimes of growing severity and sophistication. As a result, they find themselves in the undesirable position where they must put ever more trust in something which they have little or no way of properly understanding or assessing.

To build an information society that will deliver growth and prosperity, we need to tailor ICT to business and social needs, and to ensure that they become useful tools for economic and social innovation. The starting point for making ICT useful is to foster trust and to safeguard security in a networked world. In this respect, Europe's research framework programmes are committed to the establishment of an infrastructure of solid security and dependability.

The Information Society Technologies (IST) SecurIST project is a Co-ordination Action that has been charged with the preparation of a European strategic research agenda in the field of ICT for Security and Dependability, for the upcoming 7th Research Framework Programme (FP7, 2007–2013). In order to achieve this objective, the SecurIST project has established two fundamental bodies: the European Security and Dependability Task Force (STF) and the SecurIST Advisory Board.

The STF currently comprises 180 members spread across thirteen fundamental thematic areas (initiatives) of research. It provides a forum for consolidation and consensus building. The thematic initiatives are shown in the diagram below, which provides a visual interpretation of how these initiatives are integrated and work together.



Security and Dependability Task Force Initiatives Integration

The SecurIST Advisory Board is composed of European experts in information security and dependability. The charter of the board is to oversee, review, enhance and promote results from the STF (see www.securitytaskforce.eu).

In June 2006, based on inputs from the STF, the SecurIST Advisory Board has issued a document presenting its recommendations for a future security and dependability research framework in Europe, for the period 2007-2013. Under the title 'From "Security and Dependability by Central Command and Control" to "Security and Dependability by Empowerment"', the Advisory Board is recommending the following nine key research areas:

- **Empowerment of the Stakeholders:** Stakeholders of the information society include individual citizens, industry and academia, non-governmental organisations and governments. Empowerment of the stakeholder is vital as there is a clear technological trend towards decentralisation of technology, as well as of its management and control. Responsibility, authority and control have to move further towards the end user.
- **Europe-specific Security and Dependability:** Europe has a very specific heterogeneous culture, history and set of attitudes towards trust and society that requires specific research profiling.
- **Robustness and Availability of the Infrastructure:** Further research efforts are needed for the assurance of ICT network and service infrastructures, as well as the robustness and availability of critical infrastructure, such as health, energy, transport and finance.
- **Interoperability:** Research on the interoperability between security and dependability technologies and standards.
- **Processes for Developing Secure and Dependable Systems:** Research into the systematic improvement of secure and dependable system development (including hardware and software) from their design phase.
- **Security and Dependability Preservation:** In an increasingly complex world of evolving requirements, technologies and systems, the maintenance of effective system security and dependability is critical and is essential for preserving user confidence.
- **User-centric Security and Dependability Standardisation:** Strengthen the structured involvement of end users and their respective representatives into relevant standardisation activities involving security and dependability technologies.
- **Security and Dependability of Service Oriented Architectures (SOA):** The need to establish and maintain trust and to manage policy regulations and service level agreements in an SOA context, together with commensurate advances in software engineering to deliver service expectations.
- **Technologies for Security:** Underlying all of these other research areas is the need to provide higher assurance of trusted communication and handling of digital information. The two fundamental sciences and technologies highlighted are (a) cryptology and (b) trusted functionality and computing.

In addition to these nine key research areas, the Advisory Board presented four future *grand challenges* covering a long-term (10-20 years) vision. They illustrate potential longer-term possibilities and implications.

- **Countering vulnerabilities and threats within digital urbanisation:** This challenge addresses open problems that we will face in security and dependability from the expansion and globalisation of digital convergence by 2010-2015.
- **Duality between digital privacy and collective security: digital dignity and sovereignty:** This deals with future privacy issues of all stakeholders, whether citizens, groups, enterprises or states. It addresses the problem of how to override the 'Big Brother' syndrome and 'dark security', i.e., the future assurance of digital sovereignty and dignity for the various stakeholders.
- **Objective and automated processes:** This challenge addresses the problem of how to attain a controllable and manageable world of complex digital artefacts by 2015 and how to inject regular, quantitative techniques and engineering to make the field truly scientific.
- **Beyond the horizon: a new convergence:** This last challenge deals with the preparation of a new convergence looking to 2020 and beyond, which is the bio-nano-info-quantum 'galaxy', and the new security and dependability challenges that will emerge.

During July - September 2006, there was an on-line consultation process to enable the security and dependability communities to provide feedback on the Advisory Board's report. The Advisory Board is revising the report based on feedback from the consultation and will be issuing a new version at the end of January 2007. The new version of the report and other relevant documents will be available at: www.securitytaskforce.eu.

Dr Stephan Lechner(stephan.lechner@siemens.com) is Head of Central Security R&D at Siemens and a member of the Permanent Stakeholders Group established by ENISA.

James Clarke (jclarke@tssg.org) is a Programme Manager at the Telecommunications Software & Systems Group (TSSG) of the Waterford Institute of Technology (WIT) in Ireland, the co-ordinator of SecurIST.

From our own Experts

What can we achieve with Information Security Certifications?

An ongoing ENISA activity

Carsten Casper

There are numerous actual and perceived IT security risks – and these risks have to be managed. To do so, organisations employ experienced staff, define processes and deploy products. But how does an organisation know that staff, processes and products are appropriate to help mitigate risks? The use of accreditation and certification schemes is considered one element in describing the usefulness of a product, process or person. However, a lack of general recognition of certifications hinders an uptake of this market. On the other hand, wide recognition and improved visibility of such schemes would help providers and users of certifications and make the market more open and dynamic.

To address these matters, ENISA organised a workshop on the theme 'What can we achieve with information security certification? – Voice your opinion on information security certifications in Europe', which took place at the end of November 2006 in Athens, Greece. The goal was to draw together relevant expertise and discuss opinions about the use of information security certifications in Europe.

Over 20 presenters from certifying organisations, laboratories, vendors, consultancies, governments and regulatory authorities offered their opinions on certifications to an audience of more than 40 people from 15 countries, mostly from within the EU. In preparation for the event, ENISA had distributed a questionnaire and received 26 responses plus 8 position papers from the industry. In total about 70 experts on information security certifications contributed to this assessment.

During the course of the workshop it became clear that certifications of organisations, certifications of people and certifications of products have to be dealt with separately, even though there are some commonalities and, to a certain extent, some overlap. In addition, information security certifications should be seen in context with other certifications, such as privacy certifications, certifications of physical security and other IT or process certifications.

ENISA does not seek to endorse any specific information security certificate. However, there are some characteristics that are common to many different certification schemes.

