ENISA Quarterly

enisa European Network and information Security Agency

IN THIS EDITION

Early Detection, Warning and Alerting Systems

Vol. 3, No. 1, Jan-Mar 2007

A WORD FROM THE EXECUTIVE DIRECTOR

To mark the European Union's (EU) 50th birthday we have recently witnessed a three-day commemoration in Crete, where ENISA is based. Speaking in mythological terms, Crete is indeed the cradle of Europe, as it was here that Zeus brought Europa centuries ago. So with one of the EU's 28 'satellite' agencies scattered around Europe, ENISA, here on the island, Crete was a natural starting point for celebrations, and we participated actively in these events. Three Members of the European Parliament participated in the public debates which were organised on Europe and on the role and future of our Agency.

On 22 March we welcomed the members of the Management Board to Crete for their 10th plenary meeting. This took place in the City Hall of Heraklion, and was inaugurated by the Greek Deputy Minister for Development, Mr. Neratzis.

The Management Board discussed a series of issues and provided ENISA with long and short term recommendations, as well as broad guidelines for future operations. One of the highlights was the election of a new chairperson of the Management Board, Prof. Reinhard Posch from Austria, who was elected by acclamation.

Prof. Posch commented:
"I would like to extend my gratitude towards the Management Board for their support in the election of the new Chair. At the same time I would like to stress the constructive work of my predecessor Chair, Mrs. Kristiina Pietikainen, for her highly constructive and efficient work during the installation phase of ENISA."

As the Executive Director, I can only agree and support this statement.

Since the last issue of the EQ, I have had the pleasure of visiting the two new members of the EU family, Romania and Bulgaria, and we have established ways to strengthen our collaboration in the field of Network and Information Security (NIS) for the years to come. We have also received a visit from a Romanian delegation, which confirmed our mutual commitment.

We flew to Brussels recently, and addressed the European Parliament's committee on Industry Research and Energy (ITRE). Our presentation focussed on ENISA's achievements and was very well received by the members of the committee.

I am confident that this issue of ENISA Quarterly will provide food for thought on new concepts in NIS, and I encourage you all to participate actively and contribute to this joint forum for European NIS discussions.

Sincerely,

Andrea Pirotti
Executive Director, ENISA

ISSN1830-3609

A WORD FROM THE EDITOR

There are numerous Network and Information Security (NIS) incidents occurring on a daily basis. How well and fast we are informed about these incidents is an important factor in increasing our ability to respond effectively to current threats, but it is equally important that future systems are designed to be secure and to withstand both current and emerging threats.

There are many NIS incident monitoring and reporting information sources out there. These sources vary in many ways, including the reporting time, the degree of detail provided such as the abstraction of information (from raw data, statistics etc.), the technical complexity (from specialised monitoring infrastructures to generic web portals), their capabilities on monitoring and collecting data, the actual facility that is monitored (public Internet, closed infrastructure etc.) and the sector that co-ordinates the monitoring activity (public, private).

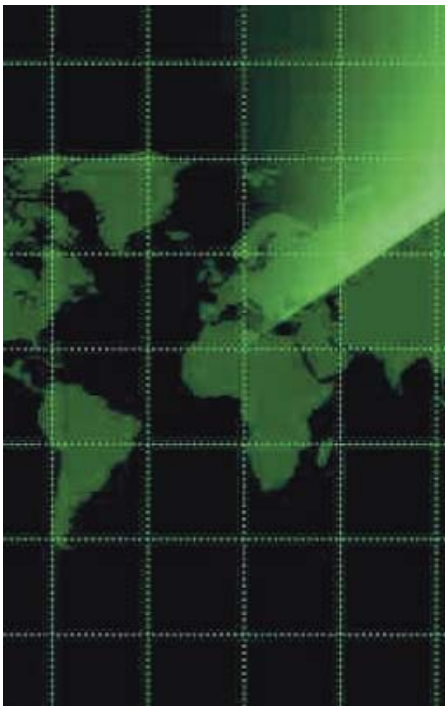
In this issue of ENISA Quarterly (EQ), we try to cover the broad area of early warning, alerting and incident information sharing systems from a number of different angles. Though we have not tried to be exhaustive nor to undertake a survey in the field, we hope the articles will shed some light on this area, and help give those who are interested a glimpse of the main topics and concerns involved with these systems. A complete study on a similar topic is underway in ENISA (see p.12).

Prof. Pohlmann, a member of the Permanent Stakeholders Group (PSG) established by ENISA, opens this issue with an article on a probe-based Internet Early Warning System, focusing on the required modular functionality that aims to gather traffic statistics and from them to identify an abnormal state. The article by Prof. Markatos, also a member of the PSG, and his team describes two research projects both of which are early detection systems and wide-scale infrastructures targeting real-time, zero-day cyberattacks, using strategies such as polymorphism and honeypots to trap attackers. While both Prof Pohlmann's and Prof. Markatos' articles focus on monitoring the Internet, the contribution by Lluis Mora and Xavier Panadero looks at a different target infrastructure by introducing us to the security threats to SCADA systems, and the need for detection, warning and counteracting these threats. ENISA is supporting a conference being organised by FIRST, the Forum for Incident Response and Security Teams, which aims to encourage co-operation and information sharing between the teams, CERTS, that monitor and respond to NIS incidents.

The article co-authored by our own experts, Marco Thorbruegge and Slawomir Gorniak, provides the background, plans and first results from a feasibility study of a European Information Sharing and Alerting System, which has been initiated at ENISA in response to a request from the European Commission. Our expert Carsten Casper discusses another ongoing study at ENISA that looks into the issues of the correlation of incident data gathered from different sources and whether it is possible to use this data to measure the impact of related policies on consumer confidence and the number of observed incidents. Isabella Santa of ENISA's Awareness Raising unit writes about the unit's extensive efforts to help and guide those trying to raise awareness, and to maximise the unit's impact by publishing one of its most important deliverables in three different languages. Finally, Silvia Portesi provides an overview of ENISA's efforts towards assisting the Member States by providing an efficient brokerage of NIS good practices.

We open the contributions from the Member States with a very interesting article from the Netherlands, in which Menno Muller describes the setting up of an effective early warning system, focusing primarily on the lessons learned, while also providing some of the technical details. The other articles from the Member States have come from the open call for contributions. Arie van Bellen updates us on the results of a year's activities in the awareness raising programme in the Netherlands and outlines future plans. Veni Markovski provides a practical insight into how Bulgaria, one of the countries which very recently joined the family of the European Union, fights cybercrime. Finally, this issue closes with a description of the Dutch research programme on Information Systems and NIS, and the important projects that are funded within that programme.

We are delighted with the response to both the request for articles for this thematic issue and the open call for contributions to EQ. We plan to have more thematic issues in the future. Please visit our web pages, www.enisa.europa.eu/eq/, for all the latest news and plans for our magazine.



In addition, we would be very happy to hear your ideas and feedback for future editions of EQ, and of course to continue to receive your valuable articles. In this way you can have your say in the European dialogue for enhanced NIS and reach out to a wide audience both inside and outside the EU. EQ's popularity is graphically demonstrated by the fact that each issue is downloaded more than 10,000 times!

Finally, I would like to thank all the authors of the articles in this issue, as it is their contributions that make this 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

Probe-based Internet Early Warning System

Prof. Norbert Pohlmann

The constantly growing importance of the Internet for our knowledge and information society makes it necessary to analyse and be acquainted with its status beyond the limits of the individual network operators. Only if we have precise knowledge of normal behaviour and its status is it possible to detect anomalies which influence the functionality of the Internet.

A probe-based Internet Analysis System is currently being designed and developed in a research and development project of the Institute for Internet Security at the University of Applied Sciences in Gelsenkirchen, in co-operation with the German Federal Office for Information Security (BSI). This project aims to create and analyse local and global perspectives of the Internet in order to facilitate the generation of early warnings.

Particular focal points of the project are the collection and optimisation of information, in compliance with data protection regulations, with the aim of storing data long term to allow the analysis of trends and developments over extended periods.

Aims and tasks of the Internet Analysis System

The objectives of the Internet Analysis System are on one hand to analyse local communication data in identified sub-networks of the Internet while, on the other, the system aims to create a global perspective of the Internet by combining a large number of local perspectives.

The main functions of the Internet Analysis System are divided into the four subsystems of pattern formation, description of the actual status, alarm signalling and forecasting.

Pattern formation: The main objective of pattern formation is to perform a comprehensive analysis and interpretation of the communication parameters of Internet traffic, with the aim of detecting technology trends, interrelationships and patterns which represent the status, behaviour and perspectives of the Internet. On the basis of this knowledge, a search is carried out for anomalies among the current measured values, and the events that lead to status changes are then analysed and interpreted. It is important to distinguish whether the anomalies are caused by 'natural' phenomena, for example, a technological change, or whether they are attributable to a cyberattack.

Description of status: Another important function of the system is the visual representation of the Internet status in a similar way to a weather or traffic jam map. Intuitive depictions are being developed in which the most important parameters are discernible at first glance.

Alarm signalling: With knowledge about the current status of a communication line and the use of historical, i.e., previously collected, information (knowledge base), it is possible in the case of significant changes to traffic volumes or communication data to generate a warning message. This would then trigger the identification and deployment of measures in order to protect and maintain the normal functioning of the Internet.

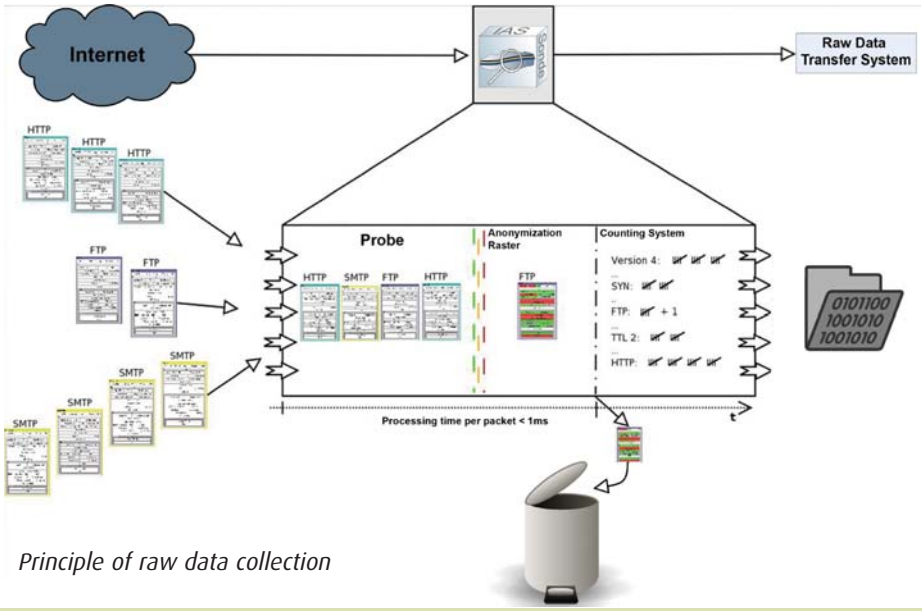
Forecasting: Through the examination and analysis of the extrapolated profiles, technology trends, interrelationships and patterns, it will be possible by means of an evolutionary process of the acquired results to forecast Internet status changes. In this manner it is possible to detect indications of attacks and important changes at an early stage and predict the effects of the damage.

Principle of raw data collection

The diagram below shows the principle of raw data collection by the probes. This is divided into three sections. Firstly, the packets are captured and fed into the probe. In the diagram we see packets from three different application sessions: packets related to web traffic (Hypertext Transfer Protocol - HTTP), packets related to file transfer sessions (File Transfer Protocol - FTP) and packets related to an e-mail exchange session (Simple Mail Transfer Protocol - SMTP). The probe is located in the middle section of the diagram. The packets of the three applications are accessed passively by the probe one after the other in their random order and evaluated.

Secondly, every packet that is accessed is channelled through several analysis filters, each of which is responsible for a certain protocol. These filters evaluate the formally defined standard communication parameters in the protocol header at the various communication levels which are not relevant to the data protection laws.

Finally, the relevant counters allocated in the counting system are incremented according to the header information of the packet. The frequency of certain header information is recorded in the same way as on a tally sheet. For example, in the diagram below, the access to the FTP packet



Principle of raw data collection

is recorded by incrementing the FTP counter by 1. The raw data are therefore aggregates of counters, i.e., counters of communication parameters that have appeared at the various communication levels over a defined period. The packet is immediately deleted physically, i.e., irreversibly and without trace, by the probe.

Reconstruction of the context of a packet or of a single communication parameter is neither possible nor necessary, for privacy reasons. At predefined intervals the counter readings, i.e., the raw data, of the probes can be transmitted to the raw data transfer system. All of this information is completely anonymous, as shown in the chart below.

ID	Description	Count
131134	IP (Protocol Number 6)	: 18.854.151
131145	IP (Protocol Number 17)	: 1.123.149
327708	TCP (Flags: SYN)	: 334.435
327723	TCP (Flags: FIN/ACK)	: 480.697
327724	TCP (Flags: SYN/ACK)	: 275.779
545857	HTTP (Request Method POST)	: 2.026
545861	HTTP (Request Method GET)	: 293.616
545863	HTTP (Request Method HEAD)	: 18.992

Counting system table in the probe

In the right-hand column of the table are the counter readings for the header information which is specified on the left. Each row in the table represents a counter. For example, line 2 of the raw data shown indicates that 1,123,149 packets with the IP protocol number 17 (User Datagram Protocol-UDP) appeared within the measurement period.

