enisa European Network and information Security Agency

ENISA Quarterly

IN THIS EDITION

Achieving higher impact in action

Approaching the end of its second year of operation, ENISA is now in the process of maturing and fine-tuning its procedures, and is focusing on achieving higher impact for its work both in the Members States and with stakeholders.

One way to do this is by refining the way in which we establish our Work Programme by involving our stakeholders even more. By understanding the expectations and the demands of the NIS stakeholders more fully, the Agency will be better placed to meet Europe's needs. Therefore, in a joint-meeting between its Management Board and the Permanent Stakeholders' Group (PSG) on 6 June in Berlin, ENISA set out a new course to develop the Agency's priorities.

By involving Member States, industry, consumers and academia, right from the beginning with the setting of priorities for ENISA, we believe that the Agency's impact will increase, and its work will be better aligned with our stakeholders' needs.

By establishing priorities for the Agency Work Programme in a two-way dialogue, ENISA will meet the combined expectations and demands of our European NIS partners. As a result, any advice or studies that ENISA provides at a European level should also be more readily and thoroughly implemented by Member States. We are most grateful to our stakeholders for ensuring that this process runs smoothly so that ENISA can take this new step in working for the benefit of Europe.

I would also like to take this opportunity to report some recent Agency landmarks, for which ENISA has received appreciation from several NIS actors.

The first highlight is the establishment of the IT security standards portal, together with the ITU. For the first time Europe now has an extensive list of IT security standards with a single point of entry, benefiting all IT security vendors, service providers and other stakeholders.

Vol. 3, No. 2, Apr-Jun 2007

ISSN1830-3609

Secondly, the new Risk Management/Risk Assessment (RM/RA) area of our website includes the first report of an overview of legal aspects in RM/RA. As such it provides policy-makers and business security experts with a strategic tool for identifying key legal RM/RA requirements and bridges an information gap within the EU. This new report is crucial for business, helping management to determine the extent to which legal guidelines apply to their NIS decisions.

Thirdly, our Awareness Raising recommendations have been translated into various languages and adopted by different NIS stakeholders throughout Europe when preparing their campaigns for the education of citizens in the use of information systems.

I would also like to mention the feasibility study on 'EISAS' – the European Information Sharing and Alert System, which was carried out at the request of the European Commission. ENISA is presently adding the final touches to this study. The debate on the design of a Europe-wide NIS information-sharing system for end-users and SMEs, to raise IT security awareness, will now have a solid foundation.

Finally do not forget the ISSE 2007 conference that will take place during the autumn in Warsaw, from 25-26 September. I look forward to seeing you there.

I cordially invite you to follow our activities closely. We are keen to encourage an intensified multi-stakeholder debate on European Network and Information Security, by engaging in dialogue with you at any time.

Sincerely,

Andrea Pirotti
Executive Director, ENISA

A Word from the Editor

Network and Information Security (NIS) is a multifaceted subject and therefore we try to cover many of its different aspects in our magazine, spanning security management, authentication, intrusion detection, NIS assessment reports, research initiatives, awareness raising etc.

This issue opens with an article by Moshe Ishai on the authentication mechanisms and policies used in the e-banking sector, arguing in favour of two-factor authentication solutions. The article by Huw Read, Andrew Blyth and Theodore Tryfonas looks at the interesting research challenge of visualising attack data. Vicente Aceituno Canal emphasises the importance of SMART metrics for information security management, and provides a number of examples of good practice for choosing the appropriate security metrics.

Our own expert, Pascal Manzano, explains the motivation and planning behind the ENISA study on providers' (network, Internet, telecommunication and content) anti-spam and general security measures. Elisabetta Carrara describes work on a Network and Information Security standards roadmap, including a searchable portal, which is a joint project involving ENISA, the ITU and the NISSG.

The Federal Office for Information Security (BSI) in Germany has recently finalised a report assessing the current state of the country's Information Technology Security. Anke Gaul summarises the findings of the assessment and compares them with the 2005 findings. Andrew Tyrer's article presents a new instrument for working with the government in the UK, called Innovation Platforms, focusing on the Network Security Innovation Platform. Bence Birkas reports on two major NIS events, Meridian and TF-CSIRT, which took place recently in Hungary. The important and rather difficult task of measuring the impact of NIS awareness raising campaigns is discussed by Rytis Rainys, using as an example a recent campaign in Lithuania.

Finally, in this issue we have a number of announcements for events which are supported by ENISA, such as ISSE/SECURE, EC2ND, RSA Europe and an Anti-spam Summit, as well as short reports from similar events that have already taken place, such as WISTP'07. Last but not least we have the most important announcement for ENISA: the public consultation on the future of the Agency that is being organised by the European Commission. Please visit the web consultation page and have your say!

While this issue is the result of contributions from an open call, we were very pleased with the response of our readers to the special issue we produced in the last quarter. We plan to continue this policy in future issues of our magazine, focusing on areas related to current and planned activities of the Agency or other issues prominent in NIS. Therefore we would particularly welcome contributions and articles in the areas of:

- *trusted computing*
- *secure software* and
- *network resilience.*

We have recently introduced a mailing list for announcements related to ENISA Quarterly, calls for contributions, availability of the new issue etc. To subscribe, please visit our web pages, www.enisa.europa.eu/eq/, where you will also be able to find all the latest news and plans for our magazine.

I am always open to your ideas and feedback on how to improve our publication. I continue to look forward to receiving your valuable articles and I am grateful to all authors. After all, it is your contributions that make EQ such an interesting read!

Sincerely,

Panos Trimintzios
Editor-in-Chief, ENISA Quarterly

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

From the World of Security - A Word from the Experts

Are Banks Strengthening their Defences?

Authentication to e-Banking Systems

Moshe Ishai

The weak link in the banks' security chain

Banks today are investing their utmost in the most progressive information security technologies and methods in order to secure their e-banking systems. The methods adopted in order to secure information as well as to monitor and prevent exposure, theft or damage to information are extremely advanced. The majority of these methods are formulated and executed on the bank's side. Malicious entities focus on the most sensitive and convenient point in order to hack into the system, which is usually the authentication phase. As soon as an attacker gains access to the system using the credentials of another user, his actions become 'legitimate' within the system, and communication, application and infrastructure security cannot discriminate and prevent the damage he might cause.

The majority of banks across the globe still authenticate their clients in the e-banking systems using a user name and password. There are a number of banks where an additional identification field is required, but the authentication process is still based on the same concept. This concept is defined as 'one-factor authentication'.

In general, an authentication methodology may include one or more of the three basic 'factors':

1. Something the user **knows** (password, PIN number etc.)
2. Something the user **has** (exclusively), such as a smart card, a One-Time Password (OTP) device, a token etc.
3. Something the user **is**, such as a biometric identification (fingerprint), palm identification, a retina scan etc.

The problem with passwords and the exploitation of this problem

Traditional password security was copied from the classic use of internal banking systems and was later used for e-banking systems. The significant change that had to be accommodated here though was not only with the use of the Internet, but also in the system's user population. This population changed from bank officials, system managers and other authorised factors to a situation where the users are the clients. This system worked well until a few years ago. However, recently, especially in the last two years, a real threat has emerged as a global phenomenon – 'identity theft'. Identity thieves have turned their 'trade' into a profession and their criminal activities are now well organised. As time goes by, their methods of deception are renewed and become more sophisticated. The different methods that are used by malicious entities include phishing and pharming.

Generally, the stealing of identities exploits the e-banking environment in two ways:

1. By stealing a user's identity (user name and password)
2. By using this stolen identity to enter the e-banking system and perform malicious actions. The business risks and ramifications of these actions include: damage to the client's trust of the bank and of e-banking activities in general, damage to the bank's reputation, damage to clients' privacy, the stealing of information on clients and their activities, and damage to the availability of service (usually, an organised phishing attack causes the lock-out of a number of accounts).

There are of course other ways to steal identity, and the act of 'stealing' may be conducted outside the Internet, such as physical theft, human fraud, social engineering etc. However, it seems that theft over the Internet is used as a 'stimulant' by identity thieves. In Britain alone over the past year phishing attacks cost banks $22.6 million. In the US, the cost of identity theft is put at over $60 billion, and it is estimated that only 56% of relevant events are reported.

Phishing and pharming attacks are generally conducted via one of the following methods:

- A fraudulent e-mail sent to a bank customer: In this case the user receives an e-mail that guarantees special benefits from the bank and asks him to enter the website. The e-mail includes a link which is supposed to point to the bank's website but, in reality, this link is to an imposter's website.
- Routing software: In this case the client's computer is attacked by a virus or worm that changes the internal routing definitions of the computer that was attacked. The next time the client attempts to log on to the bank's website he or she will be directed to a fraudulent website (without his/her knowledge) and, when the client enters a password it is the fraudulent website that will actually receive the login credentials.
- Trojan horse/spyware: This is software that is installed on a user's computer without his knowledge, and records all his key strokes (keylogger), including his password, and sends them to a malicious entity.

The main problem with all this is that the majority of attacks are carried out against the user's computer, so it is difficult (nearly impossible) for the bank to make sure their customers do not expose their passwords. To remedy this and guarantee protection for the bank's clients from impersonation, the bank should change the authentication process so that it is not solely password-based.

Coping methods

There are a wide range of products that provide strong two-factor authentication which actually offer a very general solution. We have divided the different types of authentication by category into 12 'general groups'. The basic common denominator of these strong authentication solutions (including two-factor authentication) is the fact that they are not based only on a password that is known to the user. ➲

The different methods include:

- Digital certificates that use a PKI infrastructure
- Physical means such as smart cards
- One-Time-Password (OTP) generators
- the OTP 'Time Base' category
- the OTP sequence (based either on a mathematical algorithm or on a challenge and response counter)
- USB tokens
- Flash memory (which is essentially just a storage medium containing an encrypted file and which may well be superseded by integrated circuit-based smart cards incorporating not only encrypted storage, but also a miniature CPU that can provide a stronger defence against hackers)
- Biometric identifications
- Solutions that relay on an 'out of band' challenge/response code via cellular communications or SMS which makes the cellular phone the physical element, thus strengthening the two-factor authentication process
- Solutions which use a cellular phone as a physical element as a secured platform, with an applet and a key or a certificate embedded in it to generate challenge response figures in order to authenticate
- 'Other means' which include individual one-use tickets, Passmark tickets, Pinpen, picture authentication etc.