➲

Below are some of the findings from the Workshop:

- Showing the value of any certificate is challenging. Among other things, a certification's perceived added value depends on its pervasiveness, appropriateness, accuracy and acceptance.
- The more thorough an evaluation for a certificate, the more lengthy and costly is the relevant process. Finding the right balance between time/cost and thoroughness also depends on the scope of the certificate.
- There is a trade-off between volume and quality. A certification scheme needs a certain volume of certificates to be visible in the market. On the other hand, the entity to be certified has to undergo a thorough evaluation process to ascertain quality. The more complex the evaluation process, the slower the uptake of any given scheme.
- Information security is a rapidly evolving space. Renewal or maintenance of the certificate is necessary after a certain period of time.
- Having a certificate and being secure are not the same. Certified entities can be vulnerable (even though that does not invalidate the certificate in its original scope).
- Some certification schemes are complex and pose a heavy burden on those who undergo certification, making certification difficult for small and medium-sized organisations. In such cases, a simplified version of the certificate and additional guidance could be valuable.
- Whether specific certificates should be required by law remains a topic of controversial discussion.

Further analysis and promotion of information security certification schemes will continue throughout 2007, including a discussion with relevant experts about certifications of specific matters. Interested parties are invited to participate in a virtual working group on CIRCA, the EU's online collaboration platform. (See circa.europa.eu/enisa or e-mail the author.)

Carsten Casper (Carsten.Casper@enisa.europa.eu) is a Senior Expert in Network and Information Security Policy at ENISA.

ENISA's Roadmap for Contemporary and Emerging Risks

Jani Arnell

"It must be considered that there is nothing more difficult to carry out, nor more doubtful of success, nor dangerous to handle, than to initiate a new order of things. For the reformer has enemies and only lukewarm defenders. He must confront the disbelief of mankind, who do not truly believe in anything new until they actually experience it."

Nicolo di Bernardo dei Machiavelli (1469 – 1527)

ENISA has recently finalised a roadmap for Contemporary and Emerging Risks for the coming years, a task that is clearly stated in the Agency's mandate, and one of the most essential areas of Risk Management and Risk Assessment.

The increasing need for new added value services is driving us further towards converging networks, emerging technologies and applications. This leads to an information society with more complex computing environments. Thus increasing efforts are necessary to maintain and develop information security within this evolving and pervasive computing environment, particularly as it is not clear that the countermeasures available today will be sufficient to protect our assets in the future.

ENISA is trying to identify the relevant technologies and applications of the future and whether there are Risk Management and Risk Assessment methods and tools which could identify, assess and manage emerging and future risks. As part of this task, ENISA has conducted a study aimed at drawing up a 'Roadmap for Contemporary and Emerging Risks'. The aim of this work was to identify all those action points which ENISA has to undertake so that it can provide and build up:

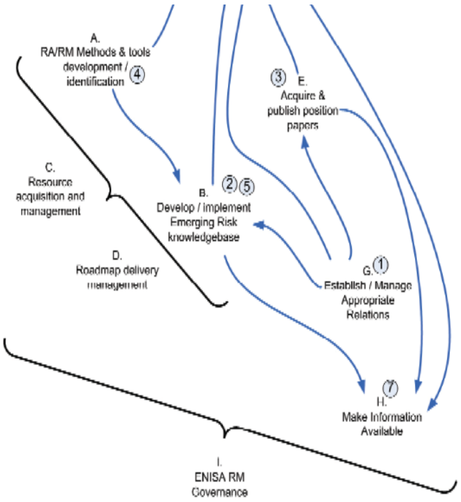
- A system, owned by ENISA and operated by its own staff and other relevant organisations, that will enable stakeholders to understand emerging technology issues and effective risk information relevant to information assurance. The system will do this by publishing authoritative information in position papers on security issues and countermeasures.
- A system, operated by suitably skilled and experienced personnel, to develop emerging risk knowledge that will assist ENISA's stakeholders in protecting themselves from emerging risks, through the identification and assessment of risks resulting from future technology, applications, exploits, environmental changes, market/economic and social changes. This system will also develop guidelines for stakeholders to identify and assess emerging risks themselves, utilising the language of business risk decision-makers.

The Roadmap produced offers information about how to maintain an awareness of threats, vulnerabilities and countermeasures. The associated methods would cover a range of technologies and target groups of users. The methods will be built up systematically within the 2006-2008 timeframe. The Roadmap comprises almost 120 individual action points which must be addressed. Work on some of these actions has already been started – and some of it completed – by ENISA's Risk Management unit, but there is much still to do.

The Roadmap consists of the following seven thematic areas:

1) establish/manage appropriate relations with government, technical and academic organisations
2) develop and implement an Emerging Risk knowledge base
3) acquire and publish position papers to track technologies, emerging markets, emerging applications and co-operation
4) identify and understand emerging risks
5) assess the identified emerging risks
6) develop guidelines for the identification and management of emerging risks
7) make information available

A high level graphical representation of the seven thematic areas and their interactions is shown below:


A.
RA/RM Methods & tools development / identification
4
3
E.
Acquire & publish position papers
C.
Resource acquisition and management
B.
Develop / implement Emerging Risk knowledgebase
2
5
D.
Roadmap delivery management
G.
1
Establish / Manage Appropriate Relations
7
H.
Make Information Available
I.
ENISA RM Governance

High-level Model of the Emerging Risk Activities

In addition, these themes could be further grouped into activities related to Infrastructure, Emerging Risks and Roadmap Maintenance.

In order to perform the identified tasks and activities represented in the Roadmap, ENISA will not only need to co-operate with the relevant stakeholders and beneficiaries but also bring people together to share information about work that has already been done in this field, and identify future usage scenarios.

Some of these tasks cannot – and should not – be undertaken by ENISA's staff alone, because of the amount of resources needed in order to be effective. Therefore ENISA will be inviting all relevant European stakeholders and beneficiaries to work together to tackle these issues, so that safe and continuous operation of emerging and future computing environments can be secured. For each activity, the Roadmap identifies current initiatives, both internal and external to ENISA, as well as the relevant actors and stakeholders.

ENISA has identified the key stages in this roadmap as follows:

- **Establishing the infrastructure**
  ENISA will be dependent on Member States to encourage individuals and governments, and technical and academic enterprises to commit to collaboration with ENISA.

- **On-going Emerging Risk activities**
  As above, ENISA will be dependent on the ongoing commitment of Member States and the pan-European network of contacts to ensure the quality of deliverables and that information in the knowledge base is kept current.

  Finally, in conjunction with Member States, ENISA will seek to learn from the activities undertaken and will adapt accordingly to maintain its position as a valuable and credible organisation.

