enisa European Network and Information Security Agency

Quarterly

IN THIS EDITION

No. 4, Mar 2006

A WORD FROM THE EXECUTIVE DIRECTOR

Dear Readers,

It is my pleasure to welcome you to the first edition of the ENISA Quarterly for 2006.

2006 is an important year for ENISA, and one in which we intend to continue to implement our mandate in earnest. Following a call for advice by the European Commission, we have already produced a report entitled 'Study on Spam and Security Measures', created by two of our technical experts, Carsten Casper and Pascal Manzano. And with a look towards the future, we have finalised our work programme for 2007 – 'Guiding Europe Towards an Enhanced Level of Network and Information Security'.

Security will become increasingly important as the pace of digitisation of our society shows no sign of slowing. Indeed, in most of Europe we have only seen the tip of the iceberg. New technologies bring constant new security challenges. For example, as the rollout of RFID tags gains momentum from supermarkets to ID cards, there are major security and privacy concerns. Indeed, new attacks on RFID tags using a cell phone were announced by Adi Shamir at February's RSA Conference. And at a recent IEEE Conference on Pervasive Computing, Rieback et al from the Free University of Amsterdam argued that RFID tags could provide fertile ground for computer viruses. The title of their paper is a chilling reminder of the risks these technologies bring with them – 'Is Your Cat Infected with a Computer Virus?'.

RFID chips have, of course, already been implanted in people. Party-goers in cities such as Barcelona and Rotterdam already use them to save time at the door and impress their friends at the bar, and some workers in the United States allow themselves to be tracked by them. Whether this is a fad or a trend is hard to say, but we need to make sure that security is given a top priority in the future applications of small computing devices.

ENISA looks forward to playing a role in fostering the European information security debate surrounding such technologies, and continuing to bring together the various interested parties. We are always open to suggestions as to how we can co-operate with other players.

On a final note, I invite you to mark the dates 10-12 October in your calendar, when ENISA will be co-organising the ISSE conference in Rome. Together with our partners, eema and Teletrust, and with the support of our hosts ISCOM, we look forward to a great exchange of ideas and networking.

Sincerely,

Andrea Pirotti
Executive Director, ENISA

ISSN1830-3609

A WORD FROM THE EDITOR

Dear Readers,

Information security has been in the news right from the outset of 2006. The much anticipated Kama Sutra worm turned out to be anticlimactic, but there has been no shortage of new browser and operating system vulnerabilities to keep us busy.

An interesting study by IBM in January of this year showed that more Americans expect to fall victim to a cybercrime than to a physical crime. Other results from the survey echo similar findings that show that a very robust minority of users do not use online banking and other services due to concerns about cybersecurity. And, despite Europe's lower exposure to the problem of identity theft, recent studies point to a deepening trust gap in Europe as well.

This does not mean that progress has not been made – spam, which was nearing epidemic proportions, is still a problem but seems to be coming under control, thanks in large part to improvements in filtering technologies. Opinions differ as to whether viruses, worms and large scale denial of service attacks are also in decline but, even as old problems subside, new ones appear on the horizon.

One of the new buzzwords is so-called spear phishing. As the name implies, spear phishing is a more targeted type of phishing attack, which in turn is harder to protect against. As usual, it takes advantage of technical weaknesses such as address spoofing together with user gullibility and trust. Users who do not realise that what appears to be the sender's address in an e-mail may not be genuine can easily fall prey to such attacks.

Most users do not realise these things – and, given the changing nature of threats, it is unrealistic to expect them to. A key problem with today's digital landscape is that it requires too much expertise to safely navigate – users are constantly confronted with warnings about expired certificates, secure domains, cookies and unsafe downloads. With millions of first-time users joining cyberspace weekly, how can we expect people to follow this jargon, let alone understand the underlying concepts?

The dynamic threat environment on the Internet means that users are constantly forced to make choices without the right expertise – after all, many end users do not know how to change the configurations in their operation systems, have no idea what a public key certificate is, and do not understand how password authentication works. And the problem is only getting worse, as systems become ever more complex without a corresponding increase in the human capacity to learn or understand.

This knowledge gap has more than just theoretical consequences. All security breaches eventually carry a cost, whether in time, money, or personal value such as privacy. Viruses can destroy data, and malware slows the user's machine and reduces efficiency. And while money lost by an online compromise of a credit card may ultimately be refunded by the card issuer, this involves significant hassle for the end user.

Today not everyone bears the costs of the insecure Internet equally. ICT and security savvy users are better able to evaluate security risks and thus have a more profitable online experience than their less knowledgeable peers. And while some end users recognise their security knowledge deficit and avoid online transactions, they too pay a cost, in terms of lost efficiency and higher prices. For them, it is a lose-lose situation – staying online puts them at risk and staying offline bears social and economic costs.

So security knowledge (which is usually, but not always, linked to one's ICT knowledge in general) is yet another factor in the digital divide, along with more traditional indicators such as income, age, socio-economic status and geography. And while eliminating this factor will not save the world, it may play a small part in bridging the digital divide and levelling the playing field between the digital haves and have-nots.

Which brings us, in a somewhat roundabout way, to this edition of the ENISA Quarterly. In this edition we focus on the organisation as end user. How do we bring security to the organisational end user? Is it through education? By providing guarantees and certificates? By outsourcing security, or by forming communities to patrol the Internet? In the following pages we have a number of authors who explore these issues and provide us with their opinions and insights.

We are particularly pleased to have a piece from security guru Bruce Schneier. In his article, he puts forward the case for outsourcing security. He is the CTO of Counterpane, a managed security services company, and will be familiar to many of our readers from his monthly Cryptogram newsletter. Those who want to hear Bruce Schneier in person will have the opportunity at ISSE 2006 in October where he will be delivering the keynote speech.
Another key issue in providing end user security is certification – how does an organisation know, when dealing with a complex system or product, that it actually is secure? Certification addresses the security knowledge gap from an organisational perspective – many organisations need to make decisions on the security merits of complex products that may be beyond their expertise. We have two articles from the French and German certification bodies exploring different aspects of certification.

CERTs are another way of moving security from the individual user or organisation to the collective. There are already over a hundred CERTs in Europe, with much advanced co-operation between them. However, most of the Internet is still not covered by CERTs and, perhaps more importantly, it is not clear how CERTs can truly reach into small communities and individual end users. In this issue, ENISA's Mehis Hakkaja takes a look at an interesting cousin of the CERT concept – namely WARPs – Warning, Advice, and Reporting Points – that tries to bridge this divide.

Increasingly (though slowly), legal action is being used as a mechanism to deal with well known security violators such as phishers and spammers. In this edition we have a piece on a Handbook produced by RAND Europe which catalogues the numerous European laws related to cybercrime – interesting reading both for cybercriminals and those pursuing them.

Lastly, a quick update on the status of the ENISA Quarterly. With nearly one thousand direct subscribers and many more that we reach through the redistribution efforts of our stakeholders, the ENISA Quarterly reaches thousands of professionals, academics and end users in Europe and around the world. As we enter our second year of publication, we are looking forward to continued expansion and encourage you to spread the word to your colleagues.

We welcome your continued support and contributions to our publication; please feel free to mail us your comments or suggestions about our magazine.

Sincerely,

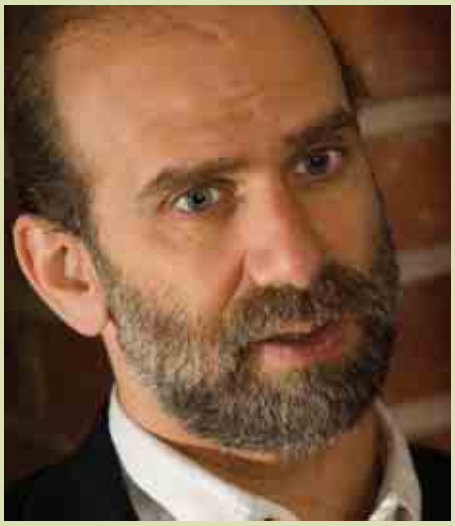
Boaz Gelbord,
Editor-in-Chief, ENISA Quarterly

Boaz is a Senior Expert in Security Technologies at ENISA

From the World of Security - A Word from the Experts

Why Outsource Security?

Bruce Schneier



In Europe as in the US, more and more companies are outsourcing their network security. This trend is driven by the increasing requirements for businesses to open their networks, and the ever-more-dangerous threat environment. For the Internet to succeed as a business tool, security has to scale. Outsourcing is how it will do that.

But if the decision to outsource network security is a difficult one, the decision of precisely what to outsource seems impossible. Managed security service companies can monitor your networks, manage your security devices, scan your networks, implement your security policies, install your security devices, and more. Other companies offer similar services, often tied to particular products or suites of products. And sometimes outsourced network security comes in a package with other outsourced network services.

On one hand, the promises of outsourced security are very attractive: the potential to significantly increase your network's security without hiring half a dozen people or spending a fortune is impossible to ignore. On the other hand, giving over your network security to another company feels like it should be inherently risky.

In reality, there is no dichotomy. Hiring another company to handle your network security can be less risky than building your own expertise inside your company. And it most definitely can be both cheaper and more effective. You already understand why; you just might not have thought of it in terms of network security.

Arguments for Outsourcing

The primary argument for outsourcing is financial; a company can get the security expertise it needs more cheaply by hiring someone else to provide it. Take monitoring, for example. The key to successful security monitoring is vigilance – attacks can happen at any time of the day and any day of the year. While it is possible for companies to build detection and response services for their own networks, it is rarely cost-effective.