However, regarding the threats mentioned above, even OTP (which is mainly but not exclusively 'time-based') might be vulnerable to phishing if the password is used quickly enough by the attacker. This is called 'On-line Phishing' or 'On-Line Fraud' and it is the next era of phishing. Basically, the phisher (attacker) performs a man-in-the-middle attack by situating himself in an 'On-line' mode after a reversed proxy faked as the e-banking website and by retyping the one-time password quickly to the real bank's website. This technique might be used even in re-authentication scenarios while committing a money transfer to a third party or an investment purchase or sale. There are banks today that have already taken this new threat into account and instigated the necessary countermeasures.

Global references

In early 2005, the Federal Deposit Insurance Corporation (FDIC) published a report recommending that financial institutions should upgrade their authentication systems to two-factor authentication.

This year, the Federal Financial Institutions Examination Council (FFIEC, a committee comprising Governors of the Federal Reserve System, the FDIC, the National Union Administration, the Office of the Comptroller of the Currency and the Office of Thrift Supervision) recommended that financial institutions offering their clients e-banking services should use authentication techniques that are adequate for the risk level of the services offered. The risk level and method of authentication should be derived from a risk assessment carried out on the e-banking system by the bank with regard to:

- Customer type (private, business etc.)
- Customer actions on the systems (payments, on-line transfers, receiving loans)
- Sensitivity of the customer information (both on the client's as well as the bank's side)
- The scope of the transactions authorised to be carried out through the system.

Fraud and identity theft over the Internet is a direct result of the use of one-factor authentication (password only), which today is not nearly satisfactory. In systems with highly-sensitive transactions, access to information or transfers to a third party, the FFIEC's recommendation is unequivocal: use two-factor authentication, similar to the means of authentication required by regulations when opening a new account. Several banks have already begun preparing to implement these recommendations.

In Europe security authentication strategies vary, but the majority of European banks apply two-factor authentication on their e-banking websites. We tend to relate this to two motivations: regulatory tendency and an effort to raise customers' trust in the banks' on-line Internet systems. Regarding the latter, the banks' concerns are driven from the field and from considerable research pointing to the distrust of customers. For example, it has been found that two-fifths of the European net users who do not use on-line banking said the reason is because they worry about security. Worse, security fears do not just prevent consumers from signing up for on-line banking – they cause some existing on-line banking users to stop! The majority of consumers in Germany, Spain, Italy, France and the Netherlands are less concerned about paying by card in a restaurant than about using on-line banking.

Basically authentication to access e-banking websites is perceived to be more secure in Europe than in the US as manifested by the fact that 75% of European consumers bank on-line compared with 43% of US households.

Future use of two-factor authentication

Banks across the world are aware of the need to strengthen the authentication process. The concern that two-factor authentication is inconvenient and that

clients will be negative towards the issue is disappearing, due to technological improvements in a number of products that provide strong authentication. As a result, these methods have become less complicated and more user-friendly. Furthermore, client awareness towards existing threats has increased their desire for banks to strengthen the authentication process in their Internet systems. This trend has been demonstrated by a survey that found that 14% of bank clients in the USA stopped using e-banking systems because of concerns about Internet fraud, such as phishing (based on Forrester's research). In addition, the survey also found that customers are willing to 'sacrifice' the comfort of using Internet sites for better security and safer surfing on their bank's website. In other words, in the trade-off between the efficiency of a strong authentication mechanism to protect the account and the client's willingness to adopt new authentication methods, the adoption of new strong authentication methods by clients wins. Some banks are now examining the ramifications of implementing a stronger authentication process in their Internet systems.

We believe that the banks' incentive for promoting this issue is derived from the practical considerations of increasing protection and clients' security when using e-banking services in the light of the identified threats. This incentive is not necessarily influenced by the banks' requirements to comply with regulatory standards and legislation.

Moshe Ishai (moshei@comsecglobal.com) is CTO and head of the Finance Division at Comsec Consulting.

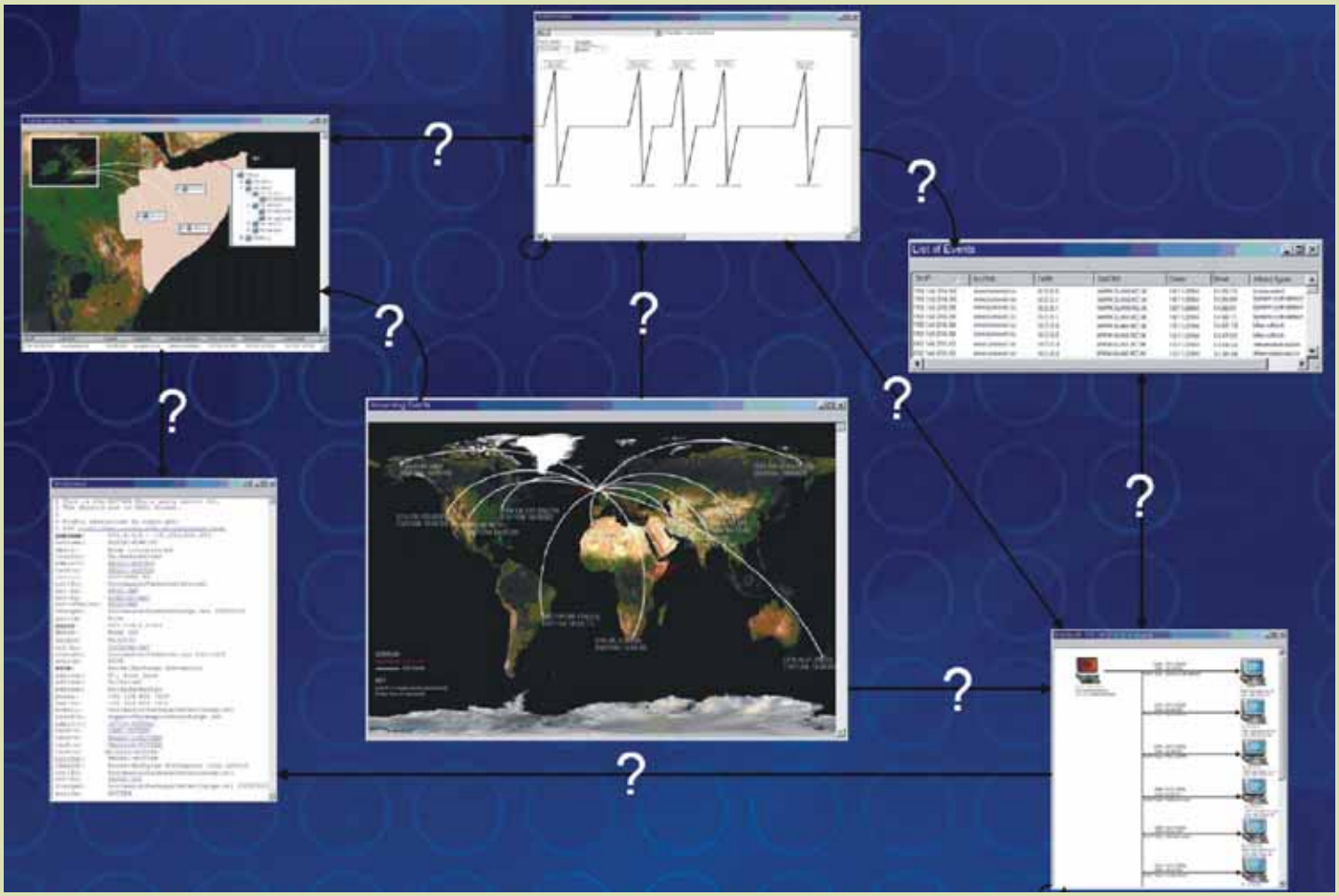
IDS Data Visualisation:
Potential and Challenges for Comprehensive Security Incident Analysis

Huw Read, Andrew Blyth and Theodore Tryfonas

Hackers, phreakers, threat agents and other perpetrators wreaking havoc on our computer networks for prestige, financial gain or extortion have always been a great concern; thus we deploy security solutions to try and stop them or mitigate the impact of their attacks. Software, collectively known as IDS (Intrusion Detection Sensors) is used to collect information about the traffic typically flowing into and out of a corporate network. The relevant technologies have matured and are now established. Network monitoring and analysis tools have been available for a long time. IDS tools such as Snort and Cisco Security Agent provide a 'signature'-based approach whereby known attacks can be identified; signatures may be updated to keep abreast of the latest known attack types.

With so many security solutions available, both open source and commercial products, the problem is not to obtain security related data, but rather to be able to reasonably process too much data. Typically organisations can expect several thousand 'events' a day, the number rising to near ludicrous totals in secure areas of government, commerce and also open university infrastructures.

This quite clearly raises a number of issues. It becomes near-impossible to analyse every logged snippet of information due to the sheer volume of collected data. Consequently, more critical attacks may go unnoticed while security analysts sort the wheat from the chaff and, in order to comprehend the attack data in detail, an analyst must have an almost superhuman understanding of the information being presented (see figure 1 below).



Fugure 1. Too many IDS tools and limited interoperability

There are several schools of thought on how to best deal with this issue; one of the interesting possibilities that has arisen in recent years is through visualisation. A number of visualisation tools have been created by industry and academia that provide us with rich, insightful imagery that enables us to analyse data in a different fashion. Most of the tools of this type, instead of attempting to show the data in raw form, tend to summarise them, emphasising or highlighting certain trends.

IDS visualisation engine

It has proved very difficult so far to capitalise upon different visualisation types without creating large, complex software that incorporates several facets into one tool. Much of our own current research is into the problems facing IDS visualisation. Visualisation and correlation tools from non-IDS vendors are important and will continue to proliferate so long as IDS vendors do not improve their own reporting interfaces. Even so, vendors usually choose to implement such proprietary functionality in a non-standardised way.

Without the presence of a common standard that allows one visualisation tool to interface to another, as a first step we have had to create a data-exchange layer from scratch. Based on this, we developed middleware that allows for the passing of standardised input and output between different visualisation tools and facilitates the rapid data exchange needed by analysts in the intrusion detection process. The entire architecture is represented at a high level in figure 2 below.

