Recommendations

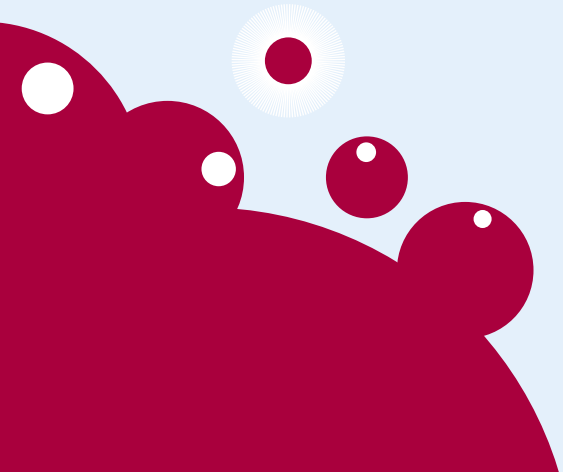
IPv6:

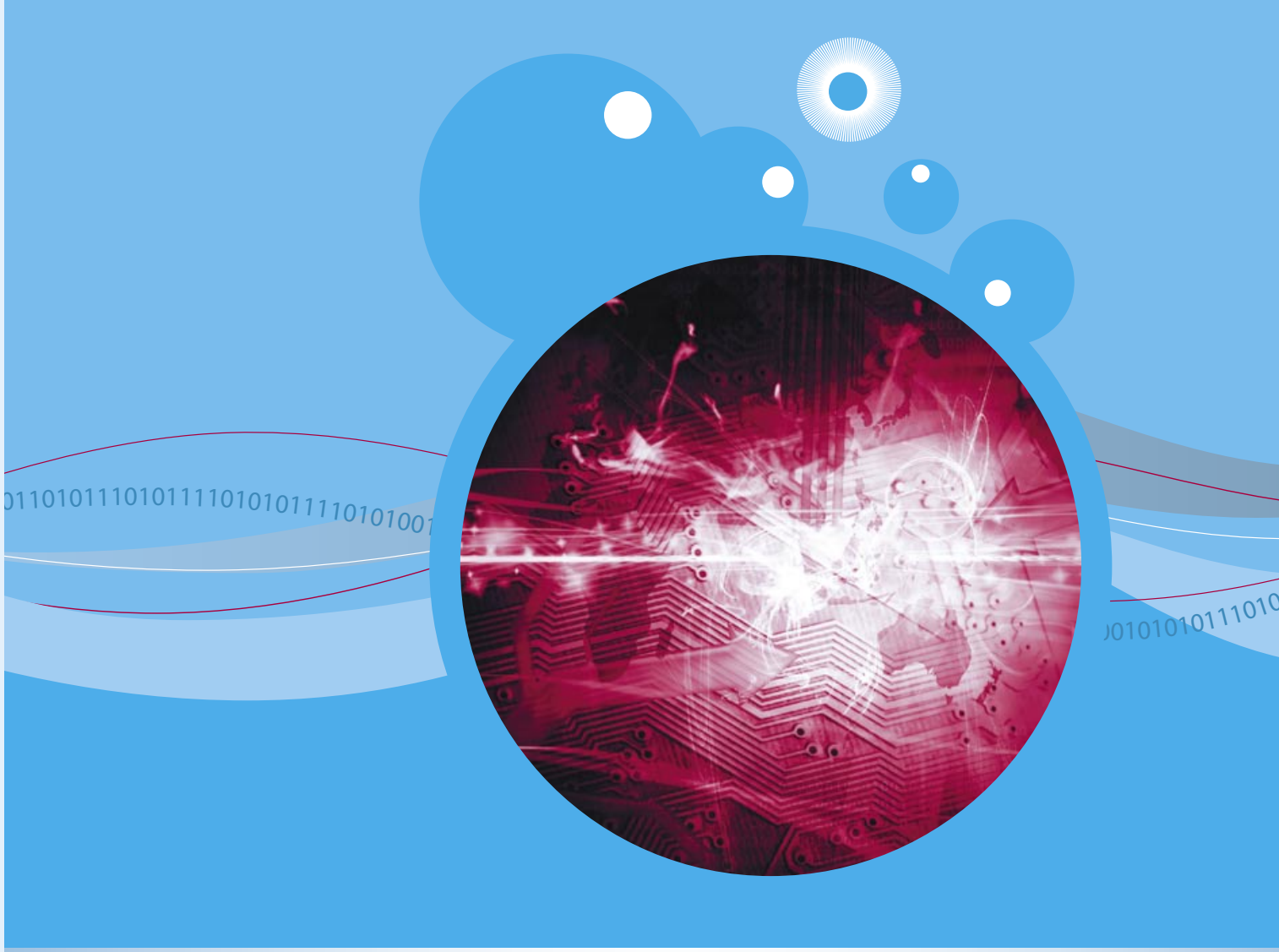
- Ensure that service providers, network operators and IT managers are made aware of the resilience enhancing features of IPv6.
- Ensure existence of a sufficient pool of IPv6 trained people.