Staffing for security expertise 24 hours a day and 365 days a year requires between five and eight (depending on vacation and overtime rules in your country) full-time employees – more, if you include supervisors and escalation personnel with specialised skills. Even if an organisation could find the budget for all of these people, it would be very difficult to hire them in today's job market. But if you think hiring them is difficult, retaining them would be an even harder challenge. Security monitoring is inherently erratic: six weeks of boredom followed by eight hours of panic, then seven weeks of boredom followed by six hours of panic. Attacks against a single organisation do not happen often enough to keep a team of the calibre needed engaged and interested. This is why outsourcing is the only cost-effective way to satisfy the requirements.

> "For the Internet to succeed as a business tool, security has to scale. Outsourcing is how it will do that."

Medical care is a prime example of outsourcing that we can use for comparison. Everyone outsources healthcare, in the sense that we do not act as our own doctor, nor does anyone hire a private personal doctor. Certainly cost is a factor in our decision to outsource, but there is more to it than that. I may only need a doctor twice in the coming year, but when I need one I may need him immediately, and I may need specialists. Out of a hundred possible specialties, I may need two of them – and I have no idea beforehand which ones. I would never consider hiring a team of doctors to wait around until I happen to get sick, so I outsource my medical needs to my clinic, my emergency room, my hospital. Similarly, it makes sense for a company to outsource its network security needs to a variety of experts.

The benefits of security outsourcing are numerous. Aside from the aggregation of expertise, an outsourced monitoring service has other beneficial economies of scale. A managed security services company can more easily hire and train its personnel, simply because it needs more employees and it can build an infrastructure to support them. An outsourcing company also has a much broader view of the Internet. It can learn from attacks against one customer, and use that knowledge to protect all of its customers. And, from its point of view, attacks are frequent. Vigilant monitoring means keeping up to date on new vulnerabilities, new hacker tools, new security products and new software releases. Outsourced security companies can spread these costs among all of their customers.

To return to our medical care analogy, you get better medical care from a doctor who sees patient after patient, learning from each one. To an outsourced security company, network attacks are everyday occurrences and its experts know exactly how to respond to any given attack, because, in all likelihood, they have seen it many times before.

What to Outsource

There are, however, limits on what you should outsource. The bottom line is that you will not outsource everything, because some things just do not outsource well. Things that do not outsource well are often too close to your business, or they are too expensive for an outsourcing company to deliver efficiently, or they simply do not scale well. Knowing the difference is important.

Think about healthcare again. We all know what aspects of medical care we like: the ambulance picks us up in seconds and rushes us to the hospital, a team of medical experts spares no expense in running tests to figure out what is wrong and in doing whatever it takes to cure us. And we all know what aspects we do not like: ill-equipped and ill-staffed hospitals, health insurers telling us that we cannot have that particular test or that a specialist is not warranted in this case. The aspects of outsourced healthcare we like involve immediate access to experts. Any medical emergency requires experts, and the faster they can pay attention to us, the better off we will be. The aspects of outsourced healthcare we do not like involve control of the process. Our healthcare is our responsibility, and we do not want someone else making life and death decisions about us. Network security is no different. Outsource expert assistance: vulnerability scanning, monitoring, consulting, forensics. Do not outsource control of the process.

Managed security service companies are experts in outsourced network security. They monitor networks, manage firewalls, IDSs, and IPSs, and provide vulnerability scanning, e-mail scanning and 'clean-pipe' Internet connections. They have the expertise to deal with compliance issues. They have consulting groups. In short, they can take the problems of network security off the backs of a corporate IT department and let them focus on their strategic decisions.

What they cannot do is determine how their IT security interacts with the customer's business. For example, they can detect when a hacker is inside a corporate network and what he is doing, but they will not know the business ramifications of different responses. They can detect an insider attacking your network, but they cannot know whether he is malicious or performing authorised testing. Some customers run highly secure networks and would rather disconnect from the Internet than have a hacker wandering around. Other customers generate far too much revenue from their Internet connection to disconnect for even a minute, and require responses that keep them operational. Managed security service companies work best when they can work with their customers, combining their own expertise with their customer's knowledge of the business processes.

How to Choose an Outsourcer

Choosing an outsourcing partner is difficult, because it is hard to tell the difference between good computer security and bad computer security. But, by the same token, it is hard to tell the difference between good medical care and bad medical care. If we are not health experts ourselves, we can sometimes be led astray by bad doctors who appear to be good. So how do you choose a doctor? Or a hospital? I choose one by asking around, getting recommendations and going with the best I can find. Medical care involves trust; I need to be able to trust my doctor.

Security outsourcing is no different; you should choose a company you trust. To determine which one, talk with others in your industry or ask analysts. Go with the industry leader. In both security and medical care, you do not use a little known maverick unless you are desperate. Watch companies that have conflicts of interest. Some outsourcers both sell products and offer managed security services. This worries me. If the service arm finds a problem with one of its products on my network, will the company tell me, or try to fix it quietly? If they discount their services in an attempt to sell products, who does their services division really work for?

In any outsourcing decision that involves an ongoing relationship, the financial health of the outsourcer is critical. Look for companies that are leaders in their field, have a strong history of security services and do not try to do everything.

The Future of Outsourcing

Modern society is built around specialisation; more tasks are outsourced today then ever before. We outsource fire and police services, government (that is what a representative democracy is) and food preparation (restaurants). In general, we outsource things that have one or more of three characteristics: they are complex, important, or distasteful. In business, we outsource tax preparation, payroll, and cleaning services. Outsourcing security is nothing new; all buildings hire another company to put guards in their lobbies and every bank hires another company to drive its money around town.

> "Computer security is all three: complex, important, and distasteful."

Computer security is all three: complex, important, and distasteful. Its distastefulness comes from the difficulty, the drudgery and the 3:00 a.m. alarms. Its complexity comes out of the intricacies of modern networks, the rate at which threats change and attacks improve and the ever-evolving network services. Its importance comes from this fact of business today: companies have no choice but to open up their networks to the Internet. Doctors and hospitals are the only way to get adequate medical care. Similarly, outsourcing is the only way to get adequate security on today's networks.

Bruce Schneier is the CTO of Counterpane Internet Security, a provider of managed security services, and the author of 'Beyond Fear: Thinking Sensibly About Security in an Uncertain World'. You can read more of his writings at www.schneier.com.

Security in Wireless Sensor Networks: Status, Problems, Current Technologies and Trends

Sead Muftic, Chih-Chun Chang

Wireless sensor networks have evolved from science fiction to a budding reality in a matter of a few years. A wireless sensor network is a collection of sensor nodes, tiny devices, usually battery powered, that acts as nodes in a larger network. The use of these networks is constrained only by the power of human imagination – from sensors on our body parts alerting a doctor to an alarming change in our vital signs, to a sensor on the earth constantly on the look out for a flood, forest fires, highway traffic control or tsunami. As with all emerging technologies, security poses great challenges to the scalability and deployment of such networks. In this article we explore the particular challenges of finding cryptographic algorithms suitable to such small devices, the key management problems and architectural issues.

Problems

Wireless sensor networks are a rapidly emerging technology with potential for many different and distributed applications. Wireless sensor networks are collections of small computers, with sensing and computing capabilities, characterised primarily by limited resources for processing and communication. They function by collecting sensor data and exchanging messages using wireless links. The nodes contain sensors needed by the applications, microcontrollers and radio transceivers, all integrated on a single chip.

In real-life situations, wireless sensor networks may have a variety of different topologies due to diverse options for their deployment. In principle, there are three basic modes of network organisation, determined on the basis of the connectivity of the nodes: hierarchical, distributed and hybrid. In a hierarchical network, there is a more powerful node, usually called the base station, which performs the functions of a central authority for other nodes. Its tasks include collecting data from other sensors and passing them to wired networks, or functioning as a network management station, synchronising and controlling the operations of other nodes. Distributed networks do not have central authority, and there is no fixed infrastructure of the network. Each sensor node communicates with its neighbours, which are located within its radio coverage. A hybrid network is a combination of hierarchical and distributed topologies.

> "Security for wireless sensor networks is today both timely and very important."

In a large-scale sensor network, where a large number of nodes are dynamically interconnected, the risks of various threats increase substantially. The nature of wireless sensor networks and their protocols make them more vulnerable to attacks, disruptions and problems than wired networks. The main problems with implementing security in wireless sensor networks range from memory and energy constraints, key management protocols and security-enhanced applications to the actual deployment environments in which the networks are used. Some of these problems are caused by limitations of sensor node technologies and thus are not relevant for networks with PCs or PDAs. This means that standard security solutions, used today for other types of networks and devices, cannot be simply transferred to sensor networks. New ideas and new solutions are needed.

Security for wireless sensor networks is today still in its infancy. The challenges of incorporating cryptographic algorithms into sensor nodes, implementing security protocols and incorporating security in network applications are currently critical design issues. Both hardware and software components have to be co-designed for basic network functions and also for security. Therefore, the comprehensive research and development of different aspects of security for wireless sensor networks is today both timely and very important.

