enisa
European Network and Information Security Agency

Quarterly

12/2005

IN THIS EDITION

A WORD FROM THE EXECUTIVE DIRECTOR

Dear Readers,

As we close 2005, it is useful to reflect on our first year as an Agency and on the state of information security in general.

Time certainly does fly. It has been five years since the heyday of the dotcom boom. Despite the lull that followed, the Internet has never stopped evolving and has become increasingly interwoven with the fabric of our daily lives. From shopping online to instant messaging with friends, more and more of our daily activities involve the Internet.

Indeed, while most people reading these pages can probably still recall the first time they sent an e-mail or visited a webpage, for many of the teenagers of today this is a completely natural part of life; for them life without the Internet would be unthinkable.

At the same time the unabated growth of the Internet, online communities, and online commerce has also led to a myriad of new threats and security risks. And while there is certainly no need for panic or undue fear, it is clear that added vigilance and measures are needed in the face of these risks.

How can users stay secure and avoid the pitfalls of phishing attacks, identity theft, and other security incidents? Many of the rules for online safety are the same as those offline; for example, to avoid many Internet scams, users would be well advised to remember the old adages that there is no free lunch, and that if something sounds too good to be true, then it probably is.

And yet user vigilance is not enough - unfortunately even the most cautious of users can fall victim to crimes that exploit technical or procedural vulnerabilities in increasingly complex systems. This necessitates a collective effort to ensure that security does not become the spoiler in our move towards a digital society. This must involve all players including the private sector, users, and public organisations.

ENISA was set up with the aim of addressing these challenges within its well defined scope, and in particular to provide a uniquely European approach that focuses on information exchange, co-operation, and learning from each other.

ISSN1830-3609

At ENISA we feel that we have made great strides in meeting this challenge during the first operational year of our mandate. Since the last ENISA Quarterly we have organised joint events in Warsaw, Rome, Bonn, and Vilnius, in addition to the ongoing work in our areas of both technical expertise and fostering co-operation. This is a testament to the hard work and dedication of our staff and primarily to yourselves for having been so co-operative and helpful along this journey. We look forward to your continued support as we enter 2006.

Wishing you all a joyous holiday season and the very best for the New Year,

Yours truly,

Andrea Pirotti.
Executive Director, ENISA

A WORD FROM THE EDITOR

Dear Readers,

Two thousand five has been a busy year for information security and for the digital world in general. Before giving you an overview of this edition of the ENISA Quarterly, the end of the year is a good time to take a really quick look at some online changes and what they mean for information security.

Experience teaches us that the online landscape is constantly changing, sometimes gradually and sometimes in fits. These changes have been labelled in many different ways, but Web 2.0 – the "web as platform" – may be the most appropriate label for 2005. This term has been put forward to capture the barrage of change associated with the buzzwords RSS, Ajax, social networking and decentralised content.

Are these changes real or just hype? In the end, Web 2.0 as a label may have more to do with marketing than technology – after all, there was no single point of transition nor is there an agreed definition for this term. Nonetheless, the Web 2.0 metaphor does capture something about the evolution in the online environment.

There is no shortage of examples. Whereas Web 1.0 was mainly a publishing medium, Web 2.0 offers more flexibility and interactivity. Instead of static pages, Web 2.0 sites provide user interfaces that are more like desktop applications. Compare for example traditional websites with blogs or traditional encyclopaedias with Wikipedia. And while some phenomena like podcasting may be over-hyped, it does seem that we are witnessing yet another shift in the way people can and do use the Internet. As one blogger put it succinctly: "Web 2.0 is really about normal, everyday people using the Web and creating things on it".

This should, in itself, be cause for celebration. However, there are serious security concerns that arise from these changes. With Web 2.0, the control of content and distribution increasingly shifts from more fixed, stable entities to people and communities and becomes generally spread out over a more complex architecture. This much more diverse community means a moving target in efforts to secure the Internet.

These developments, combined with other trends such as convergence, lead to an increasingly complex ICT environment, which is increasingly vulnerable and exposed to attack. Indeed, when it comes to security, the facts on the ground are not always encouraging. Recent research has pointed towards a growing number of users curtailing their web activities or shunning e-commerce entirely.

(In the United States, the survey *Leap of Faith: Using the Internet Despite the Dangers* released by Consumer Reports Webwatch found that 86 percent of computer users have changed their online behaviour in some way because of concerns about identity theft. A little more than half stopped giving out personal information on the Web, while 25 percent said they had stopped making online purchases.)

In others words, users are voting with their feet. Are user concerns justified? And how do we go about convincing users that, with the right precautions, the Internet can be safe?

The ENISA Quarterly strives to be one forum where such issues can be discussed. We are proud to present you in this third edition with the usual menu you have come to expect from the ENISA Quarterly – contributions from leading experts, news on ENISA's activities and news from the Member States.

We are delighted to have an opening article from Howard Schmidt, the former cybersecurity advisor to President Bush and a world renowned expert on cybersecurity. He has written us a thorough piece on the very important issue of patching software vulnerabilities. There is no doubt that patching is a major issue today that stands at the centre of much of the discussion around cybersecurity. His informative and comprehensive piece is necessary reading not only for system administrators and others dealing with patching on the ground, but for anybody who wants to understand the challenges of this important security process.

Tyler Moore and Ross Anderson from Cambridge have written us a very interesting piece on the issue of the economics of information security, giving a clear introduction to this new and exciting field of research. In this article you will learn how the world of information security is not immune from the normal laws of economics that govern so many other aspects of our lives.

Another important activity for ENISA is the tracking of standards and in this edition Charles Brookson, who is very active in security standardisation, gives us an overview of the security activities within CEN and ETSI.

As usual, this edition of the ENISA Quarterly gives you an overview of our own activities as well as the activities in Member States. We take a look at some initiatives and activities in France, Germany and Sweden, as well as our joint events in several Member States. In this edition we also have a detailed contribution from Hungary brought to us by Ferenc Suba. He is the Vice Chairman of the ENISA Management Board and will be well known to some of our readers for the great job he did hosting the ISSE conference in Budapest.

Since the publication of our last edition we have already had hundreds of information security professionals in Europe and internationally signing up for the ENISA Quarterly. We are hoping to continue to attract new readership, and encourage you to spread the word about this magazine to your friends and colleagues.

Wishing you a happy holiday season and the very best wishes for the new year,

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

Patching Strategies

Howard Schmidt

Introduction

Patching is about correcting mistakes in software. Some experts say there are five to twenty errors (or bugs) in every one thousand lines of software code. Security bugs do not usually become known and a problem until after widespread use of the software. These software fixes are called a patch, hotfix or service pack.

> *A popular network operating system a few years ago had been estimated to contain at least 35 million lines of code. That's enough for 175,000 to 700,000 potential bugs.*
>
> "Procedures for Handling Security Patches" Peter Mell and Miles C. Tracy, National Institute of Standards and Technology

Patching is not like putting a bandage on a wound or covering a small hole in a wall. It's more like serious intrusive surgery as it can be – and often is – very complicated and has effects that may not be readily apparent. After rewriting pieces of the programme, the resulting 'patched' software compilation may still be vulnerable to other bugs. It is widely believed that, unless we fundamentally change the way we develop and test software, bugs will continue to exist and create security problems.

The big problem is lots of bugs means lots of fixes, and these fixes can result in dealing with many patches per year. These resulting patches can have a direct impact on business and critical infrastructure systems. It is an ongoing issue and many reports indicate it is a problem that needs to be dealt with sooner rather than later.

Potential consequences of not patching on a timely basis include:

- Damage or destruction of data (assess risk by multiplying damage potential by likelihood of damage)
- Business processes disrupted or data integrity compromised
- Loss of customer trust and business
- Non-compliance with regulations
- Penalties (civil and criminal)

Patching is frustrating and instils a sense of anger in those professionals who have to deal with it. This makes sense. Which of us likes being boxed into a corner by a situation with few good options? We have to install patches, but more times than not we must install patches with little regard for other priorities and responsibilities. Patching is a problem that more often than not manages us rather than enables us to manage the problem. There must be a better way to deal with issues related to patching.

Traditional patching is too slow

In some cases, such as high-risk situations, we need to be able to patch in less than a day to combat what is known as 'zero day vulnerabilities'. Indeed, concern is growing that there will soon come a time when we will need to patch in a few hours or even minutes.

Relying on human action alone is often insufficient; there is need for a defined patching automation plan. In recent cases of damaging strikes, we have had advance insights into what could happen, sometimes even with months to prepare for known vulnerabilities. Yet still the attackers were able to affect thousands of PCs and servers, impacting vital businesses and services and disrupting daily work.

Research into more than 1.9 million network vulnerabilities during a recent 24-month period shows significant findings (information below on Laws of Vulnerabilities and Threats of the Future is from research and articles by Gerhard Eschelbeck, Vice President of Engineering and Chief Technology Officer at Qualys, Inc):

- Half-life – The half-life of critical vulnerabilities is 30 days and doubles with lowering degrees of severity
- Prevalence – Half of the most prevalent and critical vulnerabilities are being replaced by new vulnerabilities each year
- Persistence – The lifespan of some vulnerabilities is unlimited; old risks recur partly due to new deployment of PCs and servers with faulty unpatched images of hard drives
- Exploitation – 80% of vulnerability exploits are available within 60 days after news announcements of vulnerabilities

New automated threats accelerate need for quick patching

Security threats come in three categories:

- Simple, low-tech First Generation threats are generic virus-type attacks spread by users opening infected e-mail and inconspicuous file attachments.
- More sophisticated Second Generation threats pose bigger problems. Created with automated tools, these active worms attack vulnerabilities in systems and applications by requiring no human interaction. Replication, identification and targeting of new victims are automatic. Blended threats are common, incorporating virus, Trojan and automation.
- Recent worms have already shown characteristics of new Third Generation threats, which systematically use scanning techniques to 'pre-identify' vulnerable new targets and use various attack vectors to maximise damage before one can take the necessary steps to mitigate the threats.

> 40% of attacks in 2003 were 'pre-attack reconnaissance'

SQL Slammer rapidly hit more than 75,000 hosts running SQL Server and had a worldwide impact. It was estimated to be the fastest worm ever, infecting more than 90% of vulnerable hosts within 10 minutes. It is estimated that, at its peak, Blaster infected more than 100,000 systems per hour, taking advantage of the most prevalent vulnerability in the world at that time.