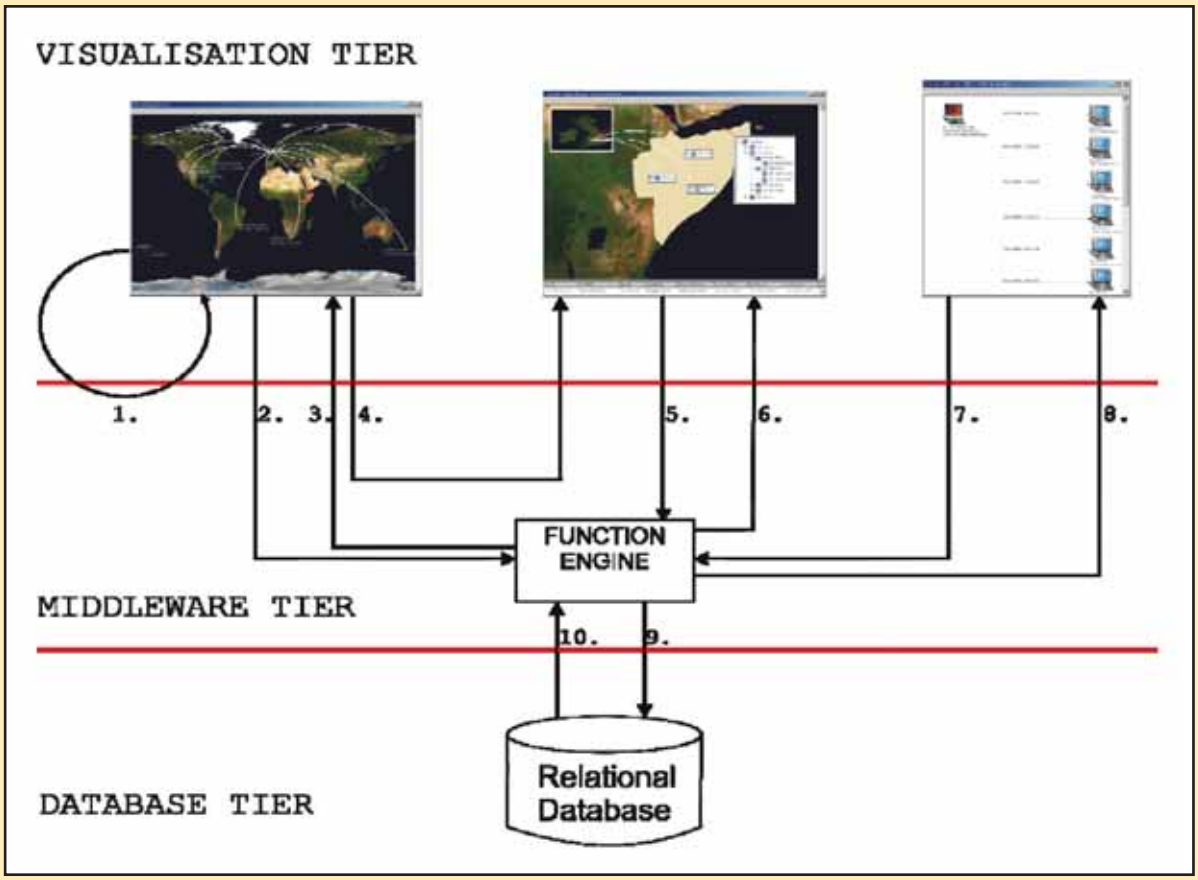
We have had success in converting small, proprietary tools and integrating them with the visualisation engine, so that they can make use of the prototype system. The general process of passing data between different visualisations is not particularly difficult to implement; one merely needs to right-click on an object (i.e. a context-sensitive area) within one tool and a small menu is generated with a list of other tools to progress to (see figure 3).

When a tool receives input data from another, it actually receives a list of primary keys (*eventid*) and a list of functions which, when executed with the *eventid*, returns the relevant data from the underlying database. These functions are relational algebraic expressions encoded in XML that provide a more generic way of querying databases (see figure 4).

The advantage of using such functions is twofold. Firstly, passing only named functions and *eventids* minimises the *physical* size of transferred data (which alleviates bandwidth constraints and keeps the data in the actual *database*). Secondly, by having these functions carry out the actual database queries, complete segregation is achieved between the visualisation programme and the database layers in the deployment topology.

Conclusions and further research needed

Currently the leading IDS tools collect more data than any individual analyst can reasonably handle within an acceptable amount of time. However, there is a firm belief amongst researchers and industry alike that visualisation tools have helped greatly with identifying attacks and hence that further developments in this area will benefit greatly the task of intrusion identification and incident analysis. Tailor-made tools help us identify specific sequences of intrusions and some even allow us to 'drill down' through data. However, these tools currently lack the desired interoperability and integration features that will unlock the potential of visualisation for security analysis.



1. XML: Event ID(s) & function(s)
2. XML: Event ID(s) & data type
3. XML: Requested data from database
4. XML: Event ID(s) & function(s)
5. XML: Event ID(s) & data type
6. XML: Requested data from database
7. XML: Event ID(s) & data type
8. XML: Requested data from database
9. SQL Query
10. Result of SQL Query

Fugure 2. Three-tier IDS visualisation architecture, from database to application layers

Figure 3. Implementation of context-sensitive database functionality in the front-end

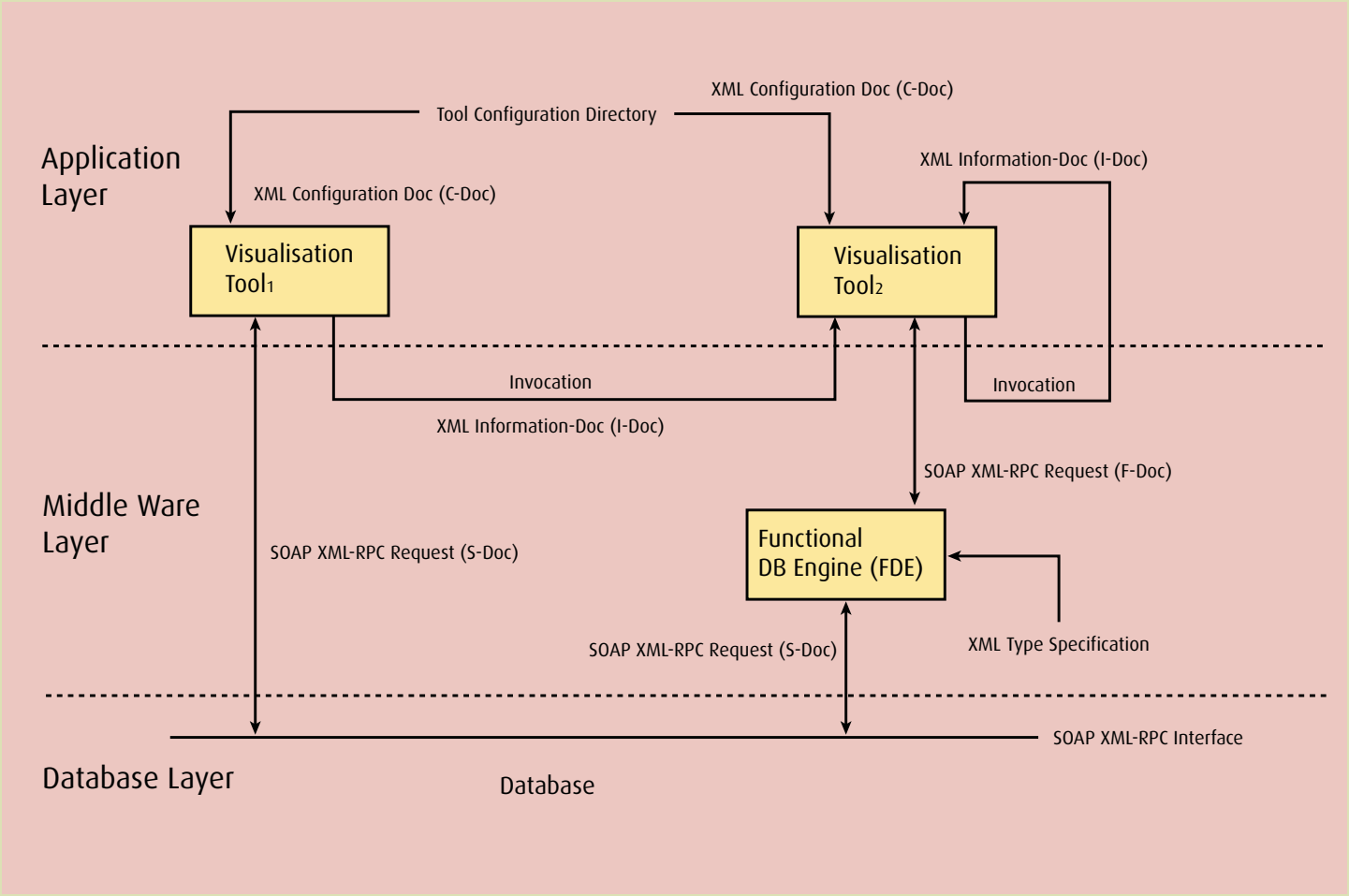


Figure 4. Interactions between different components on multiple tiers

Our work aims to help security analysts to increase their capability to interact with IDS data and look at the events intrusion sensors have picked out in shorter times and with a multiplicity of tools. With such developments this becomes less of a task for hardcore analysts working with raw event logs and instead brings the task back into the mainstream.

In using the proposed framework, individual tools can easily pass data to others. At the same time 'data mining' becomes semi-transparent because, by starting out with a large, initial set of data and passing it around via the usage of objects, the events can be whittled down to a smaller, relevant group. This also makes for less time spent on developing own Input/Output mechanisms and more time spent on creating novel visualisations, and hence there will be less dependence on a particular underlying database of a specific vendor.

Huw Read (holread@glam.ac.uk) is a Research Assistant with the Information Security Research Group, University of Glamorgan.

Andrew J C Blyth (ajcblyth@glam.ac.uk) is a Principal Lecturer at the University of Glamorgan and the Head of the Information Security Research Group.

Theodore Tryfonas (ttryfona@glam.ac.uk) is a Senior Lecturer at the University of Glamorgan and the Programme Leader for Glamorgan's popular postgraduate degrees in information security.

Security Metrics for Information Security Management

Vicente Aceituno Canal

Most readers will agree with the assertion "What can't be measured, can't be managed". This article outlines the important factors which can be measured in order to be able to practise the quantitative management of information security, and which are the management practices that become possible when we use such metrics.

Metrics

A metric is a quantitative measurement that can be interpreted in the context of a series of previous or equivalent measurements. Metrics are necessary to show how security activity contributes directly to security goals; to measure how changes in a process contribute to security goals; to detect significant anomalies in processes and to inform decisions so that processes can be fixed or improved.

Good management metrics are said to be S.M.A.R.T.:

- **S**pecific: The metric is relevant to the process being measured.
- **M**easurable: Metric measurement is feasible with reasonable cost.
- **A**ctionable: It is possible to act on the process to improve the metric.
- **R**elevant: Improvements in the metric enhance the contribution of the process towards the goals of the management system in a meaningful way.
- **T**imely: The metric measurement is fast enough to be used effectively.