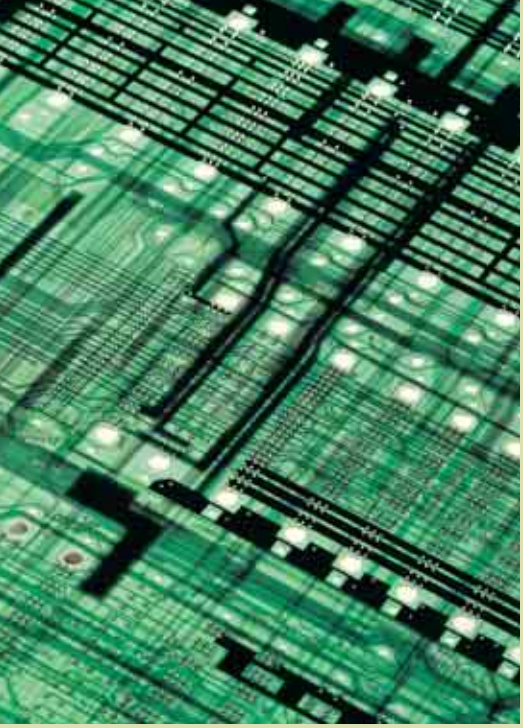
Cryptographic Algorithms for Limited Resource Devices

The research and development of cryptographic algorithms suitable for limited resource devices has intensified in the last few years. Studies aimed at developing 'light-weight' versions of cryptographic algorithms resulted in multiple techniques, which have been tested and evaluated in sensor networks. For instance, TinySec, developed by UC Berkley, is a default security mechanism in sensor radio boards (better known as motes) produced by Crossbow. The security is applied in the data link layer of a seven-layer OSI protocol, which means encryption and hashing mechanisms are applied when transmitting and receiving packets. TinySec performs verification of data correctness during their transmission at each hop, protecting the system against threats such as packet injection attacks on the network. The system is based on secret key cryptography.

Some research focuses on asymmetric cryptography. The TinyPK system, developed by BBN Technologies, uses the RSA cryptosystem. The implementation of TinyPK supports only public key operations (data encryption and signature verification) in sensor nodes. The Sizzle system, introduced by Sun Microsystems Laboratories, uses elliptic curve cryptography (ECC). It also runs a secure SSL web server within a sensor node. In order to save bandwidth, memory and computation, the server's private key, corresponding certificate and static web pages are stored in program memory. Sizzle uses an abbreviated handshake protocol, if a session has been already negotiated between a client and a server, which reuses a previously established master secret and does not involve any public key operations, such as certificate exchange/verification or key exchange.

Finding suitably light cryptographic algorithms will remain a challenge as the real-life deployment of wireless sensor networks continues to impose new constraints.

➲



Key Distribution and Management Protocols

Traditional key management protocols in wired networks with multiple components are usually based on usage of trusted servers, which perform bilateral or broadcast key distribution, such as secure group protocol or client-server security protocol. Establishing trusted servers in a wireless sensor network is difficult because of the nature of network constraints. Several studies have proposed alternatives, mainly based on key pre-deployment approaches, where keys are loaded into sensors prior to deployment in order to overcome the lack of computing and commutation power of sensor nodes.

The characteristics of several key establishment protocols for sensor networks are summarised in the table below.

Single master key scheme means that one single network-wide shared key is preloaded in all nodes, which is the simplest method. Contrary to this approach, in the *all pair-wise keys scheme*, all nodes in the network share a unique key. Sensor nodes in the *random pair-wise scheme* share a probabilistic subset of keys from a large key pool. In order to increase probability of sharing a unique key between two nodes, the keys may be generated in a polynomial way, paired with their unique identification or assigned to a particular subset of nodes. The *group-based scheme* divides connections among sensor nodes into two types, in-group and inter-group, and two key sets are provided for these two types. The *trusted base station scheme* uses a trusted and secure base station as an arbiter to provide link keys to nodes. Authentication of nodes is performed by the base station.

Five major types of key establishment protocols and their relative performance for scalability in network size, connectivity of the key-sharing graph, resilience against node capture attack and overhead of memory usage (storage complexity) are rated from 'perfect' to 'worst' in the table below. Scalability, key sharing and resilience are constrained by the limited memory size in all pair-wise keying schemes. The table also shows that none of these keying protocols achieves perfect performances in all four areas of scalability, key sharing, resilience and storage. Moreover, a good key management protocol for a wireless sensor network also needs to consider processing complexity and communication complexity, since they are relevant for energy consumption.

Security Services and Security Architecture

Data confidentiality, data authentication, data integrity and data freshness are services most often needed in sensor networks. In addition to securing individual nodes, it is necessary to design security systems that are themselves resistant to attacks and other forms of node failures. The concept of graceful degradation has been a cornerstone of distributed and fault-tolerant systems. The applicability of this approach to sensor networks and security must be explored. In particular, security systems and network applications should be able to continue to operate even if some nodes in the network are compromised or have failed.

A composable security architecture, which supports the construction of sensor networks from smaller parts that are secure and trusted, will be invaluable for the future deployment of sensor networks. The promising approach to achieving these properties is by structuring security in the form of the security middleware. It would consist of alternative security algorithms, components and protocols, as needed by the network applications and the type of data they handle.

Conclusions

Security is one of the most important characteristics of any network, but it is especially important for sensor networks. Such networks operate in open and unprotected environments, so they are exposed to an increased level of threats. Applications of sensor networks proliferate in many areas of contemporary life, and they must be enhanced with strong security features, approaching those of wired networks. Current research and development of security solutions for wireless sensors is still in its infancy. However, many universities, laboratories and companies are already pursuing research and development activities, so positive results may be expected in the near future.

Sead Muftic is a Professor at the Royal Institute of Technology, Stockholm, Sweden

Chih-Chun Chang is a doctoral student in the Department of Computer Science, George Washington University, in Washington, DC, USA

Single Master Key Based Scheme	Trusted Base Station Scheme	Group Based Scheme	Random Pair-wise Key Scheme	All Pair-wise Keys Scheme
1. Storage Complexity				
Perfect	Very Good	Fair	Bad	Worst
2. Resilience				
Worst	Perfect	*Very Good**	*Perfect**	*Perfect**
3. Key Sharing between Nodes				
Perfect	Very Good	*Good**	*Fair**	*Perfect**
4. Scalability				
Perfect	Bad	*Good**	*Bad**	*Perfect**

* means the level is limited by the size of available node memory

From our Own Experts

The Evolution of WARPs

Mehis Hakkaja

This article gives an overview of the WARP concept – Warning, Advice, and Reporting Points. WARPs are a kind of CERT – light, and therefore suitable for environments where a full blown CERT might be too costly or cumbersome. They both extend and complement the work that CERTs do. In what follows, we look at the evolution of WARPs from their origins in the UK and we examine their relationship with CERTs.

The History of CERTs and the birth of WARPs

The first CERT – Computer Emergency Response Team – was created by the US Government in response to the first Internet worm in 1988. This model, also known as CSIRTs – Computer Security Incident Response Teams, has since been replicated all over the world.

Every CERT is different and can provide a variety of services like warnings and advisories to its constituency ('constituency' is CERT jargon for the user community a CERT serves). However, to be considered a CERT, a team must provide one or more of the incident-handling services: incident analysis, incident response on site, incident response support, or incident response co-ordination.

Most European countries have one or more CERT teams in various sectors, including government, academic, commercial and others. It is clearly a well established model for providing security services. Why should we even look further?

The simple truth is that establishing and operating a functional CERT team is not a trivial commitment. Running such a team is not cheap and coverage of constituencies is still limited if we consider the European landscape as a whole. While there are over a hundred European teams mapped out in the 'ENISA Inventory of CERT activities in Europe' (available at www.enisa.eu.int/deliverables), it is clear that only a small percentage of end users and sectors are actually covered by these teams.

To improve the situation, one of the tasks of ENISA is to promote new CERTs and similar activities in EU member states and to facilitate various forms of co-operation. It therefore makes sense for ENISA to be on a constant lookout for concepts similar to CERTs which can augment their functionality and complement their work. One such relatively new and innovative concept is the WARP model.

What are WARPs?

WARP stands for Warning, Advice and Reporting Point. The WARP model was developed by the UK's National Infrastructure Security Co-ordination Centre (NISCC) to address a slightly different security goal than CERTs: encouraging users to learn from and apply the good practice and security information that is already available in published form and within communities and interest groups. At the risk of oversimplification, one can say that WARPs aim to reduce the number of security incidents, while CERTs primarily aim to reduce the impact of those incidents that do occur.

The difference has been summarised succinctly by the creators of the WARP concept at NISCC: "WARPs perform some of the tasks of CERTs but are not expected to provide the technical response service of most CERTs".

First-hand look at WARPs

Computer Incident and Response Handling experts of ENISA visited NISCC in London in November last year to hear first-hand about WARPs from the creators of the WARP concept. Together with NISCC, we took the opportunity to observe a real-life WARP based in Kent. The 'Secure Kent' WARP (SKWARP-UK) has been providing services for 14 Local Authority partners since 2004.

As we were advised on site, the WARP provides a service of early warnings of alerts and vulnerabilities that is specifically tailored to its community. By delivering relevant content in a language understood by the community's users, and by taking steps together to mitigate specific threats within the community, the WARP is able to show tangible benefits for its members and to establish trust.

We were told that it takes about four man-hours on an average day to review all messages from about 72 sources and to categorise, customise and disseminate them to the community through the WARP's Filtered Warnings Service. This service provides each member with all the relevant warnings from a single trusted source instead of having each individual member waste countless hours sifting through the confusing plethora of online warnings. Users also have the option to automatically select to see only categories of warnings they consider the most important and in this way they will receive even more targeted information.

Secure Kent serves a community consisting of 14 local authorities, in which four or five members share the workload of filtering the sources. Spreading the workload over several members helps ensure the continuity of services in irregular situations. It also further underscores the point that WARPs are truly community creations, building on the collective skills and trust of their community for their operation.