Response window has shrunk

Unfortunately, new generation threats are emerging at a pace which requires full-time diligence. In the past, the discovery/attack lifecycle was much longer than what we have been seeing lately, with the time from the advent of discovering a vulnerability to exploitation decreasing markedly. SQL Slammer happened six months after discovery, Slapper was six weeks and the Blaster and Nachi worms came just three weeks after news of the vulnerability. Sasser struck two and a half weeks after announcement of the vulnerability. The Witty worm hit one day after the vulnerability was announced, compromising an estimated 12,000 vulnerable hosts within 45 minutes. In some cases, like Witty, the attack will be over before you can patch the vulnerability. This justifies the need for faster discovery of the vulnerabilities and application of critical patches.

> 'Traditional' patching is considered to be too expensive, takes too much time and has unpredictable results

Patching has impacts in many different ways. According to the Yankee Group, the estimated average cost of applying one patch to one desktop is $254. Costs rise the larger the company size and they have a direct impact on the annual security budget. Total annual cost can be in the millions for enterprises based on patching 5,000 desktops with 40 desktop security patches.

> Patches can sometimes be unreliable or, worse, be more harmful than the potential threats

All patches cannot be tested in all environments as there are just too many potential variables. As a result, some 'break' business processes and become very disruptive and more costly.

Practical Patching

With patching, we are often in a reactive role, racing to beat the virus or worm of the day. Unfortunately, patching is often the only reliable way to deal with some of these issues. There often are alternatives – port-blocking, extra monitoring – but fixing the problem is the best way if a fix is available. To that end we have to use new tools to tackle the problem smarter, better, faster, more reliably and with less cost.

In practical terms, we patch for three reasons:

- To fix faults in the software (e.g. security, performance or functionality)
- To alter functionality or to address a new security threat (e.g. antivirus signature)
- To change a software configuration (e.g. make it less susceptible to attack, run faster etc.)

Effective Patching System

An effective patching system has certain prerequisites that must be documented and met.

A patching system is all about identifying risks, minimising false positives and effectively applying patches – including protecting systems from being negatively affected by patches.

Any patching strategy must be approved by all interested parts of the management team. In some cases, the application of a patch will require temporarily pausing a business process which might have a financial impact which must be understood by the owners of the business. Everyone needs to know in advance how the process works in an emergency.

Tracking inventory – One of the key things one needs to know is what assets you have in order to patch them. Create and maintain a current database of all patchable devices attached to the network. Track all hardware, software, applications, services and configurations. This data will help identify which vulnerabilities affect particular subsets of your IT infrastructure. Also ensure that, when new components are added, they are also added to the inventory automatically. An accurate inventory is key to ensuring that you select and apply the correct patches.

List all security controls/policies to know how to respond – Policy management is very important. It starts at the top of an organisation with enterprise policies and reaches down to standard configurations for all security devices and applications including antivirus, firewall, intrusion detection and prevention etc. Policy management used to be a manual, cumbersome process. New tools now automate many aspects of policy management and will even enforce configurations on endpoint devices, including mobile devices.

Scan systems for vulnerabilities – There are many different ways to discover vulnerabilities. Some are done with software applications you install and maintain. Doing vulnerability scans using a web services solution allows you to have the scans done for you over the web. One advantage of a web service is that it is always up-to-date with the most recent vulnerabilities. You should not have to worry about updates to scanning technology because it is a key part of your patching system.

Compare vulnerabilities against inventory control list – This step helps to minimise false positives. With some IDS systems, for example, false positives can occur more often than accurate alarms if vulnerabilities do not match what is in your inventory. Use industry standard vulnerability databases such as the Common Vulnerabilities and Exposures (CVE) list and NIST's ICAT Metabase. CVE provides a comprehensive list of publicly known vulnerabilities, an analysis of authenticity of new vulnerabilities and a unique name for each vulnerability. ICAT takes CVE to the next level with detailed information about each vulnerability. Also see SANS Top 20 and CERT Advisories for more tools to help with this.

Classify the risk – Although everything may seem like the highest priority, you cannot do everything immediately, so rank the vulnerabilities to determine what to fix first. Microsoft's rating system is defined in the table below:

Severity Rating	Definition	Recommended Patching Timeframe
Critical	Exploitation could allow propagation of worms	Within 24 hours
Important	Exploitation could compromise confidentiality, integrity or availability of users' data or damage processing resources	Within one month
Moderate	Exploitation is serious, but mitigated by default configuration, auditing, need for user action or difficulty of exploitation	Next service pack or update rollup – deploy within four months
Low	Exploitation is extremely difficult or impact is minimal	Next service pack or update rollup – deploy within one year

What to fix first - Microsoft's rating system

One of the more valuable tools which helps determine the priorities of vulnerabilities is the Common Vulnerability Scoring System (CVSS), originally developed as a project for the National Infrastructure Advisory Council and now maintained by the Forum of Incident Response Teams (FIRST). This system has proved to be invaluable in prioritising patching for specific environments and can be customised to suit your enterprise.

Pre-test the patch – Testing in your own environment is vital. Most problems with patches are due to third party applications or modifications to default configuration settings.

Verify cryptographic checksums, Pretty Good Privacy signatures and digital certificates to confirm authenticity. Make sure the patch corrects the vulnerability without affecting operations of the business process and applications.

Apply the patch (make sure you have rollback capability)

Retest for vulnerability and confirm the fix

New Strategies for Patching

Standardise and Approve Patching Processes – Focussing on process and tools is vitally important. Effective patching requires many processes to be in place and operational before you can successfully implement the automated tools.

Don't forget client machines in the patching regiment that are important and often take a back seat to the server farm. Attacks affect clients as well as servers. During an attack, simply shutting off Port 135 or other networking ports shuts off client networking (this was the strategy advised early in the Blaster attack). Either way, it is a successful denial of service attack if you are running services on Port 135.

Automate Patching Processes – Automation is no longer just a nice easier way to patch but, in the world of governance and compliance, it is now almost a requirement. You cannot effectively patch without automating most of the process. Time is of the essence in more and more cases.

Many new automation tools used for patching provide other benefits beyond patching such as:

- Inventory Management
- Policy Management
- Vulnerability Assessment & Management
- Vulnerability Databases
- Patch Management

The National Institute of Standards and Technology (NIST) report on developing a patching strategy is one of the best available. There are also a number of valuable references from various vendors.

Preserve Uptime – In some cases you have to take a system offline to patch it. Patching systems should preserve uptime. Take advantage of new N+1 web architecture. Load balancing may preserve uptime because you can take boxes offline for patching one at a time during non-peak hours.

Simplify Environments – It is easier and faster to patch when systems use similar configurations. The complexity of IT environments slows the cycle of inventory, analysis, prioritisation, testing, fixing and retesting for more than just patching.

Industry Working to Reduce the Need for Patching – Industry is working hard to reduce the number of bugs, particularly using the new generation of automated code checking tools. Industry is doing more regression testing before releasing software. Finding all the buffer overflow problems before shipping will reduce the most common vulnerabilities used by hackers.

Centralise Responsibility for Patching – NIST recommends organisations should create and manage a patching process with a patch and vulnerability group (PVG), often a subset of system and network administrators whose duties are:

- creating an organisational hardware and software inventory
- identifying newly discovered vulnerabilities and security patches
- prioritising patch application
- creating an organisation-specific patch database
- testing patches for functionality and security
- distributing patch and vulnerability information to local administrators
- verifying patch installation through network and host vulnerability scanning
- training system administrators in the use of vulnerability databases
- deploying patches automatically (when applicable)
- configuring the automatic update of applications (when applicable)

Within the PVG scheme, system administrators are the foot soldiers; they do the patching, applying patches identified by the PVG, testing patches on the specific systems and identifying patches and vulnerabilities associated with software not monitored by PVG.

Many PVG responsibilities can be automated. Automation simplifies operations, speeds patching and is less expensive due to reduced staffing requirements.

Conclusion

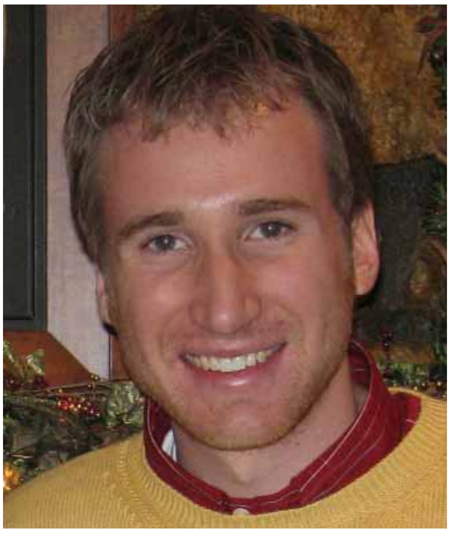
Patching is a fact of life for now. We need to be diligent and have it built into day-to-day security operations and do it efficiently and effectively. Establish a patching system strategy in concert with new technologies for automated patching. Get business unit buy-in in advance; you will need proper co-ordination and a good understanding of business risk to stop some business processes for emergency patching.

Automation simplifies many of the pains of the patching processes, is less expensive and speeds the protection of vulnerable systems.

Howard Schmidt is President and CEO of R & H Security Consulting LLC and a Former White House Cyber Security Advisor.

Trends in Security Economics

Tyler Moore, Ross Anderson



Tyler Moore

Ross Anderson

One of the most exciting and rapidly growing fields of research today is the economics of information security. Many security and privacy failures are not purely technical; rather, misaligned incentives are often to blame. For instance, people in the best position to protect a system may be poorly motivated if they do not have to bear the costs of failure. This article explores two of the key economic challenges to information security – incentives and metrics. We then discuss one of the applications, namely assessing the merits of open versus closed systems, and finally we highlight several promising research areas.

Misaligned incentives

It is an established principle of civil law that liability should be assigned to the entity best placed to manage risk; otherwise, perverse incentives may preclude the adoption of reasonable countermeasures. This has often been ignored by information security system designers. A classic example is ATM fraud. When a customer disputes a transaction, banks in the United States must demonstrate the customer is mistaken or lying to avoid responsibility. As a result, US banks have long been motivated to defend their systems properly. However, in Britain, Norway and the Netherlands, the burden of proof used to lie with the customer – creating a really hard problem for a victim of fraud. Banks underinvested in protection mechanisms until higher rates of fraud became untenable, and the liability was reassigned. Similar examples abound. Distributed denial of service attacks exploit unprotected home and university computers to target popular websites. So long as the attack does not pose a direct threat to the end user, few security measures will be adopted.