Results from the Internet Analysis System

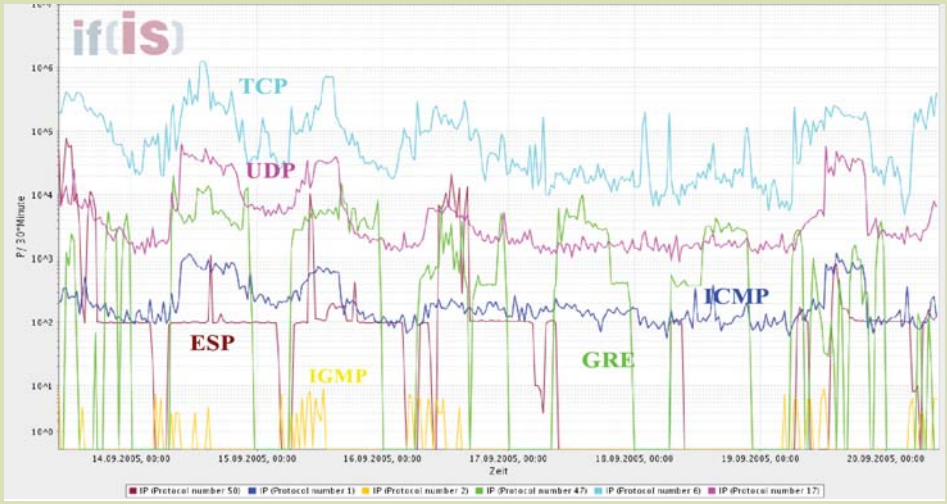
Some of the results which have been acquired are presented in the first chart below to illustrate the usefulness and the potential of the Internet Analysis System. At present there are approximately 600,000 different counters of communication parameters incorporated for the various communication levels. This large number clearly shows how complex the results can be.

Transport protocol distribution

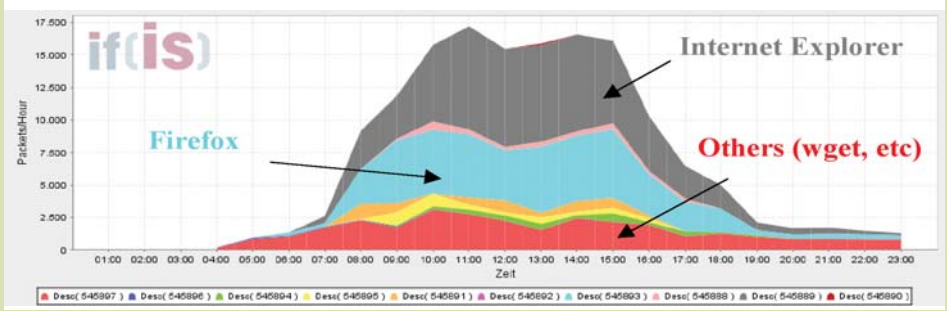
The first chart below shows the distribution of the observed packets to transport layer protocols over a period of several days for a specific communication line. From past experience, the Internet Analysis System recognises the profile and the standard deviation and can therefore display an indication of typical behaviour. Additionally, one could determine the use of certain protocols, enabling, for example, capacity planning for the use of Virtual Private Networks established with the Encapsulating Security Payload (ESP) protocol. Protocol dependencies can also be detected: the number of UDP packets appears to be proportional to that of Transmission Control Protocol (TCP) packets, which can be attributed to the dependencies of HTTP and Domain Name Service (DNS) packets.

Browser usage distribution (technology trend)

The diagram at the bottom of the page shows the distribution of various browsers over a period of one day for a specific communication line. We can see the daily profile of the various browsers. The difference between manual use, e.g., with Internet Explorer and Firefox, and automatic use, e.g., with wget, over the course of the day is clearly visible.



Protocols of the transport layer



Browser usage distribution over time

Conclusions

With the help of a probe-based Internet Analysis System, it is possible to acquire raw data continuously which provide a statistical reflection of Internet traffic. Through the evaluation of the raw data at the various communication levels, such as the network layer, the transport layer and the application layer, it is possible to derive very detailed information. By analysing the results of various probes, it is possible to depict a global perspective of the Internet and define warning levels in the case of problems, such as infrastructure failures or attacks. Further analysis of the raw data could enable the forecasting of trends in the use of protocols, network services and attacks.

The Institute for Internet Security has successfully completed the second development phase in co-operation with the BSI. The system has been validated operationally. Partners are now being sought to join the network and operate further probes and evaluation systems. Organisations which wish to operate only one probe will receive an informative report about their network traffic once a month from the central evaluation system.

In addition to operation of the Internet Analysis System, the project will also move forward into a third phase of development and research. In order to obtain additional information, further protocols will be implemented and existing ones extended. In addition, the evaluation modules and attack detection will be expanded.

In the field of research, statistical methods and data mining, algorithms will be used to design intelligent processes to accelerate the evaluation process. The quality of the results is steadily improving, owing to continual analysis and the experience gained in the analytical process.

Further information can be found on the following web pages: Institute for Internet Security, www.internet-sicherheit.de
Federal Office for Information Security (BSI), www.bsi.de/english/index.htm

Prof. Dr. Norbert Pohlmann (Norbert.Pohlmann@internet-sicherheit.de) is a professor at the Institute for Internet Security of the University of Applied Sciences Gelsenkirchen and a member of the Permanent Stakeholders Group (PSG) established by ENISA.

Real-time Monitoring and Detection of Cyberattacks

Prof. Evangelos Markatos, Kostas Anagnostakis, Spyros Antonatos and Michalis Polychronakis



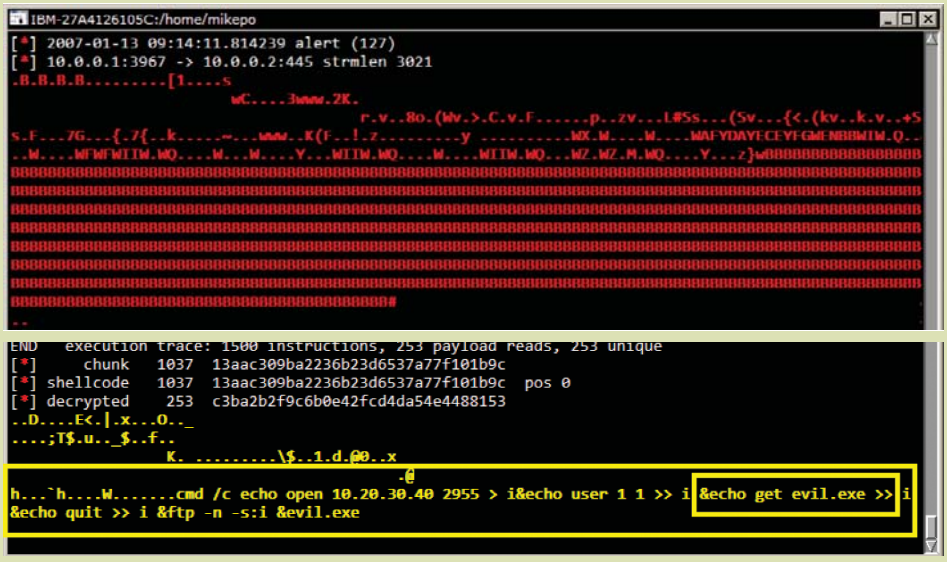

Over the last few years we have witnessed an increase in the magnitude, sophistication and speed of Internet-based cyberattacks. Motivated by fun, fame or fortune, attackers increasingly target home computers, which are then used as a springboard to perform further malicious activities, such as sending SPAM e-mail, launching Denial of Service (DoS) attacks and co-ordinating hordes of compromised computers, called 'botnets'. Such compromised computers have also been used against their legitimate owners by invading their privacy, spying on their e-mail, stealing their passwords and even blackmailing them.

Having realised the scale, ferocity and potential impact of such planet-wide Internet-based cyberattacks, the Distributed Computing Systems Laboratory at FORTH-ICS has set up and is currently co-ordinating two European projects, LOBSTER and NoAH, which target the early detection, fingerprinting and mitigation of cyberattacks. Complementary in their technical approaches, but sharing the same goal of detecting sophisticated attacks early enough, both projects have already started to produce their first success stories.

LOBSTER

LOBSTER (Large Scale Monitoring of Broadband Internet Infrastructure, www.ist-lobster.org) uses a passive network monitoring approach to detect attackers trying to penetrate legitimate computers. LOBSTER has already deployed several sensors throughout Europe, which monitor the traffic on the Internet in order to gain a better understanding of its performance as well as to spot any security incidents. Capitalising on state-of-the-art monitoring software and advanced detection heuristics, LOBSTER examines the network traffic coming in to ordinary computers for possible signs of intrusion.

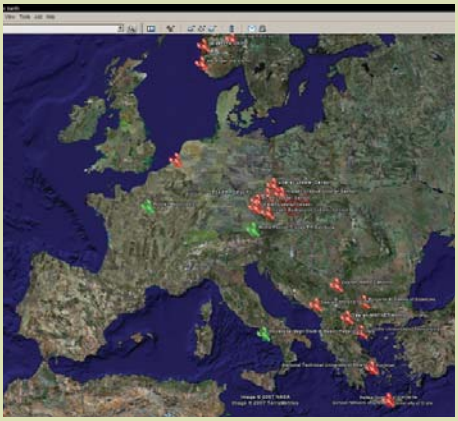
To evade such detection mechanisms, cyberattackers have developed sophisticated polymorphic attack vectors; that is, they have managed to transform their attacks into innocent-looking series of characters which at first glance do not look like part of a malicious attack. To counter polymorphic cyberattacks, LOBSTER has developed advanced polymorphism detection mechanisms that manage to inspect deep inside network packets beyond their seemingly innocent exteriors to discover any hidden attacks beneath.



The content of an incoming network packet (in red) captured by a LOBSTER sensor on the island of Crete. Although apparently innocuous, when 'executed' by a virtual machine on the LOBSTER sensor, these red characters transform themselves into the yellow characters shown in the second part of the diagram which instructs the victim computer to download and execute a cyberattack.

For example, the diagram below left shows the content of an incoming network packet (in red) captured by a LOBSTER sensor on the island of Crete. These red characters do not seem to contain any attack. However, when these red characters are 'executed' by a virtual machine on the LOBSTER sensor, they slowly but steadily transform themselves into the yellow characters shown in the second part of the diagram which, in ASCII human-readable form (shown in the big yellow box), force the target computer to connect using ftp to IP address 10.20.30.40 (anonymised form of the real IP address), to download file 'evil.exe' (shown in the small yellow box) and to execute it.

The LOBSTER sensor infrastructure has already collected dozens of such attacks which are properly anonymised and will eventually be shared in the public domain. It should be emphasised that these attacks captured by the LOBSTER sensors are against real computers (live traffic) including PCs, laptops and even IP telephones!

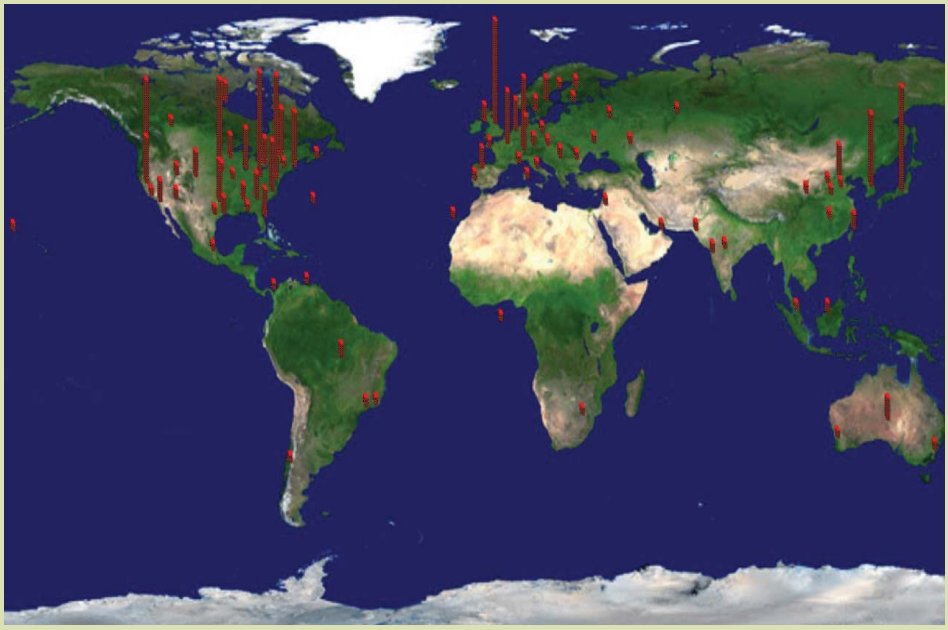


The geographic location of LOBSTER sensors

NoAH

While LOBSTER sensors monitor real-time network traffic aimed at live computers, the NoAH project, a European Network of Affined Honeypots (www.fp6-noah.org), monitors the shadows, the dark spaces and the back corners of the Internet in its quest to detect, fingerprint, and mitigate cyberattacks based on state-of-the-art honeypot technology.

A honeypot is a computer which usually does not serve any ordinary users and whose main value is in being compromised by attackers. Thus, honeypots usually listen to unallocated IP addresses on the Internet (which are usually called 'dark address space') in order to detect any unusual activity. By luring attackers and by willingly getting compromised, a honeypot captures a wealth of information about the attackers, about the mechanisms they use to



Graphical representation of the geographic origin of cyberattacks captured by FORTH's honeypots.

penetrate computers, about the software they download and about other computers they communicate with.

The attack information can be used then to understand the attacker's tactics, provide a fingerprint for it, and generate a signature that can be used by Intrusion Detection/Prevention Systems (IDS/IPS) for example, to defend against this kind of attack in the future. The diagram above shows the geographic origin of such attacks captured by NoAH honeypots installed at FORTH.

To empower ordinary home (and small business) users in the fight against cyberattacks, FORTH has developed 'Honey At Home' (honey@home, www.honeyathome.org/), which is a light-weight software-only honeypot that monitors unused IP addresses or port ranges of home-users, reporting to central NoAH honeypots all suspicious activity which might be a potential attack to that home-user. Based on sophisticated taint-based analysis, the central NoAH honeypots in turn differentiate between random activity and targeted attacks.