A schematic view of SKWARP, the Secure Kent WARP. (Source: NISCC)

To be a little more specific, there are three core services that together embody the WARP concept:

- **Filtered warnings** service – enables WARP members to receive only security-related information which is of interest to them and tailored to their level of technical expertise.
- **Advice brokering** service – a secure environment in which WARP members can discuss security issues and help each other.
- **Trusted sharing** service – a trusted environment to facilitate the sharing of sensitive information related to real security threats and incidents between WARP members.

The WARP concept is part of an information sharing strategy to protect the UK's Critical National Infrastructure from electronic attack. At the same time, the WARP model and even the WARP Toolbox (www.warp.gov.uk/) have been placed in the public domain, and are free of charge as long they are used for non-profit services. This means that participation is open to all – indeed sometimes all it takes is the commitment of a single person with very limited computational resources to establish and run a WARP.

One good low-cost example is the Guild WARP (GUWARP-UK) that serves the online members of the Guild of One-Name studies, a genealogy society, which one would certainly not perceive as a natural information security sharing community. Such examples illustrate how WARPs can reach small communities which CERTs cannot reach directly. In fact, WARPs are best created in such small communities, to encourage the flow of information about security issues into and within the community.

It is indeed the community aspect that is the primary selling point for the WARP concept. Most WARP members join the community by choice and, as a result, are more likely to take an active role in its success, both by contributing and acting on information. In contrast, CERTs are usually imposed on users by organisational or network boundaries, which sometimes results in less user participation.

Co-operation between WARPs, with CERTs, and internationally

There are several initiatives to enhance co-operation between WARPs and beyond. An example of this is the WARP Operator Forum that meets quarterly and which provides an opportunity for peer networking and for assisting new WARPs along. Another one is the Annual WARP Forum that held its second meeting on 15 March 2006 in London and where ENISA co-chaired a session on 'International Developments and CERT Co-operation'. This session explored ways WARPs and CERTs can co-operate and discussed how the WARP model could be replicated outside the UK.

There is also daily co-operation outside the framework of such events. The design of the WARP concept encourages bilateral co-operation between WARPs such as content sharing. In addition, in about six months' time, UNIRAS (the UK Government CERT, part of NISCC) is planning to provide automated feeds of warnings and advisories to any UK WARP that wants to receive them. Such developments further reduce the information-gathering burden on any given WARP.

There is promise for further co-operation between WARPs and CERTs as both have a slightly different set of skills and have different relationships to their constituencies. As an example, WARPs can help CERTs with their goal of having preventive advice more widely adopted, by leveraging the close relationship that WARPs have with their communities. In the future, WARPs could even provide feedback to CERTs regarding the type of information that is useful for a particular community, as well as relaying back lessons learned within the community.

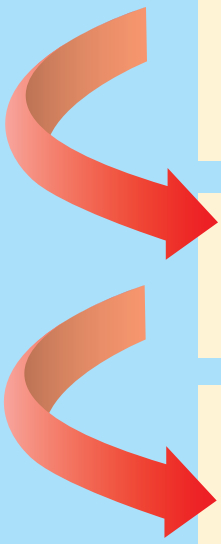
There are currently thirteen WARPs, eight operational and five developing, registered on the WARP Toolbox page (www.warp.gov.uk/WarpRegister.htm). NISCC is hoping that this number will grow to at least 20 in the UK in 2006 and that new WARPs will also emerge outside the UK.

Conclusion

The WARP concept is still evolving and we at ENISA are eager to see where this evolution leads. It certainly holds promise as an extension and complement to the CERT model and it is even hoped that the WARP model will eventually serve as a stepping stone towards the establishment of full blown new CERT teams. Indeed, while it would be good to see more CERT teams being established right away, WARPs offer an alternative approach and a more accessible first step. We encourage you to take a closer look at the WARP concept and see whether this model could serve your community's network security needs.

Mehis Hakkaja is an Expert in Computer Incident and Response Handling at ENISA

WARPs – A development model



Stage 1: Show the benefits of the WARP to the community through tailored **warning** service, so that everyone feels they are getting a personalised and valuable service.

Stage 2: Develop trust through encouraging members to help one another by sharing best practice and giving **advice** to each other through WARP facilities.

Stage 3: Encourage members to **report** their experiences of otherwise embarrassing attacks or problems (anonymously if necessary, through the operator) within the WARP for collective learning.

Building trust is difficult, especially virtually, which means that the third stage is not easily reached. However information sharing, even when it means revealing sensitive or potentially embarrassing incidents, can be of benefit to the entire community and can be fostered within a trusting online environment.

Such information sharing, when it can be achieved, is one of the great added values of the WARP model. In the future there is also the possibility of reports summarising shared experiences being made available to other WARPs or to CERTs that are linked to WARPs.

Once a WARP develops its skills and resources, it may wish to help its community to remedy incidents as well as to prevent them. This is the traditional role of a CERT, so it may be better to create a separate CERT to meet this demand rather than risk changing the WARP's existing relationship with its community. In this way a lightweight WARP can lead to the evolution of a full blown CERT.

Promoting Best Practices – ENISA activities

Raising awareness of Internet users and the co-operation of Computer Emergency Response Teams (CERTs) are two of the main areas of interest of ENISA. The agency collects examples of best practice in both fields and distributes them among its stakeholders.

In order to disseminate its findings, ENISA invited representatives from each EU member state to learn about CERTs and Awareness Raising in Europe at two workshops in Brussels on 13 and 14 December 2005. The agency was supported by more than a dozen security experts who shared their experiences and described developments and future trends. ENISA also took the opportunity to present two documents: a CD-ROM on Awareness Raising and the 'ENISA Inventory of CERT activities in Europe'.

Dissemination workshops have been recognised as a useful forum to promote an exchange of best practice and to trigger discussion. The response to the workshop from participants was very encouraging. ENISA will therefore organise similar events in the future to share its findings.

Workshop One: CERTs in Europe

Marco Thorbruegge

CERTs have played an active part in securing the Internet for almost two decades. The first teams in Europe were put together in 1992 in the Netherlands and the UK. CERT co-operation in Europe started around 1994, and the CERT landscape has grown and blossomed ever since. The 'ENISA Inventory of CERT activities in Europe 2005' lists 109 response teams and a number of co-operation, support and standardisation initiatives.

Experiences
Building up a response team from scratch is never easy; highly skilled technical staff are needed who also have sufficient social skills to support their users in both a competent and appropriate fashion. Rules and policies have to be set up to ensure a fast and professional response to security incidents, and regular training and exercises must be planned to keep the staff vigilant. And last but not least, to be fully able to protect its constituency, the new team must be integrated into the national and international CERT communities.

Two presentations from established CERTs, from the academic and government sectors, demonstrated that the basic requirements for establishing new teams are very similar, whether they are functioning in the academic, government or commercial arena.

Tools
Without proper tools, a CERT would be unable to provide its services properly. One must-have tool is a 'Trouble Ticket System' to track incidents. A database for storing incident-related data and special tools for forensic analysis and system recovery are also part of the basic equipment of a CERT. The CERT community is very active in developing such tools for specific CERT tasks.

The CERT community also develops more general tools. For example, GovCERT.nl presented their CERT-in-a-box tool, a collection of useful information for setting up a CERT, and the UK's National Information Security Co-ordination Centre (NISCC) presented the 'Warning, Alerting and Reporting Point' (WARP) toolbox (software for sharing security information inside small communities). The lesson learned here is that, for almost every aspect of CERT work, a tool already exists that is publicly available. ENISA's task is to collect this information and pass it on to its stakeholders.

Co-operation
Incident handling does not stop at the borders of the constituency's own network. In most security incidents, the constituencies of more than one CERT are affected, on both the side of the attacker and the victim. To solve an incident completely, CERTs must co-operate and exchange related information. The CERTs in Europe realised this very early in the 1990s and started to work together. The exchange of incident-related data was soon supplemented by the sharing of best practices, the training of staff and the joint development of tools. Nowadays several lively and well functioning communities of response teams exist. Besides the well known Task Force CSIRT (TF-CSIRT), which is open to every kind of response team, special interest groups for governmental CERTs (EGC) and the Abuse Teams of big Internet Service Providers (E-COAT) presented their activities at the ENISA workshop. ENISA co-operates with all these entities and looks for ways to assist their work.

Legal aspects
One of the biggest needs is support for the more technically oriented CERT staff in legal issues. The 'Legal Handbook for CSIRTs' aims to fill this gap and offers the CERTs a comprehensive and easy to navigate stock of legal information that might affect incident handling in the different EU member states. ENISA will promote this tool to enhance support in this area, and will investigate how it can be updated on a regular basis. (For more on the Handbook, see page 11.)

Conclusions from Workshop One
The ENISA workshop, 'CERTs in Europe – Lessons learned and good practice', was intended to present a complete overview of the CERT landscape in Europe. According to the participants' evaluations, this goal was achieved; 97% judged the overall quality of the workshop as good or even excellent, and 94% think a similar event in 2006 would be useful.

Even though the different communities are very active, ENISA has uncovered areas where it can make a significant contribution; enhanced support for new CERTs, the provision of training, the facilitation of tools and the collection and compilation of existing but scattered information are the most promising.

Marco Thorbruegge is a Senior Expert in Computer Incident and Response Handling at ENISA

Workshop Two: Good Practice in Awareness Raising

Isabella Santa

As part of ENISA's 2005 Work Programme, an Information Package entitled 'Raising Awareness in Information Security – Insight and Guidance for Members States' has been produced. The Package has been compiled from the analysis of successful practices and measures already underway in the awareness raising field. It offers insight into problems in this area and indicates potential solutions, providing useful tools and templates to optimise the delivery of campaign messages.