Metrics are formally defined by the following items:

- The name of the metric
- A description of what is measured
- How the metric is measured
- How often the measurement is taken
- How the thresholds are calculated
- The range of values considered normal for the metric
- The best possible value of the metric
- The units of measurement.

The problem – security metrics are difficult to find

Unfortunately, it is difficult to find metrics for generic goals such as security, trust and confidence. The main reason is that security goals are 'negative deliverables'. The absence of incidents for an extended period of time leads us to think that we are safe. If you live in a town where neither you nor anyone you know has ever been robbed, you feel safe. Incidents prevented cannot be measured in the same way as a positive deliverable, like the temperature of a room.

Metrics for goals are not just difficult to find; they are not very useful for security management. The reason for this is the indirect relationship between security activity and security goals. Most managers think intuitively that there is a direct link between what we do (which has results or outputs) and what we want to achieve (the most important things: our goals). This belief is supported by real life experiences like making a sandwich. You buy the ingredients, arrange them in proper order at home, perhaps toast them and voilá: a warm sandwich is ready. The output sought (the sandwich) and the goal (eating a home-made sandwich) match perfectly.

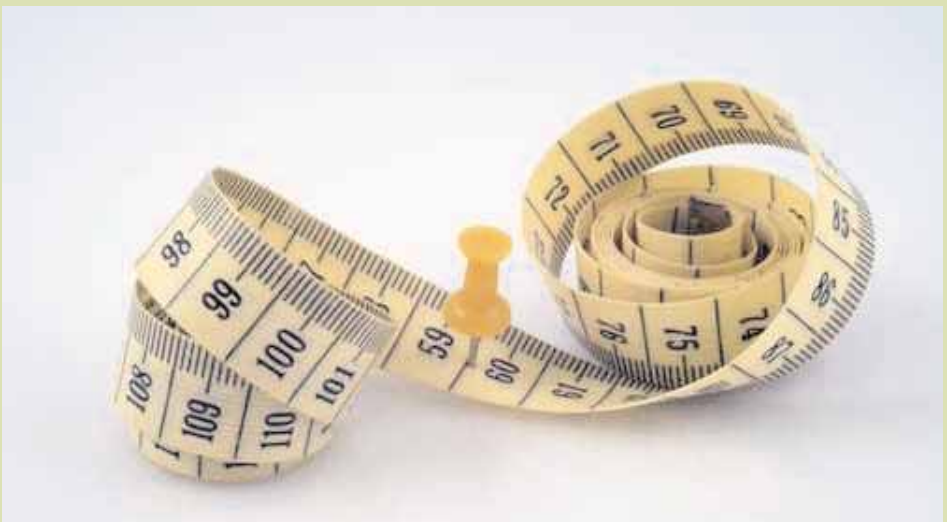
Unfortunately, there is not always a direct link between things, with a good example being research. There is no direct relationship between goals (discoveries) and the activity (experiments, publication). You can try hundreds of experiments and still not discover a cure for cancer. The same thing happens with security. The goals (trust, confidence, security) and the activity (controls, processes) are not always directly linked.

When, however, there is a direct link between activity and goal, like the temperature in a pot and the heat applied to that pot, we know what decision to take if we want the temperature to drop: stop applying heat. But how will we make a network safer? By adding more accurate filtering, or summarising filtering rules and making them less complex? We simply do not know! If a process produces dropped packets, whether more (or fewer) packets are dropped is not necessarily an indication as to whether a network is more or less secure, just like a change in firewall rules will not necessarily make the network safer.

The disparity between goals and activity present in information security prevents goal metrics from being useful for management, as you can never tell if you are closer to your goals because of other factors in the security processes.

Examples of goal metrics include:

- Instances of secret information disclosed per year. What can be done to prevent people with legitimate access from disclosing that information?
- Use of system by unauthorised users per month. What can be done to prevent people from letting others use their accounts?
- Customers' reports of misuse of personal data to the Data Protection Agency. Even if you are compliant, what can be done to prevent a customer completing a report?
- Risk reduction per year of 10%. As risk depends on internal and external factors, what can be done to actually modify risk?
- Prevent 99% of incidents. How do you know how many incidents did not happen?



Useful security metrics

If metrics for goals are difficult to come by and are not very helpful, what is a security manager to do? Measuring process outputs could be one of the answers. Measuring outputs is not only possible but very useful, as outputs contribute directly or indirectly to achieve security, trust and confidence. Using output metrics you can:

- Measure how changes in a process contribute to outputs
- Detect significant anomalies in processes
- Make informed decisions to fix or improve the process.

There are seven basic types of process output metrics:

- **Activity:** The number of outputs produced in a given time period
- **Scope:** The proportion of the environment or system that is protected by the process. For example, AV could be installed in only 50% of users' PCs.
- **Update:** The time since the last update or refresh of process outputs
- **Availability:** The time since a process has performed as expected upon demand (uptime), the frequency and duration of interruptions and the time interval between interruptions
- **Efficiency/return on security investment (ROSI):** Ratio of losses averted to the cost of the investment in the process. This metric measures the success of a process in comparison with the resources used.
- **Efficacy/benchmark:** Ratio of outputs produced in comparison with the theoretical maximum. Measuring efficacy of a process implies comparison against a baseline.
- **Load:** Ratio of available resources in actual use, like CPU load, repositories capacity, bandwidth, licenses and overtime hours per employee.

Examples of the use of such metrics are the following:

- **Activity:** Measuring the number of new user accounts created per week (a sudden drop could mean that either the new administrator is lazy or that users have started sharing user accounts).
- **Scope:** In an organisation with a large number of third party connections, measuring the number of connections with third parties protected by a firewall could lead to a management decision not to create more unprotected connections.
- **Update:** Measuring the update level of the servers in a Demilitarised Zone (DMZ) could lead to investigating the root cause if the level goes above a certain point.
- **Availability:** Measuring the availability of a customer service portal could lead to rethinking the High Availability Architecture used.
- **Efficiency/return on security investment (ROSI):** Measuring the cost per seat of the Single Sign On systems of two companies being merged could lead to the choice of one system over the other.
- **Efficacy/benchmark:** Measuring the speed of two different back-up systems could lead to the choice of one over the other.
- **Load:** Measuring and projecting the minimum load of a firewall could lead to taking the pre-emptive decision to upgrade.

There is an important issue to tackle when using output metrics – **'the Comfort Zone'**. If there are too many false positives, the metric will be quickly dismissed, as it is not possible to investigate every single warning. On the other hand, when the metric never triggers a warning, there is a feeling that the metric is not working or providing value. The Comfort Zone (not too many false positives, pseudo-periodic warnings) can be achieved using an old tool from Quality Management – the control chart. The are some rules used in Quality Management to give a warning, i.e., highlighting a condition that varies from the statistical norm which should be investigated (Western Electric, Donald J. Wheeler's, Nelson rules) but, for security management, the best practice is adjusting the multiple of the standard deviation that will define the range of normal values for the metric until the Comfort Zone is achieved, i.e., pseudo-periodic warnings without too many false positives.

What management practices become possible?

A side effect of an Information Security Management System (ISMS) lacking useful security metrics is that security management becomes centred in activities like Risk Assessment and Audit. Risk Assessment considers assets, threats, vulnerabilities and impacts to get a picture of security and prioritise design & improvements while Audit checks the compliance of the actual information security management system with the documented management system, an externally defined management system or an external regulation. Risk Assessment and Audit are valuable, but there are more useful security management activities such as monitoring, testing, design & improvement and optimisation that become possible with output metrics.

Theses activities can be described as follows:

- Monitoring watches processes' outputs, detects abnormal conditions and assesses the effect of changes in the processes.
- Testing checks if inputs to the process produce the expected outputs.
- Design & improvement finds ways to produce outputs better fitted to their purpose, with fewer false positives and false negatives (and faster outputs).
- Optimisation finds ways to produce the same outputs with fewer resources.

While audits and qualitative risk assessment can be performed without metrics, monitoring, testing, design & improvement and optimisation are not feasible without them.

What needs to be done?

S.M.A.R.T. security managers need metrics that actually help them to perform management activities. Risk assessment and audit are useful, but they are not a panacea.

While it is not necessary to drop goal metrics altogether, the day-to-day focus of information security management should be on security monitoring, testing, design & improvement and optimisation using output metrics which will show the effect of management decisions, i.e., if things are getting worse or better, if processes work as designed and if there are changes out of our direct control causing abnormal conditions in security processes. All these activities are perfectly feasible using output metrics and control charts.

Vicente Aceituno Canal (vicepresidente@issa-spain.org) is the Vice-President of ISSA in Spain and the Director of the ISM3 Consortium (www.ism3.com).

From our own Experts

ENISA Study on Providers' Anti-Spam and Security Measures

Pascal Manzano

Spam (or unsolicited e-mail) represents around 85% of all e-mails. What could be done to reduce the amount of spam? Different kinds of action can be taken or solutions used: technical, organisational, adapting legislation and increasing awareness. In order to tackle this problem we first need more information about the current status of spam. What are the techniques that already exist to fight spam? Which are the ones that are used by Internet providers? Are there any good practices? Are there any standards, protocols or architectures already developed or under development in this field? What is the level of knowledge of end-users?

To find the answers to these questions, ENISA is conducting a series of studies to gather information from Internet service providers, national regulatory authorities and national and international providers' associations. The goal is to identify and promote best practices!

In 2006 ENISA conducted the first study in the series, looking into the technical and organisational measures that electronic communication service providers take with regard to IT security measures and the countermeasures they have introduced to combat spam. The reports are available at:
www.enisa.europa.eu/doc/pdf/deliverables/enisa_security_spam.pdf
www.enisa.europa.eu/doc/pdf/deliverables/enisa_security_spam_part2.pdf

This year ENISA is following up the previous work in this field by extending the coverage of the questionnaire to a wider audience and involving more countries. The study will include *Internet, content, network* and *telecommunication* service providers. The goal is to identify and consequently promote best practice.

The first step in this follow-up study is to collect information from Internet and e-mail service providers. A questionnaire was made available on-line (https://webgate.ec.europa.eu/publications/surveys/DG/ENISA_SPAM/) for providers' technical and security teams to download and complete. The deadline to contribute was the end of June.

The data collected is now being analysed and compared with last year's figures to identify any trends. During this phase, interviews with some providers may be conducted in order to ascertain the details of their practices with regard to countermeasures.