- **Delivering the Roadmap**
  ENISA will consult the Member States and its ad hoc working groups to identify the needs of individuals, ensuring they understand the current knowledge in the area, what further information is required, and in what form the additional information should be provided.

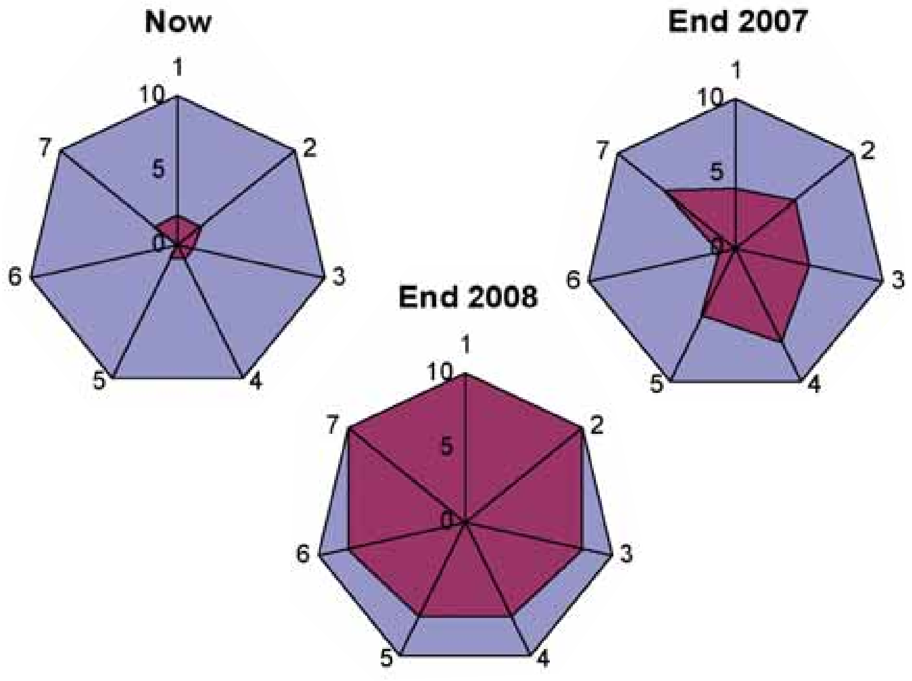
  Due to the large amount of information that is expected to be handled, ENISA will be dependent on its pan-European network of contacts to ensure any papers produced are relevant, correct and non-proprietary, and that other information prepared for dissemination is reviewed and methods and tools are tested.

The spider diagrams below indicate the proposed rate of completion of the activities within the Roadmap. ENISA's 2007 Work Programme includes starting the development of Risk Assessment/Risk Management methods and tools for emerging risks.

It is envisaged that four thematic areas (3 to 6) out of the total seven, will not be fully completed in 2007, but will form an ongoing process. The processes for this will be set in place by the end of the 2008 work programme.

Further details regarding the Roadmap will be available at the ENISA Risk Management web pages: www.enisa.europa.eu/rmra. Soon these pages will include another section with information about contemporary and emerging risks.

Jani Arnell is an Expert in the Risk Management unit at ENISA.



Estimated completion of identified activities by year: 2006-2008

The numbered areas in the diagrams represent the following tasks:

1 establish/manage appropriate relations with government, technical and academic organisations

2 develop and implement an Emerging Risk knowledge base

3 acquire and publish position papers to track technologies, emerging markets, emerging applications and co-operation

4 dentify and understand emerging risks

5 assess the identified emerging risks

6 develop guidelines for the identification and management of emerging risks

7 make information available

ENISA Authentication Language Workshop and Interest Group

Giles Hogben

A clear language for describing authentication methods is vital in establishing the trustworthiness of electronic transactions both for citizens as well as for governments and enterprises. It is important to be able to evaluate and compare available authentication methods using consistent and relevant descriptions. An initial study period by ENISA revealed that a number of parallel initiatives exist in this area. Therefore, in November 2006, ENISA organised a workshop which brought together experts working in this area to discuss how efforts could be synchronised to create commonly understood and interoperable descriptions of authentication methods.

The most important result of the workshop was an agreement to set up an interest group to work towards an interoperability standard for authentication descriptions. The final deliverable of this interest group will be a formal specification of a language and a definition of assurance mechanisms for the language.

The interest group will initially work on use-cases to provide a full set of requirements and benchmarks for the language. The use-cases initially include E-government, Federated Identity Management, anonymous access control via selective attribute disclosure, GRID and academic scenarios, network layer and Mobile authentication. The group will then divide the work on the language into the following packages:

- **High-level concepts for authentication classification** – this is aimed at human-readable descriptions which can be quickly and easily understood by end users. This will allow classification of authentication mechanisms for easy evaluation and comparison. The group will also investigate the possibility of quantifying authentication mechanisms using numerical levels.

- **Detailed low-level authentication description language** – for a precise description of authentication mechanisms by technical evaluators and for legal purposes. For example a certifying body might evaluate an authentication mechanism using 'Level 2', but they would need to document a detailed justification of this evaluation using a standardised low-level language.

- **Assurance mechanisms for descriptions** – usually descriptions of authentication mechanisms must be certified in some way in order to be trusted. This package will look at how a Common-Criteria-like mechanism could be used to certify descriptions using the language.

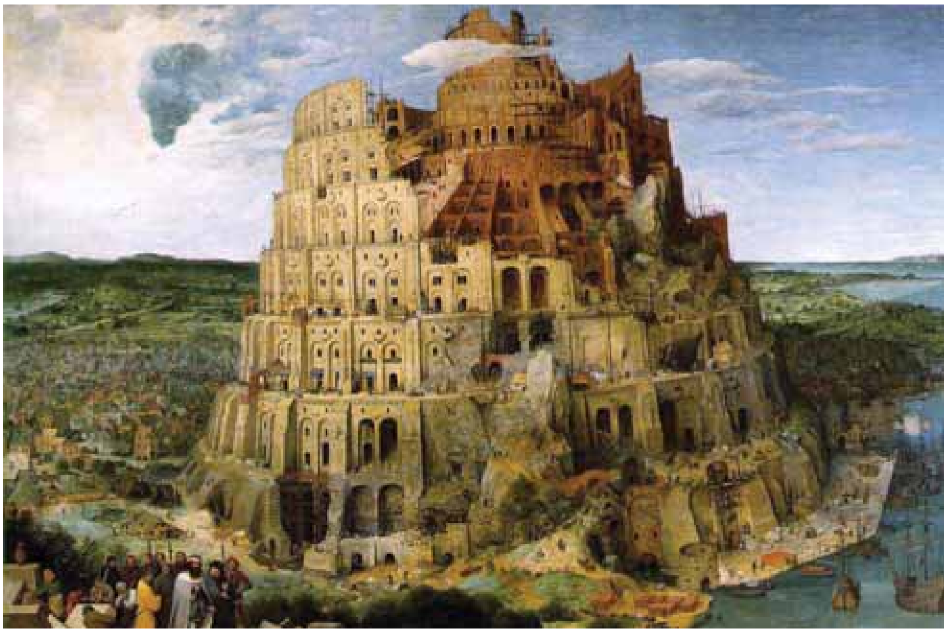
Other important conclusions from the workshop were:

- The language should also consider how to describe reputation-based authentication. Reputation as a means of authenticating users (for example in spam filters) is a growth area, which also carries important threats such as denial-of-reputation.
- In order to establish true cross-border interoperability of authentication tokens, the concepts of the language should be interpretable across different legal systems. For example, the privacy level of a given mechanism may be interpreted differently in different jurisdictions.
- If authentication contexts are to be quantified (i.e. levels applied), then a clear basis must be established for the application of the levels. Current candidates for criteria can be broadly divided into risk level, attack level and confidence level.
- The language should allow description of privacy and anonymisation features of authentication contexts.
- The language should include the ability to describe enrolment procedures used in creating authentication mechanisms.

ENISA will publish an Action Plan based on the conclusions of the workshop and initiating the interest group. It will be available in January 2007 at: www.enisa.europa.eu/pages/authentication/.

We also encourage the participation of experts in the interest group. Please contact the author if you are interested in joining the group.

Giles Hogben (giles.hogben@enisa.europa.eu) is an Expert in the Network and Information Security Policy unit of ENISA.



The Tower of Babel by Pieter Breugel, the Elder.

From the Member States

Strategy to Improve Internet Security in Sweden

Anders Rafting

In January 2006 the National Post and Telecom Agency (PTS) in Sweden, which is responsible for electronic communications, including the Internet, was asked by the Swedish Government to submit proposals for a strategy to improve Internet security in Sweden. In July PTS delivered its proposals and the Government adopted them as a national strategy in December 2006.

The aim of this strategy is to facilitate and clarify future work to secure the infrastructure of the Internet. The vision is that, in ten years' time, the Internet will be more secure, rapid and easily accessible to everyone in Sweden. The strategy focuses on those parts of the infrastructure that are unique to the Internet, and not on all vulnerable software. On the one hand, security within the Internet infrastructure is the providers' responsibility for networks and services to meet market requirements, but on the other, the commitment of public bodies in procuring security-enhancing measures is also necessary since there are security demands that providers do not satisfy.

The goal of Sweden's strategy is to secure the critical functions of the Internet infrastructure, preventing substantial disruption or interruption of Internet services for large groups of individual users or vital public businesses, authorities or organisations.

In drawing up its proposals, PTS considered the following trends and threat profiles:

- Society is becoming increasingly dependent on the Internet
- Society is becoming increasingly vulnerable to IT attacks
- New vulnerabilities in protocols and software programmes are constantly being discovered
- Laws, legal proceedings and policies do not keep pace with the developments and the globalisation of technology
- Convergence in networks, terminals and services is continuing to increase
- Inadequate security in user environments constitutes an ever-increasing risk
- The growing complexity of systems and networks makes ensuring their security ever more difficult
- Developments in the market involve increased internationalisation
- The number of wireless networks and services is growing

In response, PTS adopted the following strategic positions:

- The physical infrastructure of the Internet should be protected against accidents, disruption, wiretapping and manipulation of information during transmission.
- Resistance to disruption in the domain name system should be increased.
- Resistance to disruption to the exchange of traffic between Internet operators should be increased.
- Users should be trained and informed in order to enhance security awareness.
- The assumption of responsibility for user security should increase among Internet operators and the providers of software and equipment.
- National awareness of the Internet infrastructure should be promoted. This should be done in a broader context regarding information security. The comprehensive approach and co-ordination of research should be improved.
- Swedish participation in international fora should be increased. This should be done with collaboration between the private and public sectors.
- Crisis management regarding the Internet infrastructure should be improved.

PTS has drawn up an action plan that comprises a number of measures to meet these strategic positions. In each case the plan shows the allocation of responsibility, the level of importance, the timeframe and the estimated cost. A management plan has also been prepared which lays down how the action plan should be implemented. For example, the management plan contains guidelines regarding how often the action plan should be updated and which party is responsible for the update.

PTS has already started work in response to the adopted strategic positions by taking a number of measures to secure the Domain Name System (DNS) for the Swedish top-level domain '.se' through the deployment and use of the IETF standard DNS Security Extensions (DNSSEC) (www.dnssec.net/). In addition, in 2006 PTS started to secure the inter-domain routing system. Both of these measures deal with securing critical parts of the Internet infrastructure with the aim of improving the overall security of the Internet infrastructure.

Securing the Domain Name System in Sweden

The Swedish top-level domain, '.se', is the first national top-level domain in the world to introduce DNSSEC, which offers a more secure method of name resolving on the Internet. However, it is not sufficient that the '.se' zone is configured for DNSSEC. Underlying domains and the end users' name servers also need to support DNSSEC. In line with the implementation of DNSSEC, carried out by the .SE Internet Infrastructure (IIS) Foundation (the non-profit organisation responsible for the Swedish Internet top level domain, '.se'), PTS has performed tests of DNSSEC on the '.se' domain. PTS experts have worked to provide a description of functionality and definitions in DNSSEC, while focusing on testing the implementation and administration of DNSSEC on a sub-domain to '.se'.

The results of the tests show that the implementation of DNSSEC is generally simple. What is missing today is effective tools for the automation of DNSSEC administration, i.e., for key generation and zone signing. Standardisation of such tools appears to be a necessity if the deployment of DNSSEC is to take off. Otherwise, the increased manual work needed for administration will counteract the increased security that DNSSEC offers.

Despite the imperfections mentioned, DNSSEC is the right choice to increase trust in the domain name system and on the Internet as a whole. As a first step, DNSSEC should be deployed by operators, at higher levels of the DNS hierarchy. Then enterprises, organisations and authorities with very high security demands can ask for DNSSEC support from the DNS operators and, if applicable, implement DNSSEC in their own nameservers, that is, the name resolvers they administer themselves.

➲

Securing Inter-domain Routing in Sweden

The original design of inter-domain routing did not include mechanisms to secure the information in the system and, as is the case for any system that is exposed in the network, there is the possibility of an attack. Vulnerabilities have been identified and efforts are currently being made to improve the security of the routing system.