Information packages and awareness raising

The second ENISA workshop was an opportunity for sharing the main findings of this Information Package with the Member State representatives.

The workshop focused on a unique set of information security challenges affecting SMEs and home users. Through a combination of presentations, case studies and panel debates, participants explored further cutting edge topics, key issues and emerging good practice in the awareness raising field.

Reviews of implemented good practice reveal that:

- Member States can positively influence the public's behaviour towards information security
- The audience should be properly evaluated
- Communication channels need to be investigated to optimise the delivery of the campaign message
- More measurements of success are needed
- Lessons learnt sessions should be established
- Co-ordination or public-private partnerships should be clearly defined

Effectiveness and efficiency of awareness raising initiatives

Acceleration, convergence and complexity are three concepts which need to be fully considered for improving the effectiveness and efficiency of awareness raising initiatives:

- Changes in conditions and requirements are occurring every day as information security is a fast moving area. Knowledge sharing, education and change management are crucial to raising awareness within the implementation of a culture of security (acceleration)
- Finding a common denominator within the Member States is important to facilitating Community co-operation, exchanging information and promoting best practice (convergence)
- Interests/needs, knowledge, preferred channel, geography and culture should be taken into consideration when defining the profile of each target group (complexity).

Conclusions from Workshop Two

The representatives of the Member States rated the Awareness Raising workshop as very useful in terms of information sharing (75%) and networking (65%).

ENISA will promote the exchange of information and provide material that could be customised and presented to the Member States to facilitate their work on awareness raising.

Isabella Santa is a Senior Expert in Awareness Raising at ENISA

CSIRT Legal Handbook

Lorenzo Valeri, Neil Robinson

Lorenzo Valeri and Neil Robinson

The ENISA Workshop, 'CERTs in Europe – Lessons learned and good practice', held in Brussels on 13 December 2005, saw a live demonstration of a new tool developed by RAND Europe and Lawfort to support CERTs – or, to use the technically more correct term, CSIRTs (Computer Security Incident Response Teams) – in legal issues.

CSIRTs are usually small groups of technical specialists responsible round the clock for responding quickly to a computer security incident within an organisation. A CSIRT will normally be operational 24 hours a day, 7 days a week.

History of the CSIRT Legal Handbook

The CSIRT Legal Handbook was originally developed in 2003, when Directorate General Information Society and Media at the European Commission asked RAND Europe to prepare a first edition. In early 2005, DG Information Society and Media again asked RAND Europe, this time with the help of Lawfort (a Belgian law firm), to update the 2003 edition. The 2005 edition thus represents a significant revision, taking into account recent developments in national legal frameworks and extending its scope to cover all current EU member states. The Handbook is consistent with the user requirements of Europe's CSIRT communities. Additionally, the Commission asked that a CD-ROM and online edition of the Handbook be produced, so that the 'user footprint' of the Handbook could be as wide as possible.

The 2005 Edition of the 'Handbook of Legal Procedures of Computer and Network Misuse' (or 'CSIRT Legal Handbook' for short) is designed to bridge the gap between those at the sharp end of dealing with Network and Information Security (NIS) incidents and the criminal justice system. Very often, CSIRTs are operating with few resources, and the Handbook is ultimately intended to help them understand whether an incident is prosecutable and, if so, under what law and what sort of punishment can be expected for the perpetrator. The Handbook also aims to keep CSIRTs appraised of any relevant legislation when they may be responding to an incident (such as data protection law) and dealing with evidence (such as particular evidence requirements in some countries).

The Handbook is available in print and online (at www.csirt-handbook.org.uk), in an easy-to-use, searchable format.

The 2005 CSIRT Legal Handbook remains globally distinctive in the field of information security. It provides a comprehensive, up-to-date collection of information on European and national rules, regulations, and laws concerning computer misuse, according to an established 'taxonomy' or classification of types of misuse. This classification of incidents is as follows:

- Target Fingerprinting
- Malicious Code
- Account Compromise
- Intrusion Attempt
- Denial of Service
- Unauthorised Access to Information
- Unauthorised Modification of Information
- Unauthorised Access to Communication Systems
- Unauthorised Access to Transmission
- Spam

In addition, the Handbook details procedures for working with responsible law enforcement bodies, providing current contact information and guidelines as to when and how law enforcement must be informed of incidents. Finally, extensive references and links allow the reader to follow up with more detailed enquiries.

In updating the Handbook, RAND Europe researchers reviewed the existing incident taxonomy, analysed standard enquiries and reporting needs of the CSIRT communities, surveyed national legal frameworks and relevant industrial initiatives, and created an online format to provide the information and modify it when required.

The online database permits keyword searching and browsing of specific national data such as:

- the full text of cyber-crime statutes
- background information relating to the legal environment
- descriptions of the structure and operation of the judiciary and law enforcement
- principles and procedures relating to data retention
- relevant traffic monitoring and evidence collection processes
- government and industry led reporting mechanisms
- bibliographical references

The project also undertook a small quantitative analysis of the data gathered for each of the Member States. It found that there was a wide discrepancy in the legality of various incidents across the Member States. In some countries, some types of incidents (for example, Unauthorised Access to Information) were punishable under many different laws, while in other countries the same incident is not covered by any law. For example, in Spain, Unauthorised Access to Transmissions is punishable under nine different laws, whereas in Sweden this incident is only punishable under one. Likewise, in Germany, Account Compromise is not punishable as a federal crime. Interestingly, many countries still do not have any legislation to deal with Target Fingerprinting – the act of reconnaissance prior to conducting an incident. Additionally there were wide differences in the maximum possible penal sanction available under many different legislative frameworks. In the Netherlands, the maximum available penalty for Denial of Service is 15 years – but in Ireland this incident is only punishable by a fine.

In conclusion, the 2005 Edition of the CSIRT Handbook is a valuable tool for CSIRTs across Europe and additionally is a useful resource for all those interested in how the legislative environment for dealing with NIS is evolving.

For more information, or to submit comments or improvements, please contact:

RAND Europe (Cambridge)
www.rand.org/randeurope
neilr@rand.org

Lawfort
www.lawfort.be

Dr. Lorenzo Valeri is a Research Leader at RAND Europe

Neil Robinson is an Analyst at RAND Europe

From the Member States

CIRCA – Computer Incident Response Co-ordination Austria

The Austrian Early-Warning and Information Infrastructure Protection System

Andrea Cuny-Pierron

CIRCA is the main body in Austria in the field of Internet early warning systems. It is a public-private partnership whose main actors are the Federation of Austrian Internet Service Providers (ISPA), the Austrian Federal Chancellery and the A-SIT (Austrian Secure Information Technology Centre).

CIRCA is designed as an information exchange and incident reaction network at the national level in Austria. It is aimed at multidisciplinary incident experts from ISPs, IT security firms, critical infrastructures, companies with large networks and organisations from the public sector. In this article we show how these parties co-operate to provide a platform for reacting immediately to Internet security incidents.

Organisational structure of CIRCA

CIRCA consists of two organisational parts: one for the public sector and one for the private sector. Each of these has a list server which acts as a means of communication between the participants. A given incident is communicated on one of three mailing lists – labelled 'information', 'warning', and 'alert' – depending on whether the incident is considered to pose a low, medium, or high risk respectively. About 50 participants have access to the lists and they may also use it as a discussion forum. The two list servers also communicate with each other, so that alerts on the public server are also transmitted to participants in the private sector and vice versa.

Information sharing is beneficial – but one does have to be careful. After all, some of the information that is exchanged between participants is very sensitive, since it relates to security problems that the participants might not want publicised, such as a security breach at a bank. A code of conduct has therefore been established between the participants. The key provision of this code is confidentiality – participants may not publicly disclose information obtained via CIRCA. This measure is meant to foster an open exchange of views and information between the participants.

The most important Austrian ISPs have joined CIRCA and committed themselves to responding in a co-operative and co-ordinated way to major incidents. At present, there are no competing systems to CIRCA in Austria, though there are a number of CERTs – the academic network, ACO-net, has its own CERT, as do some large companies and public administration services. Although participants must provide their own manpower resources, there is no fee for participation.

Note that, unlike other early warning systems, CIRCA does not involve the end user. It focuses on the security of the underlying Internet infrastructure itself and was not conceived to cope with incidents at the level of the private user or small installations.

A short history of CIRCA

The idea of creating a national platform in Austria first emerged after the spread of the 'love bug' virus. Because it took some time for the virus to cause substantial damage, having a proper warning system in place would have helped minimise the damage. But how was one to build such a system from scratch? Two things were clear – any appropriate warning system would first require the assembly of a network of experts and would then require a system to disseminate warnings.

The three initial main players were ISPA (www.ispa.at), the Federal Chancellery (www.bka.gv.at), the academic ACO-net (the main academic network in Austria) and the Austrian anti-virus company, IKARUS (www.ikarus.at). The first steps involved finding the IT security experts in the different organisations who would be willing and able to co-operate within the CIRCA framework. This took some time, since, for obvious reasons, organisations are very sensitive about sharing information on possible security breaches or incidents.

The next step was to implement two list servers to enable participants to exchange secure mails (digitally signed and encrypted) about Internet security incidents or other critical information. One of these systems was set up at the Federal Chancellery, the other at ISPA. After an initial testing phase, this system is now fully operational, and members are able to enjoy the full benefit of the CIRCA system.

CIRCA – A series of sensors looking for incidents

So how is CIRCA actually implemented? Clearly, detection lies at the heart of an early warning system. To build up an early warning system it is necessary to gather information about incidents that have occurred or that are being planned at a very early stage of their development, since viruses and worms are spreading more quickly than in the past and the available response window is shrinking.