Conclusion

In conclusion, by monitoring live network traffic and unused IP address space and searching to detect, fingerprint and mitigate attacks spreading on the Internet, both projects LOBSTER and NoAH are already making tangible contributions towards early real-time cyberattack detection.

Evangelos Markatos (markatos@ics.forth.gr) is the director of the Distributed Computing Systems laboratory at FORTH-ICS, a Professor of Computer Science at the University of Crete and a member of the Permanent Stakeholders Group established by ENISA.

Kostas Anagnostakis (kanag@ics.forth.gr) is a researcher at I2R in Singapore and visiting associated researcher at FORTH-ICS.

Spyros Antonatos (antonat@ics.forth.gr) is a member of the Distributed Computing Systems laboratory at FORTH-ICS and a Ph.D. Candidate at the University of Crete.

Michalis Polychronakis (mikepo@ics.forth.gr) is a member of the Distributed Computing Systems laboratory at FORTH-ICS and a Ph.D. Candidate at the University of Crete.

Building an Effective Early Warning System

Urs E. Gattiker

There are a number of myths related to early warning systems (EWS). One would have you believe that an EWS will make a difference to security status and will better protect the information assets of citizens, end-users and Small and Medium-sized Enterprises (SMEs). Moreover, some governments feel that the introduction of an EWS adequately addresses the security challenges for 'A single European Information Space' (for all the seven myths about Early Warning Systems see http://cytrap.eu/blog/?p=64).

This article discusses how to set up and operate an EWS efficiently in order to help raise awareness and provide the tools that enable users to better protect their information assets. The article is one step on the long journey towards a higher level of awareness of security by users and, most importantly, towards improving the prevention of cyberattacks.

Defining the target group

Before launching an EWS one must define the objectives for such a venture in order to be able to assess whether it was a success afterwards (see: Continuous improvement of an EWS – the key to success – http://cytrap.eu/blog/?p=34).

Providing information that helps to improve the preventative capacity of an SME or a self-employed person is somewhat different from what is needed to improve security for a home-user's PC. But even for home-users, the most effective approach differs according to the different users (age, background etc.). For instance, teenagers tend to prefer Instant Messaging for communicating, while silver surfers use e-mail for the most part. Such differences do, of course, have major implications regarding awareness raising and prevention.

The checklist opposite addresses these issues in more detail by focusing on eight critical areas that must be addressed to maximise the added value of an EWS and minimise the risk of failure.

➲

CHECKLIST: awareness raising and security protection with EWS – the eight steps to success

Benchmarks and security metrics are needed to assess the performance and added value provided by an EWS. To address security metrics strategically, however, some critical issues must be discussed and defined beforehand.

1) **Define which target groups will be served**
Risks if ignored: The lack of sensitivity to the differences in users' needs, desires and preferences will reduce the value they will give to the content and output produced. As far as the security of Information Technology (IT) is concerned, what a silver surfer (i.e., an older user) might need is not the same as what a teenager might be interested in.
Possible solution: Target groups must be identified clearly, for example, home-users or SMEs, thereby enabling the EWS to provide content that is seen as highly relevant and helpful by the group to be served.

2) **Provide the warning content in a language easily understood by the identified target group**
Risks if ignored: Most of the time, the information that a technical person needs to extract from an alert makes little sense to a non-technical user. In fact, the latter may just not read the advisory being provided if it is too technical. On the other hand, if the information provided is not technical enough, a system administrator may neither trust the source nor have confidence in its output.
Possible solution: Use the appropriate language for each target group and separate technical from non-technical information.

3) **Issue alerts and warnings in a timely fashion**
Risks if ignored: Users might be informed by the local news cast before they receive the alert from the EWS. This will decrease their trust and confidence in the alerting services offered.
Possible solution: Either avoid distributing warnings or else make sure that high quality advisories can be issued quickly (for example within 8 hours) including during long public holidays such as Easter, Christmas and New Year. Continuous coverage may be a good marketing tool, but it is often unnecessary. In addition, a number of Computer Emergency Response Teams (CERTs) which claim to issue warnings 24/7 fail to do so on long weekends or overnight. This undermines people's trust in such services.

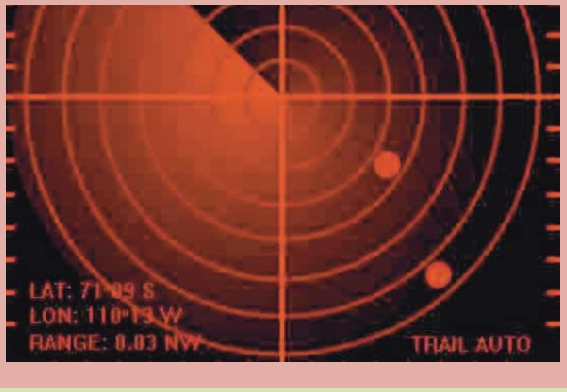
4) **Provide services to help improve a user's security position**
Risks if ignored: An enhanced security culture is unlikely to develop if the user does not stop taking risks with spam or phishing mails.
Possible solution: Focus on providing information that can be used immediately to improve the protection of the user's systems. An example would be issuing security guides that outline to a user in easy to follow instructions how to mitigate or isolate a threat identified today, well before the vendor releases the necessary patch, which may take anything from 15–120 days.

5) **Refrain from duplicating existing services but strive to offer added value**
Risks if ignored: Simply issuing virus alerts will just duplicate vendor services and is therefore unlikely to add significant value. In any case, knowing about today's Trojan horse attack does not prepare the user for the next pandemic.
Possible solution: Identify and define a service or niche that will add value in the eyes of today's subscriber and tomorrow's reader. In turn, refraining from duplicating vendor services will increase the value for the recipient.

6) **Identify performance targets including the security metrics that help to achieve strategic objectives**
Risks if ignored: Hoping to achieve one objective, while the reward, effort and resources are put into unrelated tasks certainly lowers overall performance. An EWS may obtain funding for an awareness campaign, while the funding agency is hoping that home-users become more careful about protecting their information assets, such as passwords, usernames, national ID numbers and banking information, against cybercrime.
Possible solution: Security metrics must be developed to help assess how effective EWS awareness is in achieving a lower number of reported cases, for example of identity theft in the target group. Hence, the strategic objective and how it will be put into operation to measure performance, i.e., the security metrics to be used, must be identified before initiating the EWS operations.

7) **Avoid security metrics or Key Performance Indicators (KPIs) that fail to take mediating and moderating factors into consideration**
Risks if ignored: Data collected via a user survey in regions A, B and C may suggest that 80, 90 and 50 percent of respective respondents had at least five or more serious virus incidents within the last year. But this information on its own will be meaningless unless the factors that might affect the results are clearly indicated.
Possible solution: For example, it might be advisable to check and control for the potential effect in cases where respondents had their Internet Service Providers (ISPs) scan their incoming and outgoing e-mail for malware infection(s). Other control variables might be age and gender. Once these factors have been taken into account, it might be very interesting to find out what moderating or mediating effect an EWS awareness campaign might have had on the uncontrolled variables, such as malware infections.

8) **Identify performance targets that enable participants to use different approaches**
Risks if ignored: In addition to providing measurable controls of the effect of EWS on malware incidents due to the scanning of e-mails for malware by the ISP, particular situations might require different approaches to awareness and prevention.
Possible solution: Similar performance targets across settings should be identified if appropriate but, most importantly, differences must be taken into careful consideration (various Windows editions, Linux users). For example, if botnets are an issue in one region, an awareness raising campaign can be judged successful if there was a clear drop-off in the number of discovered botnets after the campaign was launched. In another region the prevalence of wireless networks used in private homes might suggest an awareness campaign focusing more on that issue would be more effective than targeting botnets.



The eight points in the checklist are discussed in detail below, in particular how they relate to KPIs for measuring the rise in awareness achieved with EWS.

Awareness raising will help but....

When raising awareness about security issues, one must always target a clearly defined user group which, based on its behaviour, is vulnerable to specific threats. To illustrate, if youngsters are unaware that the Bluetooth connection on their mobile phones is turned on, it will make them vulnerable to specific attacks. In order to reduce this vulnerability, therefore, users must first be aware that this vulnerability exists and, second, must change their behaviour by switching Bluetooth off when it is not needed.

If awareness raising efforts are productive, they will result in behavioural change. Changing one's behaviour, therefore, is the key to better security because that alone will reduce one's risk of becoming the victim of an attack.

Safer surfing requires behavioural change – Good KPIs can help

Focusing the EWS services on the target group is critical. It is also obvious that the information provided (see point 2 in the checklist) should be customised in a form and format to suit the targeted community. Making users change their on-line behaviour to reduce the risk of them becoming a victim of cyberattacks must be a key issue (see point 4 in the checklist). Hence, awareness raising efforts should focus on how much they have encouraged and continue to encourage people to behave in such a way that their on-line risk is reduced. Knowing about privacy and security is commendable, but handling those issues following best practice is better.

In turn, KPIs should not be limited to measuring only how successful awareness raising campaigns are but instead must also address and measure how much behavioural change is related to these efforts. An example could be to assess if the awareness campaign reduced the reported cases of identity theft or the number and size of botnets that were discovered.

Why benchmarks could let us down

As one might conclude from the above, the identification and developing of KPIs is a challenge, to say the least. KPIs or security metrics used to assess the effectiveness of such efforts must differ to suit varying situations KPIs cannot be based solely on the number of people who have received a security tip, guide or alert or who have been informed via the media. A more practical KPI is one that focuses on measuring the outcome, for example behavioural changes

by users due to awareness raising interventions, based on certain activities.

Because of this, security metrics are types of key indicators that are becoming increasingly important in the IT security and risk management field. Such metrics help in assessing the effectiveness of awareness campaigns and the implementation of security policy in organisational settings. For instance, large corporations tend to use security metrics such as:

- viruses detected in user files - 92.3%
- viruses detected in e-mail messages - 92.3%
- invalid logins (failed password) - 84.6%

While these numbers are definitely important, their usefulness at a strategic and policy level is limited. For instance, while virus files may be detected, having an updated anti-virus programme mitigates this risk considerably. Not clicking on the virus-infected attachment further reduces this risk.

KPIs must be linked to the efforts undertaken by, or performance targets given to, an EWS. To illustrate, if an awareness campaign is being prepared, how will its success be measured? What will be the deciding factors as to whether the campaign is judged a success or not.

The future of Early Warning Systems

Unfortunately, most public EWS services, regardless of the target group they try to reach, provide the same fare regarding awareness raising and prevention services. Surely, SMEs have different needs to government departments, and home-users are not a homogenous group (silver surfers use different applications from those used by teenagers).

As the checklist shows (especially points 7 and 8), Gmail, CyWorld, Myspace, Skype and other Web 2.0 developments are new services which are fast becoming the next disruptive technology for CIOs (Chief Information Officers) and policy makers. Young employees were the first who began using these services from home and whilst still at school. They are now bringing these tools and methods with them into the workplace.

Finally, if moderating variables, such as a user's age or the type of operating system (Windows 95 versus Windows XP versus Linux) and the software used, for example, open source versus proprietary software, have not been taken into account, findings cannot be interpreted coherently and conclusions drawn may give rise to more questions – if not outright confusion – than clarification. To this end, the fact that some European countries' are moving towards the use of more and more open source software will surely result in the need for different strategies for achieving better information security awareness. To illustrate, France's push to use open source in public administration (see http://cytrap.eu/blog/?p=114) will result in different security risks and outcomes for home-users, compared with a country where government agencies use proprietary software. In these situations, the awareness campaigns and the benchmarks used should not be the same. Once these issues are addressed, KPIs have an important part to play in the assessment of the effectiveness of awareness campaigns.

The author would like to thank Francois Thill for his insightful comments. Additional information and an extensive version of the article can be found at: www.blog.CyTRAP.eu

---

Prof. Urs E. Gattiker (EWS_KPI@CyTRAP.eu) is the CTO of CyTRAP Labs and the director of CASEScontact.org, an Early Warning System for citizens and SMEs.

An Introduction to SCADA Systems Security

Lluis Mora and Xavier Panadero

SCADA (Supervisory Control and Data Acquisition) is the underlying information system that controls critical infrastructure and processes around the world – resources and equipment that we depend on for our daily life, such as transportation, utilities or industrial processes, are all monitored and controlled by these systems.

This article presents a brief introduction to SCADA systems and their components, as well as their evolution towards open systems and protocols over the last few years. This evolution and the particular characteristics of SCADA systems, such as its criticalness and uninterrupted operation, have introduced unique challenges for those tasked with protecting them. How can one secure an environment that cannot be patched easily and where scanning usually causes more trouble than benefit?

This article explores each of these security challenges, focusing on the source of the vulnerability and suggesting courses of action to isolate and, wherever possible, solve them, using information security practices that have proved useful in other contexts or in different environments.

Introduction to SCADA systems

SCADA refers to the information systems that support industrial process supervision – mechanisms which monitor and manage these processes remotely from a central point.

SCADA systems have eliminated the need to monitor and adjust process parameters physically. A sensor network transmits information on the component status to a central operations room where operators decide if the process needs to be adjusted. Often these decisions are automatically taken by a central processing unit that relieves operators of repetitive tasks, allowing them to interact with the system at a higher level.

The advantages of SCADA systems have placed them at the core of information systems in the operation of most infrastructures we consider to be key in our daily lives nowadays:

- Transportation (railway, air, road controls)
- Utilities (water, power and gas supplies)
- Industrial systems (chemical, refining etc.)

SCADA components

A SCADA system collects information through a network of distributed sensors, consolidating it in a graphical visualisation so that operators can easily evaluate the process status and decide whether to take any action. This is then sent back to the network as control commands.

