



ENISA Quarterly

IN THIS EDITION

Early Detection, Warning and Alerting Systems

A Word from the Executive Director
A Word from the Editor

From the World of Security –
A Word from the Experts

Probe-based Internet Early Warning System
 Real-time Monitoring and Detection of Cyberattacks
 Building an Effective Early Warning System
 An Introduction to SCADA
 FIRST Conference puts Spotlight on Digital Privacy

From our own Experts
 EISAS: a feasibility study
 Data on Security Incidents and Consumer Confidence
 The European e-Identity Conference
 ENISA Awareness Raising Goes International
 European NIS Good Practice Brokerage

From the Member States
 Starting up an Early Warning System in the Netherlands
 Looking Back at the First Year of 'Digibewust' (The Netherlands)
 Bulgaria Fights Cybercrime
 Sentinels: Dutch Information Systems and Network Security Research

ENISA Short News

Page	
1	
2	
3	
3	
3	
5	
6	
9	
11	
12	
12	
13	
14	
15	
16	
17	
17	
20	
21	
22	
24	

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

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.sentinel.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-INFOS, 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.sentinel.nl

Rik D.T. Janssen (info@sentinel.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.