To this end CIRCA has established a system of different sensors to obtain early indications. There are three classes of sensors used:

- Human sensors such as operators from ISPs. They report on incidents or suspicious network activity.
- Statistical reports of occurrences of viruses or worms from firewalls and anti-virus programmes installed at different organisations.
- Honey pot mail addresses in frequently used homepages to collect viruses or worms for analysis (this activity is still under development).

The information from the sensors can be reported manually or automatically in the system and is then available for all CIRCA participants. The actual data is stored on the two list servers that have already been mentioned, one for the public and one for the private sector. These two servers run identical software and all messages that are exchanged between participants are digitally signed and encrypted.

Emergency readiness and critical infrastructure

Critical infrastructures such as the electricity supply are becoming more and more dependent on the functioning of the Internet, either directly or indirectly. For this reason CIRCA considers CIP (Critical Infrastructure Protection) as an increasingly important task.

A related focus for CIRCA is the ability to deal with emergency situations such as the full or partial breakdown of the Internet at a national level. In such a situation it is important that the main operational players are informed about the measures they should take to manage the situation and restore the network to normal. With this goal in mind, CIRCA has defined a set of interim procedures and technical devices to establish a crisis team in such situations.

It should be emphasised that CIRCA has an important role to play in securing critical infrastructures and in emergency response since, in the case of serious incidents, individual actions or interventions from the main actors running the Internet may be counterproductive. This makes co-operation and co-ordination within the CIRCA framework all the more critical.

A look to the future and a look beyond Austria

In this article we have seen the reasons behind the creation of the CIRCA network and have taken a glimpse at some of its technical and procedural features. For the time being, the system is mainly driven by human actors. In the future, the concept of automated sensors will have to play a bigger role. Also, the emergency procedures under development need to be tested and improved to effectively face emergency situations.

The basic concept of CIRCA is not unique to the situation in Austria and could benefit from international collaboration. CIRCA intends to explore the opportunities for international co-operation with other warning networks or institutions engaged in the essential functioning and securing of the Internet. It is hoped that this exchange of information will be beneficial for both CIRCA and its partners.

Andrea Cuny-Pierron is a Project Manager with CIRCA and Internet Service Providers Austria

Feedback on the Evaluation and Certification of Security

Pascal Chour

More and more countries are setting up a plan for assessing and certifying the security of IT products according to the Common Criteria (CC). Increasing numbers of evaluations are taking place around the world but, along with their success, comes criticism. This article attempts to answer some of this criticism. It is based on feedback received for Information Technology Security Evaluation Criteria (ITSEC) and, more recently, CC evaluations, which have been conducted in France since 1991.

A few reminders about security evaluation according to ITSEC and CC

Security evaluation checks a product's conformity to its security specification, called its 'security target'. It also checks the effectiveness of the security functions, which ward off identified threats. More than its conformity, it is generally its effectiveness – and particularly the vulnerability analysis level (VLA in the CC) – which interests well informed users. However, both are linked; the confidence that is placed in the vulnerability analysis level depends on the confidence that is placed in its conformity.

Security criteria introduce the idea of a level of confidence (these are called E1 to E6 for the ITSEC, and EAL1 to EAL7 for the CC). The higher the level, the more information the product developer must provide and the greater the work carried out by the evaluation laboratory.

Today, criteria are applied in the context of so-called 'national schemes' managed by states, for example, the DCSSI in France, the CESG in the United Kingdom and the BSI in Germany, to mention the oldest in Europe. These schemes serve a number of functions – they license laboratories (the Information Technology Security Evaluation Facility, ITSEF) to perform the evaluations, they certify their work and they sign agreements for mutual recognition of certificates between different national schemes. The certificate granted by the national scheme confirms that the model of the evaluated product or system meets the specified characteristics of security. It also confirms that the evaluation was conducted in accordance with the rules and standards in force, with the required skills and impartiality.

Other concerned players in an evaluation are:

- The sponsor who funds the evaluation
- The developer who develops the product (who in some cases may be the same as the sponsor).

Another party which should be mentioned is the contractor. This is an organisation which uses certification as a selection criterion when acquiring products. Examples of important contractors in the security certification context are the federal government in the United States or major banks in France.

Security evaluations can, however, be complex undertakings, and there have been a number of criticisms levelled at the entire process. The main criticisms relating to these evaluation and certification schemes are:

- The perceived high cost of certification
- The delays the process is seen as incurring
- The abuse of certificates by some developers
- The obscure nature of some of the criteria.

Criticisms about costs

The main factors determining the overall cost of the evaluation are:

- The evaluation level (EAL) targeted and The resistance level (VLA) targeted
- The extent to which the developer controls the full development process
- The complexity of the product
- The developer's experience in security and familiarity with the evaluation criteria
- The criteria themselves and what they impose.

With regard to this last point, it is true that criteria requirements and the evaluation process mean that, intrinsically, the cost of an evaluation is significant. While some studies have shown that it is possible to cut costs in the process, research has shown that simplifying the criteria does not lead to significant cost reduction.

As far as the targeted EAL (and VLA) levels are concerned, the internal (developer) and external (evaluation and certification) costs increase with the level.

Up to CC level EAL4 (the corresponding ITSEC level is E3), a controlled development procedure must be capable of providing the main information requested in terms of conformity. The information required in terms of effectiveness is rarely generated in the course of traditional development methods. It must therefore be produced specifically for the evaluation, resulting in increased costs.

Beyond EAL4, the use of semi-formal and formal methods increases costs to such an extent that few developers practise these methods. They are obliged therefore either to undertake training or to call on external experts so as to be able to satisfy the criteria requirements.

One last comment on costs – according to developers who undertake an initial evaluation, the internal costs of the CC in their development are the same as the external costs (evaluation and certification fees). This would indicate a very high cost of evaluation, but these estimates should nonetheless be taken with a grain of salt.

Criticisms about delays

We have already seen that the tasks involved in evaluation are fairly substantial. Since the most resource-intensive tasks are difficult to carry out in parallel, the minimum timeframes for a full evaluation can easily span several months. However, there is another side to this story, and it is sometimes the security certification process itself which is to blame for the lengthy timeframes. Some developers overlook the fact that they themselves are also responsible for extended timeframes. There are several reasons for this:

- Perhaps most obviously, the evaluation identifies non-conformities or vulnerabilities. These have to be corrected by the developer, and the evaluator must then reassess these corrections. There can be a period of several weeks or even months between the moment that the developer is told about the problem and the moment that he or she delivers a corrected version of the product. Subsequent corrective time and re-evaluations increase the timeframe that was initially fixed for the certification.

- Secondly, there are some developers who do not sufficiently understand the inherent complexity of the evaluation procedure. The thoroughness of the procedure and depth of the analyses conducted may come as a surprise to some, a situation that was common in the 1990s. Some products were not tested sufficiently and presented functional faults such that it was simply impossible for the certifying laboratory to carry out its work. Today an improvement in the situation can be seen as certain developers have gained experience, while others have benefited from the advice offered in the course of the evaluation.

To respond to some of this criticism, procedures have been put in place to enable a reduction in the timeframes, particularly for new versions of previously certified products.

If the modifications have only a minor effect on security, evaluation sponsors can use a so-called 'assurance continuity' procedure. In this case the certification body confirms this fact with a maintenance report which avoids having to implement the full blown certification process.

When the modifications are more substantial, a new certification cannot be avoided and the product must be evaluated again. However, even in this case, the tasks and the accompanying timeframes can be reduced by re-using where possible information obtained during the initial evaluation.

Improper use of the certificate

In the past, certificates have sometimes been misused and did not tell consumers about the true security level of the product. For developers, it is tempting to evaluate a product on a minor security function and to associate the certificate obtained with all the other security functions of the product. Another abuse is to mention an unrealistic hypothesis in the security target about the conditions for using the product. These practices, which mislead the consumer and are ultimately counterproductive, are more limited today as consumers become better educated about certification.

There are several concrete ways to help ensure that consumers are better informed:

- A product can be evaluated in compliance with a protection profile, which is CC jargon for the specification of a generic need. The protection profile validates the fact that the security target has a certain substance and that it meets a user need. (Admittedly, the effectiveness of this system has been reduced by the overabundance of protection profiles, which creates confusion and complicates the choice for consumers in certain fields.)

- Providing consumers are sufficiently competent, they can read the product security target. This information must be publicly available for certificates subject to mutual recognition agreements. Security targets and certification reports are available at www.commoncriteriaportal.org and can also generally be found on the websites of the certification bodies in the issuing countries – at present there are nine.

- Another way involves validating that the product security target meets a particular organisational need before beginning the evaluation. As an illustration, consider how this is done in France: the qualification procedure includes a list of security products for the administration whose security specification has been validated beforehand by the DCSSI. The qualification procedure offers three levels of evaluation (standard, enhanced, high) that match the three levels of confidence that are used for classification within the administration. The qualification process to check this level of confidence is based on the CC evaluation. If the product is certified, then it can also be used at the targeted level and is placed in the DCSSI catalogue of qualified products (www.ssi.gouv.fr/fr/politique_produit/catalogue/index.html).

Obscurity of the jargon

All techniques create their own jargon. Security is no exception to this rule, and nor is security evaluation. A pendulum effect has occurred in this area; the ITSEC allowed great freedom of expression in drawing up the security targets. The CC tried to improve the formalisation of this expression, but this resulted in an abundance of acronyms and jargon which made documents difficult to read for inexperienced users. However, a security target involves several reading levels (the product description, in particular, is written in non-technical language) and informative annexes can explain things to novices in a way that they can understand. In this field, just as in others, it is the quality of the drafter that determines whether the security target is easy to understand or not. The qualification procedure set up by the DCSSI for the French scheme takes this aspect into account when validating security targets.