However, dumping liability on end users achieves little, since most users do not have the expertise to defend against such attacks. Many ISPs and mail service providers offer spam filtering services. More recently, liability has started to shift in practice to network operators. Their main incentive is that networks which produce large volumes of spam place their peering arrangements at risk.

Many open questions remain. We do not yet know the optimal balance between technical and regulatory mechanisms. How much reliance should we place on prevention, and how much on filtering? Should vendors of insecure platforms be liable? How much filtering should be done on egress from source networks, how much by the destination networks, and how much by the destination mail systems? What is clear is that any viable solution will have to consider both technology and incentives.

Measuring security strength: markets, auctions and return-on-investment

One common factor in many computer security problems is the existence of informational asymmetries. Akerlof won a Nobel Prize in Economics for explaining the pitfalls of a market with asymmetric information: if buyers cannot readily determine the quality of goods on offer, then they will not pay a premium for a high quality version. This drives out producers of quality goods, since they will not be compensated for their efforts. Used cars are a classic example – it is often impossible for a buyer to tell the difference between a good used car and a "lemon". The market price then falls to the price of unreliable cars, which undermines sales of good cars.

The software market too is a market for lemons. Because there is no good way for consumers to tell secure products from insecure ones, companies do not invest in product security. Certification schemes such as the Common Criteria were an early response; more recently, researchers are looking for ways to use markets to elicit information. Early attempts included vulnerability markets, where the current market price for an undiscovered exploit indicates the current level of system security. Refinements include establishing vulnerability auctions and collecting historical data to help predict the rate of subsequent discoveries.

Open versus closed systems

One of the hottest debates in security has centred on open versus closed systems. Are open systems such as GNU/Linux more secure than proprietary offerings such as Windows?

Here, too, security economics can provide some valuable guidance. If security vulnerabilities are uncorrelated with each other, then open and closed systems would be equivalent: opening up a system would make bugs easier for both the attacker and the defender to find and would thus help them both equally. The problem therefore becomes an experimental one: are security vulnerabilities correlated or not? Early statistical evidence suggests that they are. A recently discovered vulnerability is more likely to be rediscovered by someone else than one would expect from random chance.

Security economics can also throw light on the behaviour of markets that are open, or closed. For example, Hal Varian presented a surprising result at a Digital Rights Management (DRM) conference in January 2005 – that stronger DRM would help platforms more than the music industry, because the computer industry is more concentrated (with only three serious DRM suppliers – Microsoft, Sony and the dominant firm, Apple). Before the end of the year, the music industry was protesting that Apple was getting an unreasonably large share of the extra revenue being generated by online music sales. This surprised industry observers; the music industry in particular had expected that stronger DRM would help it make more money. It was a striking demonstration of the predictive power of economic analysis when applied to technical security mechanisms.

Towards a network perspective

Network analysis can be a powerful tool for information security economists. Networks are everywhere, from academic citation patterns to terrorist cell communication structures to underground file-sharing darknets. Each of these networks has distinct structural properties – from the density of connections between neighbours to the centrality of particular nodes. In fact, while much progress has been made in identifying the distinguishing characteristics of networks, the relationship between these properties and resulting attack and defence strategies is not at all well understood.

Social scientists use network analysis to examine the complicated interactions of large, decentralised groups in human society. But these tools have striking relevance for computer scientists as well. Decentralisation makes possible computer networks without unified control. The BGP (Border Gateway Protocol) routing that underlies the Internet is one example; peer-to-peer networks are a second; and the ad-hoc networking techniques under development by the sensor-network research community provide a third. Nodes can choose their behaviour, their transaction partners and even whether to participate in the system. The difficulties imposed by asymmetric information extend naturally to such networks, since individual nodes cannot view a network's complete topology or observe all its communications.

Many questions pertinent to security appear. Is it better for defenders to aggregate or disperse in the face of censorship attacks? Which network topologies are most resilient to targeted attack? What socially optimal network structures might balance the costs of maintaining security against the advantages of interconnection? And how do networks formed in practice differ from the best case? We can offer answers to some of these questions and discuss the direction solutions to others might take.

Several peer-to-peer systems, from the Eternity Service to Chord, distribute content randomly throughout the network. Yet for other systems, including most file-sharing applications like Gnutella and Kazaa, users are allowed to choose which content to share. Offering nodes discretion motivates them to spend more on defence. This is because individual preferences do not necessarily align with those of the larger community. A user with left-leaning political views may quickly lose interest in protecting shared information if he must serve right-wing content too. Yet a successful defence depends on the collective efforts of the system's users. Providing choice can maximise individual utilities as well as individual incentives to invest in defence. Future large-scale systems may be more a federation of networks, or of clubs, than large homogeneous entities.

For many networks, a small number of key players are critical to operational success. As a result, adversaries seeking to undermine the network target these nodes for attack. Music industry agents attempting to disrupt peer-to-peer file-sharing networks target individuals believed to have been running major nodes, using techniques from technical attacks to aggressive litigation. The same principle works in politics: as a handful of leading individuals often do much of the work to hold a society together, subverting or killing these leaders is likely to be the cheapest way to make an invaded country submit. But how might the defenders react? What are the optimal strategies of attack and defence? And how do defence tactics change under imperfect information, where co-ordination is imprecise?

Much has been made of the positive externalities generated by interconnection in networks. For instance, Metcalfe's Law claims that the value of a network is proportional to the square of its size. Yet there are also costs associated with network growth, notably security-related ones. In fact, without a single entity in control, the marginal costs of adding new nodes can actually rise with the network size. Peer-to-peer networks often grow to the point that free-riding cannot be mitigated effectively: the benefits brought by new nodes (e.g., files for sharing) no longer outweigh the security costs of new members. Over-participation then destroys the network. (An early example was CB radio, whose utility was undermined by congestion.) An interesting challenge is to capture these costs and examine the resulting impact on network formation.

We suspect that the scalability of security is a fundamental limiting factor in network growth, and indeed in the ways in which technology and society interact. A village is different from a city, and a global network is something else again. When designing dependable infrastructures for networked global society, we need to understand these issues better.

Conclusion

The economics of information security started out when we recognised that systems often fail for non-technical reasons. Security economics remains a vibrant cross-disciplinary effort, bringing in people from a wide variety of backgrounds, and throwing up deep and fascinating new challenges. Starting from the analysis of operational questions such as the right level of security investment and the incentives facing security managers, it has developed through the analysis of controversial questions such as the merits of open versus closed systems to such basic issues as the ways in which networks – and the institutions they support – scale in the face of accident, error and attack.

Until now, the field's annual event – the Workshop on the Economics of Information Security (WEIS) – has been held in the USA, but in 2006 it will come to Europe for the first time. To learn more about security economics, mark your diary for WEIS 2006 in Cambridge, England, on 26-28 June.

Tyler Moore is working for a PhD in security economics at the Computer Laboratory, Cambridge University, England.

Ross Anderson is Professor of Security Engineering at Cambridge University.

Security for ICT and the work of the European standards organisations

Charles Brookson

With the increasing complexity of information and communication technologies (ICT) networks and systems nowadays – and the growing ingenuity of those who would exploit them for illegal gain – security is not an additional feature that can be patched on after the adoption of a new technology; it is a key factor that has to be taken into consideration from the beginning of the standardisation process. Indeed, in many cases security can be a winning driver that enables the overall success of the technology.

CEN (the European Committee for Standardisation) and ETSI (the European Telecommunications Standards Institute) therefore have an essential role to play in both safeguarding and enabling the future of new ICT. This article outlines some of their security activities.

From its inception in 1988, ETSI has been at the leading edge in setting many security standards. The Institute achieved outstanding success with the standardisation of the Global System for Mobile communication (GSM™), which included authentication, anonymity and customer privacy – the first full world-wide commercial deployment of encryption and smart cards. Many other standards have built on ETSI's expertise in authentication for billing purposes and encryption for customer privacy; work to date has included Digital Enhanced Cordless Telecommunications (DECT™), Terrestrial Trunked Radio (TETRA), video standards, Multimedia Internet Protocol (IP) and subsequent mobile and fixed services. Today ETSI's security standardisation activities reach every aspect of ICT.

Security on the move – mobile telecommunications

The wireless infrastructure that terminals use to access the network makes mobile technologies very vulnerable to attack. New services on mobile phones (such as messaging, the transmission of pictures and the availability of videos and music) have all required additional security mechanisms; the definition of these has been accomplished by updates to various existing security specifications and the preparation of new 3G-specific documents by the Third Generation Partnership Project (3GPP™), of which ETSI is a founding partner.

The most recent release of the 3GPP specifications addresses a long list of features including network sharing and Digital Rights Management (DRM) to control payment for copyright material such as music and films. The new 'Priority' service will allow users of the appropriate category (typically the emergency services, government agents, the military) high priority to network services in crisis conditions, when there is a danger of overload of a potentially impaired network.

Lawful Interception

The ETSI Standard providing specifications for the handover interface for the lawful interception (LI) of telecommunications became operational in the Netherlands in 2003. It is the first official international standard designed for this purpose, and demonstrates ETSI's world-leading expertise in this field. This standard refers to both packet data and switched-circuit communications. Specifications for IP-based services (for example, Internet and e-mail) and upcoming Next Generation Networks (NGN) are now being developed.

Work has also started on the lawful interception of Wireless Local Area Network (WLAN) Internet access. Other LI work in ETSI addresses data retention, IPCablecom, satellite systems, TETRA and NGN, and, in co-operation with 3GPP, LI for the Universal Mobile Telecommunications System (UMTS™) and GSM.

Algorithms

ETSI creates cryptographic algorithms and protocols to be built into its standards to prevent fraud, unauthorised access to public and private telecommunications networks and to provide customer privacy. Recent achievements include the design of a privacy algorithm for GSM – A5/3 – based on the 3GPP algorithm Kasumi, the encryption algorithm for UMTS, and a new example authentication algorithm for GSM, based on Milenage. Both Kasumi and Milenage were also designed by ETSI. Development of new encryption and integrity algorithms to safeguard against a possible future breach of security is almost complete.