During 2006 PTS performed experiments with routers and simulation models to analyse the risks associated with a number of known and possible vulnerabilities. PTS's experiments targeted a few known vulnerabilities and risks in a broader perspective; that is, to ascertain to what extent attacks might affect Swedish Internet users. The goal was partly to examine how much protection is available, partly to spread knowledge about protective measures and, if possible, to determine the most effective defences to reduce the number of potential affected users.

Experiments with known attacks in lab networks indicate that certain types of threats, for instance attacks against TCP (Transmission Control Protocol) connections to break or affect BGP (Border Gateway Protocol) peering sessions, are significantly more difficult to carry out in practice than has previously been indicated in certain reports. Newer software versions have improved protocol implementations and include modifications to the treatment of key messages which makes it very difficult for an attacker to succeed unless traffic on the link can be monitored. Additional protection of peering connections can be afforded by CPU-consuming MD5-based hashing (Message-Digest 5 algorithm). However, this might increase vulnerability to DoS-attacks (Denial of Service attacks).

The simulations of potential consequences that were carried out concentrated on studying attacks based on the injection of false information into the system. Half a dozen organisations were selected from different sectors and a large number of different route hijacking scenarios were simulated as targeting these organisations. Each scenario represented a different attack origin. Results for a deaggregation type of attack indicate that the consequences, in terms of the number of affected end users, do not vary much between the different targets. On the other hand, the impact on the user varies greatly according to the origin of the attack because of filtering policies and varying AS (Autonomous System) influence in the network. The results suggest that deaggregations by customer ASs have a very small probability of impacting the system, thanks to extensive defensive filtering. The impact from attacks launched from different Swedish Internet Service Provider (ISP) ASs, on the other hand, varies from none (in about half the scenarios) to up to 60-70% of end users being affected. However, due to market concentration, there are only a few scenarios that lead to extensive consequences and, for most scenarios, fewer than 10% of users are affected.

The simulations point to some specific scenarios that could potentially have a significant impact, and it would be interesting to follow up the specifics with ISPs to validate the policy information from the routing registry and to determine if it would be feasible to introduce stricter filters for these specific scenarios. As a longer term goal, it would be better to strive for the incorporation of enhanced security support into the protocols, since filtering cannot provide a complete solution, and co-ordination between different organisations is currently difficult.

A complete report of the experiments on inter-domain routing will be published in early 2007 on PTS's website (www.pts.se). PTS can also supply further information concerning the results of and the experience gained from the actual deployment of DNSSEC, not only in Swedish ISPs' resolvers but also in other crucial organisations'.

The full national strategy, 'Strategy to Improve Internet Security in Sweden', is available at: www.pts.se/Archive/Documents/EN/Strategy_Internet_security_2006_12_July_2006.pdf.

Anders Rafting (anders.rafting@pts.se) is an Expert Advisor at the Department of Network Security at the National Post and Telecom Agency (PTS) in Sweden.

e-discussion on e-security in Poland

Krzysztof Silicki and Miroslaw Maj

In October 2006, NASK and ENISA co-organised the conference SECURE 2006 in Warsaw, with the theme 'Security – Time for a Breakthrough'. The SECURE conference is the most important event of this type in Poland, as it provides a forum to disseminate knowledge about network and computer system security.

SECURE 2006 provided an opportunity to reflect on decades of CERT Polska activities and to look to the future. How has the condition of computer security changed over the last few years? What were the major breakthroughs? What awaits us in the near future?

NASK (www.nask.pl) is the Research and Academic Computer Network of Poland. NASK is a telecommunications operator that provides integrated services for enterprises, institutions and corporations. CERT (Computer Emergency Response Team) Polska (www.cert.pl), is part of NASK, and is responsible for responding to cases of security breaches on the Internet.

These questions were put to the delegates of SECURE 2006. An electronic system was used in order to conduct polls among up to 100 people who participated in the discussion. These people are employed mainly by large corporations and institutions and have varying positions, both managerial and operational. The questions and the scope of the discussion topics were chosen by CERT Polska.

➲

Participants in the e-discussion

The percentage of managers (34%) and administrators (37%) who participated was almost equal. About 40% of the managers group comprised people responsible for informatics or telecommunications, while the rest were directly involved in IT security. The administrators group was divided almost equally between those two areas (52% and 48%). About 30% of the overall participants did not fit into one of the four basic groups, which proves the diversity of the e-discussion participants.

Representatives of big corporations (with over 250 employees) were the majority (63%). Representatives of small companies with 20 to 100 employees made up approximately 20% of the respondents. Representatives of medium-sized companies (100 to 250 employees) made up 9% of the respondents. The smallest companies (less than 20 workers) also represented 9% of the participants.

Is the Internet safe today?

The discussion was opened with that question.... and it brought a rather pessimistic response: almost all of the participants think that the Internet is not safe and almost half of them are afraid that it will become worse. The discussion was preceded by a presentation by Rob Thomas from Cymru Team, which introduced the scope and some of the methods of the Internet underground scene and showed the scale of threats to Internet security. This could have influenced participants' answers! Despite this rather gloomy perspective, approximately one-third of participants stated that 'the Internet is not safe', but 'things are progressing in the right direction'.

What is the biggest threat to the Internet these days?

Identity theft was acknowledged as the biggest threat. Awareness of this threat is rising due to, among other things, information propagated by the media. In fact, the danger of identity theft lies in the fact that it leads to actual security breaches on the Internet, such as the loss of money from one's bank account.

The participants who took a more technology-oriented point of view on the matter considered *botnets, worms and viruses* as the most dangerous threat. It is obvious that several threats may have common elements, for example, a virus may create a botnet which is used to steal an identity. But the main point of this question was to consider well known threats and to identify the most significant ones.

Who is responsible for the poor state of security in the Internet?

The short answer is that individual users and hardware and software makers were most frequently blamed.

Not surprisingly perhaps, participants in the poll showed a tendency against self-criticism but, at the same time, their answers were similar to experts' opinions on the matter.

Summary of the results from the electronic voting

Who won the struggle for the Internet over the last 10 years?

Hackers	21.9%
Administrators	13.5%
It is a draw	64.6%

What is the biggest threat to the Internet these days?

Botnets	25.8%
Worms, viruses	19.4%
Phishing	4.3%
Spam	39.8%
Identity theft	39.8%
Others	4.3%

Who is the most responsible for weak security?

Individual users	34.5%
Network administrators	10.4%
Internet service providers	8.3%
Hardware and software makers	36.9%
Governments	9.5%

What could be done to best improve security?