As a result of this study we will create a number of reports. A technical report will target providers and security experts, exposing the observed facts, statistics, trend analysis and best practices. Another report will cover discussions and exchanges with the European Commission regarding a review of existing legislation. We also plan to become involved in anti-spam awareness initiatives aimed at end-users by producing recommendations translated into many languages.

Finally, we will disseminate the results of this study at a workshop that we are planning for the final quarter of 2007.

For further information, please contact: provider.study@enisa.europa.eu

---

Pascal Manzano (pascal.manazano@enisa.europa.eu) is an Expert in the Security Policies section at ENISA.

Call for Papers

3rd European Conference on Computer Network Defence (EC2ND), organised in co-operation with ENISA, 4-5 October 2007, Crete, Greece

The theme of this conference is the 'Protection of Computer Networks'. The event will draw participants from academia and industry throughout Europe and beyond to discuss hot topics in applied network and systems security. EC2ND invites submissions which present novel ideas at an early stage, with the intention of acting as a discussion forum and a channel for feedback for promising, innovative security research.

Topics will include but are not limited to: Intrusion Detection, Denial-of-Service, Privacy Protection, Security Policy, Peer-to-Peer and Grid Security, Network Monitoring, Web Security, Vulnerability Management and Tracking, Network Forensics, Wireless and Mobile Security, Cryptography, Network Discovery and Mapping, Incident Response and Management, Malicious Software, Web Services Security and Legal and Ethical Issues.

Accepted papers will be published by Springer as part of the Lecture Notes in Electrical Engineering (LNEE) series, which will be indexed in the ISI(r) Index to Scientific & Technical Proceedings.

Important Dates: • Submissions due: 8 July 2007 • Notification: 8 August 2007 • Final version due: 10 August 2007

Conference Location:
The conference will be held at the Hotel Aldemar Royal Mare Village in Hersonissos, Crete (www.aldemarhotels.com/EN_Crete-Royal-Mare-Village.html)

For more information visit the EC2ND web pages at: http://2007.ec2nd.org/

An ENISA Joint Portal for NIS Standards

Elisabetta Carrara

ENISA is engaged in the monitoring of ICT trends and developments, analysing their security implications. Following standards development is an important component of this activity, and ENISA is monitoring the activities of the major Standards Development Organisations (SDOs), both in the European and international context – NIS has no geographical borders.

Open standards are key to enhancing interoperability, thus enabling the success of services. Many standardisation activities exist and a multitude of standards are produced by different SDOs – in general, we see a very prolific, dynamic and constantly growing scenario, yet it is fragmented. Duplication of effort may exist, sometimes inconsistencies may arise. SDOs need to co-ordinate their activities, and users need an easy way to navigate through standards. How can ENISA help?

The lack of a central depository where standards and ongoing standardisation activities are collected and referenced is a concern that has been voiced more than once by standardisation bodies and NIS stakeholders. ENISA is taking action to address this issue and has joined a new project called the "ICT Security Standards Roadmap".

The project was initiated by the ITU Telecommunication Standardisation Sector (ITU-T). At the beginning of the year, ENISA and the Network and Information Security Steering Group (NISSG) joined the ITU-T's effort, and started to work together to create a new portal for IT security standards. The first version of the Roadmap is now available on-line.

One of the objectives of this portal is to provide a central tracking facility for NIS standards. It facilitates the identification of standards and standardisation activities, co-ordination among standardisation bodies and the reduction of duplicate work, as well as making the identification of existing gaps easier. The Roadmap comprises five parts, of which Part 1 and Part 2 are available in this first release:

Part 1: ICT Standards Development Organisations and their work
Relevant organisations are identified together with their work programmes. This part also lists existing security glossaries.

Part 2: Approved ICT Security Standards
This part is the database of existing NIS standards. The catalogue can be accessed from an organisational view or a functional view. The former classifies the standards by the relevant SDO, while the latter according to NIS topics. In this first version of the database, we adopted a simple functional view by using a priori defined topics.

The remaining Parts forming the Roadmap are at a very early stage and will be finalised over the coming months:

Part 3: Security standards under development
This will be the database of work-in-progress standardisation items and activities not yet approved and published, as well as information on inter-relationships between groups. Part 3 is an important activity, as it is intended to help reduce potential overlaps between existing activities.

Part 4: Future needs and proposed new security standards
The Roadmap will highlight areas where gaps exist in standardisation, and areas where proposals for new standards are under examination.

Part 5: Best practices
Some excellent work has already been achieved in NIS Best Practices – and we would like to offer an easily accessible reference document.

ENISA and its partners will continue to work to improve the Roadmap in order to make it a comprehensive tool to facilitate NIS standardisation. For future releases, we also plan to provide a more comprehensive functional view, by having a more detailed topical categorisation.

The ICT Security Standards Roadmap is hosted by the ITU-T and can be found at: www.itu.int/ITU-T/studygroups/com17/ict

Elisabetta Carrara (elisabetta.carrara@enisa.europa.eu) is an Expert in the Security Tools and Architecture section at ENISA.

The 5th German Anti-Spam Summit

Eco, the Association of the German Internet Industry, is organising its fifth anti-spam summit in Cologne, Germany, on 5 September 2007. The motto of this year's summit is "5 years of Anti Spam in Germany & Europe – Is the Internet beyond remedy?"

The summit will offer interesting presentations and discussions from and between Internet Service Providers (ISPs), filtering manufacturers, law enforcement and international projects on the latest developments in spam techniques, with feedback from the battlefield. If you want to understand why in 2007 spam still represents more than 90% of e-mail traffic, you should attend! This international/European conference will be held in English.

In the last four years, more than 100 decision-makers from Internet industry, ISPs, law enforcement and public authorities have attended each summit.

ENISA is supporting eco with the organisation of the event. More information on: www.eco.de/5.DASK

From the Member States

Evil Lurks Around Every Corner

Report on the IT security situation in Germany in 2007

Anke Gaul

The first "Report on the IT security situation in Germany" was published in August 2005. Now, almost two years later, the Federal Office for Information Security (BSI) has published another assessment of the current state of IT security in Germany. This report shows that awareness of the risks of using information technology (IT) has increased in some social groups. At the same time, however, the quantity and quality of attacks on both private and company IT systems have increased drastically. The potential risks have not decreased – quite the contrary. The situation with IT security is thus not expected to ease up either over the short or long term.

The advantages offered by ever-changing communication channels in the Information Society are indisputable. They span expanded educational opportunities, a democratisation of general access to information via the Internet and increased efficiency in many areas. The dark side is the emergence of a new type of vulnerability in the corporate as well as private sectors. New challenges are created as systems become more interconnected and many (day-to-day) activities are shifted to the virtual world.

It does not end with simply identifying the risk

The number of Internet users in Germany, with more than 60% of households on-line, is continuously on the rise. Simultaneously, the number of people who have come into contact with the hazards of the Internet in one way or another is also increasing. Four out of five users say that they have been affected at least once. Viruses and worms are the front runners in this context.

Most users were already aware of the various possibilities for attack when we published the 2005 IT security report. However, few practical measures had been undertaken at that time as a result. This situation has changed because those who have been personally affected have a heightened awareness, thus causing them to protect their computers more actively. According to data collected by BSI, the percentage of private users who use a virus scanner increased within three years by 14% to a total of 90%, and the use of personal firewalls has also risen.

Risk identified – is that enough? Certainly not! It is still the case that vital warnings, e.g. about the potential risk of surfing with unrestricted administrator rights, are ignored.

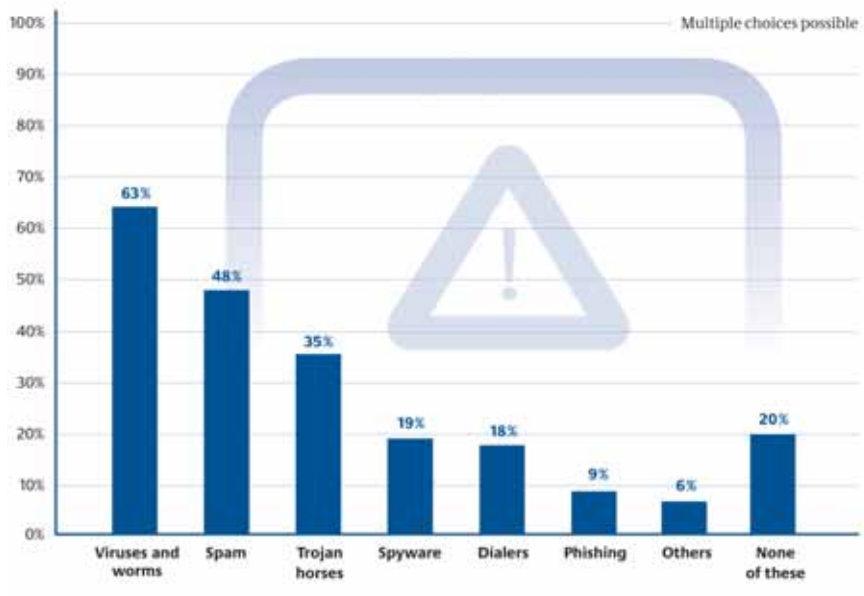
A contradictory picture results: although users are generally aware of the need for IT security, there is also a tendency to try to delegate responsibility for providing remedies to the problems to Internet service providers and the manufacturers of IT security solutions. This is obviously important, as IT security must be given a higher priority as a necessary product feature of systems and services. However, each technical measure for securing an IT system is only worth half as much if the people using it are not sensitised for IT security, do not accept IT security measures and do not actively practise IT security.

IT security is (still) not a top-level matter!

A paradox also exists in the business world: the individuals responsible for IT give IT security a high priority. Budgets, however, speak another language. Only on rare occasions is more than 10% of the entire IT budget invested in IT security, and this figure has fallen dramatically over the years. The reason is that top managers are not sufficiently aware of the risks. The threat to one's own company is commonly underestimated, and security risks are seen as technical problems rather than relevant business problems. And wrongly so! IT security is and will remain a top-level matter; apart from the very relevant costs to the business of IT problems and a potential loss of image associated with them, the issue of personal liability is becoming increasingly important.

The level of awareness is higher in industries regarded as critical infrastructures, i.e. those that provide vital services for the general good such as telecommunications or power supply. In these industries, people are fully aware of the risks posed by the use of IT and understand IT security as a process that extends from the management level to the operating level and the control of individual measures.