Smart Cards

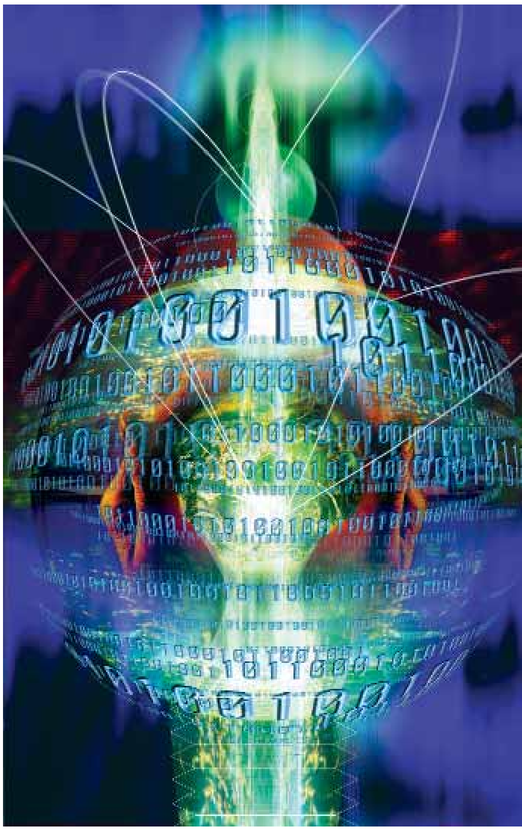
ETSI is active in smart card standardisation for mobile communications, mobile commerce and other applications. The main thrust of ETSI's current work aims to allow users access to global roaming by means of their smart card, irrespective of the radio access technology used. A new Technical Specification on Extensible Authentication Protocol (EAP) support in the Universal Integrated Circuit Card (UICC) was recently approved, specifying the use of a smart card as a secure access device to a WLAN and for PC security functions.

While the smart card in ETSI basically means the SIM card in your mobile, CEN's work on smart cards typically addresses the successor of magnetic stripe technology cards, i.e. cards with a micro-processor. The micro-processor enables a high security level. Amongst current topics being worked on within CEN TC224 (machine readable cards, related device interfaces and operations) are the uses of these cards as a citizen electronic card, and in electronic signature applications.

Safety and security of the citizen

ETSI is involved in the standardisation of emergency telecommunications in Project MESA (Mobility for Emergency and Safety Applications). This is a transatlantic partnership project, established by ETSI and the North American Telecommunications

➲



Industry Association (TIA), although membership has expanded, and the Project now also has members in Canada, India, Korea, Australia and Japan. Its aim is to define a digital mobile broadband system which will revolutionise the efficiency of first responders and rescue squads during an emergency or a disaster. At these times, the data rates needed for advanced services, together with the demand for mobility, reach far beyond the scope of current established wireless standards.

To provide a speedier solution than the development of brand new technologies, Project MESA has adopted a 'System of Systems' approach, which involves linking together a variety of existing and foreseen technologies and systems. The key factor is interoperability. Project MESA has recently defined the system technical requirements for this and, by 2006, expects to begin drawing up the final technical system specifications to produce a roadmap for future standardisation activities.

Meanwhile, CEN intends to look into standards for supervisory control and data acquisition (SCADA) systems and distributed control systems, which are vital for critical infrastructures including electric power generation, transmission and distribution, oil and gas refining and pipelines, water treatment and distribution, chemical production and processing, railroads and mass transit. Existing standards were developed without considering security as they were intended for isolated industrial environments. However, the security situation of SCADA – and indeed for numerous other technologies and situations today – has changed dramatically over the last few years!

Electronic signatures

Standardisation activities completed by CEN and ETSI under the European Electronic Signature Standardisation Initiative (EESSI) resulted in numerous standards to support the development of a European electronic signature infrastructure. Maintenance and enhancement of these standards continues in both CEN and ETSI. ETSI is now starting work on electronic signature profiles. CEN has also initiated new work on electronic signatures in relation to e-Invoicing, which is the subject of an EU Directive; this and other e-Invoicing issues are being addressed in an open CEN/ISSS Workshop.

Biometrics

Today's most visible need for Biometrics applications is for border control purposes as a result of the decision to introduce biometric data into travel documents to improve the accuracy of identification and prevent counterfeiting. As an enabler of identity verification systems, biometrics may well have applications in modern on-line public services, such as e-Government, e-Learning and e-Health. CEN is helping to identify standardisation needs in this area through the CEN/ISSS Focus Group on Biometrics.

And much more...

Space does not allow us to discuss here CEN's work on data protection and privacy, or the new work recently initiated in ETSI on Radio Frequency IDentification (RFID) for storing and remotely retrieving data, TETRA, or satellite communication services and applications (including mobile and broadcasting) – or the numerous other detailed aspects of security standardisation being pursued by the two organisations.

Future challenges

The threat to terminal devices from viruses and Trojan horses increases by the day, and ways must be found to protect customers. There has been a noticeable increase in legislation world-wide, driven by growing security concerns over the last few years. This has intensified activities, for example, in interception, communications during emergencies and prevention of crime.

In areas such as e-Learning, e-Health, e-Government and e-Business, the challenge will be to ensure technology is not just implemented but is also widely used. This will require a reliable and secure network infrastructure. But it will also depend on trust on the part of users – both citizens and businesses – that privacy, confidentiality, secure identification and other issues are rightly addressed.

Security standardisation, sometimes in support of legislative actions, therefore has an important role to play in the future development of ICT.

To identify new security threats – and conceive ways of tackling them – ETSI is hosting a free workshop on 'Future Security – the Risks, Threats and Opportunities', at its headquarters in Sophia Antipolis in the South of France, on 16 and 17 January 2006 (portal.etsi.org/securityworkshop).

To find out more about how standards are helping to ensure the security of ICT, visit www.cenorm.be/isss/ and www.etsi.org.

Charles Brookson is an Assistant Director with the Department of Trade and Industry in the UK and Chairman of ETSI's OCG Security committee.

Past ENISA events

CONFERENCE ON NETWORK AND INFORMATION SECURITY: POLITICAL AND TECHNICAL CHALLENGES – Rome (Italy), 2-4 November 2005

Information and Communication Technologies (ICTs) are part of our everyday life and we are becoming increasingly reliant on them. They are present in public and private activities, and represent key factors in managing major events. The security of networks and information is thus a vital issue, and one that is complex and challenging. Sharing information and experiences, adopting a supranational approach and creating a culture of security are of crucial importance to the success of the Information Society.

The "Conference on Network and Information Security: Political and Technical Challenges" provided an ideal environment to address these and other important issues of network and information security. The event took place in Rome (Italy) from 2-4 November 2005 and was organised by the Italian Ministry of Communications and Fondazione Ugo Bordoni, in co-operation with ENISA and with the participation of the Ministries of Technological Innovations and Interior, the Italian Agency for Civil Protection and the Italian Prime Minister's Office.

The conference provided a well balanced discussion on both the political and technical aspects of Network and Information Security. The first session was chaired by Luisa Franchina, General Director of the Italian Ministry for Communications. During his opening address, Paolo Romani, Undersecretary of Ministry for Communications, stressed inter alia the vital importance of sharing information and experiences. In his key-note speech, Andrea Pirotti, ENISA Executive Director, presented his vision of how to forge a European approach to the current and future challenges in Network and Information Security.

The first part of the conference included an overview of the different security policies adopted, best practices and lessons learnt in the field of Network and Information Security. The second part focused more on an analysis of countermeasures adopted by various countries and initiatives and projects in the field.

The conference gave the opportunity to national, European and international stakeholders, representing both the private and public sectors, to share and discuss their experiences related to Information and Network Security.

For information and material about the conference, visit: www.iscom.gov.it/news05.htm

READINESS FOR HANDLING NETWORK AND INFORMATION SECURITY INCIDENTS

On November 24-25 2005, the first European Network and Information Security (NIS) conference, Readiness for Handling Network and Information Security Incidents, took place in Vilnius, Lithuania. The conference was jointly organised by the Communications Regulatory Authority of the Republic of Lithuania (RRT), ENISA and the Lithuanian Ministry of Transport and Communications. It was the first major event in Lithuania dedicated entirely to network and information security issues and attracted more than 150 participants from all over Europe, representing the public, private and civil sectors.

The conference was opened by Petras Povilas Čėsna, the Minister of Transport and Communications of the Republic of Lithuania. He noted that, as information and communications technologies had become an integral part of our daily life, their benefits carry both rights and responsibilities. Only with this mindset can we address the alarming phenomena of data theft, fraud, harmful content etc. The Minister further emphasised that, as these criminal phenomena are generally not limited to the jurisdiction of one single state, the response to such crime has to be international.

Tomas Barakauskas, Director of RRT, argued that it is impossible to achieve the goal of building a culture of information society across our countries, if modern information and communication systems cannot offer security to the end user or foster trust in the electronic environment. He said, "We hope that, by close co-operation at all societal levels, it is possible to create mechanisms for solving those pertinent problems that would stimulate the trust of users in electronic media. The latter creates the conditions for development and implementation of new business models, opening new opportunities for service users."

"Let us together build a culture of security. Let us try to prevent incidents by 'good housekeeping'", said Andrea Pirotti, Executive Director of ENISA, in his keynote speech. "Be prepared for the case that an incident will occur, select in advance both strategies and technologies that will help you to reach our common goals. Try to learn from your own experience and that of others and adopt 'best practice' solutions."

Major players in the network and information security fields were invited to the conference to present their views, including CECUA, EUROCHAMBRES, IBM, Microsoft, HP Laboratories, Panda Software, CISCO, TERENA, FIRST, UNIRAS and the UK's National High Tech Crime Unit.

The first conference session was dedicated to network and information security incidents from the end user's perspective. The speakers emphasised that malware (e.g. viruses, Trojans, worms), theft of personal data (e.g. phishing, pharming), spam and DoS/DDoS (distributed denial of service attacks) are the most common security incidents. Some speakers predicted that security incidents involving mobile networks and services will increase; WiFi security and mobile viruses are areas of particular concern.

➲

Executive Director Andrea Pirotti, Petras Cesna, Tomas Barakauskas and Tomas Lamanauskas

It was noted that security incidents are not limited to a particular operating system or platform and affect services across all sectors. With the growing sophistication of attacks, geographical and time barriers are not an obstacle for the spread of malicious activity. The biggest impact for users and businesses is the loss of privacy, data and money. In the virtual world (as in the real world), there is no total guarantee against criminal activities, and thus the aim must be risk minimisation rather than risk elimination. With this aim in mind, raising awareness, the use of protective tools and enhanced co-operation have proved the most effective elements in decreasing the number of network and information security incidents.