More educational action	46.7%
Increased administrators' skills	6.5%
Usage of safety techniques	28.3%
Improvements at the organisational level	18.5%

When should a government be involved in Internet security through regulatory mechanisms?

Never	9.3%
In serious situations (minimal degree)	47.7%
It should control most important situations	43.0%

Will there be a breakthrough in Internet security due to the reciprocal co-operation of all involved parties?

No, it is impossible	14.5%
Yes, the market will force it within the next 10 years	51.8%
It will take more than 10 years	15.7%
It will be forced by regulatory mechanisms	18.1%

Portrait of a hacker

In the 90s, the term 'hacker' was already common on the Internet but was used to refer mainly to an enthusiast of computer systems, who is interested in learning about their operational details.

Today a hacker is perceived as a thief, a criminal who ransacks on the Internet.

Paradoxically enough, the Internet is often described as a safe environment. It is an ideal situation for hackers when Internet users have an illusion of safety, while in fact the Internet is an environment that promotes the development of the 'underground' criminal economy.

Software security

Doubtless progress has been made. For example, in 2002 Microsoft launched its Trustworthy Computing program, which included courses for its programmers on security issues, the creation of safe and infallible code, modernisation of the process of development, audits of existing written source code and elimination of threats before a product is made available on the market. Compilers used by programmers have now improved (a programmer need not be solely responsible for the security of the programme he is writing). However, the question as to whether we can talk about a breakthrough remains unanswered.

Who won the struggle for the Internet over the last 10 years?

Did hackers win more than administrators in the last 10 years? The majority of the participants thought the result of this battle was a draw.

Doubtless both the development of the Internet infrastructure and broadband access to the Internet have had a major impact on the emergence of new threats. First, with better and pervasive access to the Internet, spammers became more active. Later, other threats, such as worms and Distributed Denial of Service (DDoS) attacks became more dangerous. It was no accident that the worm Slammer (2003) started in North Korea. North Korea had very well developed broadband access to the Internet. Slammer proved that the previous attacks of Code Red and Nimda (2001), which, at the time, were regarded as very dangerous, were no more than a cover for real, massive network threats. Futuristic ideas of 'black hats' – 'how to turn off the Internet in 15 minutes' – became real.

Will the problem of viruses and worms be solved fairly soon?

Nowadays viruses and worms often occur on the Internet and are perceived as significant threats. Will this problem be solved in the future? The views on that matter are also pessimistic. Over 80% of the respondents have a negative opinion. Moreover, half of them expect things to get worse. It seems that this problem is unavoidable. If worms and viruses disappear at some stage, it will only happen because they have been superseded by other, even more harmful threats.

However, on the positive side, a security rule of thumb has been established (for individual users and corporations). Best practice includes the use of antivirus programs, firewalls and system patches. These techniques combined can protect against the majority of attacks. However, despite the extensive use of security tools such as antivirus software, firewalls and intrusion detection systems, we cannot really say that general security has been improved.

Effective propagation of the 'I-Love-You' virus in 2000 opened a new era of attacks based on social engineering. Since then, the most effective attacks have followed the rules of social engineering and stem from inducing a user to perform a (usually simple) action, for example, to click on a web link. Since 2003, social engineering and other techniques used by hackers have developed a distinctive 'economic' character. The same thing also happened when phishing became popular.

What could be done to best improve security?

If we consider the list of threats, it is obvious that the most common threats (identity theft, botnets, viruses and worms) are, to a certain degree, based on social engineering. Technology may serve only as a support in that struggle. Being aware of the threats is the real weapon, and an important step in defending against them.

The e-discussion participants had no doubts – about half of them claim that network security depends on frequent and well thought out education. Who should be responsible for that? The answer given was: the media and schools with the help of specialised security centres. We do not want (or we do not count on) governments to be responsible for security education (although schools are a kind of governmental institution).

Is the infallibility and security of written code increasing?

Most of the respondents recognise the progress that is being made in the security and infallibility of software. The answer "yes" was picked by a quarter of the respondents. Almost the same number of respondents decided that this is particularly true for large software corporations. 22% thought that progress is slow. 10% answered that there has been no progress and the remaining 19% could not decide whether there has been progress or not.

Over the last decade several new technologies have emerged. These are closely connected with the Internet and involve a rapidly increasing number of its users. However, they have also brought new threats. For example, there is P2P technology, which revolutionised the way users exchange files.

Setting aside the problem of sharing illegal software, the importance of instant messaging is increasing rapidly, making protection of a company network more difficult. Typical firewalls are no longer sufficient. Instant messaging software was not designed with security as a strong requirement. The problem of WiFi – the technology which made the Internet available where there is no cable infrastructure – is broadly similar. On the other hand, due to its weak security (mainly as a result of the early stage of 802.11 development), unauthorised access to the Internet through wireless local area networks was very common. A similar problem arises with Voice over Internet Protocol (VoIP) – this technology is revolutionising vocal communication, but it has several security issues. The early versions of the Session Initiation Protocol (SIP), the most common protocol for VoIP, were heavily criticised for its insecurity. Cases of impersonation (impulses theft) became a serious problem. It is clear that safer protocols do not necessarily supersede less secure ones, or the development process becomes too slow (IPv6 vs. IPv4, SNMP, and DNSsec).

The rate of serious attacks increased when wireless local area networks became more

➲

ENISA's Ronald De Bruin delivering a keynote speech at SECURE 2006

popular. Wireless networks became a perfect environment conducive to anonymous hackers' activity, hidden behind unprotected wireless networks, which resulted in an increased number of crimes. There are many examples that this anonymity (which is, fortunately, sometimes not as anonymous as it initially seems) attracted a new class of dangerous criminals who deal with the distribution of illegal contents, e.g., child pornography.

Do developers of new technologies consider their security?

The answer to that question divided the participants into two groups: the majority (approximately 65% of participants) regard new technologies as being designed with security as one of the main requirements; the remaining 35% disagreed with that statement.

The number of attacks on web applications is increasing. This may be because it is relatively easy to find poorly protected targets. Moreover, the degree of complexity in these applications means it is easier to make a mistake that might introduce a vulnerability. Large software companies that develop operating systems have made an effort to improve the process of software development (in terms of security and safety mechanisms within the company). On the other hand, web applications are being developed by companies which are not fully aware of the threats and which do not usually implement security at the heart of their products. Many web applications are often developed by amateur programmers or those who are not security-conscious.

Internet threats such as Slammer or Blaster attacked networks of vital importance to the functioning of industrial and financial systems, such as atomic power plants (Slammer) or energy networks (suspected: Blaster). Threats to SCADA (Supervisory Control And Data Acquisition) networks are also being recorded more and more frequently.