The following are the typical components of a SCADA installation, starting with those closest to the physical process being supervised:

- **Acquisition peripherals** convert sensor measurements to digital information using Programmable Logic Controllers (PLC).

- The **Remote Terminal Units** (RTUs) facilitate the connection of acquisition peripherals to the network that connects the various components.

- **Communication systems** offer the transmission channel between the central system, the SCADA Human-Machine Interface (HMI) and the RTUs, using technologies as disparate as point-to-point links, satellite/radio connections, ethernet networks, the Internet etc. The protocols that are used for SCADA communications are designed for efficiency and reliability – although there is a great variety of protocols both open (DNP3, IEC 60870-5) and proprietary (Modbus, Fieldbus), but very little attention is paid to data confidentiality and integrity in their design.

- The **central system** is in charge of collecting the information from each RTU. This information is processed, analysed and subsequently presented to an operator using an easy to use visual interface (HMI), that allows the operator to take decisions and to tune process parameters.

The evolution of SCADA systems

Historically SCADA systems have been closed environments built around proprietary protocols and systems; they have been declared as secure because they were isolated, they were custom-made and only a handful of people knew how they really worked.

The constant need to reduce costs has driven standardisation of SCADA components to facilitate interoperability, pushing most of the vendors into a shift to Internet Protocol-based (TCP/IP) networks and standard PC platforms, in an effort to maximise the reuse of the existing infrastructure.

One of the results of this evolution is that SCADA is no longer an unknown system – the 'security through obscurity' justification is not valid any more. Anybody can learn how SCADA systems work and apply traditional exploitation techniques to these open platforms, as they use hardware and software with known vulnerabilities.

Likewise, even though in most environments there is still the feeling that the SCADA network is isolated, there are an increasing number of interconnections with other networks, both because of business requirements, such as billing systems, Enterprise Resource Planning (ERP) systems, decisions support systems etc., and cost cutting efforts, for example, the convergence of control networks with corporate networks and remote maintenance.

Over time, the qualities that made SCADA a unique and isolated environment have disappeared, while at the same time the security concepts we have built on top of these qualities have not been updated.

The inherent vulnerabilities of SCADA

The following are some of the vulnerabilities that are present in SCADA systems because of its uniqueness:

• Difficulty to patch vulnerabilities

SCADA systems usually support the operation of critical environments that need to work for years without interruption. It is almost impossible to stop the operation of

support systems (UNIX/PC platforms, HMI etc.) in order to install updates; it is virtually out of the question to do so on embedded systems (RTU, PLC etc.) in which even short maintenance interruptions are unacceptable.

• Functionality over security

The design of SCADA systems targets reliability and response times over other factors; SCADA systems are critical systems on which the successful outcome of the controlled process depends. Integrity and confidentiality are factors 'covered' by the network isolation so they are rarely factored in.

This translates to all levels in a SCADA system: communications between devices with no encryption, for example, HMI, RTU, PLC, critical information stored in plain text, such as passwords, network addresses, unrestricted access and modification of PLC devices etc.

The introduction of security components such as encryption, authentication or security logs requires additional memory and processing (CPU) resources that might not be available on embedded systems. To top it all, these security measures might potentially affect system availability.

An example is operator authentication: the SCADA system requires absolute availability for supervisors, so the need for authentication has been removed or, in the best case, access credentials are shared by operators.

Another example that usually surfaces during the forensic analysis after an incident or attack is the lack of event and access logs in SCADA system devices.

• Better safe than sorry

Some of the security controls that are used in other kinds of environments cannot be directly translated to SCADA systems.

One of the security team's preferred tools, the 'port scanner', is usually one of the worst enemies of live SCADA networks. 15-year-old operating systems, PLCs with very basic or non-standard implementations of network stacks etc. and components not designed for unexpected input will just crash and burn during a 'traditional' network security assessment.

There is a need for innovative, 'non-aggressive' methodologies for SCADA systems' security assessment, based on controlled investigation in a laboratory and complemented by a complete risk analysis in a production environment.

• Blind trust

Historically, security in SCADA systems has been based on the trust offered by an isolated and closed network.

Trust in the network has extended to trust in its users. This is a group that has always been well defined and identified because there were only a limited number of people who had access to the control network. Nowadays, with numerous interconnections and reusing corporate networks to control SCADA components, it is probably impossible to say who has access to the control network. This can bring the 'insider' menace to a new dimension.

With blind trust in SCADA security, it seems as if there is no need to provide security for each of its components:

- Plain text communications over public networks (Internet, GPRS, WiFi etc.)
- Developed code is functional, but poorly secured (buffer overflows etc.)
- People and component authentication
- Maintenance outsourcing

Types of SCADA attack

Most of the currently reported incidents have an internal origin; lack of authentication and the proper separation of duties usually results in users being granted access to critical functionality that they do not necessarily understand – thanks to the basic quality of HMI, which allows interactions with the system without the need to understand the underlying process.

Complete accessibility, along with the lack of authentication and auditing controls, facilitates human error and makes an attacker's life easier through simplified tasks. For example the attacker could compromise the central unit or the HMI consoles, thus allowing other attackers to have a high-level vantage point over the processes they are targeting.

On the other hand, there is a huge amount of published information on SCADA infrastructure components, such as protocols, remote units etc., that allows an attacker to become a SCADA expert, discovering and exploiting new vulnerabilities at a lower level. This information is not restricted to user manuals and other superficial information; an attacker can easily find supposedly 'confidential' information on particular project implementations by browsing published vendor 'success stories' or by connecting to publicly accessible File Transfer Protocol (FTP) servers that system integrators use to exchange information with customers.

Some of the SCADA infrastructure components, such as RTUs or PLCs, are usually located in remote locations, physically isolated and thousands of miles from the central unit as, for example, the supply control units in utilities networks. Gaining physical access to the facilities that house these remote devices is usually easy and, although they are physically remote to the central unit, logically they are connected to the SCADA system (and potentially to other corporate networks), offering an attacker a point of entry to a seemingly isolated network.

The transmission medium through which these remote locations connect to the SCADA infrastructure can become an additional security problem: packet radio, Very Small Aperture Terminal (VSAT), WiFi etc. – wireless transmission mechanisms that, without an additional encryption layer, can compromise communications confidentiality.

As time has gone by, SCADA systems have evolved towards commercial platforms and open protocols, PCs, TCP/IP etc., – on top of vulnerabilities particular to the SCADA environment, traditional attacks against these platforms should be taken into account, for example worms, commercial software vulnerabilities etc.

Conclusion

The main conclusion to be drawn from this discussion is the clear need for a security culture change in the control systems community; current exposure and security problems affecting SCADA systems are usually unknown or ignored. Integrity and confidentiality are often considered an enemy of system availability and a great deal of simple security solutions are just ignored because of their potential to affect service levels, such as:

- Logical isolation of the control/operation networks
- Firewalls, packet filtering devices and the detection of SCADA intrusions
- Vulnerability assessments
- Authentication controls
- Auditing and logging mechanisms.

There is a need to introduce security as a critical factor both in the design and operation of SCADA systems, identifying and assuming the unique challenges that these systems present – even if that means changing the way we perceive security in SCADA environments.

Lluis Mora (llmora@neutralbit.com) is a researcher at Neutralbit, specialising in vulnerability assessments and the penetration testing of networks, applications and products.

Xavier Panadero (xpanadero@neutralbit.com) is a researcher at Neutrabit with extensive experience in the IT security sector, focusing on vulnerability research and the innovation of new security technologies for control system devices and networks.

FIRST Conference puts Spotlight on Digital Privacy

Supported by

Around 400 of the world's top computer and Internet security practitioners are expected to come to Spain for the 19th Annual Conference of FIRST (the Forum of Incident Response and Security Teams). This year's event will be held at Seville's Melia Sevilla Hotel from 17-22 June. The conference theme is related to the hazards and responsibilities of digital privacy: 'Private Lives and Corporate Risk'.

FIRST (www.first.org/) is one of the leading agencies in the global fight against cybercrime. It is a non-profit organisation which consists of delegates from the Internet Emergency Response Teams of 180 corporations, government bodies, universities and other institutions spread across America, Asia, Europe and Oceania. FIRST hosts a Global Security news feed at: www.first.org/newsroom/globalsecurity.

"Privacy is now the hottest topic in our business", explained conference joint organiser, Ian Cook. "We know that so much damage has been done by accidental losses and leaks or deliberate thefts, with millions of innocent people exposed to fraud and identity theft, that governments all over the western world are planning new laws to regulate public and private bodies and force them to go public when their data bases are lost, leaked or violated. The consequences of that, in reputation terms alone, for those 'named and shamed' will be catastrophic."

The 2007 FIRST conference will include sessions designed to help delegates understand how privacy breaches most commonly occur, how they can be prevented, what organisations should do if the worst does happen, and how damage to reputation and credibility – with its consequent onslaught on corporate value – can be limited when privacy is invaded.

"But we also want to explore the hugely important ethical dimensions", added fellow organiser, Arjen de Landgraaf. "Here we are, 23 years after George Orwell's *1984*, and the technology of the Big Brother state has now settled into place. What challenges does this pose to individual liberties? How can they be met? Who should be grappling with them? And, critically for delegates at the conference, what does it imply for those of us whose daily work puts us out there and exposed at the plumb centre of the privacy arena?"

Keynote speakers at the conference will include ENISA's Executive Director, Andrea Pirotti; Lord Toby Harris, the UK Home Secretary's appointee on the Metropolitan (London) Police Authority; Francisco Garcia Morán, Director General of DG Informatics for the European Commission; Mary Ann Davidson, Oracle's Chief Security Officer; BT's futurologist, Graham Whitehead; and George Stathakopoulos, General Manager of Product Security for Microsoft. Other speakers include Carsten Casper, ENISA's Senior Expert for Security Tools and Architectures, who will introduce an EU initiative on the collection of data on information security incidents and consumer confidence.

This year's event will again include 'special interest group' meetings, which have previously attracted considerable interest. For example, at last year's FIRST event in Baltimore, delegates from national security co-ordination teams joined with representatives from the major Information Technology vendors to discuss and resolve misunderstandings and inconsistencies of approach and to establish new protocols for co-operation. Another special interest group was established combining international law-enforcers with corporate Internet response and security teams.

Other, somewhat 'lighter', features of the 2007 conference programme include the famous 'Beer 'n' Gear' sessions, where vendors and providers demonstrate new equipment over refreshments in a relaxed environment, and the 'GeekZone' presentations with a hands-on format aimed at smaller, technical audiences of up to 30 people.

FIRST General Chair, Mike Caudill, stated: "Over the years, FIRST's conference has proved itself to be the foremost computer and Internet security forum in the world. Delegates learn not just about the latest analyses, strategies and prevention techniques in incident management – they hear first hand how the industry's principal figures manage breaking security issues, and they have the opportunity to interact and network with colleagues from around the globe, exchanging ideas, experiences, best practices and advice.

"Every year the conference seems to get better and attract more people. This year, as we meet in Spain, we will be addressing the number one concern of the moment – privacy. This promises to be the best and most significant of our conferences yet."

For further information about the FIRST Seville Conference, visit: www.first.org/conference/2007/

or contact the Co-organisers:
Ian Cook (ian.cook@pentest.co.uk)
Tel. +44 (0) 7968 782122

Arjen de Landgraaf
(arjen.de.landgraaf@cologic.co.nz)
Tel. +31 (0) 6 218 174 68

From our own Experts

EISAS – European Information Sharing and Alert System: a feasibility study

Marco Thorbruegge and Slawomir Gorniak

Public authorities in Member States (MS) and in European Union (EU) bodies have a key role to play in properly informing users so that they can contribute to their own safety and security. This is clearly emphasised in the European Commission's Communication to the Council, Parliament, Economic and Social Committee and the Committee of the Regions (COM(2006) 251). The Communication further declares that the possibility of facilitating "effective responses to existing and emerging threats to electronic networks" should be explored.

This need is mirrored by the European Commission's request to ENISA "to examine the feasibility of a European information sharing and alert system (EISAS)", which highlights the role of ENISA in fostering a culture of network and information security in Europe. ENISA agreed to carry out this study in 2007 as it fits very well within the scope of the Agency's activities.

But what does the term 'information sharing and alert system' really mean? Such systems can be divided into three main categories according to the information that they provide. They can be:

- Passive – 'good practices' related to Network and Information Security (NIS) ('How to choose good passwords', 'How to deal with Internet banking' etc) and other information that changes relatively infrequently
- Active – current security advisories and alerts about circulating worms or viruses, available updates or discovered weaknesses in most popular software
- Short term – visualisation and warnings concerning actual state of the network and possible countermeasures.

The information can be disseminated in many different ways. The basic approach is of course a web portal, but others also exist, such as mailing lists, RSS feeds, the Short Message Service (SMS), phone calls and even mass media, such as newspapers, radio and television.

Currently there are many systems and initiatives across Europe and in the Member States that have as their goal the sharing of appropriate and timely information on NIS vulnerabilities, threats, risks and alerts, as well as on good practices. ENISA was asked to analyse the current state of affairs in the public and private sectors and to identify possible sources of security information that can potentially contribute to an EISAS. The main goal of such a system would be to raise awareness on NIS issues among European citizens and Small and Medium-sized Enterprises (SMEs). The expected result of the Commission's request is a recommendation whether – and, if so, how – an EU-wide, multilingual system could be realised by combining existing systems. This last point is probably the most important for the whole study.

Many activities have to be studied and assessed in order to fulfil the European Commission's request. The first step is to analyse existing information sharing systems and possible sources of NIS-related information. These include vendor or independent organisations' advisories, web portals containing recommendations and best practices, and so-called 'real-time' network monitors. All these initiatives have to be carefully analysed by ENISA, to find out whether they could contribute to a potential pan-European system as a source of information, or perhaps even whether such a system could be based on some of them.

