www.enisa.europa.eu

Interview – Demosthenes Ikonomou, Slawomir Gorniak and Panagiotis Saragiotis


Demosthenes Ikonomou


Slawomir Gorniak


Panagiotis Saragiotis

ENISA Security Tools and Architectures Section http://www.enisa.europa.eu/sta/ experts, Demosthenes Ikonomou, Slawomir Gorniak and Panagiotis Saragiotis, are the editors of two recently published ENISA reports on technologies with a potential to improve the resilience of communication networks. The second report on the subject was recently released with the results of a survey of European Network Operators assessing the efectiveness of three technologies – Internet Protocol version 6 (IPv6), Domain Name System Security Extensions (DNSSEC) and Multi Protocol Label Switching (MPLS) on the resilience of their networks. It follows a report, published earlier this year, focusing on the resilience enhancing features of those technologies.

What is the background for these report by ENISA and what is included in the reports?

The latest report has been published in the frame of ENISA's work programme in the area of resilience of public networks and addresses the technological aspects. In 2008 ENISA launched a call for experts that would advise on choosing some technologies for a more in-depth study of their resilience features. During a workshop held in Brussels in March 2008 http://www.enisa.europa.eu/doc/pdf/resilience/ENISA_Workshop_Report_final.pdf, it was decided that ENISA will concentrate on MPLS, IPv6 and DNSSEC and those are the technologies that this study tells about. Earlier in the year, ENISA published a study on the "Resilience Features of IPv6, DNSSEC and MPLS and Deployment Scenarios". The study provides an overview of the characteristics of the selected technologies as well as an analysis of their public communication network's resilience enhancing features. A number of deployment scenarios for the technologies are also presented.

Furthermore, in order to assess the effectiveness of the above mentioned technologies as well as problems and gaps that could compromise the availability of networks and services, a survey of network operators in EU Member States was carried out. The analysis of the inputs collected has become input to the

preparation of guidelines on the effectiveness of these three technologies, especially in terms of their potential to improve the resilience of public networks (but also highlighting their shortcomings). The guidelines produced in the course of 2009 will be primarily addressed towards National regulators and policy makers but also network operators.

What did the survey among the service providers tell you?
The survey aimed at assessing the effectiveness of the chosen three technologies. It was conducted on a sample of different European service providers, in order to cover a broad spectrum of them. The study presents the profile and some statistics of interviewees, but most importantly – how MPLS, IPv6 and DNSSEC are deployed, which of their resilience features are used, how its impact is depicted on Key Performance Indicators and which are in general the opinions of the operators on the use of the three technologies. Technical aspects of various deployments and challenges connected to them are also described.

Could you mention some of the most interesting findings?
One of the most interesting findings was that we don't really have to care about MPLS – since this technology is well established, widely used, its resilience features are well known, we can say that in this field we are on the right track. The situation is a bit different when it comes to IPv6 and DNSSEC. Operators see IPv6 almost only as a remedy to the shortage of IPv4 addresses, ignoring the resilience features of this protocol. The majority of the service providers in the EU, have plans to deploy IPv6 simply because they are really obliged to by the upcoming shortage of IPv4 addresses. On the other hand, DNSSEC is somehow not well known to the operators, although it can offer significant advantages in terms of improving the security of their offered services. Another interesting finding is that most operators don't see any need of further regulatory interventions concerning the three technologies, but policy actions, guidelines and recommendations of deployment.

What are your recommendations/conclusions?
The recommendations coming out of this report cover a quite broad area. The most important is that all service providers, connecting users to the Internet, should have resilience (not only security!) in mind from the earliest phase of development of their networks. This is a known sentence, but we still haven't reached the appropriate level of awareness in this area. To this aim, the existing expertise should be used, including best practices, experiences of other providers, knowledge bases etc. A very important issue is to train specialists that will be able to bring the knowledge down to the organisations.

What are ENISA's next steps in terms of analysing resilience of communication networks?
As a direct continuation of this study ENISA launched a number of activities in relation to DNSSEC, which is a technology that promises a lot in terms of resilience but is still not widely used. ENISA wants to foster the use of DNSSEC and is in the following years in the course of conducting a number of studies aiming to publish a number of guides on good practices for deployment, on awareness raising on DNS Resilience and for developing policy and practices statements for Trusted Anchor Repositories.

The initial focus in this area of work was on the technologies of the transport layer of communications networks. However, public communications networks constitute the basis upon which a plethora of applications/service is offered via service providers that in many cases are independent from the network operator. In this respect, what is of interest to users of ICT services is end-to-end resilience and security and not only a resilient and secure transport network. Rather than aiming at identifying performant architectures it is more appropriate to identify the design principles.

For press release:
http://www.enisa.europa.eu/pages/02_01_press_2009_05_28_resilience_report.html

Full reports:
"Resilience Features of IPv6, DNSSEC and MPLS and Deployment Scenarios"
http://www.enisa.europa.eu/sta/files/resilience_features.pdf

"Stock taking report on the technologies enhancing resilience of public communication networks in the EU Member States"
http://www.enisa.europa.eu/doc/pdf/resilience_tech_report.pdf

FAQ:
http://www.enisa.europa.eu/doc/pdf/faq_resilience_tech_report.pdf

For further details contact:
Demosthenes Ikonomou, ENISA, Demosthenes.ikonomou@enisa.europa.eu
Security Tools and Architectures, ENISA, sta@enisa.europa.eu
http://www.enisa.europa.eu/sta/

Ulf Bergstrom, Press & Communications Officer ENISA,
press@enisa.europa.eu, Mobile: +30 6948 460143