Will Internet threats become a more serious problem for industrial networks in the future?

The majority (70%) of the answers to that question were that there would be sporadic but serious attacks on industrial networks. Such attacks would highlight the importance of this problem. Only 2.4% of the respondents answered that such attacks were no more than 'tabloid news'. The respondents who answered either that there would be a catastrophe due to such attacks or that they would be solved in the future were equally divided (just a small percentage of the respondents in each camp).

Does the legal system keep pace with Internet incidents?

Hardly anyone answered positively to this question. Most respondents said that it was not possible at all. This is not perhaps surprising as it is clearly a difficult objective. However, many people were optimistic that the law will keep pace with the development of the Internet. About 10% of the respondents believed that current law is sufficient but it is the implementation of the law that must be improved. It is worth considering whether we should draft another act on spam, spyware, malware, botnets, phishing or other incidents, or if we should analyse whether current laws allow us to penalise culprits adequately for their crimes committed in cyberspace. This discussion leads to the next question.

Safety vs. Regulations

The last decade was an important period in the development of a legal system for IT security. Regulations to protect private information, personal data and electronic transactions, and a system of penalties for violating these rules, were developed and included in a criminal or civil code. These rules are not always effective, and some of them seem to be unworkable. There is insufficient promotion of good practice through self-regulatory activities. It is possible that such activities would give the best results in restricting criminal activities on the Internet.

New defence techniques

The future remains the most interesting question. Will any new defence technology become common practice? Will it be, for example, an early warning system? Or maybe it will be a system of widespread control over computers on the Internet, which will permit Internet access only by computers that are sufficiently secured? Will it be a totally new solution?

Effective education about the economic aspects of cyber crimes would bring some improvements. We are still under the illusion that, in the virtual world of the Internet, crimes are also virtual. Maybe, if it were possible to convert the effect of an attack into specific monetary costs, we would have an effective motivation for taking action!

When should a government be involved in Internet security through regulatory mechanisms?
About half of the respondents answered that governments should be involved to a small degree. If we add in the 10% who answered categorically that regulatory mechanism is not needed at all, it seems that there is a significant fear of being ‘overregulated’. On the other hand, there were opinions that governments should regulate most Internet security issues. It is clear, therefore, that there is some hesitancy about this matter: on the one hand, there are problems with the rapidly developing cyber space, which may sometimes resemble chaotic Brownian motion, but, on the other hand, there are negative connotations attached to regulating, such as censorship or ‘Internet Governance’, which suggest we should be very careful about agreeing to overly restrictive regulations.

Will any new defence technology become popular in the foreseeable future?
From the answers to this question, it appears we are awaiting some unknown breakthrough. Most answers were: ‘other, still unknown solution’. Less common answers were: ‘systems resistant to massive attacks, which are able to survive any attack in a satisfactory state’. These systems are being developed particularly by the army, as systems which do not allow insecure or compromised computers to access public networks.

The situation regarding an early warning system is similar. Will there be any advanced technique which provides an efficient shield? We do not know, but even if that does happen, it will present a new challenge to construct a weapon to penetrate this shield. In any event, some respondents thought that concentrating on the development of new technologies would not bring a breakthrough, because the level of users’ education is a very important factor.

There are many parties interested in these issues: producers of software and hardware manufacturers, security systems providers, Internet operators, individual and institutional users, government agencies or administrators of justice. Their viewpoints usually differ, giving rise to many obstacles (e.g., economic, regulatory or technological). A breakthrough in IT security is possible only if all interested parties join and work together to achieve their collective aspirations and expectations.

Rob Thomas of Cymru Team and Krzysztof Silicki and Miroslaw Maj of NASK at the speaker panel discussion during SECURE 2006

Who is mostly responsible for weak Internet security?
Participants in the SECURE 20006 conference were convinced that software and hardware makers and users themselves are mostly responsible for weak Internet security (each of these groups received 35% of the votes). The three remaining groups (administrators, Internet service providers and governments) received an almost equal share of the rest of the votes.

Thus, the major responsibility for creating improved security rests at the beginning and the end of the ‘chain’ of participants in the electronic communication market. We might start with software and hardware security. If the manufacturers give us safe products, we would be in a better position at the start, and the risk of flaws emerging would decrease. On the other hand, users control the proper usage of these programs. They may use them in an informed and safe manner, or in ignorance, or even illegally.

Is co-operation between all interested parties possible? Will it result in a breakthrough in IT security?
What did the participants think of the possibility of a breakthrough through co-operation between all interested parties? More than half of the respondents thought that this process would take place within the next 10 years and would be forced by the market. The need for such co-operation was reinforced by those (20% of the participants) who chose a similar option – that such co-operation would be forced by appropriate regulations. It appears once more that auto-regulation of the market is preferable to legal regulation.

Will there be any positive breakthrough in IT security?
Answers to this important question were divided. The majority of participants were optimistic – they think that a breakthrough will happen in the next few years. If we add in the 10% of participants who claim that this breakthrough has already happened, almost two-thirds of the answers are positive. However, there are also sceptical opinions from respondents who think that nothing will change in the future (24%) or even that the situation will become worse (11% of the participants).

Thus, one should ask the next question.

What could be done to improve security?
Almost 50% of the answers received pointed clearly to the necessity for education. Confidence in the importance of becoming aware of threats was overwhelming. Although we must agree, we should try to establish certain directions for such actions. Considering recent improvements in IT security, the participants suggested that protective techniques and emphasising the extra-technological (organisational) layer are also very important. Clearly we should not focus only on one specific factor, such as education.

Summary
Analysing the discussion as a whole, several important opinions were expressed. There is a popular belief that manufacturers and individual users have the greatest influence on the improvement of security. That opinion is important; individual users are a crucial factor in network security, although, on the other hand, many products with serious security holes are still offered to the market.

ENISA’s Marco Thorbruegge presenting Wrap-up and Outlook of CERT activities

After several years of widespread use of the Internet, the time has come to ‘tidy’ this method of communication. As with other areas, after the first stage of dynamic development, the time comes to establish rules, so that, as much as possible, the interests of all users will be protected. In this process we should focus on the users’ own initiative, by promoting best practice or implementing self-regulatory mechanisms. We should not rely upon rules issued by a superior, then implemented as general rules. In practice, such regulations are rarely efficient in a dynamically developing environment. A general framework of rules is certainly necessary, as it is in any domain, where minimal regulation does not restrict but rather puts things in order.

While discussing the development of Internet threats, it is also worth mentioning the ability to infiltrate key infrastructures of society and the economy, such as transportation, energy, telecommunications, finances etc. Successful attacks on these infrastructures may be very dangerous, and it is essential to protect them.