Conclusion

We have seen that there are important and valid concerns regarding the security evaluation process, such as costs, delays, certificate abuse and obscure jargon. In this article we have tried to demonstrate that there has been much improvement in minimising these concerns. Security evaluation remains a valuable tool in helping consumers understand the security functionality they can expect from products.

Pascal Chour is Head of Certification at DCSSI (the French National Communication Security Agency)

BSI Issues Certificates Under ISO 27001, Based on *IT-Grundschutz*

Miriam Serowy

The best way for organisations to prove to their customers that they work according to best practice in a given field is to prove that they comply with certain standards.

For many years, business and authorities alike have used the BSI (the Federal Office for Information Security in Germany) *IT-Grundschutz* (baseline protection for IT systems) certificate to prove to their clients that they have a sufficient level of IT security. To ensure that the *IT-Grundschutz* certificate issued by the BSI also covers the international certification standard for information management systems ISO 27001 (formerly BS 7799-2), the procedure under *IT-Grundschutz* was adapted to the requirements of the standard. By the same token, the certification criteria and licensing criteria for auditors were adapted to ISO 27001. From 1 January 2006, the BSI can also verify organisations for ISO 27001 on the basis of *IT-Grundschutz*.

What is the difference between the regular ISO 27001 and ISO 27001 on the basis of *IT-Grundschutz*?

In addition to the analysis and evaluation of IT security management systems, certification under ISO 27001 on the basis of *IT-Grundschutz* consists of a technical and organisational analysis and an evaluation of specific IT security measures based on the *IT-Grundschutz* catalogues. Thus, the combined certification under ISO 27001 on the basis of *IT-Grundschutz*, as offered by the BSI, provides a better overview of the measures that have actually been implemented than a simple ISO certification. Since this standard is internationally established and recognised, it will be of particular interest to businesses operating in international markets.

Amendments to *IT-Grundschutz*

In order to comply with the requirements of the ISO 27001 standard, the *IT-Grundschutz* manual had to be revised and has been replaced by BSI standards (standards 100-1 to 100-3) containing BSI recommendations on methods, processes and procedures as well as on approaches to and measures for IT security. In addition to these BSI standards, *IT-Grundschutz* catalogues have been introduced addressing the elements, threats and measures that had already been dealt with in the old manual.

Particular note should be given to the significant changes made in the field of information management systems.

The BSI 100-1 standard on information security management systems (ISMS) defines general ISMS requirements. These requirements, which are written in simple language, should be considered as a systematic introduction and as guidelines for users, no matter which method they use. The BSI 100-1 standard is fully compatible with the ISO 27001 standard and incorporates the recommendations of ISO standards 13335 and 17799.

The BSI 100-2 standard on the *IT-Grundschutz* procedure systematically describes how to set up and run an IT security management system. Important issues addressed in this standard include the role of IT security management and the necessary structures. It thoroughly discusses how to develop an IT security strategy in practice, how to choose adequate IT security measures and what to pay attention to when implementing the IT security strategy. It also elaborates how to maintain IT security during ongoing operation. *IT-Grundschutz* provides an interpretation of the rather general requirements of the standards ISO 27001, ISO 17799 and ISO 13335, and contains a great deal of useful information and practical examples, helping users to put the standards into practice.

Together, the *IT-Grundschutz* catalogues and procedure not only explain what should be done, but also give advice on the technical and organisational implementation. Approaching IT security on the basis of *IT-Grundschutz* is a tested and efficient way to fulfil all requirements of the above mentioned ISO standards.

ISO 27001 requires the identification of a risk assessment methodology but leaves it up to individual companies to decide what sort of additional risk analysis they want to carry out. The BSI 100-3 standard sets out one possibility for making a risk analysis, which focuses mainly on standard security measures in the areas of organisation, personnel, infrastructure and technology, as defined in the *IT-Grundschutz* catalogues.

(Note that the proposed risk analysis method does not require significant additional effort and uses as many elements from the *IT-Grundschutz* procedure as possible. Therefore, this method is particularly suitable for companies which have already successfully implemented the *IT-Grundschutz* measures and now want to make an additional risk analysis that seamlessly continues the *IT-Grundschutz* security analysis.)

How to obtain a ISO 27001 Certification based on *IT-Grundschutz*

First, a licensed ISO 27001 auditor will examine whether the requirements set out in the relevant BSI standards are fulfilled before an ISO 27001 certificate based on *IT-Grundschutz* can be issued. As part of this examination, the auditor reviews the reference material drawn up by the organisation or company, conducts an on-site examination and compiles an audit report. The audit report, which must be prepared in accordance with the audit criteria for ISO 27001 audits defined by the BSI, has to be submitted to the BSI, which, on the basis of the report, then decides whether to issue a certificate under the ISO 27001 standard in line with *IT-Grundschutz*.

The audit criteria have also been adapted to the requirements of the ISO standard. The major new features are that some audits require an expanded security analysis and an expanded risk analysis. The addition of these two very comprehensive and sophisticated procedures to the audit and certification procedure under the ISO 27001 standard on the basis of *IT-Grundschutz* marks the major difference between the old and the new certification procedures.

As a rule, an additional security analysis has to be carried out if:

- the security requirements of a company go beyond what is normally necessary (elements requiring strong or very strong protection)
- the IT network comprises vital applications or components that are not covered by the standard elements listed in the *IT-Grundschutz* catalogues
- applications or components are used in environments or for purposes not provided for in *IT-Grundschutz*.

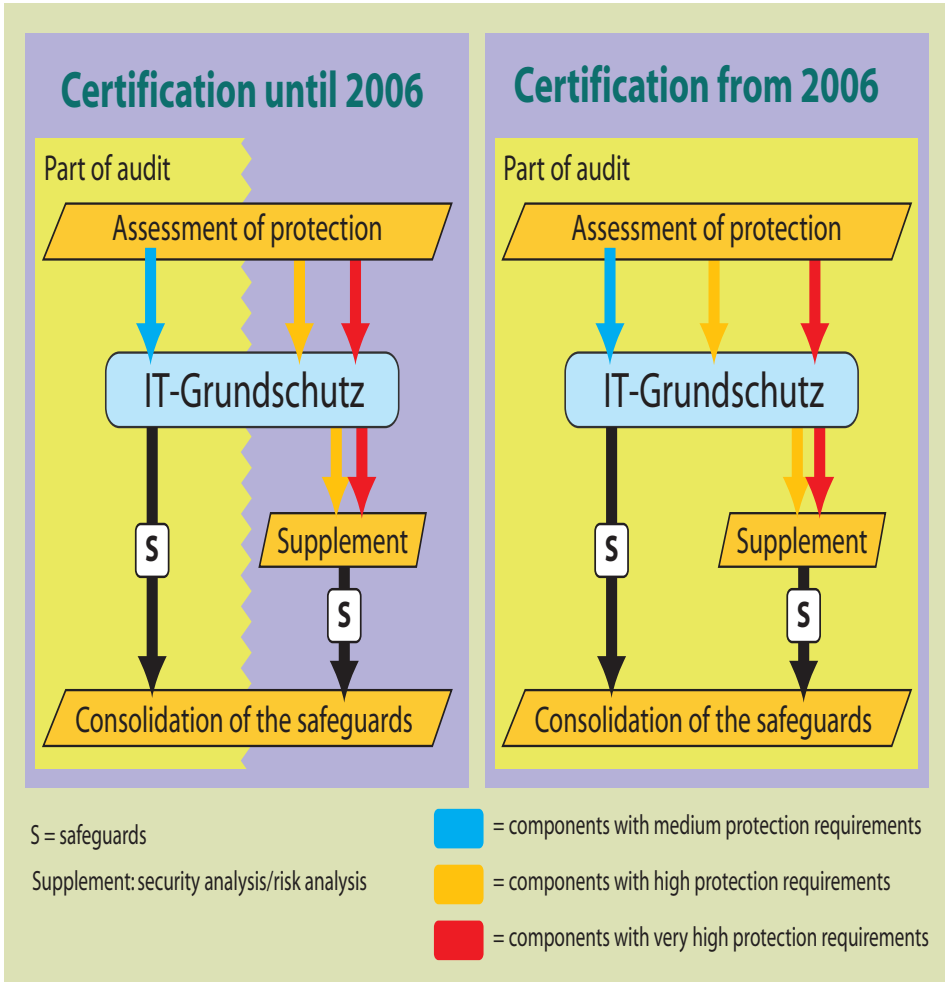
Licensing of ISO 27001 *IT-Grundschutz* auditors

In the course of changing the certification procedure, the procedure for licensing IT auditors has also been adapted to the requirements of the ISO standard EA 7/03 for auditors of information management systems. After a short transitional period, the *IT-Grundschutz* auditors of the BSI will be trained exclusively on the ISO 27001 standard.

Summary

After revision, *IT-Grundschutz* now includes the international standard ISO 27001. This will contribute further to the status of *IT-Grundschutz* as a well-established, powerful tool for implementing IT security in an organisation and as a well-defined procedure for building up an information security management system.

The BSI standards, the *IT-Grundschutz* catalogues and the audit criteria for ISO 27001 audits, as well as the licensing criteria for ISO 27001 auditors, are provided on the BSI web server at www.bsi.bund.de/gshb/zert/index.htm.



This diagram shows the main difference between the old and the new audit procedure. From 2006 onwards, the supplementary security analysis and risk analysis must be part of the audit.

