26/05/09

www.enisa.europa.eu

FAQ to ENISA's report on technologies to improve the resilience of communication networks

This FAQ covers the latest report prepared by ENISA, but also includes information about a previous report on resilience of communication networks focusing on resilience features of three technologies – Internet Protocol version 6 (IPv6), Domain Name System Security Extensions (DNSSEC) and Multi Protocol Label Switching (MPLS).

Why has ENISA conducted this report on resilience of communication networks?

In the context of its Multi-annual Thematic Programme, ENISA aims to evaluate and contribute in the area of resilience of public eCommunications in Europe. The main motivation for this work is the fact that resilience is an issue of critical importance to the EU economy and its citizens as it impacts day-to-day operation of businesses and affecting daily lives of EU citizens.

The ICT sector contributes 25 % to the EU's GDP growth and 40 % to its productivity growth, which further proves the importance of a secure European ICT infrastructure.

The purpose of this document is to provide information on and raise awareness of the network resilience and secure connectivity. ENISA's main objective is to offer a state-of-the-art survey about the plans to deploy and/or experienced and applied impact in terms of network resilience in relation to three technologies, namely IPv6, DNSSEC and MPLS.

The Agency has also recently also published a study on the "Resilience Features of IPv6, DNSSEC and MPLS and Deployment Scenarios" http://www.enisa.europa.eu/sta/files/resilience_features.pdf. The study provides an overview of the characteristics of the selected technologies as well as an analysis of their network's resilience enhancing features. Furthermore, a number of deployment scenarios for the technologies are described.

What is presented in this report?

The report presents the results of a survey among a number of European service providers in the EU, on the state-of-the-art of deployment of new and emerging technologies and their impact on improved network resilience. The report also includes recommendations and case studies of deployment scenarios.

Regarding IPv6, the survey aimed at receiving information and concrete figures about the deployment and usage of IPv6.

The goal of the survey on MPLS was to receive input about the deployment and use of MPLS, which was investigated in the context of its impact on network resilience as well as corporate network resilience strategies.

Regarding DNSSEC, its usage and its impact on public eCommunication networks resilience as well as on corporate network resilience strategies were investigated.

In addition to investigating the service providers views on MPLS, IPv6 and DNSSEC, this survey also aimed at gathering information on the regulatory environment and incentives given to service providers in regard to the deployment of these technologies.

What has ENISA done previously in this field?

The first report in the field of resilience of communication networks was published at the end of 2008: http://www.enisa.europa.eu/sta/files/resilience_features.pdf.
It included an analysis of the three technologies with emphasis on their resilience enhancing properties and the current deployment status.

During 2008 ENISA carried out an assessment of the effectiveness of three current or emerging technologies, namely MPLS, DNSSEC, IPv6 that have been identified by various stakeholders as having the potential to improve the stability and integrity of public eCommunication networks.

In October 2008 ENISA released a comprehensive European report on “*Stock Taking of Regulatory and Policy Issues related to Resilience of public eCommunications Networks*”, which presents 23 different national regulatory and policy strategies that are being used to facilitate, support and strengthen efforts to improve dependability and resilience of public eCommunications Networks.

The report identified that there was a significant variety in the deployed strategies, policies, initiatives and regulatory provisions across the EU, but despite these differences,

certain preliminary strategy commonalities across Europe for increasing resilience were highlighted.
http://www.enisa.europa.eu/pages/02_01_press_2008_10_29_strengthen_resilience.html

What were the findings of the first report?
Some of the conclusions from the first report stated that the three technologies are likely to help improve resilience, but some of their features may be overstated. In some cases there are even important concerns about increased risks to resilience by using these technologies. With respect to the deployment status, it has been found that all of them have undergone evaluation and trial deployments. However, some important issues may only be exposed through commercial, large-scale deployment.

How was the survey for the latest report conducted?
Unlike consumer surveys, where a sample large enough for statistical analysis is used, in our case we were limited in size of “population” (number of operators that have different scope of network security issues).

A number of interviews with network operators in EU Member States were carried out. The analysis of the inputs collected is expected to become the input for the preparation of guidelines for example on possible deployment actions.

The selection of interviewed service providers had for main goal to cover a wide and sufficient sample to cope with the requested topics of network resilience focusing on the three technologies.

Why were these three technologies chosen?

During the first quarter of 2008 ENISA organised a consultation workshop http://www.enisa.europa.eu/doc/pdf/resilience/Workshop/AGENDA.pdf bringing together all relevant European stakeholders in the area of resilience of electronic communication networks. The feedback received during this workshop helped the Agency to focus its efforts on the topics that mostly affect resilience of public eCommunications and prioritise them.

The workshop provided the opportunity to exchange views about, among others, regulatory and technical issues related to network availability and integrity measures, business continuity, emergency calls and priority communications, recovery and testing plans, DNS protection measures, security in BGP, and other issues.

http://www.enisa.europa.eu/doc/pdf/resilience/ENISA_Workshop_Report_final.pdf.

Can you describe these technologies briefly?