The session on innovative technological solutions for handling network and information security incidents revealed that patching software and hardware vulnerabilities is crucial in handling security incidents, and keeping up-to-date software and hardware systems is vital to achieving proper online security. Several technological solutions were presented that are based on incident prevention rather than on response. Blocking attacks through behavioral detection is a developing field, with so-called intelligent technologies increasingly prominent. Security policy is essential; well defined business, service or network recovery plans can minimise loss and ensure system stability and security.

The final session of the conference addressed advanced organisational models for incident handling on the national level and paid particular attention to CERTs (Computer Emergency Response Teams).

It was agreed that security incidents are a worldwide problem. Different countries and numerous network owners handle NIS incidents using similar approaches and with multilateral co-operation. Among a number of remarkable initiatives, CERT groups are co-operating at the multinational level, – including, for instance, TERENA (Trans-European Research and Education Networking Association) and FIRST (Forum of Incident Response and Security Teams). These organisations not only share information, exchange experiences and best practice but also provide training for members of CERT teams (e.g., TRANSITS – Training of Network Security Incident Teams Staff). The nature of the activities undertaken by CERTs is also changing – modern CERTs not only react to NIS incidents after they have happened but are working increasingly on the prevention of incidents (alerting and intrusion detection systems).

Tools for sharing information on an international basis were introduced, including the Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries (RAND Europe), WARPs (Warning, Advice & Reporting Points) and Traffic Light Protocol.

With rapid growth in the number of ICT users worldwide, the associated problem of network and information security is constantly growing, presenting new challenges. Numerous reports about the latest computer viruses, data theft, electronic network break-ins, unsolicited electronic mail and harmful content in public networks raise concerns among users, service providers and state institutions. It is obvious that today NIS is no longer a problem for individual states, but for the whole global electronic community. Moreover, NIS represents a common challenge to all stakeholders to work together closely to make the electronic environment more stable, secure and trustworthy, thereby delivering better incentives and infrastructures for the development of the information society.

This conference provided deep insights into how we should tackle the challenges of today and provided important input into the deeper and wider processes of building a network and information security culture in Europe and beyond.

Andrea Pirotti and Tomas Barakauskas raising a toast at the gala dinner

SECURE 2005 Conference

Krzysztof Silicki, Technical Director of NASK, Andrea Pirotti, Executive Director of ENISA, and Maciej Kozlowski, Director of NASK

The SECURE 2005 Conference took place from 25-26 October in Warsaw. The main theme raised, at this ninth SECURE conference was an attempt to define the roles and responsibilities of the different actors in the field of electronic communication, such as governments, vendors, Internet service providers (ISP) and Internet users, which impact on ICT security, in view of the growing threats to the Internet from the underground economy.

SECURE 2005 was organised in co-operation with ENISA, with the patronage of the Polish Ministry in charge of ICT (currently Interior and Administration). Additionally, the sector partners were: Computer Associates, Cisco Systems, Internet Security Systems, Juniper, NCR and Symantec. The Polish Press Agency (PAP), Rzeczpospolita newspaper, Computerworld weekly magazine, Gazeta Samorzadu i Administracji monthly magazine and BiznesNet.pl (the Internet business portal) were engaged as media patrons.

Threats coming from the Internet ”underground” annoy all Internet users, whether individuals, small companies, corporations, the banking sector or public administration departments. According to the experts, the design of new ICT security protocols and applications is still vulnerable and full of security holes. Viruses, Trojans and botnets are the nightmare of Internet users. Small enterprises that implement information and telecommunication technology to develop their businesses do not have enough time and financial resources to safeguard their security adequately. Corporations suffer from inconvenient procedures, numerous ”security alerts” and the necessity for frequent systems patching. Banks often hide their security problems, for fear of losing prestige. Regarding the low computer systems resistance to network attacks, there is often an ICT security vicious circle that is hard to deal with without regular co-operation between all involved in electronic communication.

The goal of this year’s conference was to raise these issues. Additionally, as every year, SECURE offered an opportunity to learn about the latest solutions and achievements in computer security.

Presentations by the ENISA representatives constituted an important part of the conference agenda. Executive Director of ENISA, Andrea Pirotti, spoke about the European approach to information security, the current status of ENISA and its plan for the future.

During an opening session a keynote address was given by Minister Michal Klaiber and Minister Wlodzimierz Marciński, who presented a governmental approach to ICT development in Poland.

In his speech – ‘Technical Challenges of Securing the Information Society’, Boaz Gelbord, a senior expert from ENISA, echoed the main conference theme. He very vividly presented the problem of the vicious circle in the security world.

Professor Andrzej Adamski from the Toruń University illustrated the practical result of the vicious circle problem. With detailed information about the statistics of computer crime, he highlighted the seriousness of the problem, comparing it with a wheel spinning out of control. This presentation provoked discussion among many participants, including governmental officials.

During the panel discussion led by Krzysztof Silicki, NASK Technical Director and Polish representative in the ENISA Management Board, and Miroslaw Maj, CERT Polska team manager and Polish Liaison Officer, participants tried to answer the main conference question – Who is responsible? As expected, this was just the start of a much broader discussion! Few natural answers like “end users” or “vendors” were put on the table. But none of them was sufficiently convincing. Even the answer “the market”, based on the obvious assumption that the economics of ICT security should be a factor, left participants with doubts. It could be logical to conclude that really nobody is responsible for this situation.

During the vendor panel many security products and solutions were presented. The vendors maintained that all of them are novel and are becoming increasingly effective, but it is unlikely that the problem of responsibility will disappear soon and the discussion about responsibility will continue.

The Professor Tomasz Hofmokl NASK Award

The Professor Tomasz Hofmokl NASK Award “For Promoting the Idea of Information Society” in 2005 was bestowed upon Wlodzimierz Marciński for creating the governmental bill and helping to pass the ”eGovernment Act”, which lays the legal foundations for the development of the information society in Poland.

Other presentations

Rafal Cichocki from the Gdynia Maritime University discussed wireless network building and security issues in industrial and warehousing environments. He emphasised the importance of configuration, reliability and upgradeability of designed systems as well as security considerations, such as authentication, authorisation and data protection.

Krystian Dobrzyński from the Koszalin Technical University spoke about methods for monitoring and searching illegal content on P2P networks. He provided information on the communication protocols, clients and servers of the most popular P2P systems and indicated ways to obtain information about shared data, especially illegal content, and to identify computers containing such content.

CERT Polska presentations

CERT Polska representatives, Slawomir Górniak and Przemyslaw Jaroszewski, talked about the security of messaging applications, Miroslaw Maj spoke on the role of a group of specialised response teams such as CERTs, CSIRTs and ABUSE Teams that work within telecommunications operators' organisations and receive reports on threats to customers’ computer systems. Bartosz Kwitkowski provided a detailed analysis of the message attachments in malicious electronic mails. Piotr Kijewski discussed the novel aspects of building early warning systems. Marek Dudek from NIFC Hotline Poland (illegal content hotline) addressed the role of dyżurnet.pl and other organisations in removing illegal content from the Internet.

Who is Responsible?

The main theme of SECURE 2005 dealt with the question of who is responsible for information security. This question has both a rhetorical and a pragmatic angle to it – whoever is responsible, should, in principle, be required to do something about it.

Boaz Gelbord (Senior Expert in Security Technologies at ENISA) explored the responsibility issue during his keynote speech on the second day of the conference. What follows is a short excerpt extracted from his speech.

Who is responsible for Internet security? The question itself immediately gives rise to two further questions – what do we mean by responsibility? And what do we mean by Internet security? Let us briefly explore these two points before we look at who is actually "responsible".

For the average person, the concept of responsibility actually encompasses three different notions – the sense of obligation, liability and accountability. Obligation is a somewhat vague term that implies the person charged by a system with the overall running of a process – the place where "the buck stops". Liability on the other hand has a clear meaning – the liable party is the one who must pay for the cost of things going wrong. Lastly, accountability refers to who needs to answer for themselves when things go wrong. While these three roles may coincide in some situations, we will see in the online environment that this is not necessarily the case.

With one definition out of the way, let us turn our attention to an even more controversial definition - What constitutes cybersecurity? Does it mean preventing illegal content? Or preventing fraudulent sales on eBay? Or protecting against hackers? This is not always easy to decide, particularly since underlying security measures often co-exist with closely related aspects such as locking in customers, forming a gateway to the end user, digital rights management, marketing and even censorship. Clearly one's definition of cybersecurity strongly influences who one considers to be responsible. The multiple interpretations of what constitutes cybersecurity have clouded the debate and have made it difficult to assign responsibility in different domains.

But it is not only definitions that make assigning responsibility difficult. Constant technical changes also make it difficult to assign responsibility in a static and well defined way. The convergence of traditional technical networks and the general move towards an IP-based future are constantly changing the security landscape, because traditionally closed networks (voice, cable, even traditional mobile) are all of a sudden exposed to an open and vulnerable environment. The move towards "anywhere anytime access" necessarily implies an opening up of networks and a complex service chain. Who is responsible for security in such a scenario? And who does a user turn to in the event that things go wrong?

This problem is compounded by the fact that, as a general trend, security is underestimated in new technical platforms, because the initial applications are low value and thus require low security. However, the same platforms are later used to house high value applications. Indeed, when the Internet began to evolve as an instrument for data exchange in academic environments, it was difficult to fathom that, in a few short years, it would be used for critical information exchange in the area of health and financial services. The fundamentally insecure architecture of the Internet was never designed for such sensitive transactions.

Let us now return to the issue of responsibility. There are many possible parties that could be considered to be responsible, depending, as we have seen, on the particular security domain and the particular meaning of responsibility. These include, but are not limited to, Internet Service Providers, software or hardware producers, users, governments and so forth. Almost any party directly or indirectly involved in the service chain or supporting infrastructure is a potential candidate.

There are of course no easy answers for the responsibility issue, but we must avoid the most tempting solution – to assign all responsibility to the hapless end user. Today's current systems are too complex for users to effectively configure and manage. Users, most of whom are from non-technical backgrounds, have no desire or ability to manage and configure their own systems. For example, any security system that relies on an end user knowing exactly what a public key certificate is is doomed to fail. There will always be a substantial portion of users who are simply unable or unwilling to learn such concepts. Confronting end users with the "under the hood" details of their online lives results in users being frustrated at the sense that they have little understanding of the underlying machinations of their online security.