Miriam Serowy is a desk officer in the certification section of the German Federal Office for Information Security (BSI)

International Conference on Availability, Reliability and Security (ARES) 2006

ENISA is supporting the International Conference on Availability, Reliability and Security (ARES) 2006, which will be held from 20-22 April at the Vienna University of Technology, during the Austrian EU presidency.

At this event, Dr. Louis Marinos, Senior Expert for Risk Management at ENISA, will deliver the keynote speech on Risk Management and Risk Assessment.

In addition, ENISA is organising a workshop on Risk Management entitled 'ISRM – Information Security Risk Management'. Its objective is to bring together European and international players from industry and research to exchange ideas, and to discuss European developments and organisational implementation issues in this important area.

Further information about ARES can be obtained at www.ares-conf.org. Information about the ISRM workshop can be found at www.ares-conf.org/?q=isrm.

New Awareness Raising Website in Lithuania

Rytis Rainys

On 7 February 2006, to commemorate Safer Internet Day in Europe, a new website, www.esaugumas.lt ('e-security'), was launched in Lithuania.

The website aims to provide a platform for gathering and spreading topical information on network and information security issues in Lithuania and is expected to become a national interactive information and network security forum. It was developed as a multi-stakeholder initiative and launched by the Communications Regulatory Authority of the Republic of Lithuania (RRT) in co-operation with the Ministry of the Interior and private businesses. It is the first website in Lithuania where all members of society can find relevant and topical information on electronic security issues.

The main purpose of the website is to present information on electronic security in a language, manner and style understandable to different groups of users. The site will provide information about ICT security problems, make recommendations and provide tools that could increase the security level of a home ICT user, as well as small, medium and large corporations and institutional bodies.

The website will provide information to meet the needs of visitors from all sectors:

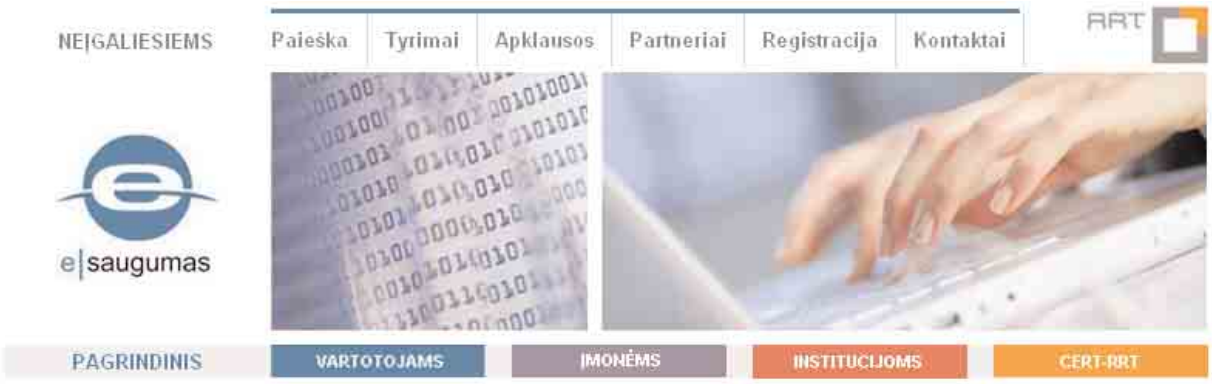
- **Home computer users** will find information about the most frequent problems on the Internet such as computer and mobile viruses, spam and fraud on the Internet, together with recommendations on how to avoid potential incidents.
- **Private sector organisations** will find methodological material on the security policy modelling in an organisation and risk management, as well as other important information such as dangers to electronic information security.
- **State institutions and their employees** will be able to familiarise themselves with network and information security related legislation, and find relevant training material.
- **CERTs** will find information about CERT activities in Lithuania, and international CERT institutions like TERENA and FIRST. The website also offers the possibility of reporting an incident to CERT-RRT.

The website already provides information on different aspects of research in the field of network and information security. In the future, the website will be interactive, with regular updates planned and with various testing software and security tools made available to users. These will help users evaluate their security level and implement appropriate security measures on their computers.

Of course, such a site is only useful if users actually come to the site and make use of the information. Early signs are encouraging – in its first month more than 4000 visitors came to the site. The site has already yielded interesting results – in response to the site's 'Question of the Day', we learned that 26 percent of respondents received at least one phishing e-mail per day.

RRT and its partners hope the website will become the number one portal of its kind in Lithuania, providing ICT users from the private, business and public sectors with information on network and information security.

Rytis Rainys is Head of the Network and Information Security Division of the Communications Regulatory Authority of the Republic of Lithuania



Dutch National Campaign on Digital Awareness: Digibewust

Arie van Bellen

There are numerous online risks – some visible and some not – against which we must protect ourselves, our businesses, our computers and our children. Risks such as viruses, spam, identity theft and credit card fraud all contribute to a feeling of insecurity and lessen user trust in digital applications. This lack of trust still forms a substantial barrier to user acceptance of new technologies and applications.

How do we address these risks and the accompanying trust deficit? Clearly the volatile online world requires us to foster an enhanced user awareness and to stimulate appropriately cautious online behaviour from everyone – businesses, governments and consumers alike.

It is to this end that the notion of 'digibewust' was introduced in the Netherlands. To be 'digibewust' ('digi-aware') means to make full use of the possibilities of the digital world while being fully aware of the possible dangers and risks. A 'digibewust' user understands the nature of online risks and can take appropriate action to mitigate them. This in turn helps achieve enhanced trust in the Internet.

To stimulate this awareness in the Netherlands, the campaign 'Digibewust' was launched by the Dutch Minister of Economic Affairs, Laurens Jan Brinkhorst, on 7 February, the European Safer Internet Day 2006. This new campaign is a joint initiative of the Dutch Ministry of Economic Affairs, ECP.NL, KPN, Microsoft and TPG Post. It currently focuses on children, parents and teachers, and in the next stage will also focus on SMEs and elderly people.

Minister Brinkhorst during European Safer Internet Day

The campaign is a part of the overall 'Digibewust' programme, a three-year public-private initiative which is being executed by ECP.NL, the platform for eNetherlands, on behalf of the Dutch Ministry of Economic Affairs. The programme aims to increase awareness of the safe use of all forms of electronic communications amongst citizens and companies. Existing information and education activities are being brought together within the programme to increase their impact and new activities are being developed.

For information about the campaign or the programme, please contact ECP.NL at info@digibewust.nl

For Dutch language information, please see www.digibewust.nl

Arie van Bellen is Programme Director of Digibewust and the Director of ECP.NL

eTEN Call for Proposals 2006 Published

The European Commission has published the eTEN call for proposals 2006. The call for proposals will close on 19 May at 16h00 (Brussels local time).

Pursuant to the eTEN work programme 2006, the Commission invites consortia to submit proposals on the following themes: eGovernment, eHealth, eInclusion, eLearning, 'Trust and Security' and Services for SMEs.

Proposals for Trust and Security should address the deployment of services with higher levels of security, authenticity, confidentiality and privacy for communications and transactions, services supporting the security governance of the Internet or contributing to a culture of security. Of particular interest are services using digital identities, solutions improving protection against spamming and other attacks at the network level, early warning systems for network security incidents and services helping to limit the damage caused by loss or theft of identity tokens, services exploiting trust and security features of IPv6.

Everyone who intends to submit a proposal should read the call publication, the 2006 Work Programme, the guide for Proposers 2006 and the evaluation guide 2006. All documentation can be found on the webpage dedicated to the call: www.europa.eu.int/information_society/activities/eten/calls/cfp20061/index_en.htm

Announcing ISSE 2006

This October Rome will play host to the Information Security Solutions Europe (ISSE) conference, which ENISA is co-organising with eema (the independent European association for e-business). Now in its eighth consecutive year, ISSE is Europe's largest independent debate on key security issues and challenges facing IT professionals.

Sharing information, research, expertise and best practice is one of the key ways for organisations to better understand the current security challenges and identify common solutions, and is one of the main aims of ISSE.

We are delighted that ISCOM (Institute for Communications and Information Technologies) will be hosting the conference at their Ministry building in Rome. TeleTrusT will again be organising the extensive three-track programme, which will include high-level guest speakers and industry authorities. These speakers will be introducing examples and case studies from different business sectors and fields including eGovernment and the public sector, health care, eBusiness, the financial sector and enterprise security. The hot topics already confirmed for debate include cryptography, identity management, mobile security, biometrics, compliance, networks, Public Key Infrastructure (PKI), data protection, security management, embedded security and trusted computing.

At this year's event we are also privileged to have one of the best minds in IT security – Bruce Schneier – sharing his insight during his keynote speech on the first day. Schneier is an internationally renowned security technologist and author and is well known as a refreshingly candid and lucid security critic and commentator. His keynote speech promises to be an enlightening and compelling introduction to the conference.

Roger Dean, Head of Special Projects at eema, summarises the value of the event:

"With identify fraud on the increase and global network security threats as real as ever, the need to share our experiences and strategies in ICT security has never been greater. This year's ISSE enables government and business to join forces again to debate important issues and formulate practical solutions."

For further information and to register your attendance for ISSE 2006 in Rome, please contact eema at isse@eema.org or visit the website at www.eema.org/isse.

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 may sign up to the ENISA Quarterly by sending an e-mail to press@enisa.eu.int with "subscribe" in the subject line. To unsubscribe send a mail to the same address with "unsubscribe".

Editor-in-Chief: Boaz Gelbord
boaz.gelbord@enisa.eu.int

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