There are several factors to be taken into account during the assessment:

- rapidity – how quickly the information is disseminated
- clarity of data
- reliability – will all related information be disseminated and without 'false positives'?
- exchange mechanisms – is the content easy to exchange and parse?
- language – are they available in the most frequently used languages?
- coverage of systems – the most widely used
- geographical coverage (this holds for sensor networks).

The assessment will lead to an analysis of the feasibility of a Europe-wide system and the development of possible scenarios.

Despite the fact that the study is not yet finalised, it is already possible to predict some possibilities. As the simplest approach, a European sharing and alerting system could consist of a portal grouping links to all known national and international initiatives. A much more advanced solution could be the formation of a separate information portal, processing data received through other existing systems and representing the results in a unified form. However, previous experience should be considered – there are already some initiatives for the development of such a system, but until now none of them could be considered as fully successful – at least on wide deployment. Other scenarios include the proposal of a framework that could allow the establishment of national systems in interested Member States, facilitating the knowledge gathered during the study and the relevant experts, which in some cases could be seconded by other Member States.

The last step of the ENISA EISAS feasibility study is the assessment of the added value of such a system. In other words, will such a system contribute towards enhancing the overall culture of security in Europe? And, if so, how and to what extent? For this task, performance indicators will be needed in order to estimate and then analyse the impact that EISAS would have.

The terms of reference for this request were agreed between ENISA and the European Commission in mid-2006. In this document it is stated that ENISA might form an Expert Group for the task that should include security specialists from the Member States who already run their own information sharing systems. This group is now established and is helping ENISA in the tasks described above.

Work on the EISAS feasibility study at ENISA is still an ongoing issue. In April 2007 the first results will be disseminated to the Member States at a validation workshop in Brussels. This meeting will also be an excellent opportunity to assess what has been achieved so far and to make adjustments. The final study will be delivered on 4-5 June at the security conference hosted by Germany during its Presidency of the EU.

Marco Thorbruegge (marco.thorbruegge@enisa.europa.eu) is a Senior Expert in ENISA's Computer Incident and Response Handling unit.

Slawomir Gorniak (slawomir.gorniak@enisa.europa.eu) is employed by NASK in Poland, and is a seconded national expert in ENISA's Computer Incident and Response Handling unit.

Data on Security Incidents and Consumer Confidence –

You cannot get hold of it for love or money!

Carsten Casper

There is no reliable, neutral and European-wide data on information security. ENISA will find out how difficult it is to solve this problem.

www.enisa.europa.eu/pages/data_collection

Every solution must be appropriate for the size of the problem – information security should be no exception here. However, reliable information about on-line threats and security incidents is a scarce resource. Everybody would like to know more, but no-one wants to share his own (often negative) experiences.

This is not only true for companies which implement security measures in response to an internal risk analysis, it is also true for policy makers – except that their portfolio of measures consists of laws, regulations and directives. However, when it comes to a risk analysis prior to the initiation of such measures, then policy makers often skate on thin ice. So far, there is hardly any analysis that is international and independent at the same time.

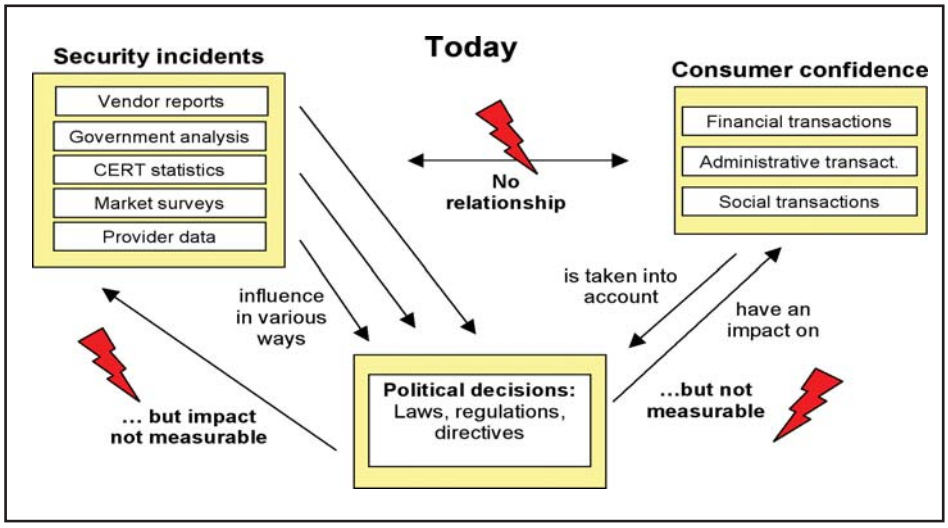
However, a sound legal framework is crucial to protect the citizen, not overburden the industry and maintain an efficient public administration. Legislators could make spam and spyware illegal, set a severe fine for hacking, force Internet Service Providers (ISPs) to manage the SMTP port or require them to report the security measures they have implemented, as it was suggested last year by an ENISA report. In any case, unilateral attempts are rarely effective; they have to be co-ordinated, at least on the European level, in order to be successful.

Judging the success of such regulatory measures is not only a question of a reduced amount of security incidents – however this is measured. It is more important that companies and citizens trust the Internet (again), which has to be proved by statistical data on financial, administrative or social on-line transactions.

Measuring these two parameters – security of the Internet and consumer trust – is the goal of an initiative of the European Commission. However, considering that large parts of the network infrastructure are in private hands, both the main contributors as well as the main beneficiaries can be found in the private sector.

Are we ready to share?

The motivation for exchanging data is more important than the question about what type of information is actually exchanged. Why should a Computer Emergency Response Team (CERT), a Managed Security Service Provider, a network operator, a vendor or a public authority be willing to share information on security incidents with others, even if that exchange happens only once every year in aggregated form? 'Give' and 'take' are two sides of the same coin.



Every partner who is asked for contributions needs an incentive – be it material gain, political influence or a market advantage. Also, not every partner can contribute in the same way: some possess a wealth of data, others are willing to contribute human or Information Technology (IT) resources, still others can offer logistical support.

In addition, the circumstances of the exchange are crucial. The first challenge is bringing everybody to the same table. Soon it will become apparent that there are far too many potential partners to reach an agreement in the short term, especially in a cross-border scenario. Moreover, some partners will have quite opposite interests. So the primary goal is to define a framework for information exchange that is both reasonable and practical.

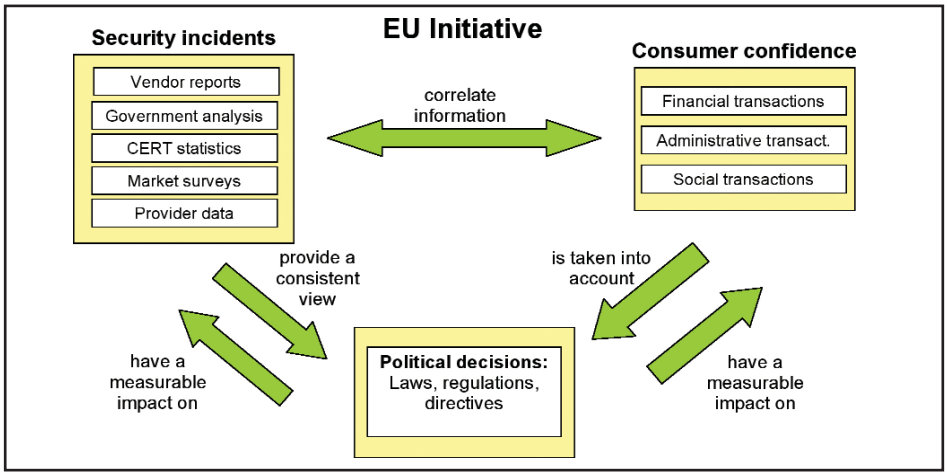
Mutual trust is the main prerequisite here. Even if data is aggregated and made anonymous – which would be more than sufficient for political decisions –, such data does represent a certain value, for example if it competes with established vendor reports. Others might fear that data can be traced to the source, despite the aggregation. Of course this depends on the way that data from different sources is assembled and by whom.

Another important aspect is that the framework guarantees a certain level of quality, but at the same time does not pose an unnecessary burden which could deter valuable partners. Ideally, there would be different levels of co-operation. At one extreme, a partner might contribute only information that is publicly available anyway, and so he just transforms the data into a different format. At the other extreme, a partner could participate in the definition of the exchange format and provide data with a high granularity, but also benefit from detailed evaluations and a high level of influence.

How can we exchange data?

It is common sense that technical, organisational and legal measures have to go hand in hand in order to achieve an optimal solution. The private sector will only benefit if politicians do not rely on experts' opinions alone, but can also base their decisions on up-to-date statistical data. On the other hand, such data would also be valuable for companies directly, for no-one intends to keep the yearly reports confidential.

Certainly, every company can consult reports such as the newest CSI/FBI Computer Crime and Security Survey (www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml) or the Information Security Breaches Survey analysis produced by the UK's Department of Trade and Industry (DTI) (www.security-survey.gov.uk). However, by and large these reports have a national focus, are created at different times and with different methods, and do not reflect the situation across the whole of Europe. In addition, there are reports from security vendors which describe the situation in a larger geographical context, but these are not free from vendor interests.



The aforementioned initiative is supposed to overcome these constraints, defining a framework for data collection that balances the interests of product vendors, service providers and other private and public entities from all over Europe. The question remains whether such an endeavour is realistic. ENISA will try to find an answer and would like to hear your opinion. How valuable would such a framework be for your public or private organisation? Which prerequisites and potentials do you see?

ENISA has started to contact a number of potential partners individually. If you have comments or if you feel that your organisation has something to contribute to this framework, contact carsten.casper@enisa.europa.eu

Casten Casper (carsten.casper@enisa.europa.eu) is a Senior Expert in ENISA's Security Tools and Architecture unit.

ENISA and eema, Europe's leading independent, industry association for e-Identity and e-Security (www.eema.org), are co-organising a two-day event on electronic identity. In two parallel tracks, more than 100 experts will discuss how to manage employee, citizen and private identities. ENISA's track will focus on social networking, Web of Trust and authentication interoperability, while the eema stream will concentrate on more general and business aspects of electronic identity.

Day 1: Workshop on Next Generation eID

During this day we will look at the hot topics of reputation systems and social networking.

Identity in Social Networking

Social networking is set to be this year's hot topic in electronic identity, with a huge growth in the number of users and an increasing requirement for secure management of the vast amounts of personal information exchanged. The workshop will focus on emerging identity-based threats including the excessive disclosure of private information, cyber-bullying, identity theft and 'squatting' in social networking sites.

Reputation and Web of Trust systems

Reputation is a major growth area in establishing trust in electronic identity attributes. Applications include spam-filtering, peer-to-peer download management and seller-reputation systems such as eBay's feedback ratings. Areas to be explored include the appropriate ranking of newcomers to reputation systems, trust-metrics, multi-level reputation schemes and denial-of-reputation, combining reputation and Public Key Infrastructure (PKI) and the use of semantic-web technologies for reputation.

For more information and the Call for Papers, visit the web pages of the Workshop on Next Generation eID at: www.enisa.europa.eu/pages/eID/Eid_ws2007.html

Day 2: Workshop on Authentication Interoperability

We will look at interoperable solutions for describing authentication mechanisms, such as:

- Interoperability of languages for describing authentication mechanisms
- Describing trust properties of authentication to end-users
- Assurance issues of authentication metadata
- Quantifiable levels for evaluating authentication mechanisms
- Use-cases including: eCommerce, eBanking, eHealth, eGovernment, National eID cards

For more information and the Call for Papers, visit the web pages of the Workshop on Authentication Interoperability at: www.enisa.europa.eu/pages/authentication/auth_ws2007.html

eema track

The eema stream will run in parallel with ENISA's workshops and will focus on more general aspects of electronic identity such as:

Managing Identity – Exploring the management of network and physical access/ID management and the supporting technological, data and personnel issues.
Securing Identity – Looking at how we can help protect identities and make our systems more robust.
Federated Identity – Exploring effective strategies and practical case studies to deploy and manage federated identity systems.
e-Provisioning – Analysing the management, technical and compliance challenges faced in manual and automatic e-provisioning and de-provisioning.
eID Cards – Covering eID card interoperability issues, the latest technological solutions and cultural challenges.

For more information and the Call for Papers on the eema track and to register for the event, visit eema at: www.eema.org

ENISA Awareness Raising Goes International

Isabella Santa

Using the Internet and other new technologies means we can make and keep in contact with people and cultures from all over the world to an unprecedented extent. Thanks to the Web, most of the barriers to communications of the past have vanished – with the exception of one: the language. The content of the Web aims at a broad audience, but in order to be effective, it should be presented in the users' native language wherever possible.

Against this background, the Awareness Raising unit of ENISA has reflected on the possibility of promoting its findings by translating *'A Users' Guide: How to Raise Information Security Awareness'* – which has been available in print and on-line on the ENISA website in English since last June – into other languages: French, German and Spanish.

The Awareness Raising unit believes in the importance of establishing a presence, building a brand and disseminating its messages across language barriers, aiming at continually expanding its reach. Going international will allow the unit to promote its material in a faster, more effective way, supporting citizens and equipping them with the skills they need to live and work in the information society.

The Users' Guide provides practical advice for EU Member States to prepare and then implement awareness raising initiatives related to information security, recognising that awareness of the risks and the safeguards available is the first line of defence for the security of information systems and networks. The report features step-by-step advice to help form the basis of an effective and targeted awareness campaign and the information is organised for the benefit of different audiences, such as public and private organisations.

The published Guide aims to:

- Illustrate a sample strategy for how to plan, organise and run an information security awareness raising initiative
- Highlight the potential risks associated with awareness initiatives in an effort to avoid such issues in future programmes
- Provide a framework to evaluate the effectiveness of an awareness programme
- Offer a communication framework
- Contribute to the development of an information security culture in Member States by encouraging users to act responsibly and thus operate more securely.