But even educated users find themselves paying the price for bad online security. It is striking that, although the Internet is a truly global communications platform, the markets it creates are still, for the most part stubbornly local, particularly in Europe. And even more local is the recourse that users have available when things go wrong. At the end of the day the user is the one who bears the brunt of the cost in terms of money and time for cybersecurity breaches (from the few hours it takes to recover a credit card payment charged in error, to the hundreds of hours it can take to recover from identity theft). Just how heavy this price is is strongly dependent on the particular country in question as well as the resources available to the user.

A great challenge in the further development of the Information Society will therefore be to make sure that the cards are no longer stacked against the end user in the online arena and that users do not need to fear that no one is responsible for their online security. A clear discussion of roles and responsibilities such as the one taking place at SECURE 2005 is a welcome contribution to that effort and ENISA is happy to have had the opportunity to exchange ideas on this important issue with our Polish and European colleagues.

Talking CERT co-operation: ENISA's Marco Thorbruegge and Miroslaw Maj of CERT Polska

INFORMATION SECURITY MANAGEMENT METHODS IN EUROPE: NEW PERSPECTIVES AND ROAD MAP

On 10 and 11 November BSI was pleased to welcome guests from over a dozen European countries to the BSI Information Security Management Workshop in Bonn, which was co-organised with ENISA.

Risk management and assessment are among the main tasks of ENISA and are, in fact, principal elements of every IT security concept. BSI has focused on this subject since its foundation in 1991 and, in collaboration with German industry, developed the methodology of IT Grundschutz in 1994. Since then, the IT Grundschutz Manual has become a security standard in industry and administration in Germany; more than 4000 registered users in Germany and throughout Europe apply the IT Grundschutz Manual.

Information security management experts from all over Europe were given an overview of current risk assessment and management models and a basic introduction to the IT Grundschutz methodology. With presentations reflecting the experience of applying the Grundschutz Manual in both private and public institutions, the workshop showed that IT-Grundschutz is a reliable concept that provides secure, effective and economic solutions.

As Information Security experts from various private and public organisations of European states presented their different approaches to IT Security, it became clear that it is necessary to build bridges between these approaches. On the one hand it was pointed out that, as a European Authority, ENISA plays an important co-ordinating role in the generation of such bridges. On the other, the participants agreed that smaller European countries in particular are making an invaluable contribution to the development of Information Security standards because they are obliged to cope with those different approaches. Thus, the workshop showed how the different international strategies may be used as combined methods. In addition, it provided striking proof of the excellent collaboration that already exists between older and younger EU member states. Last but not least, the workshop was itself an excellent example of successful public-private partnership and demonstrated good co-operation with the industry.

In the panel discussion, representatives of ENISA, BSI, SEMA (Swedish Emergency Management Agency) and Vodafone Information Systems discussed the anticipated challenges of Information Security in the near future.

In his final remarks, Alain Esterle, Head of the Technical Department of ENISA, who chaired the panel, expressed his readiness to meet the identified need and assist in bridging existing approaches to security management in Europe. To this end ENISA would serve as a catalyst to initiate a permanent dialogue between national information security agencies, industry and interested stakeholders. In this way, the bridging of various existing approaches and the facilitation of mutual acceptance for future certification procedures can be achieved.

CEBIT

The CeBIT is the world's largest trade fair for information technology and takes place each year in Hanover, Germany. Whereas the issue of "security" was presented in separate spatial areas by hardware and software suppliers in the past, at CeBIT 2005 all such services were offered for the first time in a common "Security Hall".

The feedback from visitors and exhibitors was so positive that IT security will continue to be a focus in CeBIT 2006 (9-15 March 2006). The Federal Office for Information Security (BSI) and the Federal Ministry of the Interior will again have exhibition stands on site and will be involved in the series of lectures at the Convention Centre.

NATIONAL LIAISON OFFICERS DAY

Tim Mertens

21 National Liaison Officers (NLOs) from all over the European Union met at Heraklion, the seat of ENISA on Crete, from 17 until 19 November 2005.

The first part of their meeting provided a comprehensive overview of the activities of the two ENISA operational departments: the Co-operation and Support Department, headed by Ronald de Bruin, and the Technical Department, led by Alain Esterle.

The Co-operation and Support Department is divided into four sections: Awareness Raising, Computer Incident and Response Handling Policy, Relations with Member States and EU Bodies, and Relations with Industry and International Organisations.

The Technical Department, comprising three units, gave presentations on NIS Policies for Organisations, Risk Management and NIS Technologies. Each presentation was followed by questions and answers, and very fruitful discussions took place.

The second part of the meeting focussed on NIS activities by the three major European institutions: the Presidency of the EU (currently held by the United Kingdom), representing the Council; the European Parliament; and the European Commission.

On behalf of the UK-Presidency, Maria Burroughs spoke about the major features of the Presidency's IT agenda: general recognition of the essential contribution of the role of ICT in the Lisbon Agenda, agreement and launch of a 'radical' i2010 programme, the implementation of the 2003 Telecommunications Package and preparation for its review in 2006. She also introduced ongoing issues and follow-up activities in the World Summit on the Information Society and in particular questions about Internet Governance. Ms. Burroughs then reported on the very successful CIIP Meridian Conference (an EU Presidency and G8 event), which took place from 5-6 October 2005 in Greenwich, England, and was attended by 80 government officials from 30 countries. Finally she mentioned a conference about 'Transforming Government Services' and explained the current status of data retention, where legal issues have not yet been resolved.

Dr. Jorgo Chatzimarkakis, a Member of the European Parliament, outlined a possible future role for ENISA. As EU Politics are 'done for the Europeans – and what they need most is achieving the goals of Lisbon' – ICT plays a key role in the European economy – and will become increasingly important. 'But', he said, 'ICT needs a constant, safe and secure environment to develop further – otherwise consumers' confidence will shrink!'. Dr. Chatzimarkakis sees ENISA's role in stabilising the ICT environment as a basis to achieve the Lisbon Goals. With regard to ICT research, he acknowledges that a lot of work is already being undertaken (ICT in FP6 and FP7, Galileo, JRC and STOA (Scientific Technology Option Assessment)) and he sees ENISA as a 'guard and integrator' in this area.

In his talk, Rogier Holla from the European Commission identified the unprecedented requirements for security which are

➲

The panel discussion at the National Liaison Officer Day in Heraklion

emerging as a result of increasing interconnection, interdependence and system complexity with the growing use of 'open' information infrastructures. The Commission acknowledges that NIS is primarily a private sector activity but it needs government input to set priorities and achieve a balance. Mr. Holla outlined the various activities of the Commission, including the Network Security elements of the eEurope 2002 and 2005 action plans, the i2010 action plan and '2006: Strategy for a Secure Information Society'. As a recent example of a regulatory instrument, the Commission proposed a 'Framework Decision on attacks against information systems', which was adopted by the Council in February 2005. Mr. Holla gave an overview of the Commission's plans to establish a 'European Early Warning System', which would function as a public-private partnership, dealing with most threatening attacks, and providing widespread information to the right people at the right time. The European Commission is to ask ENISA to explore the feasibility of this scheme with private players and public organisations.

The event concluded with an internal workshop for the Liaison Officers at which, amongst many other issues, future co-operation methods and possibilities were discussed. ENISA distributed the first version of the new Who's Who, which lists contacts and other essential information about national authorities and bodies dealing with NIS in each Member State. This directory will soon be publicly available. ENISA expressed its appreciation to those Member States who delivered the country data.

One of ENISA's main aims is to serve as a platform for Member States to exchange information and experiences, both with ENISA and among themselves. Participants generally felt that the meeting had been very productive and a valuable starting point for further activities.

Executive Director Andrea Pirotti with the three speakers: Maria Burroughs (UK-Presidency), Rogier Holla (European Commission) and Jorgo Chatzimarkakis (European Parliament)

Tim Mertens is a Senior Expert Relations with EU Bodies and Member States at ENISA

The ENISA National Liaison Officers

Hungary's National Information and Network Security Projects

Ferenc Suba, János Drencsán

Introduction

Recent European and international developments have prompted the Hungarian government to increase its commitment to information and network security. The result has been several major projects initiated by the Ministry of Informatics and Communication (IHM, www.ihm.gov.hu) in Hungary, the creation of the Information Security Subcommittee within the Information Society Co-ordination Committee (ITKTB, www.itktb.hu/inba) and increased international activity in network and information security.

This article aims to give an overview of some of the major Hungarian projects and initiatives in information security. The largest government security-related project is CERT-Hungary, the government's own computer emergency response team. Based partly on Hungary's participation in the Common Criteria Recognition Agreement since 2004, the government also has several projects aimed at bringing international standards to a Hungarian audience. Promoting international business development, two government projects have been established to help Hungarian information security firms enhance their international presence. In addition, the government takes an active role in putting Hungary on the map, for example, the IHM gave considerable support to the ISSE 2005 conference in Budapest this year.

CERT-Hungary

Introducing CERT-Hungary

At the beginning of 2004, the Ministry of Informatics and Communications contracted the Theodore Puskás Foundation to establish a Hungarian governmental CERT. CERT-Hungary became the country's third such organisation after Hun-CERT, which serves the Hungarian Internet service providers, and NIIF-CSIRT, which serves the Hungarian academic network. The fact that these organisations did not have enough resources to serve the entire governmental sector or to provide 24/7 accessibility led to the official establishment of CERT-Hungary on 1 January 2005. This organisation has started with a basic set of services which is continuously expanding.

Ferenc Suba talking at the ISSE Conference in Budapest

CERT-Hungary's constituency includes the Hungarian public, businesses and of course the civil sector. Besides being a governmental CERT, CERT-Hungary also takes on the role of a national CERT. Like most national CERT organisations, CERT-Hungary offers free services available to the Hungarian public through its website, www.cert-hungary.hu, or via electronic mailing lists.

Individual organisations need to be registered at CERT-Hungary as a supported organisation to receive additional services. As a governmental CERT, CERT-Hungary offers some free services such as customised vulnerability reports free of charge to civil organisations. CERT-Hungary also provides a variety of value-added services that are offered at cost to the supported organisations in the civil sector. For corporations and other organisations not in the public sector, CERT-Hungary can provide customised services based on their individual needs. The fees for these customised services are cost-based, since CERT-Hungary is a non-profit organisation.