Personal experience with on-line threats



Internet threats already encountered by citezens

Potential security risk

The first PC viruses were reported more than 20 years ago. At that time, viruses were transferred from PC to PC data on floppy disks. In today's networked world, on the other hand, they are spread around the world within seconds and infect unprotected PCs. Numerous new malware types are reported every day. It is Trojan horses, not viruses and worms, that are becoming the greatest danger.

Modern Trojan horses offer the attacker a wide range of communication and control options as well as a number of functions that can be combined at will. In concrete terms, Trojan horses are used to set up bot networks and conduct phishing attacks, and their use in targeted spying has increased noticeably.

The type of programming has also undergone a change: malicious computer programmes are increasingly modular in their design. (Small programmes, so-called downloaders, are at the fore here.) Subsequently, they can download more malicious functions from the Internet at specific times or if instructed by the attacker, and the malicious programmes on the infected systems can be replaced by optimised versions.

For companies and government agencies which depend on the confidentiality of their data, as well as for private users who increasingly rely on the Internet for financially-related activities, this has dramatically changed the threat. Espionage, identity theft and extortion represent worthwhile 'business models' for Internet criminals, thus making every user a potential victim.

The 2007 report points out that Internet risks are significantly on the rise both in terms of quantity as well as quality. Even though awareness has improved, risks have become ever more ominous.

The user as risk?

To the same degree that innovative technologies ensure sustainability and create both business and social opportunities, the complexity of the new developments also harbours risks for manufacturers and users. Technologies such as Voice over IP (VoIP), WLAN and RFID, as well as process control systems (SCADA) are far advanced today in terms of the standard of technical security. The risk primarily exists in the practical application by the user.

For example, when IP communication and telecommunications are merged, both services can be disrupted or fail at the same time. For the operation of VoIP systems to be reliable and secure, security measures must be integrated into the planning of both technologies at an early stage. Particularly in the private sector where deployment is currently higher than in companies, this is often not the case. Inadequately secured WLANs let attackers penetrate corporate networks or home PCs, collect confidential data and cause financial harm. The total percentage of open WLANs has generally decreased but overall the security situation continues to be a threat because weak security mechanisms are usually in use.

New risks are also created by mobile phones which are used more and more as smart computers with their own operating system as well as a number of functions, applications and interfaces. Although the risk of mobile devices becoming infected is currently low in comparison with PCs, it is definitely real.

Trends – "I'll tell you who I am...."

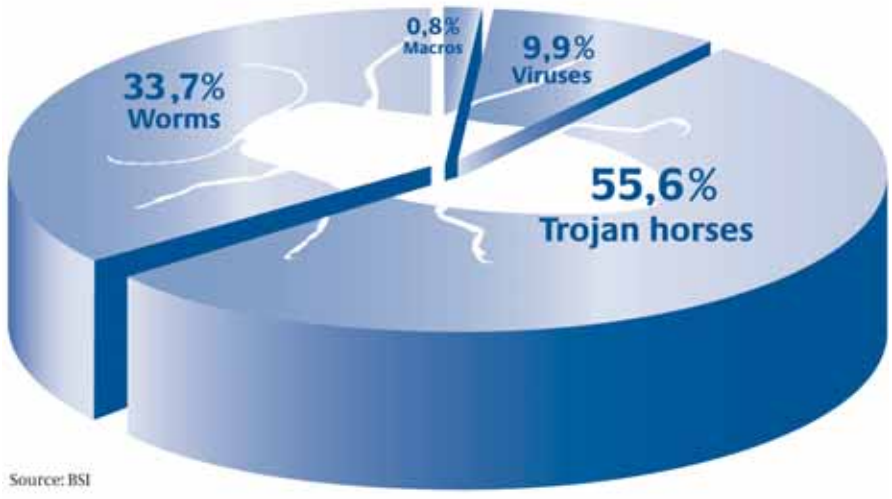
Technical innovations and their integration into day-to-day functionality are not solely responsible for the increased need for IT security.

Economic, social and legal trends that ultimately have a natural and reciprocal connection to technological innovations influence the significance of IT security and create a new IT security culture. IT security must not be seen as an isolated matter. Knowing about current developments in the economy and society at large can contribute much to being able to estimate the (future) importance of IT security more effectively.

One of the most important keywords in this context is certainly 'Web 2.0'. The Internet constantly offers new technologies and services which enable the direct exchange of information. The massive increase in

➲

Malware occurrence 2006



Registered malware in the Berlin-Bonn Information Network (IVBB) in 2006 in %

interactivity in the virtual world – which seemingly encourages users' needs to divulge ever more private information on the Internet – has resulted in a high level of availability of personal data on the Web. The communication here is generally not directed at clearly defined target individuals. The information contained in blogs, on open web pages or in discussion forums can thus be misused by third parties. Social engineering has long been a prevalent approach by criminals who have adapted to this trend: they approach their victims by addressing them personally in an individual manner which allows them to create a level of trust the goal of which is to find out personal data such as login information for on-line services.

Another important aspect is legal trends and developments. IT security today is a decisive factor in the value chain. Low internal corporate security standards that increase the risk of crises bring with them not only a low level of financial credibility but also, under some circumstances, higher liability insurance premiums. If damage is caused, the question of legal responsibility arises. A number of existing legal liability regulations can be directly applied to commercial users of IT systems. As a reaction to a number of corporate collapses in both the United States and Germany in recent years, the requirements to be met by internal company management are now increasingly established in in-house laws (keyword 'compliance', the observance of legally stipulated guidelines and minimum requirements).

Living IT security: Claims and reality

The Report on IT security in Germany shows a massive need for action in all social groups. The security skills of users must be improved at all levels.

Furthering security awareness among the general public plays a key role. A decisive factor is the right motivation. Only when users recognise the sense behind the individual measures, will they implement these consistently and follow security recommendations. However, the central element is still the citizens' individual accountability. Whether private individual, employer or colleague, they have to prevent or at least minimise the negative impact of concrete dangers. There is not and will never be a worry-free package solution in the area of IT security – education and sensitisation with the aim of enhancing the general public's skills in dealing with the PC and Internet, as well as personal accountability, should therefore also play a key role in the future.

Education and increased awareness also play an important role in German companies. Insufficient knowledge of the problem means that insufficient financial and personnel resources are available in the area of IT security. The onus is on managers to take their responsibility seriously, as IT security is a matter for top-level management. The security process must be initiated at the management level and then supported and organised by all members of the company. Holistic guidelines and agreements put down in writing for governing IT activities in the working environment should be supplemented by measures for enhancing the awareness of employees. The necessary resources must be made available to implement the IT strategy.

Enhancing security competence in both the business and private realms is a key component in improving the overall conditions for the secure use of IT. Because it is becoming more and more time-consuming to keep risks at a reasonable level and ensure confidentiality, availability and the integrity of information, there is also a need for action by the providers of information and communication technology. How IT products and systems work from a technical standpoint is not transparent for a large number of users. Suppliers are thus obliged to give the issue of IT security a high priority and, for example, create transparency with respect to the security properties of IT products through the standardised testing and certification of products. Integrating, whenever possible, automated security measures from the outset to keep the necessary interaction by the user to a minimum could further increase the security level and reduce the potential risk.

Conclusion

A great deal has changed since the first BSI security report was published in 2005. An increasing number of activities are being performed using technology, and business and private activities have increasingly shifted to the virtual world. This is accompanied by the ongoing professionalisation and commercialisation of IT threats. It is difficult to make a reliable assessment of how the threats will actually develop. Only one thing is certain: security measures on the part of manufacturers, administrators and government agencies are countered by the constantly changing methods of attackers and their adaptation to new circumstances. The potential risk also increases at the same pace as the growing distribution of a technology. The IT security situation is therefore not expected to relax over the long term.

Despite the fact that the 2007 report shows heightened awareness for IT risks in some groups, there is still potential for improvement. For example, sometimes companies argue that security measures have to be cut back to save money if budgets are tight. This is a dangerous way of thinking. Damage caused by system failures or espionage attacks can quickly amount to many times the sum which is invested in security measures. Ultimately, therefore, IT security always pays off for users in all areas as well as for society as a whole. It is the type of insurance that every citizen, every government agency and every company has to have.

The Federal Office for Information Security published the second report on current IT security in Germany at the end of May this year. An English language version can be downloaded from www.bsi.bund.de/english/publications/index.htm.

Anke Gaul (anke.gaul@bsi.bund.de) is an Adviser on Information, Communication and Public Relations at the BSI.

The Network Security Innovation Platforms in the UK

Andrew Tyrer

Innovation Platforms

In November 2005 the United Kingdom's (UK) Department of Trade and Industry's (DTI) Technology Strategy Board (TSB) introduced the concept of Innovation Platforms. Innovation Platforms are a new way of working for Government and are seen as an opportunity to position business and Government more closely together to generate more innovative solutions to major policy and societal 'challenges'.

The Network Security Innovation Platform

Now that electronic networks are commonplace and increasingly critical to society, network security is seen as a major growth area and one where the UK is well placed to create added value through the provision of both products and services. The Network Security Innovation Platform (NSIP) was created to respond to and answer this particular 'challenge'.

Network security is concerned with the resilience of a communication network infrastructure, and with the security of the information being transmitted across that network. This will inevitably include the people using the network, and it is therefore relevant to include the usability of such systems.

Existing Government requirements for network security include identity cards and e-borders, and many other Government Departments are major prospective users of secure networks.

A few facts from the Information Security Breaches Survey 2006 technical report (www.dti.gov.uk/sectors/infosec/infosecdownloads/page9935.html) highlight the importance of network security to both UK companies and to us as individuals:

- in the last hour £50,000 of credit card fraud will have taken place in the UK (totalling £440m last year), and
- in 2006, 62% of UK companies had a network security incident and the average cost of a company's worst incident was £12,000.

However, the real 'challenge' that faced the NSIP was in bringing together key Government Departments, academia and business to identify where innovation could be used to solve specific problems. If successful, the UK would then have a unique opportunity to influence the global market, and for UK firms to exploit the opportunities on offer.

First things first

The NSIP's early work in this area identified that the weakest link in network security is not usually a technological vulnerability but the people who work within the system. To give a simple example, the most secure system can be penetrated easily if staff with legitimate access write down their password or let it be used by someone else. This might seem an urban myth but a recent poll of over 1800 adults in the Information Security Breaches Survey 2006 technical report found that:

- just over one third recorded their password or security information by either writing it down or storing it somewhere on their computer
- nearly two thirds never changed their password
- 1 in 5 people used the same password for non-banking websites as well as their on-line bank.