Finally, participants were convinced of the necessity for co-operation between all interested parties, including users, manufacturers, telecommunications operators, employers and governments in order to establish a common vision for the development of security. It is comforting to know that the participants thought that such co-operation would be forced by the market itself. There is no sense in passively waiting for such co-operation between all the interested parties. For this to be efficient, we should understand and be aware of the role and importance of the individual stakeholders involved. We are confident that this e-discussion will contribute to increased awareness of that need.

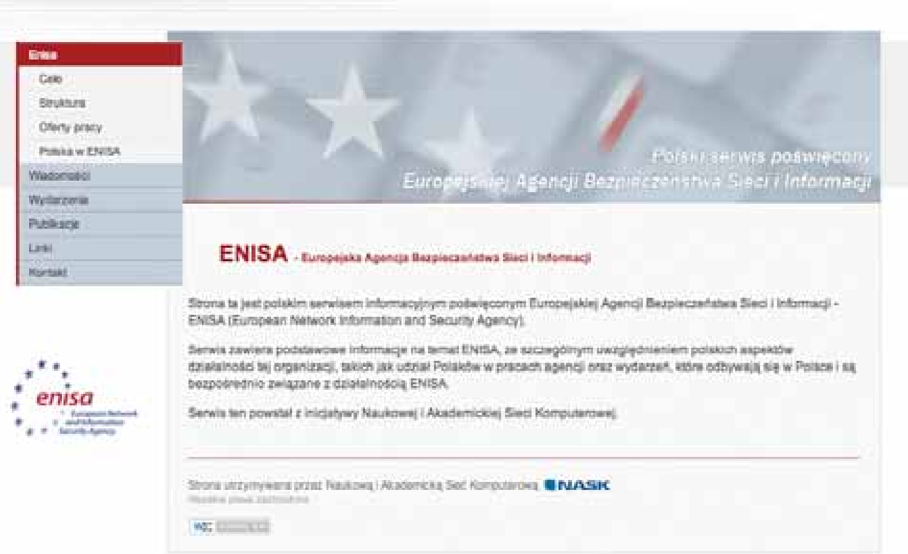
Krzysztof Silicki (krzysztof.silicki@nask.pl) is the Technical Director of NASK and a member of ENISA’s Management Board.

Miroslaw Maj (miroslaw.maj@nask.pl) is the head of CERT Polska and a member of the Network of Liaison Officers established by ENISA.

A Good Example from Poland – ENISA website in local language

NASK has created and maintains a Polish website about ENISA and Network and Information Security activities.

For more information on this very interesting initiative visit: www.enisa.pl.



ENISA - Europejska Agencja Bezpieczeństwa Sieci i Informacji

Strona ta jest polskim serwisem informacyjnym poświęconym Europejskiej Agencji Bezpieczeństwa Sieci i Informacji - ENISA (European Network Information and Security Agency).

Serwis zawiera podstawowe informacje na temat ENISA, ze szczególnym uwzględnieniem polskich aspektów działalności tej organizacji, takich jak udział Polaków w pracach agencji oraz wydarzeń, które odbywają się w Polsce i są bezpośrednio związane z działalnością ENISA.

Serwis ten powstał z inicjatywy Naukowej i Akademickiej Sieci Komputerowej.

Strona utrzymywana przez Naukową i Akademicką Sieć Komputerową NASK

ENISA Short News – Fourth Quarter 2006

Jobs at ENISA
New job opportunities are launched at ENISA
(www.enisa.europa.eu/pages/07_05.htm)

Who is Who in the EU: the revised and extended guide to NIS contacts in Europe
ENISA has prepared an extended and updated second issue of the 'Who is Who Directory 2006 in Network and Information Security'. All 25 EU Member States and all Members of the EEA (Iceland, Liechtenstein and Norway) have provided entries.
(www.enisa.europa.eu/pages/05_01.htm)

Joint Agencies campaign
ENISA is part of the Joint Agencies campaign: EU Agencies – working for you
(ec.europa.eu/news/eu_explained/061201_1_en.htm)

Ten new CERTs in the former Soviet Republics
ENISA promoted the first ever meeting between key players from Azerbaijan, Armenia, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Moldova, Turkmenistan, Ukraine and Uzbekistan on the setting up of new CERTs (Computer Emergency Response Teams). (www.enisa.europa.eu/pages/02_01_press_2006_11_15_ten_certs_soviet_republic.htm)

Mapping Awareness Raising initiatives in Europe – a new 'Information Package'
ENISA presented an updated, comprehensive outline of Awareness Raising initiatives, good practice recommendations and methods in the EU, identifying that almost all programmes focus on SMEs and Home Users.
(www.enisa.europa.eu/pages/02_01_press_2006_11_10_awareness_package.htm)

ENISA in Malta
ENISA co-organised a two-day conference together with the Malta Communications Authority. The conference focused on identifying best practices, aimed at improving NIS at a national level, and discussing possible mechanisms for ensuring coherent action between different stakeholders.
(www.mca.org.mt/newsroom/openevent.asp?id=24&source=4)

Promotion of a Common Language for Authentication Methods
ENISA organised a workshop to collect and discuss opinions about a common language to identify security levels of authentication methods in Europe. This was a first step in a process leading to the formalisation of a unified language for describing authentication levels.
(www.enisa.europa.eu/pages/authentication/index.htm)

Information Security Certifications
ENISA organised a workshop to find answers to questions about information security certifications and to discuss opinions about their use in Europe.
(www.enisa.europa.eu/pages/certifications/index.htm)

ENISA in Lithuania
ENISA co-organised the 2nd European Network and Information Security Conference that took place in Vilnius, Lithuania. The main objective of the conference was to provide a forum for discussing how to ensure security in networks and information systems operated by institutions and private organisations, including SMEs.
(www.securityconference.rrt.lt/index.php?3611573)

Call for Expression of Interest in Membership of ENISA's Permanent Stakeholders Group

The Permanent Stakeholders Group (PSG) advises the Executive Director of ENISA in the performance of his duties according to the Agency's regulations.

During 2007 ENISA is going to change the composition of the PSG and is looking for potential new members.

The call for expressions of interest in membership will be open from January until April 2007.

Full details of the call can be found on ENISA's website (www.enisa.europa.eu) after 17 January.

ENISA wishes to thank all the contributors to the publication. Please remember that all contributions reflect the views of their authors only, and are not in any way endorsed by the European Network and Information Security Agency. ENISA assumes no responsibility for any damages that may result from use of the publication contents or from errors therein.

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

Editor-in-Chief: Panagiotis Trimintzios
eq-editor@enisa.europa.eu

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