As part of the International Watch and Warning Network (IWWN), CERT-Hungary is responsible for Critical Information Infrastructure Protection (CIIP) in Hungary. We have also developed direct communication channels to the national police force, so as to step up action against high-tech criminals.

Our partners

When starting up, we have found that both national and international CERT organisations were eager to help us establish CERT-Hungary. Other non-profit organisations, such as the Virus Competency Centre at the Budapest University of Technology and Economics (BMGE) and the Centre of Information Technology, also contributed. Since Hun-CERT had already been established and been operational in Hungary for several years, their assistance played a major role in the setting up of CERT-Hungary. Their geographical proximity allowed them to take an active role in helping to establish our organisation. They wrote several studies for CERT-Hungary, as well as our operational manual. They also installed the RTIR ticketing system for incident handling, and trained the team members to use it effectively for handling incidents.

Several international CERT organisations such as CERT/CC, US-CERT, GovCERT.nl, and BUND-CERT assisted with our development. In the course of bilateral talks with these organisations, the CERT-Hungary team gained a lot from their experiences and this learning process has also laid the foundation for a stable working relationship as well as good personal contacts.

Future plans

CERT-Hungary intends to intensify its involvement in the international CERT community. We have asked to join the Forum of Incident Response and Security Teams (FIRST) and have requested accreditation by Trusted Introducer (TI). We are also sharing our recent experiences with our neighbour, Slovakia, which is now in the process of creating its own governmental CERT.

CERT-Hungary is also working hard to increase and improve its services. The cert-hungary.hu website will switch to a new content management system (CMS) at the beginning of 2006. This new CMS has been developed by CERT-Hungary to meet our need for high security and certain functionality specific to our operations. The new portal for CERT-Hungary is expected to improve our Internet presence and our image.

CERT-Hungary plans to open two new websites at the beginning of 2006 to promote Internet security. One of them is www.biztonsagosinternet.hu which is aimed at a non-technical audience. It will help the less technically inclined to become familiar with the basics of desktop security and will promote safe Internet usage. The other website, www.halozatbiztonsag.hu, will be aimed at a technical audience and will provide a forum for Hungarian system administrators and information security experts.

Our future goals also include building up close co-operation with the Banking Association of Hungary, with which CERT-Hungary has already co-organised a joint exercise. Moreover, as of January 2006, CERT-Hungary will be providing services for the National Informatics and Communication Inspectorate.

MIBÉTS

Hungary has no current method for national information security evaluation. Until now, mostly foreign and international evaluations have been used. However, as these are not available in the Hungarian language, this creates a linguistic barrier for most firms in Hungary. As a result, for projects relating to national security or for other government projects where information and network security are important factors, foreign certificates are not acceptable.

Since it was clear that Hungary needs its own scheme for evaluating and certifying the security of IT systems, the Ministry of Informatics and Communication started a project to develop the Hungarian Information Security Evaluation and Certification Scheme (MIBÉTS).

To meet the needs of Hungarian organisations, the scheme had to be simple enough so that long processes and high costs would not form a deterrent to adaptation by organisations. MIBÉTS was based on international standards like the Common Criteria (CC, ISO/IEC 15408) and the Common Evaluation Methodology (CEM, ISO/IEC 18045). These documents were too long and complex for Hungary so the British Simplification (UK_SYS) had to be applied. National experiences in evaluation and certification were also included in the development of the Hungarian scheme.

To simplify the evaluation and certification scheme, Hungary made several adaptations, such as only including the Evaluation Assurance Levels (EAL) from 2 to 4 (Level 1 has no relevance to security, while levels 5 to 7 are too long and too expensive for the Hungarian adaptation). To ease the evaluation and certification process we also allowed the auditor to help the developers in collecting the evidence for reaching the desired level.

In the future, project managers will aim for evaluating entire systems, not just software. As a result, the focus will increasingly be on practical security with the addition of penetration testing and vulnerability evaluations to the scheme.

MIBIK

While MIBÉTS is the Hungarian adaptation of the Common Criteria, there was also a need for something more general at the organisational level. On the international scene the acceptance of the BS 7799 (ISO/IEC 17799) standard is growing fast. The Hungarian government needed a document that would cover the BS 7799-2:2002, with some customisations specific to Hungary, so it decided to develop the Hungarian Information Security Management Framework (MIBIK).

MIBIK currently has two sections, one covering the requirements (IBIK) and the other covering the evaluation methodology (IBIV). The Information Security Management Requirements (IBIK) are based on the ISO/IEC 17799, the ISO/IEC TR 13335 international standards plus some relevant NATO and EU regulations. The Information Security Management Evaluation methodology (IBIV) is based on Hungary's own 8th Recommendation by the Inter-ministerial Committee on Informatics, the BS 7799-2:2002 standard and the relevant PD 3001 – PD 3005 work documents.

The third section of the MIBIK, currently under development, is the Information Security Management System (IBIR) which applies the Plan-Do-Check-Act model to cover all processes in an organisation. This results in efficient information security management through a continuous development process.

Other projects

eSec.hu, HITEC

It is in the interest of the Hungarian government to create an environment where Hungarian IT firms can flourish. To bring attention to Hungarian IT security companies on the international scene, the Hungarian government initiated the eSec.hu project to introduce the products of these companies. The Hungarian Cyber Security Package from eSec.hu presents Hungarian IT companies that offer turn-key solutions utilising advanced technologies. This security package addresses security audits, protection from internal and external attacks, e-identity and digital rights management, and features leading Hungarian information security companies.

Besides promoting Hungarian IT security companies, the Hungarian government has also established two Hungarian Information Technology Centres (HITEC) in the USA and China to enable business development and technology transfer.

Information technology system control methodology

The Hungarian Ministry of Finance has developed a COBIT-based methodology for controlling IT systems. Since last year, a governmental decree orders the use of this methodology on all governmental IT systems. The goal is to guarantee the government's efficient operation in case disaster hits one of its organisations.

Governmental information security recommendations

The Electronic Government Centre (EKK) in Hungary is developing recommendations for securing the government’s computer systems. This will be a practical guide at the operational level for creating and managing computer systems owned by the government.

Conclusion

In recent years, Hungary has shown considerable development in network and information security. This article has sought to provide an overview of governmental activity in this important area to further stimulate discussion and co-operation with our European colleagues. Based on active co-operation and a learning process made possible by ENISA and the bilateral partners, the Hungarian government is committed to bringing the best information security practices and technologies to Hungary and to sharing its achievements both nationally and internationally.

For more information on the Hungarian government projects, please feel free to contact Dr. Ferenc Suba at ferenc.suba@cert-hungary.hu.

For further information about the eSec.hu project, Antal Kuthy may be reached at antal.kuthy@egroup.hu.

Ferenc Suba is a Special Envoy of the Minister, General Manager with CERT-Hungary and Vice-Chair of ENISA MB.

János Drencsán is a Project Manager with CERT-Hungary.

SEMA visits ENISA

Linda Englund

On 10th November a five-person delegation from the department of Information Assurance and Analysis at the Swedish Emergency Management Agency (SEMA) visited ENISA. SEMA has the task of co-ordinating information assurance at a national and international level in Sweden, and the two agencies exchanged information about their planned activities and sought to define areas in which to establish co-operation.

Each delegation first introduced their key issues, covering topics such as awareness raising, IT Security management (ISM) and risk management/risk assessment. This was followed by discussions both on the topics themselves and on the possible scope for future co-operation.

The following areas of mutual interest and potential co-operation were identified:

- Sharing of best practice, for example, in awareness raising and risk management.
- Sharing information about research projects with a view to possible collaboration in joint projects.
- Communication - ENISA information could be spread in Sweden by the SEMA network and vice versa.

About SEMA

SEMA co-ordinates Sweden's efforts to prepare to manage serious crises. The agency works together with municipalities, county councils and government authorities, as well as the business community and other organisations, to reduce the vulnerability of society and improve its capacity to handle emergencies.

SEMA has overall governmental responsibility for information assurance in Sweden and is also responsible for the co-ordination of national information assurance at a policy level. The agency monitors the development of information security in terms of threats, vulnerabilities, risks and protective measures and presents an annual assessment of the situation to the Swedish government.

The Information Assurance and Analysis Department at SEMA is charged with managing information assurance. This involves maintaining an up-to-date overall picture of society's information security in terms of threats, vulnerabilities, risks and protective measures, covering both policy and technical issues. This overview forms the basis for the annual assessment which is presented to the government. To complete this picture, SEMA gathers information from numerous sources such as academia, open source intelligence, security and intelligence organisations, CERTs, public and private organisations and from SEMA's own IDS (Intrusion Detection system).

ENISA's Head of Co-operation and Support Department, Ronald de Bruin, leading the discussion during the SEMA visit

SEMA is also working within the area of public-private partnership; the agency is currently developing fora for information exchange based on the British NISCC (National Infrastructure Security Co-ordination Centre) concept. These fora will share, in a trusted environment, information about threats, vulnerabilities and solutions to manage risk between the various players in different areas of responsibility. It is anticipated that the fora will be composed of private sector bodies, public sector bodies or a combination of the two.

The agency also works in a preventative capacity with IT security issues, conducting IT security analyses, and gives advice and makes recommendations to both public and private organisations and agencies. To raise awareness of relevant issues, SEMA conducts education, provides tools aimed at different target groups and produces a newsletter and various reports. In this context, the agency also participates in joint national initiatives, working alongside other agencies and organisations.

SEMA finances, initiates and develops research in information security. However, as Sweden is a small country, it also maximises its efforts with participation in international research initiatives. For example, co-operation has been established with Crisis Management Research and Training (CRISMART) and Comprehensive Risk Analysis and Management Network (CRN).

Finally SEMA serves as society's contact point for information security and as an international contact point for the government. At times it also represents Sweden in international collaboration.

For further information, please contact:
Linda Englund: linda.englund@krisberedskapsmyndigheten.se

The annual Swedish society's information assurance status assessment is available in English at:
www.krisberedskapsmyndigheten.se/6193.epibrw

Linda Englund is a Strategic Analyst in the Information Assurance and Analysis Department of the Swedish Emergency Management Agency

BSI publishes additional materials for IT security in companies in critical infrastructures

Stefan Ritter

The Federal Office for Information Security (BSI) has been making an important contribution to the protection of critical infrastructures in Germany for many years.