- IPv6 is the next-generation protocol for the Internet. It is designed as the successor of IPv4 flaws, providing a significantly larger address space compared toIPv4, Quality of Service hooks and built-in security features for encryption and authentication of end-to-end communication.

  DNS is a distributed dynamic database with a hierarchical structure that maps names of machines to protocol-level addresses. DNS is a service that the vast majority of Internet users and services rely upon. The operation of popular Internet services such as e-mail, the web, or instant messaging, depend on it. The basic principle of DNS is the use of human-friendly domain names for Internet service addresses, as names are readable and memorisable, instead of numbers (Internet Protocol addresses), which are practical for computers only.
- MPLS is a networking technology built around a label based forwarding paradigm. An MPLS header containing one or multiple labels (organized in a label stack) is attached to packets. Label Switch Routers (LSRs) forward these packets based only on the label information. Both Layer 2 (L2) and Layer 3 (L3) packets can be encapsulated in MPLS.

What does resilience mean and how is it improved?

By the terms resilience we refer to the ability of a system to provide and maintain an acceptable level of service in face of faults (unintentional, intentional, or naturally caused) affecting normal operation. The main aim of the resilience is for faults to be invisible to users.

Improving the resilience of a network is an issue of risk management, which includes risk identification, evaluation and acceptance or mitigation. A widely accepted list of risks to the resilience of networks includes flash crowd events, cyber attacks, outages of other support services, natural disasters and system failings. The mitigation of identified risks involves technical measures such as resilient design, resilient transmission media, resilient equipment and technologies that improve resilience.

What where the findings of this study?

- In terms of MPLS, the survey shows that MPLS is deployed already for some years and is well known as an established technology. MPLS improves network resilience significantly and its deployment was mainly driven by the demand for improved resilience.

- The interviews on IPv6 have shown that its deployment is:
  - Mainly driven by the increasing demand on IP address space.
  - Not the business driver for the introduction of IPv6.

  The interviews further show that no KPIs (Key Performance Indicators) have been defined for measuring the effectiveness of IPv6 in terms of resilience. The introduction and deployment of IPv6 still lacks of experienced best practices and demand for IPv6 is at a low level.

- In terms of upcoming or already deployed security extensions to the DNS service, the following conclusions can be drawn:
  - Operators agree that the deployment of DNSSEC provides essential improvement to network resilience and in particular to network security;
  - Information security policies focusing on DNSSEC security guidelines, key management and recommendations are missing;
  - Tools are missing for easy deployment of DNSSEC on all services that rely upon DNS;
  - Customers adopt DNSSEC easily and quickly after getting familiar with its improved resilience features.

- Regarding regulations the survey shows that:
  - Regulatory intervention either at national or EU level was not considered necessary;
  - Existing regulatory environment is seen to be adequate;

- The need for information security policies, security practices and best practice guidelines relating in particular on IPv6 and DNSSEC deployment, management and operation was identified.

What are ENISA's conclusions and recommendations in this report?
Some of ENISA's recommendations in this report on resilience of communication networks, concerning IPv6 and DNSSEC are briefly presented below.

Regarding IPv6 the expert views on the shortage of available public addresses is that this will occur by 2011-2012. There are a variety of possible options, but the one aiming at supporting the IPv6 adoption in Europe is likely to bring the greater benefits for Europe, its economy and society. Possible actions should address common IPv6 connectivity availability, awareness of IT managers, network security during the integration, availability of a sufficient pool of trained specialists and proper exploitation of European expertise.

A more pro-active solution is the launch of targeted actions by ENISA, aimed at supporting and encouraging resilient IPv6 networks in Europe.

Following the survey results some of the recommendations in terms of IPv6 are:

- Ensure that service providers, network operators and IT managers are made aware of the resilience features of IPv6
- Ensure existence of a sufficient pool of IPv6 trained specialists
- Encourage proper exploitation of European expertise on IPv6 resilience features, in particular in best practice and operational excellence on network resilience

Adoption of DNSSEC is not going to be a project with immediate return on investment but rather a long term strategy aiming to increase the trust in the Internet,. ENISA's recommendations around DNSSEC, based on the survey results are:

- Ensure that service providers and network operators are made aware of the resilience features of DNSSEC;
- Ensure existence of a sufficient pool of DNSSEC trained specialists;
- Encourage proper exploitation of European expertise on DNSSEC resilience features, in particular in best practice and operational excellence on network resilience;
- Encourage key management policies, encourage the development of information security policies focusing on DNSSEC security guidelines and security management principles;
- Promote coordination and alignment of security management between service providers within the EU member states;
- Encourage the development of DNSSEC deployment recommendations;
- Promote distribution of best practices and operational experience in DNSSEC business.

What are the next steps in the area of resilience?

In 2009, ENISA will continue investigating possible ways for enhancing the resilience of public eCommunication networks, not limiting itself to technologies, architectures and protocols. In this context, incentives will also be considered with a view on their impact on business practices and the associated regulatory framework.

For full report:
The first report: http://www.enisa.europa.eu/sta/files/resilience_features.pdf

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

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