Furthermore, not only can security be compromised accidentally, but it can be done deliberately for illegitimate purposes such as fraud; the NSIP is concerned with both these issues.

Having established that in order to strengthen network security there is a need to address human, as well as technological, vulnerabilities, the NSIP looked to see which problems would encourage the development of innovative solutions.

Next steps and call for proposals

Human vulnerabilities in network security may arise inadvertently, due to a lack of understanding of security by the network user, or deliberately, due to insider fraud.

Additionally, organisations need to establish effective security cultures and must be able to assess the potential risks (both benign and malign) that are posed by their employees.

With this in mind, the NSIP launched a call for proposals as part of the Technology Strategy's Autumn 2006 competition (www.dti.gov.uk/innovation/technologystrategy/competitions-for-funding/page34928.html). The Human Vulnerabilities in Network Security (www.dti.gov.uk/files/file34920.pdf) call invited proposals that addressed the following questions:

- What social structures, rules and attitudes should exist in an effective security culture?
- How is it possible to create and embed these cultural characteristics in an organisation?
- To what extent is it possible to assess the risk that employees will abuse their access to an organisation's assets for illegitimate purposes (e.g., abuse their computer network access)?

This was a new area of activity for the DTI, linking technological innovation with behavioural science, and the NSIP worked closely with the Economic and Social Research Council (ESRC), another DTI first, in designing this call.

NISP funded projects

There was a total of four successful proposals, and the initial six-month feasibility stage projects started in April 2007. The projects are investigating the following areas:

- **Integrating Security Technology and Organisational Culture for Employee Risk** (BAE Systems and Loughborough University) – aimed at developing a novel organisational and human factors focused network security risk assessment package
- **Trust Economics** (Hewlett-Packard Ltd., Merrill Lynch, University of Bath, University of Newcastle and University College London) – aimed at developing a predictive modelling framework that assesses the effectiveness of the security policies that regulate the interaction between humans and information systems
- **The Analysis of Human Behaviour from Network Communication** (Chronicle Solutions and the University of Plymouth) – aimed at developing a potential technology solution for the analysis of digital communications in order to identify and act on potential security threats introduced by humans to information and IT services

- **CatalysIS – A tool to improve risk culture and identify human vulnerabilities in Network Security** (The National Computing Centre Ltd. and the University of Manchester) – aimed at improving attitudes towards risks both to and from information systems, specifically a software-based tool that provides a network security awareness programme that is tailored to the individual employee.

There is follow-up funding of up to £4m available for the successful projects. It is worth noting that the successful projects could generate a total of £125m of extra income from successful market penetration resulting from their research.

What next?

The NSIP has identified a number of other areas where the size of global opportunity and the UK's capacity to develop and exploit that opportunity is sufficient for it to focus on identifying other challenges. One such challenge is in ensuring privacy and consent in identity management infrastructures.

Digital identities are becoming increasingly important and will be a fact of life in the UK by 2010. These high assurance identities will be based on establishing the existence of an identity in society, which may initially be seen as privacy-intrusive, and by linking this pre-established identity to the individual. Such an identity could then form the master key to enabling many entitlement services.

This new identity infrastructure must offer assured privacy and depend on truly informed consent. Each time users sign into an identity service or enrol in an access control system, they will need to understand what information they are providing to whom – as well as how it will be used and further disseminated – before consenting to provide it. They will also need to be confident that only the information required for that particular entitlement would be provided.

The DTI, through the TSB's NSIP, is working with the Identity and Passport Service (IPS), the Home Office, the ESRC and the Engineering and Physical Sciences Research Council (EPSRC) to develop a work package that will sponsor a £10m, three-year research and development programme into how to balance the potentially intrusive nature of identity services and network security with users' expectations of privacy and consent. This research will be cross-disciplinary, combining social science with technological innovation.

An initial workshop is planned for 9 July 2007 to discuss and refine the areas of importance for that research, as well as to identify where the research is needed and where the UK has potential to develop world-leading commercial services. The findings of this workshop will help inform the structure and focus of an EPSRC sand-pit concept workshop to be held in early October 2007.

This has been a challenging year for the NSIP, but significant progress has been made and it is a case of 'watch this space' for further developments.

For more information on the NSIP visit:
www.dti.gov.uk/innovation/technologystrategy/innovation_platforms/page33796.html

For more information on other Innovation Platforms visit:
www.dti.gov.uk/innovation/technologystrategy/innovation_platforms/index.html

For more information on the DTI's innovation policy and Technology Programme visit:
www.dti.gov.uk/innovation/technologystrategy/index.html

Andrew Tyrer (andrew.tyrer@dti.gsi.gov.uk) is the Network Security Innovation Platform Manager of the DTI Technology Strategy Board.

RSA CONFERENCE EUROPE 2007

22-24 OCTOBER | EXCEL LONDON | UNITED KINGDOM

RSA Conference Europe will bring together information security professionals and leading technology and service vendors under one roof. This intensive three-day event will combine 100 tutorials, keynotes speeches, class-track sessions and special interest groups with an exhibition showcasing the very latest innovations in security.

The conference, which is jointly organised by ENISA, offers the opportunity to:

- Gain fresh insights into the latest security best practices and trends
- Listen to keynote sessions delivered by the industry's most respected leaders and innovators, including Bruce Schneier, internationally renowned Security Technologist and CTO of BT Counterpane, and Frank Abagnale, the subject of the film, "Catch Me If You Can"
- Attend sessions across 10 tracks including Authentication, Hackers and Threats, Developing with Security and Wireless
- Visit the RSA Conference Exhibition to discover the latest products, services and solutions
- Network with your peers and join the RSA Conference community

London calling

For the first time, RSA Conference Europe is being held in London, Europe's largest financial centre and the European headquarters of 33% of the Fortune Global 500. The ExCeL London campus, near Canary Wharf, has six on-site hotels to suit all budgets, excellent road and public transport links, and London City Airport is just 10 minutes away by car or taxi.

This three-day experience is unparalleled in scope, in quality, in reputation. Join the community, and become part of the future of information security!

Registration to the event is now open at:
www.rsaconference.com/2007/europe

Hungary Put on the Map of IT Security

Bence Birkas

Hungary recently held two conferences covering two important aspects of IT security. The Meridian 2006 Conference mainly involved policy-makers from the field of critical information infrastructure protection, while the joint TF-CSIRT/FIRST meeting provided an excellent forum for computer security incident response teams.

Meridian 2006 Conference – Budapest, 25-27 October 2006

This conference had as its theme the "connecting and protecting" of critical information infrastructures. The event aimed to establish Meridian as a process whereby good practice is shared and new co-operative relationships are fostered. Participants included senior officials involved in Critical Information Infrastructure Protection (CIIP) policy-making from the governments of 23 countries. The three-day event was organised by the Theodore Puskas Foundation of Hungary (the host of CERT-Hungary), and a renowned spa hotel provided an excellent venue with a chance for a little recreation alongside the busy conference programme. The organisation of the conference was supervised by a Steering Committee consisting of representatives from Hungary, the UK (CPNI), the USA (DHS), Sweden (SEMA) and the Netherlands (MinBZK), as well as Malaysia (MCMC) and ENISA.

On the first day of the event, the private sector had a chance to raise CIIP issues, which were followed up in workshops on the subsequent two days. In addition, tabletop exercises dealt with information sharing protocols. The conference provided the opportunity to present views and best practices on national CIIP policies.

The conference ended with the handover of the Meridian Presidency from the UK for the following year. The new president, Hungary, proposed the following actions:

- starting a quarterly Meridian Newsletter on CIIP issues
- promoting the Meridian process among the Central European countries, with emphasis on the newly joined countries
- promoting bilateral co-operation in the field of CIIP, providing a role model for learning from and implementing the strategies of mentoring counterparts
- taking European government-related CIIP issues further by representing Meridian efforts in EU bodies.

More details of the Meridian process can be found at www.meridian2006.org, as well as the previous editions of the Meridian Newsletter.

The next Meridian event will be held in Stockholm from 24-26 October 2007 and will be hosted by the Swedish Emergency Management Agency (SEMA). For more information, visit the event's web pages at www.meridian2007.org.

20th TF-CSIRT meeting – Budapest, 29-31 January 2007

CERT-Hungary, the governmental incident response centre, hosted the joint TF-CSIRT/FIRST meeting. The three-day event was held at the Budapest Technical University, and participants came mostly from the European CSIRTs, representing academic, national and corporate sectors. By courtesy of FIRST, a number of participants were welcomed from the Americas and Asia as well.

The programme was put together by TERENA and TF-CSIRT, and covered current organisational and Research and Development (R&D) issues. In addition, the Hungarian hosts had the opportunity to introduce their functions and activities. Presentations included updates on various ongoing projects from the field of R&D, such as CSIRTs and Grids, the RIPE Incident Response Team (IRT) Database, and the Geánt2 (GN2) Joint Research Activity on 'Security' (JRA2). Other topics included news about ENISA and TRANSITS activities, such as the feasibility study into a European Information Sharing and Alert System. The programme also provided several opportunities to share in-depth technical details at the hands-on classes, with the help of the FIRST (Forum of Incident Response and Security Teams) community.

The three-day event provided plenty of time for discussion and the exchange of ideas. Participants also had the chance for a taste of Hungarian hospitality, while the Hungarian hosts benefited from the pool of international expertise gathered together in Budapest.

Bence Birkas (bence.birkas@cert-hungary.hu) works in the International Relations section of CERT-Hungary.

eSignatures Standardisation Survey

European Commission

We invite you to make your own contribution to a revamped Electronic Signature standardisation scheme for Europe.

European Commission Study on the Standardisation Aspects of eSignatures: a public survey

SEALED, DLA Piper and A-cross Communications are currently conducting a public survey for the European Commission on aspects of eSignatures standardisation. This on-line survey aims to establish objective findings reflecting the market needs in this area. This is a perfect opportunity for all to make a contribution towards a revamped eSignatures standardisation scheme for Europe.

www.esstandardisation.eu

The survey will be on-line until the end of August 2007.