Critical Infrastructures are "organisations and facilities that are vital for public welfare and whose failure or disruption could result in long-lasting supply bottlenecks, substantial disturbances to public order and/or other dramatic consequences". They are categorised into the following sectors:

- transportation and traffic
- energy
- hazardous materials
- telecommunications and information technology
- finance and insurance
- services
- public administration and justice system
- other.

As part of its work in protecting information infrastructures, the BSI provides companies which are part of critical infrastructures with specific additional resources. Two of these are the sample guideline, “IT security at a critical infrastructure – a practical example", which was recently published by the BSI, and the IT-Site Security Check, "IT security audit materials for the site quick-check in critical infrastructures".

The sample guideline is the product of co-operation with an international operating company in the oil industry and is used by the company in real life. It was revised by the BSI and adapted to the BSI Baseline Protection Manual and now gives every company the opportunity to test, if necessary to adapt and, in the process, to improve the effectiveness of its own IT security practices.

The guideline is modular in format and was produced from a large number of individual security concepts and augmented by sample solutions. Once put into practice, the rules cover the entire spectrum of IT security in a large-scale enterprise. The rules are short, succinct and easily understood by those affected. A conscious decision was taken to dispense with the description of technical and manufacturer-specific details to ensure that the rules can be applied broadly and that they remain current in the long term.

Proceeding from the excellent experience of the company that produced the sample guideline, the BSI provides a so-called IT-Site Security Check that is based on it. In a manner analogous to the rules of the sample guideline, audit materials, consisting of recommendations for implementation, lists of questions for employee interviews, and site inspections, as well as assessment aids, were developed. They should assist in verifying the implementation of the sample guideline and clearly present the status of IT security in the company.

Companies that are part of critical infrastructure are usually internationally active. The BSI takes their requirements into consideration by also providing the additional materials in English.

In addition, the BSI thus already fulfils the concepts of the European Programme for Critical Infrastructure Protection (EPCIP) in advance. The experience of individuals is made available to all so that they too can benefit from this "good practice".

The additional materials and further information on the subject of critical infrastructure are available for download from:
www.bsi.bund.de/fachthem/kritis/utilities.htm.

Stefan Ritter is a Senior Expert in Critical Infrastructures at the Federal Office for Information Security (BSI) Germany.
Contact: Stefan.Ritter@bsi.bund.de

Managing risks with the EBIOS method

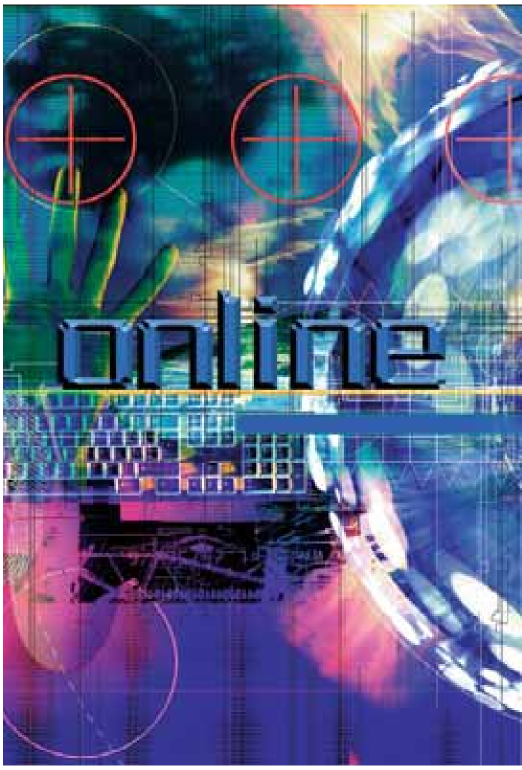
Matthieu Grall

One of the main tasks of ENISA is to promote risk assessment and risk management methods. The EBIOS method (Expression of Needs and Identification of Security Objectives) is currently addressed within the "ENISA ad hoc Working Group on Technical and Policy Aspects on Risk assessment and Risk Management".

The EBIOS method is used to assess and treat risks relating to information systems security (ISS). It can also be used to accept the way risks have been treated and to communicate about risks within the organisation and to partners, and therefore assists in the entire ISS risk management process.

Created and maintained by the DCSSI (the French Prime Minister service dealing with information security), it contributes to the international recognition of security projects by guaranteeing compatibility with international standards such as ISO Guide 73 (risk management concepts), ISO 13335, ISO 15408 (Common Criteria), ISO 17799 and ISO 27001 (Information Security Management System). It is widely used in the public sector (all ministries and bodies under their administration), in the private sector (consulting firms, small and large companies), in France and abroad (European Union, Quebec, Belgium, Tunisia, Luxembourg etc.) and by numerous organisations using or benefiting from ISS risk analyses.

By providing information to support decision-making (detailed descriptions, strategic stakes, detailed risks with their impact on the organisation, explicit security objectives and requirements), EBIOS is a valuable negotiation tool. Moreover, it provides greater awareness for everyone involved in a project (top management, financial, legal or human resources departments, contracting authorities, prime contractors, users), increases the involvement and standardises the vocabulary.

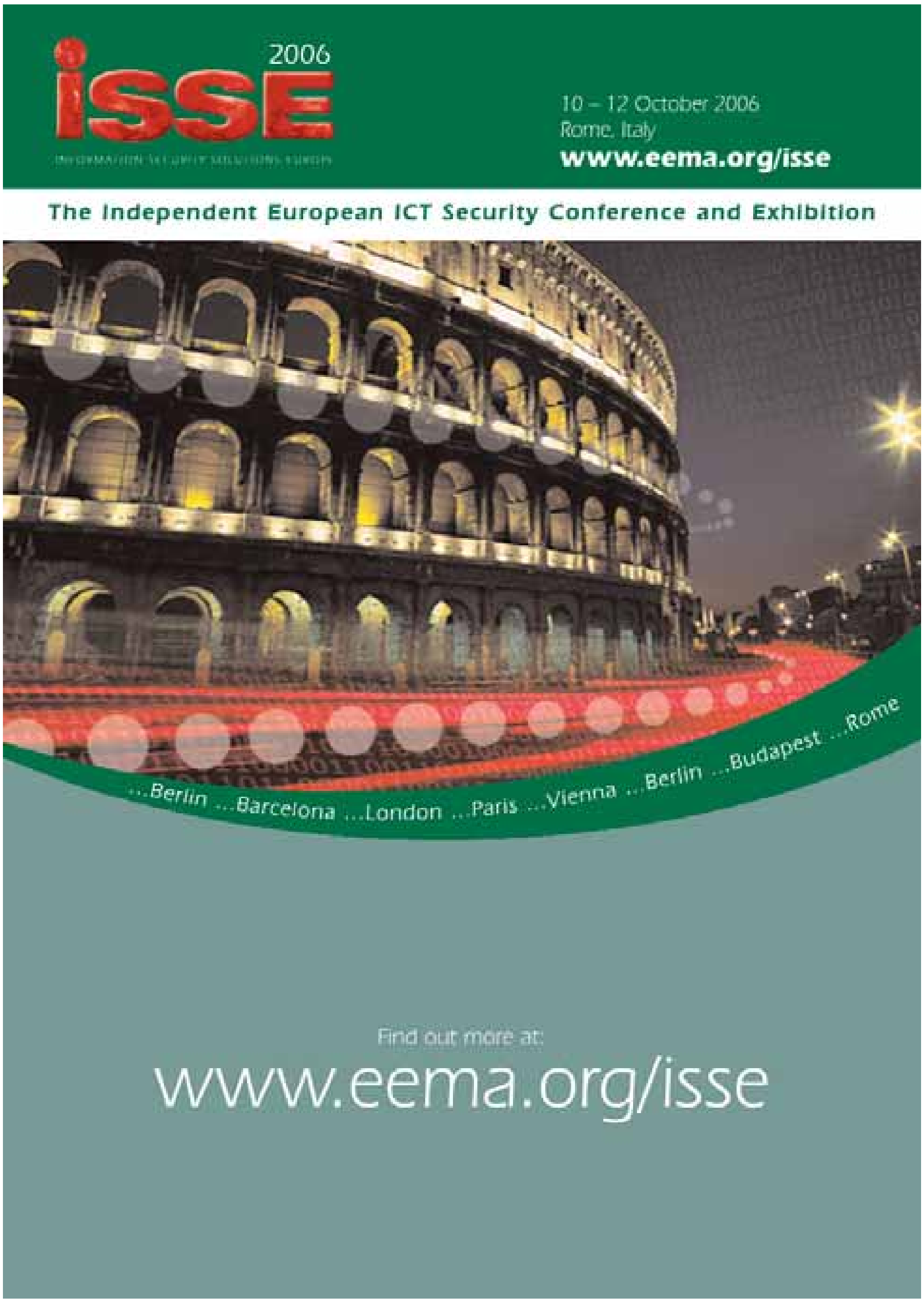


EBIOS can be used during the design phase or on an existing system, for many different purposes and security initiatives, such as preparing ISS master plans, policies, trend charts or various types of specifications such as protection profiles, security targets, System-specific Security Requirement Statements (SSRS) for NATO, action plans etc. This global approach guarantees the consistency of ISS methodological tools. Unlike scenario-based risk analysis approaches, the structured approach of the EBIOS method allows the component elements of risks to be identified (essential elements, attack methods, vulnerabilities, final impact etc.), which guarantees an exhaustive risk analysis. It is designed to provide ongoing risk analysis and global ISS consistency, and its flexible approach provides ISS actors with a wide range of tools. Its scope covers everything from a global study of an organisation's complete information system to a detailed study of a specific system (Web site, electronic messaging, recruitment management etc.).

The EBIOS knowledge bases introduce and describe the types of entity, attack methods, vulnerabilities, security objectives and security requirements. They already include many catalogues of best practices such as ISO 17799 or ISO 15408, and any other catalogue can be added to these bases (e.g. IT Baseline Protection Manual or other local standards).

The EBIOS method, its user freeware, its best practices and much more information are available free of charge on the DCSSI site: www.ssi.gouv.fr/en/confidence/ebiospresentation.html.

Matthieu Grall is an Information Systems Security expert at the Central Directorate for Information Systems Security (DCSSI)



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".

Edited by: 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.