The report identifies the main processes and activities necessary to run an awareness campaign. These processes have been defined as follows: plan and assess; execute and manage; evaluate and adjust. For each process, the relevant activities have been identified. A series of steps and recommendations have also been included in order to help the reader understand the strategy for executing awareness initiatives and programmes better.

In particular, the Guide emphasises the importance of:

- **Effective communication planning**
  A communication strategy is at the centre of any awareness programme but the strategy needs to be adapted to a specific context.

- **Change management approach**
  Applying a change management approach to an awareness initiative is crucial as it helps to close the gap between a particular issue and human responses to the need to change, even in the case of a cultural change.

  Using the main principles of change management, such as targeted

The Awareness Raising Monthly Teleconference

The Awareness Raising (AR) unit of ENISA would like to promote regular discussions among experts working on raising information security awareness.

HOW?

The AR unit will organise short conference calls lasting a maximum of 30 minutes each.

WHEN?

Every third Friday each month, starting from 16 March 2007 at 10.00 (GMT); 11.00 (CET); 12.00 (GMT+2).

WHY?

The AR unit aims to promote knowledge sharing and to establish and support dialogue within institutions of the EU Member States and other stakeholders. In addition, the unit aims to help establish an AR community, bringing together AR experts from the public and private sectors.

The proposed framework for discussions is as follows:

1. Representatives of one or two Member States will provide updates on their latest awareness project or initiative
2. Participants will be given the opportunity to make a request to the other experts for specific awareness materials or information
3. Any other business relevant to the promotion of Network and Information Security and co-operation in defining future required activities for raising awareness

For more information on this initiative, please send a message to the following address: awareness@enisa.europa.eu.

communications, involvement, training and evaluation, helps towards ensuring that the objectives are met and provides a sound platform for future or follow-up programmes.

- **Measurement of the value of awareness programmes**
  The need for security awareness is widely recognised. However, there are few public or private organisations that have tried to quantify the value of awareness programmes. Evaluation of an awareness raising campaign or programme is essential in order to understand its effectiveness as well as to make the necessary adjustments based on what has been learned to date. Evaluation metrics cannot be universally applied to all target groups since needs and situations differ greatly.

In conclusion, the new language versions of the Users' Guide will help to further increase public awareness in the field of information security, and both educate and reach out to additional users.

The Users' Guide is available on-line in different languages on the ENISA website: www.enisa.europa.eu/

Isabella Santa (isabella.santa@enisa.europa.eu) is a Senior Expert in the Awareness Raising unit at ENISA.

European NIS Good Practice Brokerage – Kick-off Workshop

Silvia Portesi

In co-operation with the German EU Presidency, ENISA organised the Kick-off Workshop on European Network and Information Security (NIS) Good Practice Brokerage. The event took place in Brussels on 22 February 2007 and brought together National Liaison Officers (NLOs) and other national experts in NIS from Member States (MS).

European NIS 'market place'

The exchange of good practices between Member States is essential to enhance the level of NIS on a pan-European scale. Several MS already share experiences in NIS, but in order to further develop EU-wide NIS capabilities, it is essential that more and more MS are involved in this process. It is also important that additional NIS areas are covered and that a more structured basis is given to the exchange of good practices.

To this end, as laid down in its Work Programme 2007, ENISA facilitates a European NIS 'market place' by acting as a broker. Once ENISA has identified demand and supply and found suitable ways in which Member States might co-operate, the Agency injects its technical expertise into joint initiatives, encouraging a dialogue between different stakeholders, and supporting and fostering the dissemination of the results of the co-operation initiatives.

Kicking off NIS Brokerage with new ideas

During the workshop, representatives of both ENISA and the German EU Presidency stressed the importance of identifying Member States' urgent needs and of setting up a sustainable and ongoing process of NIS brokerage.

ENISA presented the results of a survey of NLOs that had been carried out prior to the workshop to collect material to trigger discussion at the meeting. The findings of the survey show that co-operation and joint activities already exist in areas such as Computer Emergency Response Teams (CERTs), electronic signatures, spam and awareness raising, but that there is also a demand for further, more intensified, co-operation in awareness raising, CERTs and standardisation/certification.

For example, a useful start towards that end was identified in the field of awareness raising. It was suggested that a joint and continuously updated list of projects should be compiled, which includes their purposes and their target groups (e.g., teachers, parents, teenagers etc.).

In addition, suggestions and ideas for an on-line platform for European NIS Good Practice brokerage were presented. An on-line platform, which is also mentioned in ENISA's Work Programme 2007, should facilitate the brokerage function.

The exchange of views, common meetings, topical exchange groups, traineeships and exchanging visits by experts were identified as possible types of co-operation. In addition, the importance of structuring existing co-operation activities was highlighted: this could represent added value for all Member States. Putting in place models to spread the newly gained knowledge was also considered crucial. A central repository for good practices was widely discussed, and the use of an on-line platform for information exchange was seen as an essential and natural supporting tool to match demand with supply, and to spread good practices and outcomes from both existing and future co-operation easily.

Towards an On-line European NIS Good Practice Brokerage

Several ideas for the content of the on-line platform were discussed. There was general agreement that, in addition to the documentation of successfully completed co-operation activities, the on-line platform should contain an overview of Member States' initiatives, policies, projects and best practices, as well as a collection of reports, common tools and information that could be 'reused' (customised and translated where appropriate) in other Member States.

Regarding technical requirements, the platform was envisaged as an operational and continuously updated page on ENISA's website. Easy accessibility and good search tools would be a must. The on-line platform could also offer services such as a forum for discussions, a database of practices, policies, projects, initiatives etc., a directory of contacts, a list of events and topical newsletters.

Next steps

This Kick-off Workshop proved a successful starting point. The forthcoming presentation on existing co-operation initiatives at the IT-Security Conference on 4-5 June 2007 in Berlin (under the auspices of the German EU Presidency) will be another important milestone.

Silvia Portesi (silvia.portesi@enisa.europa.eu) is an Expert in ENISA's unit for the Co-ordination of Activities with Member States and EU bodies.

From The Member States

Starting up an Early Warning System in the Netherlands

Menno Muller

The aim of the Dutch government is to have 65% of all its services to citizens available on-line by the end of 2007. This is expected to increase significantly the number of electronic transactions between citizens and governmental systems. Monitoring the relevant data-flows is a daunting task. However, from a security perspective, it is vital to keep an eye on what is going on. This increased data traffic demands smarter monitoring tools for the organisations involved.

GOVCERT.NL is the Computer Emergency Response Team (CERT) for the Dutch Government that supports the government in preventing and dealing with ICT-related security incidents.

One of GOVCERT.NL's initiatives is the development of a monitoring service for its constituents to help the government move from a reactive to a proactive approach to on-line security.

So what has GOVCERT.NL learned after having spent about a year and a half in the monitoring realm?

This hands-on article describes GOVCERT.NL's experience in building and deploying an advanced monitoring system. It focuses primarily on the lessons learned. It also provides a brief technical description of the GOVCERT.NL monitoring service.

Make sure to take-off

In mid-2005, after an inspiring workshop on honeypots, GOVCERT.NL embarked on the development of a monitoring system. The system comprises a network of smart sensors with honeypot technology installed, located at the constituents' networks. The technique was mainly based on Prelude-IDS (Intrusion Detection System) technology (www.prelude-ids.org). It was implemented at a number of constituents and used for six months. This small-scale pilot exercise proved a valuable tool for the organisations using it. Of course it was not entirely flawless, but it had promising potential. The techniques involved are discussed at length in the technical elaboration at the end of this article.

By the end of 2005, GOVCERT.NL had acquired a first view of the usefulness of a monitoring system. The outcome of the pilot evaluation was used to decide on the features needed in order to develop a scalable and maintainable monitoring system. This is the point where SURFnet, the Dutch Academic CERT, became involved in the process. At that time, SURFnet had just finished the development of an in-house IDS. A live demonstration proved that this open source system met GOVCERT.NL's requirements. One important feature of that system was that it eliminated any false positives. The SURFnet IDS now forms the core of the GOVCERT.NL Monitoring Service.

The basic monitoring service for GOVCERT.NL's constituents was developed during 2006. The system detects worms, viruses and known exploits. It visualises these attacks in the form of graphs and maps, making Internet threats tangible. This is just the sort of useful information decision makers often have to manage without.

Lessons learned

Make sure to take-off

Decide what you want to achieve in the future, create a sound plan and *start*; (potentially) better ideas are bound to pop up! So avoid getting caught up in just changing plans continuously and not actually getting started.

Work with the future in mind

Make sure you know where you are heading. Use the bigger picture as a future goal, to decide whether – and where – new initiatives fit into this future plan. Then gradually work your way towards it.

You are not on your own

Take a good look around; there is already much out there. Do not reinvent the wheel. Get in touch with organisations that are already involved in (network) monitoring. For example, the Network Monitoring Special Interest Group for the Forum for Incident Response and Security Teams (FIRST) is a very good point of reference.

Legal matters

A monitoring system collects all sorts of data, for example, source IP addresses, payloads and scanned ports. It is likely that personal data might be involved, which suggests one will have to deal with privacy legislation where applicable. In this case you should contact your governmental organisation(s) dealing with this matter and sort out what applies in your case. Seek help from a legal advisor and do not let it stop you from getting started.

Think and test before you act on the technical result

Weigh the pros and cons of the technical options very carefully, for example consider a centralised honeypot (a computer connected to the Internet that does not serve any purpose other than attracting attacks) vs. a distributed one. Do not underestimate seemingly trivial aspects; it took GOVCERT.NL quite a while to find a usable combination of hardware and (bootable) USB sticks.

One picture vs. a thousand words

The visualisation of monitoring results is of paramount importance. Make sure to invest in a top quality user interface – particularly when users other than Information Technology (IT) specialists will be working with it.

Let the user decide

Install a user group to gather feedback on the usability of the monitoring system. Communicate what you have done with their suggestions carefully.

Work with the future in mind

The final goal of this project is a full early warning system – a system that detects zero-day exploits and new, previously unseen malware. Using the information detected, the system will warn constituents of Internet threats at an early stage, acting like a modern Internet weatherman.

There is still a long way to go to reach that point. The following initiatives have therefore been introduced to help achieve the ultimate goal.

The number of Web-based attacks exploiting vulnerable web browsers is increasing. Unfortunately the current configuration of the widely used tool, Nepenthes, a malware-collection tool that emulates known vulnerabilities and then downloads malware which tries to exploit these vulnerabilities, will not detect such attacks. Therefore one of the spearheads of the GOVCERT.NL campaign is the integration of a powerful, either off-the shelf or self-developed, client honeypot system into the system. This will greatly extend the scope of the present monitoring systems.

As Nepenthes depends heavily on software components that simulate vulnerabilities, GOVCERT.NL aims to develop new functionality. The focus is on finding new ways to detect unknown exploits. One initiative in this area is the integration of Argos (www.few.vu.nl/argos/) into the monitoring system. Argos is an emulator for capturing zero-day attacks and is currently being developed by the Vrije University (VU) at Amsterdam. Exploring the possibilities of integration of Argos is a joint project with SURFnet. Another way of integrating Argos could be to implement a pre-processor that incorporates a shell-code detection technique. As the best solution has not yet been found, several alternative approaches are being investigated.

Finally, in 2007 the pros and cons of using and positioning internal sensors will be considered. Positioning sensors inside the constituent's network is technically possible with the current set-up, but has a number of implications, including legal aspects. All these implications need to be investigated and addressed.

You are not on your own

It is only fair to say that GOVCERT.NL has not achieved everything on its own. During the course of the project, several organisations have been contacted for assistance. This has resulted in a number of valuable contacts and even a formal joint co-operation arrangement with SURFnet.

Another important example of collaboration is the establishment of an international working group. In June 2006 the FIRST Network Monitoring Special Interest Group was established (www.first.org/global/sigs/monitoring/). This is basically a group of organisations that share a common interest in network monitoring and offers useful information to any considering embarking on a similar project.

In this respect one should not forget the research community! There are many interesting research and development projects in this area and there is considerable potential mutual gain to be derived from combining the practical attitude of CERTs and CSIRTs with the more theoretical research approach (and with much software development strength). GOVCERT.NL therefore co-operates with several universities both nationally and internationally.

Legal matters

A monitoring system monitors and collects data of all sorts, including source IP addresses, payloads and scanned ports. Organisations that store data with personal information have to comply with their local privacy legislation. It is worthwhile, therefore, to consider seriously which data one needs or wants to store. One should make contact with governmental organisation(s) dealing with this matter and identify what applies. One option may be to contract a legal advisor to help in this procedure. Legal compliance is clearly an important issue, in which often the amount of work involved is underestimated.

For example, in the case of GOVCERT.NL, because the monitoring system collects IP address information, the Dutch Data Protection Act became relevant. This Act basically boils down to good data-ownership; organisations need to ensure that necessary precautions have been taken to prevent data from becoming compromised or lost.

GOVCERT.NL contracted a legal advisor to write a report stating all the measures taken to ensure that personal data is well protected. The final step was formal approval by the Data Protection Authority.

Another example concerns the decision to use sensors outside the constituent's networks. Placing the sensors internally is bound to generate much personal data, for example, e-mail. By placing the sensor outside the network, GOVCERT.NL avoids the rather intricate discussion as to how to deal legally with such information. Nevertheless, in 2007 GOVCERT.NL will research the pros and cons of implementing internal sensors, since it offers a number of interesting benefits.