Measuring the Impact of Security Awareness in Lithuania

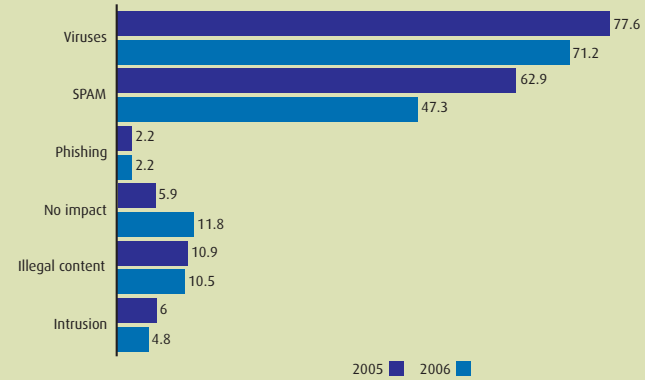
Rytis Rainys

The development of the Information Society is a priority in Lithuania. The rate of user subscriptions to mobile and Internet services increased from 3% in mid-2003 to 46% by the end of 2006. This is clear evidence that nowadays, for a significant proportion of society, many aspects of business and everyday life are dependent on electronic communication and its security .

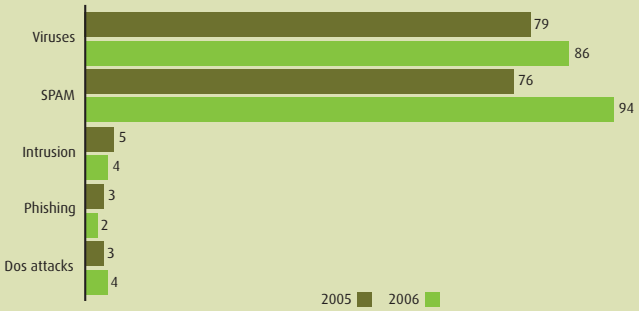
A survey was conducted in 2005 in order to identify the main problems of network and information security in Lithuania. The results demonstrated that almost 80% of home-users and enterprises had faced problems with computer viruses and spam (see first two diagrams below). Given that more than 150,000 viruses have been developed during the last 20 years and the fact that spam presently comprises 80%-90% of the total volume of e-mail, these results are not surprising.

The most vulnerable and unprotected part of the consumer sector is end-users. As the price of computers and Internet connection has dropped, the number of new Internet users has increased dramatically. When connecting to the Internet for the first time, a user needs constructive advice on the security issues and the possible threats that lie in this infrastructure. In Lithuania, network and information security activities in the last few years have been focused mainly on end-user education and awareness raising projects because only when users are aware of the potential problems can they meet the challenges of security.

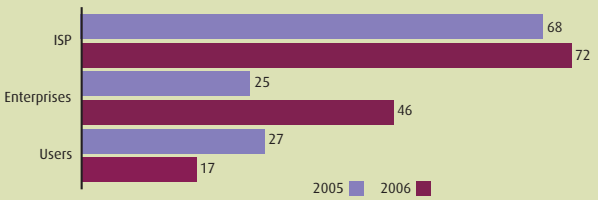
A number of awareness raising activities were undertaken in 2005 and 2006. In line with the European Commission programme 'Safer Internet', two dedicated Internet websites, www.esaugumas.lt ('e-security') and www.draugiskasinternetas.lt, were created and about 200,000 leaflets explaining phishing methods were distributed through the commercial banks of Lithuania. The national Computer Emergency Response Team (CERT-RRT) distributed several important alerts and recommendations on vulnerabilities.



Security incidents faced by users in 2005 and 2006 (%)



Security incidents faced by enterprises in 2005 and 2006 (%)



Users who incurred damage due to security incidents in 2005 and 2006 (%)

But solely raising awareness is not enough in order to protect users. Only a small section of informed customers take specific action to safeguard their computers and valuable data, even when many more know they should. To deal with this situation, it is necessary to improve the 'ready-to-use' tools and their distribution to customers, especially for new Internet users.

To that end a special public-private partnership project, 'Protect your computer!', was launched in Lithuania with co-operation between 16 partners from the public, private and civil sectors of society, to issue users with CDs containing security tools. The project was funded exclusively by the private sector. During a campaign in June 2006, 100,000 CDs containing security software packages were distributed in all regions of Lithuania, including rural areas, and also in 1500 Lithuanian schools. The CD offers advice and suggestions to PC users, including how to secure the privacy of their computer and the information contained on it, and contains easily installable software to combat cyber threats. A virtual CD is available on a special website from which more then 50,000 programme downloads have been recorded.

The impact of those awareness and 'ready-to-use' tools could be demonstrated by the results of the 2006 survey that showed decreasing numbers of end-users being confronted by computer viruses, spam, phishing or spyware (see first diagram left) – it was found that the number of end-users who suffered damage from security incidents decreased from 27% to 17%. However, an increasing proportion of enterprises and Internet Service Providers (ISPs) suffered damage from security incidents (see third diagram left) and this is the area where more effort should be targeted in the immediate future.

Rytis Rainys (rrainys@rrt.lt) is Head of the Network and Information Security Division in the Communications Regulatory Authority of the Republic of Lithuania.

ISSE/SECURE 2007

25-27 September 2007 Warsaw, Poland

Europe's Only Independent Security Conference

ISSE is Europe's leading information security conference, renowned for its rich educational content and unbiased perspective. ISSE's world-class conference programme is designed to educate and inform ICT security professionals, policy-makers and industry leaders on the latest developments in technology, solutions, market trends and best practice in a wide range of security topics.

Now in its ninth year, ISSE 2007 is poised to attract over 400 delegates from across Europe, providing an informal and stimulating environment for attendees to learn, share experiences and explore solutions with their European counterparts – focusing on security as a key component of business processes and electronic transactions and discussing related issues including return on investment, total cost of ownership, risk management and interoperability.

This year, ISSE will take place in Warsaw and will be jointly organised with SECURE 2007, Poland's longest running annual security conference. Through presentation sessions, debates and workshops, ISSE 2007 will focus on key security topics such as:

- Trusted Computing
- Information Security Management
- Awareness Raising
- Identity Management
- Interoperability & Security Standards
- European Policy Issues
- Mobility Security
- Emerging Technologies

Fast & Secure On-line Registration

For registration and further information including the full conference programme, please visit www.isse.eu.com.

ISSE/SECURE 2007 Organising Partners

eema enisa European Network and Information Security Agency NASK

wistp'07

Workshop in Information Security Theory and Practices

Angelos Bilas

WISTP'07 - the First Workshop on Information Security Theory and Practices: Smart Cards, Mobile and Ubiquitous Computing Systems - was held from 9-11 May 2007 in Heraklion, Crete, Greece. The workshop was co-organised by: FORTH-ICS, Greece; ISG-SCC, Royal Holloway, University of London, UK; and XLIM, University of Limoges, France.

With the rapid development of information technologies, computer systems – and especially embedded systems – are becoming more mobile and ubiquitous, increasingly interfacing with the physical world. Ensuring the security of these complex and yet resource-constrained systems has emerged as one of the most pressing challenges today.

The aim of this first workshop was to bring together researchers and practitioners in related areas and to encourage the exchange of information and co-operation between the research community and the industrial/consumer community. The event attracted excellent keynote speakers, had a strong technical programme and was supported by prominent sponsors, including ENISA.

The workshop consisted of technical paper presentations, one special session for student papers and talks by five invited speakers. To contribute to the structuring of the community, a networking meeting to discuss EU FP7 projects proposals took place on the third day of the event.

For more information on the technical programme, please visit http://wistp2007.xlim.fr.

Angelos Bilas (bilas@ics.forth.gr) is an Associate Professor in the Department of Computer Science of the University of Crete in Greece, and a researcher at the Institute of Computer Science (ICS) with the Foundation for Research and Technology-Hellas (FORTH).

Public Consultation on the Future of ENISA
European Commission

As part of the mid-term evaluation of the European Network and Information Security Agency, the European Commission has launched a Public Consultation in June, which will be open until **9 August.** The consultation allows anyone from the wider public to express their opinion by answering a series of questions related to the remit and the structure of ENISA, which is intended to guide further discussions on the future of the Agency.

More information and the interactive questionnaire can be found under
http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=EnisaFuture

For further information on the evaluation process of ENISA, please visit
http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=3462

ENISA Short News – Second Quarter 2007

Panagiotis Trimintzios

Legal Overview in Risk Management Risk Assessment
ENISA has produced a report with the first overview of legal aspects of Risk Management/Risk Assessment (RM/RA). This report is a unique, new compilation of normative texts, providing policy-makers and business security experts with a strategic tool for identifying key legal RM/RA requirements.
(www.enisa.europa.eu/pages/02_01_press_2007_06_26_legal_regulation_in_rm.html)

Collaboration with ITU in order to launch NIS Standards portal
In collaboration with the International Telecommunication Union, ENISA has launched a new portal for IT security standards, for the first time giving Europe one single access point for IT security standards.
(www.enisa.europa.eu/pages/02_01_press_2007_06_07_ENISA_ITU_new_portal.html)

ENISA comments on the massive cyber attacks against Estonia
(www.enisa.europa.eu/pages/02_01_press_2007_05_24_ENISA_commenting_on_massive_cyber_attacks_in_Estonia.html)

Studying providers' countermeasures against spam
ENISA is conducting a study on the technical and organisational measures that European electronic communication services providers take with regard to IT security and the countermeasures they have introduced to combat spam.
(www.enisa.europa.eu/pages/02_03_news_2007_06_08_ENISA_ISP_Spam.htm)

Meeting between ENISA and Spain
On 21 June, a bilateral meeting between the Secretary of State of Spanish Government for Telecommunications and Information Society, Francisco Ros, and the Executive Director of ENISA, Andrea Pirotti, took place at the Spanish Ministry of Industry. Possibilities for co-operation were the main items on the agenda.
(www.enisa.europa.eu/pages/02_03_news_2007_06_27_enisa_spain_meeting.html)

Feasibility Study on European Information Sharing and Alert System (EISAS)
Technical Frequently Asked Questions and a Presentation on the Draft Study are now available on-line.
(www.enisa.europa.eu/pages/faq_technical.html)

New Chairperson heading the Management Board of ENISA
At its recent meeting, the Management Board of ENISA elected Prof. Reinhard Posch from Austria by acclamation as its new Chair.
(www.enisa.europa.eu/pages/02_01_press_2007_04_18_ENISA_New_Chairperson.html)

ENISA meets with IPA Japan
On 24 May, ENISA representatives met with representatives from the IT Security Center (ISEC) of the Information-technology Promotion Agency (IPA), which is the Japanese Government Organisation under the Ministry of Economy, Trade and Industry. The main items on the agenda were ways to achieve collaboration between ENISA and this important Third Country Agency.

ENISA's Joint Events
ENISA is supporting a number of events throughout Europe in 2007. A full list is now available on-line.
(www.enisa.europa.eu/pages/04_01.htm#2007)

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

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

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

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

European Communities, 2007 Reproduction is authorised provided the source is acknowledged.