Think and test before you act on the technical aspects

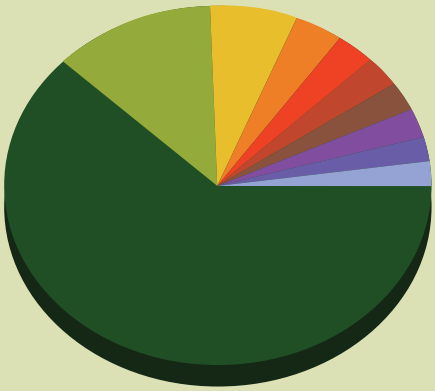
During the pilot exercise, a distributed honeypot was used; there was a network of intelligent sensors, with each sensor acting as a separate honeypot. A major problem with this setting was technical maintenance; every time an update was needed a cumbersome procedure had to be performed for each individual sensor.

A centralised network of honeypots is much easier to maintain and update than a distributed arrangement. One potential drawback in this approach, though, is loss of computational power, since using each sensor's potential processor capability creates room for more intricate analysis.

One should also not underestimate some seemingly trivial aspects, such as the selection of appropriate hardware; it took GOVCERT.NL considerable time to find a usable combination of hardware and bootable USB sticks. It is apparent that one should thoroughly test the system before putting it into use.

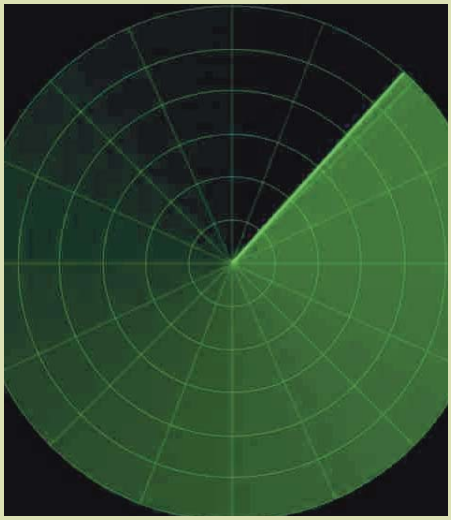
One picture vs. a thousand words

The visualisation of monitoring results is of paramount importance. One should invest time and money, if necessary, to design and deploy a good user interface. This is particularly important when the system has a wide variety of end-users with varying expertise and backgrounds. An attractive front-end makes the monitoring system



August 2006

A graphical representation of monitoring results taken from the GOVCERT.NL system, showing that 62% of malware is not recognised.



more 'tangible' for decision makers. This may mean installing features that do not necessarily extend the system's technical scope but will immensely enhance its look and feel.

Let the user decide as well

Much of the feedback received relates to the user-interface and ways to improve it, for example, by adding geographical information such as Google Earth and automatic pdf (portable document format) output files generation. This again relates to the paramount importance of the visualisation capabilities. Visualisation makes threats tangible and hence serves as a means to justify IT security investments.

Other motives for constituents to join the GOVCERT.NL monitoring service include:

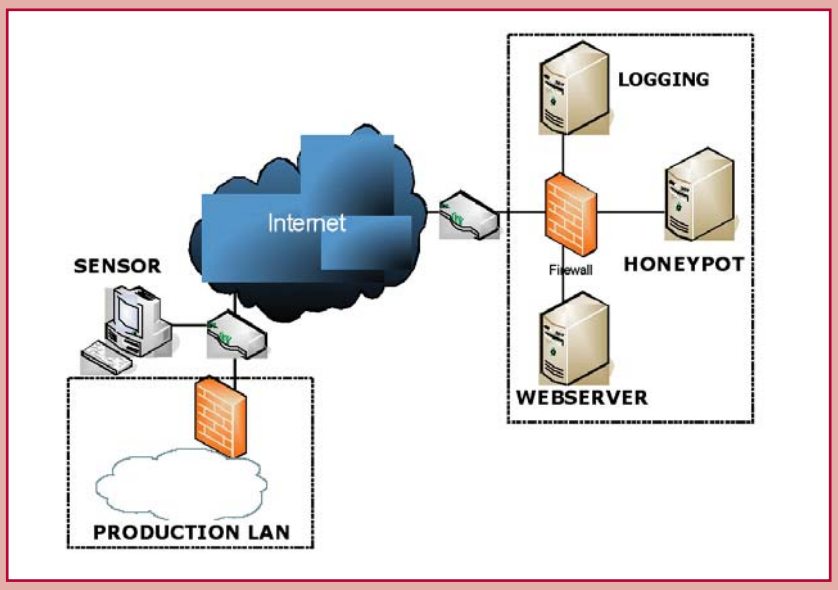
- Help with patch management decisions
- An extra information source to correlate with firewall logging (which provides an insight into attack trends)
- An extra control in case of a fully outsourced IT department
- An easy way of experimenting with new technology.

In the light of this, GOVCERT.NL has set related goals and ambitions. Firstly, it is expected that its monitoring system will assist GOVCERT.NL in becoming more proactive in terms of warning its constituents of potential threats based on statistical information it collects. Secondly, the system is of increasing importance in the incident response area where it can provide valuable background information. Moreover, as the number of zero-day exploits in cyberspace is increasing, the need for such services is becoming more apparent.

Menno Muller (menno.muller@govcert.nl) is a project manager at GOVCERT.NL and is responsible for development of the Dutch Monitoring Service.

In technical terms, how does it work?

The figure below shows the concept upon which the GOVCERT.NL monitoring system is based. The architecture is based on the SURFnet IDS (http://ids.surfnet.nl/).



Monitoring system architecture

Concept and Sensors

The system comprises one central honeypot, located at GOVCERT.NL, together with a number of non-intelligent sensors which are installed directly behind the constituent's Internet link. The sensors are connected to the centrally placed honeypot using a layer 2 Virtual Private Network (VPN) tunnel, using the OpenVPN (http://openvpn.net/). So the honeypot is connected virtually to the sensor's subnet. The sensor acts as a network hub between the local network and the honeypot, making it invisible at the IP layer (OSI layer 3). The sensor itself is a small rack mountable (1u) system that boots from a USB stick, for which one of the Knoppix Linux releases was adjusted.

All the traffic destined for the sensor's IP address is monitored. For privacy reasons, the sensor does not operate in promiscuous mode, so it cannot intercept e-mail etc. To rule out false positives, a honeypot is used to 'listen' on one unused public IP address of GOVCERT.NL's constituents. As this is an unused IP address, normally it should not receive any data. Consequently all data packets that do arrive at that IP address are suspicious.

Honeypot

The honeypot used is a server in the GOVCERT.NL network presently running Nephenthes (http://nepenthes.mwcollect.org/) as the honeypot technology. Nepenthes is a so called 'low-interaction' honeypot. These types of honeypots simulate known vulnerabilities, in a controlled environment, to collect information about possible malicious attacks. This is opposed to 'high-interaction' honeypots that run a full system. Nepenthes continues the interaction with downloads of the malware that an attacker wants to place on the sensor. This is then stored for analysis.

User interface

Constituents have access to their own data, based upon an X509 certificate, username and password.

Current scope of detection

The monitoring system recognises the automated misuse of vulnerabilities. Automated means that the attack is launched by an attacker and that no user interaction is required to infect a system. The range of attacks that will be recognised includes: scans, probes, worms, bots and Trojan horses. The system uses a number of virus scanners to define the nature of the malware offered.

Looking back at the First Year of 'Digibewust': the Digital Awareness Programme in the Netherlands

Arie van Bellen

Last year on 7 February, which was European Safer Internet Day, the campaign 'Digibewust' ('digi-aware') was launched in the Netherlands. This campaign was called into life by the Dutch Ministry of Economic Affairs together with corporate businesses, including Microsoft, KPN and TNT Post, to stimulate digital awareness in the Netherlands. To be 'digitally aware' means to make full use of the possibilities of the digital world, while at the same time being aware of the possible dangers and risks. A 'digibewust' user understands the nature of on-line risks and takes appropriate action to avoid them. This in turn helps achieve enhanced trust in the Internet.

Digibewust can now look back at a very successful first year. One year after the Digibewust programme was introduced to ENISA Quarterly readers (EQ issue 1st Quarter 2006), we reflect on the experience gained, lessons learned and future plans.

More than fifteen parties are now working together in the initiative. Both corporate businesses and government, as well as pressure groups, are part of Digibewust: the Ministry of Economic Affairs, KPN, UPC, Microsoft, TNT Post, Consumentenbond (Dutch consumer organisation), NVPI, NVB (the Netherlands Bankers' Association) etc. Still more must join to strengthen the campaign even further.

Last year programmes targeted children, their parents and teachers. Different educational activities have been developed to reach these target groups – all with great success. In September 2006 the on-line game, Gebouw 13 (www.gebouw13.nl/) (Building 13), was launched. This game targets children between the ages of 8-14 years. By playing this game, a child learns about the possibilities and opportunities, but also the risks of the digital world. Currently more than 100,000 children have found their way into Building 13!

Another example is the password campaign for teenagers. Two television commercials were created, one about the necessity of keeping your password to yourself and the other with tips for creating a strong – but at the same time easy to remember – password. These commercials were broadcast by TMF (the Dutch part of MTV) in January 2007. At the same time, over 250,000 Boomerang cards (freecards) were distributed at schools and libraries. When dealing with this target group (teenagers), it is important not to be patronising, but rather to convey the message with humour and to be a bit 'over the top'.

It is also very important to involve a target group early enough when developing an awareness activity. For instance, the DigiRaad, a council consisting of 12 children aged 12-18, tested Building 13. But they also gave advice about topics that are hot for teenagers. They helped to elect the most digitally aware politician of the Netherlands. This politician was Martijn van Dam, a Member of Parliament from the Dutch Labour Party, who received the first Digibewust Award on Safer Internet Day on 6 February this year. Princess Máxima of the Netherlands was also present at the event in order to emphasise the need for a safer digital world. The involvement of such high level individuals underlines the importance of the Internet security issue.

Digibewust could not have achieved all this without the help of others. Without its public-private partnerships, Digibewust would not have succeeded, would not even exist. The campaign is in constant need both of experts in the area of children and their use of the Internet, and also parties willing to contribute financially to these activities.

For 2007 the focus of Digibewust will be on Small and Medium-sized Enterprises (SMEs). It is planned to initiate different activities to stimulate the digital awareness of SMEs. For example, practical tools such as a port scan and virus scan will be added to the www.digibewust.nl website, safety aspects of web shops will be examined and educational activities such as a password campaign and advertorials will be set up.

To receive more information about Digibewust, please contact ECP.NL at: info@digibewust.nl.

For information in the Dutch language, please see: www.digibewust.nl.

Arie van Bellen (info@digibewust.nl) is the Programme Director of Digibewust and the Director of ECP.NL, the platform for e-Netherlands.

Roger van Boxtel (chair of ECP.NL and a member of the jury for the Digibewust Award) presents the Digibewust Award to Martijn van Dam, Member of Parliament, Dutch Labour Party.

Bulgaria Fights Cybercrime – Some Practical Aspects

Veni Markovski

Institutional development in Bulgaria

With the formation of the current Bulgarian government in August 2005, for the first time development of the information society became a top priority for the Bulgarian cabinet. This has happened largely as a result of Prime Minister Mr. Stanishev's personal agenda.

The Bulgarian government has created a special body, the State Agency for Information Technologies and Communications (SAITC) to the Council of Ministers. Previously, these issues were handled by the Ministry of Transport and Communications. Plamen Vatchkov has been appointed as head of the Agency. Both he and Prime Minister Stanishev, together with President Parvanov, former President Stoyanov, former Prime Minister Kostov and other prominent figures, are members of the Internet Society of Bulgaria.

SAITC is authorised to work in co-operation with the Secretariat of the National Security Council (NSC) in the field of co-ordination of cybersecurity activities, based on a resolution from the NSC to the Council of Ministers. The Agency was also given the task of ensuring the security of the governmental information network. Contacts have been made with similar agencies in the USA.

As one of the new countries that joined the European Union (EU) in the last round of accessions in January 2007, Bulgaria is making a concerted effort to combat cybercrime because both Bulgaria and the other new country, Romania, are widely regarded as the frequent origin of cybercrime. The combating of cybercriminals is the responsibility of the Interior Ministry's Department for Combating Organised Crime (GDBOP).

During 2006 considerable effort was also spent in Bulgaria on combating the usage of so called pirated software. Representatives from major software companies, mainly members of the Business Software Alliance (BSA) through their Bulgarian representatives, initiated a campaign to push for protection of their rights. The work of the GDBOP was criticised in the media, however, because it was aimed at end-users, while distributors of illegal CDs were left to be investigated by the Sofia City Police (SCP), which is a more general unit. Throughout the year, the SCP confiscated more than 160,000 CDs of software, films and music. At the same time the GDBOP managed to discover only 2,000 illegal CDs. Newly appointed Chief Prosecutor Boris Velchev also expressed his surprise that police action is aimed at end-users, while it is the organised distributors who should be pursued.

SAITC has also collaborated with the Bulgarian Police in shutting down spoof websites of foreign banks. US banks, which had requested the co-operation of SAITC, were impressed by the speed at which spoof websites were taken off the Internet. On average, this was achieved in less than two hours, thanks to the excellent co-operation between SAITC and the GDBOP.

The Bulgarian non-governmental and private sectors have also been supporting the fight against cybercriminals. Many organisations participated in the Safer Internet Day in 2006, and even more have signed up to participate in 2007. The Bulgarian Internet Service Providers have been co-operating with the Police in combating illegal activities on the Internet. With the co-operation of SAITC and the private sector, VeriSign, the registry for .com and .net top level domains, installed a Regional Resolution Server in Bulgaria, making it the first East European country to host such a server.

Further information can be found on the website of the South Eastern Europe Conference on Cyber Security Co-operation: www.cybersecuritycooperation.org

Veni Markovski (veni@veni.com) is a senior advisor on International Projects to the Chairman of the Bulgarian Governmental Agency for Information Technologies and Communications (www.daits.government.bg). He is the founding chair of the Bulgarian Internet Society (www.isoc.bg) and the ICANN regional liaison for Russia and the other countries in the Commonwealth of Independent States (CIS).

Some important cybercrime cases in 2006

In 2006 the GDBOP recorded a number of successes against cybercriminals, including the following:

20 January
Eight people were arrested in three Bulgarian cities. They had developed spoof bank websites, in order to perform phishing to try to collect personal data and credit card information from people all over the world. More than 90% of the credit card details that were stolen were from the US. The criminals, mainly teenagers, were using the stolen information to buy equipment, but they had also managed to obtain cash through a company dealing with express money transfers.

7 March
A 32-year old investigator from the second police district of Sofia, the Bulgarian capital, copied information from his office computer to his personal computer. He also installed a file-sharing programme, which gave access to his police documents. As a result, a Bulgarian journalist managed to download 260 files of important police documents.

27 March
A 38-year old man from Sofia has been charged with sending e-mail threats to two Bulgarian journalists. The man threatened that they would be killed if they did not leave the country. The e-mails were signed as if sent by the leader of a right-wing nationalist party in Bulgaria.

13 May
A 22-year old paedophile has been charged with distributing pictures with violence involving young children. In the last year he had also circulated pornographic pictures of young girls. At the beginning of May, the man published an announcement on one of Bulgaria's dating sites that he was looking for little children, for 'discreet sex', mentioning that he preferred children from the Plovdiv region. The man was caught while he was on-line using a computer at an Internet cafe to send illegal pictures to other users.

18 July
An organised gang offering sex with children was shut down. A Bulgarian newspaper published an article about a website which offered young boys for sex, after which the GDBOP managed to locate and charge three men in Sofia, who had built up an organisation to lure teenagers and underage boys into homosexual activities, meeting them first on the Internet.

Sentinels: Dutch Information Systems and Network Security Research

Rik D.T. Janssen

The need to obtain focus and mass in Dutch scientific research into the security of Information and Communication Technologies (ICT) led to the establishment of the Sentinels research programme on security in ICT, networks and information systems. Funded from both the public and private sectors to the tune of 10 M€, the programme started in 2004. It aims to give a very significant boost to security expertise in the Netherlands, by providing and managing resources for scientific research in information security; building a national ICT-security community; and disseminating the results into industry and government in the Netherlands. Links with European and international partners will also be expanded.

Sentinels receives public funding from three Dutch organisations: the Ministry of Economic Affairs, the Netherlands Organisation for Scientific Research (NWO), and the Technology Foundation STW.

Sentinels consists of two parts: the first involves scientific research, with results obtained in collaboration with industry; the second makes sure knowledge generated from these projects is exchanged with industry and government in the Netherlands (and possibly abroad).

Scientific research

Procedure - The granting of research projects was completed in an open competition in two rounds, one in 2004, another in 2006. Matching industrial contribution was required for all research proposals to ensure industrial relevance and commitment.

Both open calls invited scientific staff from Dutch universities and research institutes to submit a brief summary of a research proposal. These were evaluated using the following criteria: Does the proposal fit within the framework of the Sentinels programme? Is there sufficient matching from industrial partners? Does the proposal address both scientific and application issues?

After a positive evaluation, applicants were invited to submit a full proposal which was then reviewed by at least five external experts from industry and academia. To ensure that Sentinels proposals are innovative enough, whenever possible, international reviewers were also asked to comment.

Projects - In 2004, six proposals were granted, in 2006, five (see facing page).

Project progress monitoring and industrial input

For each project, a user committee has been formed. This committee makes sure that research stays on track and the researchers do not divert too much from the applications of their research. The committee is the forum for communication between project personnel and participating users (for example from education, industry, government, public authorities, hospitals etc.). Each committee meets about twice a year.

Knowledge exchange

Knowledge, generated from Sentinels' projects, is exchanged in a number of ways with interested parties such as industry and government:

- through the user committees
- through workshops, publications, websites and other public knowledge exchange events
- through the Sentinels Vici-researcher
- through the Sentinels Ambassador

Sentinels Vici-researcher - A Vici-grant is a Dutch grant for senior researchers at universities, who have shown that they can successfully develop their own innovative lines of research. They should also be able to act as coaches for young researchers. Using this grant, Vici-researchers will be able to build up their own research team, often in advance of a regular professorial appointment. Their lines of research are given a structural place within the research institution.

Sentinels will fund such a Vici-researcher in information security at a Dutch university. In the future, this person should evolve to a professor who is specifically responsible for education and research in the field of information security. By using budget from the programme, anchoring is ensured, and the Vici-researcher collaborates with all kinds of Sentinels activities such as knowledge exchange activities and promoting the Sentinels vision and range of ideas.

Sentinels ambassador - Like the Sentinels Vici-researcher, the Sentinels Ambassador is an important instrument to ensure that research results from Sentinels remain visible and accessible to industry even when the programme has ended. He is very capable in promoting the Sentinels range of ideas and in provoking questions from users, and he is the central point of access for anyone in need of security expertise in ICT in industry, government and research. The Sentinels Ambassador started work in 2005.

Programme management

Programme management is the responsibility of a hierarchy of committees

Proposals granted in 2004

JASON: Generic and Secure Remote Management Infrastructure

The core of the practical problem in this project is to build remotely manageable devices that are owned, controlled and/or accessed by several parties with different, sometimes even conflicting interests. Payment terminals are examples of such devices. For these devices to be successful, they will have to satisfy strong security and privacy guarantees.

IPID: Integrated Policy-based Intrusion Detection

Currently available intrusion detection tools monitor events at a relatively low level of abstraction. Due to the large number of events that occur at that level, these tools are either ineffective (by generating a large number of false negatives) or inefficient (by generating a large number of false positives). The objective of IPID is to increase both the effectiveness and efficiency of these tools by relating low-level events to a smaller number of events at a high level that are meaningful to the business.

Practical Approaches to Secure Computation

This project focuses on cryptographic primitives and methods which do not yet belong to the standard toolkit of the security engineer. As opposed to the situation where two trusting parties wish to secure their communication channel from malicious outsiders, secure computation can deal with a fundamentally different scenario of two or more parties who wish to achieve some joint task securely, even though they are mutually distrusting and wish to keep sensitive, private information secret from each other.

ProBiTe: Protection of Biometric Templates

ProBiTe concerns the integration of biometric identification in security systems. It focuses on the problems of combining biometric identification and template protection, since storing biometric templates in a database introduces security and privacy risks. These risks increase if the database is part of a network.

DeWorm: Worm Monitoring on Internet Backbones

DeWorm is aimed at developing an automated response system that is capable of detecting zero-day worms on the Internet, generating signatures for the attacks, and using these signatures to track and/or block malicious traffic. The goal is to make it fast enough to react to fast-spreading worms.

PINPAS JC: Program INferred Power-Analysis in Software for Java Card

The PINPAS JC project studies side-channel attacks on smart cards, in particular fault attacks for the JavaCard platform. Various fault-based attacks will be assessed, both at the source and byte code level. Formal methods will be used to specify security requirements and to prove the safety of reference applets. A software environment for experiments will be constructed, which can also be used for validation of the impact rating and the countermeasures developed during the project.

Proposals granted in 2006

S-Mobile: Security of Software and Services for Mobile Systems

The objective of S-Mobile is to create solutions for the trusted deployment and execution of mobile applications in heterogeneous environments. While today the development of third party applications for mobile platforms (mobile phones, cars) is tightly controlled by single entities (i.e., telecom operators, mainly due to security risks), there is a need to open the software market to third party applications. S-Mobile will make this possible.

VISPER: The Virtual Security Perimeter for Digital, Physical and Organisational Security

The security perimeter, which was once defined as the fence around the premises of an organisation, is becoming increasingly flexible and adaptable. This can be observed in the digital domain (where data moves from organisation to organisation through networks), the social domain (where one individual may play a variety of roles in co-operating organisations) and the physical domain (where appliances such as mobile phones and laptops move around). Alignment may be achieved by making the security perimeter explicit in business processes, security policies and security mechanisms.

SEDAN: Searchable Data Encryption

Personal digital data is stored in very diverse places, such as web e-mail or medical data. In our connected world, this data is often outsourced to external servers, sometimes in other countries. This raises concerns about security and privacy. This project addresses these concerns by storing the data in an encrypted format such that unauthorised parties cannot read the data, while still allowing efficient access by authorised parties.

VRIEND: Value-based Security Risk Mitigation in Decentralised Enterprise Networks

In industrial practice, security engineering is risk management: how to mitigate security risks given a finite budget? Today the Information Technology (IT) of a business is connected to that of others in a value web of business partners, suppliers and customers, which each have their own requirements. This creates new security challenges. One solution is to extend current risk management practices with methods and techniques to deal with security risks.

PEARL: Privacy Enhanced Security Architecture for RFID Labels

In RFID systems, very small tags communicate wirelessly with tag readers as soon as they are close enough to each other. The data transmitted by the tag can provide identification, location information or specifics about the product tagged. Widespread use of RFID tags raises privacy concerns, such as, for example, RFID tags in clothes. The goal of this project is to develop tools and methodologies for using RFID systems while preserving the user's privacy.

For extended summaries and more information on these projects, visit: www.sentinels.nl/projects/summaries/.

headed by the Steering Group, whose members represent industry and the financiers of the programme. A Programme Office assists with administrative support. Further details and a list of committee members can be found on the Sentinels website.

Conclusion

In the first three years, Sentinels has funded interesting and challenging research projects. The different events and collaborations have led to a much more coherent, public-private organised research community in this young field of expertise. By having both a Sentinels Vici-researcher and a Sentinels Ambassador, Sentinels information systems and network security research is actively promoted by experts from both a university and from industry.

Relations with government and the European Union have been strengthened. Many of the researchers are actively participating in EU-projects and the Sentinels Ambassador maintains permanent relations with the EU (for example, DG-INFSO, ENISA). In addition, one of the members of the Board (Edgar R. de Lange, Ministry of Economic Affairs) is on the ENISA Management Board. With more than half of the project time still ahead, Sentinels seems to be well on track already.

More information is available at: www.sentinels.nl

Rik D.T. Janssen (info@sentinels.nl) is Programme Officer at Technology Foundation STW, a Dutch funding organisation, and one of the founders of the Sentinels research programme. He runs the Sentinels Programme Office.

ENISA Short News – First Quarter 2007

Panagiotis Trimintzios

Call for membership of the Permanent Stakeholders' Group (PSG) of ENISA
The call for membership to PSG is open. Prospective candidates are asked to submit their applications by 15 May 2007. (www.enisa.europa.eu/pages/03_03.htm)

10th Management Board meeting of ENISA
From 22-23 March, the ENISA Management Board conducted its 10th Meeting in Heraklion, Greece. The agenda included: election of Chairperson and Vice Chairperson of the Management Board, the European Commission procured Evaluation Report on ENISA, the Board's short- and long-term recommendations for ENISA, process update and discussions on the preparation of the Work Programme for 2008.
(www.enisa.europa.eu/pages/02_01_press_2007_03_21_ENISA_10th_MB_Agenda.html)

Study on Emerging Risks in the area of Information Technology
ENISA presented its latest study on the Collection and Dissemination of Information related to Emerging Risks in the area of Information Technology. Projections regarding developments after 2010 show that the increasing dependency on ambient computing and communication devices will imply new risk scenarios affecting the privacy and security of all ordinary citizens.
(www.enisa.europa.eu/pages/02_01_press_2007_03_19_ENISA_Study_Emerging_Risks.html)

New deliverable on Risk Management/Risk Assessment for SMEs
ENISA has produced the publication *'Risk Management – Information Package for SMEs'*. This manual helps small and medium-sized enterprises (SMEs) in their efforts to apply Risk Management and Risk Assessment to their network and information assets efficiently.
(www.enisa.europa.eu/pages/02_01_press_2007_03_14_rmra.html)

The successful Awareness Raising Guide goes international
ENISA is promoting one of its most widely used publications, *'A Users' Guide: How to Raise Information Security Awareness'*, by translating it into French, German and Spanish.
(www.enisa.europa.eu/pages/02_01_press_2007_02_28_aw_guide_international.htm)

New EU Member State delegation from Romania visits ENISA
(www.enisa.europa.eu/pages/02_01_press_2007_02_27_romania_visit_2007.htm)

CERT co-operation – History and Future
ENISA and experts from CERT Polska have together completed a study into the co-operation between CERTs and its further facilitation by the relevant stakeholders.
(www.enisa.europa.eu/pages/02_03_news_2007_02_06_cert_updates.htm)

Technology Trends Report
ENISA's unit for Security Tools and Architectures has recently published its yearly *'Overview of Current Developments in Network and Information Security Technologies'*. This comprehensive report discusses the development of IPv6, wireless systems, Radio Frequency Identification (RFID), Voice over IP (VoIP) and multimedia, and Next Generation Networks (NGN) and the ways they impact on security. It also describes cryptographic primitives, routing security, Domain Name Server (DNS) security/anti-spam/identity management tools and endpoint security.
(www.enisa.europa.eu/doc/pdf/deliverables/enisa_overview_of_nis_developments.pdf)

Contact Network in NIS Technical Fora
ENISA has published a report on 'Technical Fora' that describes the way ENISA interacts with the research and standardisation community.
(www.enisa.europa.eu/doc/pdf/deliverables/enisa_contact_network_in_nis.pdf)

New website to tackle Emerging Risks launched
(www.enisa.europa.eu/rmra)

Safer Internet Day: educating young people in Europe
For the second year running, ENISA participated in the Safer Internet Day blogathon, which was held on 6 February.
(www.enisa.europa.eu/pages/02_03_news_2007_02_07_safer_internet_day.htm)

Looking ahead: ENISA's Work Programme 2007 is on-line
(www.enisa.europa.eu/pages/02_01_press_2007_01_16_work_programme_2007.htm)

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