DNSSEC:

- Make sure that service providers and network operators are made aware of the resilience features of DNSSEC.
- Encourage the development of key management policies.
- Ensure that information security policies focus on DNSSEC security guidelines and security management principles;
- Promote coordination and harmonisation of security management between service providers within the EU.
- Encourage the development of DNSSEC deployment recommendations.
- Promote distribution of best practices and exchange of operational experiences in DNSSEC business, emerging technologies and architectures.

The complete reports are available for download at:
http://www.enisa.europa.eu/sta/h_library.html.





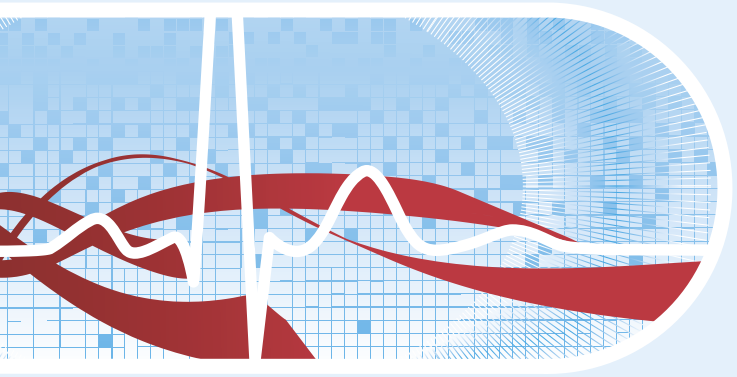
For further information please contact:

European Network and Information Security Agency – ENISA
Security Tools and Architectures Section
http://www.enisa.europa.eu/sta/
Email: sta@enisa.europa.eu

P.O. Box 1309 71001 Heraklion - Crete - Greece
Fax: +30 28 10 39 1410

Analysis of Technologies with a Potential of Enhancing the Resilience of Communication Networks

enisa
European Network and Information Security Agency



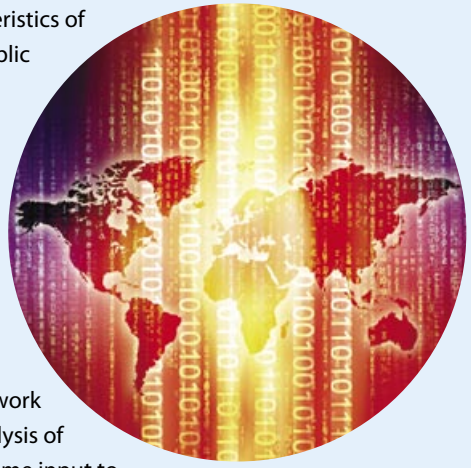
Analysis of Technologies with a Potential of Enhancing Resilience of Communication Networks

Any component of a networked service may fail due to equipment malfunction, human error, or deliberate malice. The growing complexity and inter-dependency of modern network services results in individual failures having widespread and unanticipated consequences. By the term "*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.

Resilience and security of communication networks and services that they support is an issue of critical importance to the EU economy and its citizens as it impacts day-to-day operation of businesses, affecting daily lives of EU citizens. The European Commission in its reform proposals amending the current regulatory framework (eCommunications Directive) acknowledges the importance of resilience of communications networks and services by proposing increased responsibilities for network operators through stronger obligations to ensure security and integrity as well as the mandatory requirement for breach notifications to National Regulatory Agencies (NRA) and consumers.

ENISA, the European Network Information Security Agency, recognised this need and launched a programme with the ultimate objective to collectively evaluate and improve the resilience of public communications networks in Europe. In terms of technologies, the deployment of existing and/or emerging technologies such as Multi Protocol Label Switching (MPLS), Internet Protocol version 6 (IPv6) and Domain Name System Security Extensions (DNSSEC) are promising for providing increased network resilience. During 2008 ENISA carried out an assessment of the effectiveness of those technologies.

This analysis was carried out from two perspectives. The first consisted of analysing the characteristics of the selected technologies and their public communication network's resilience enhancing features http://www.enisa.europa.eu/sta/files/resilience_features.pdf. In parallel, the effectiveness of the above mentioned technologies as well as problems and gaps that could potentially compromise the availability of networks and services was assessed through a number of interviews of network operators in EU Member State. The analysis of the received inputs is expected to 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, policy makers and network operators.



Key Survey Findings

MPLS:

- MPLS is deployed already for some years and is well known and established technology.
- MPLS improves network resilience significantly.

IPv6:

- IPv6 deployment is mainly driven by the increasing demand on IP address space.
- Network resilience is not a business driver for the introduction of IPv6
- No improvement of resilience has been observed by service providers after the introduction of IPv6.
- The introduction and deployment of IPv6 lacks of experienced best practices.
- Customer demand for IPv6 is at a low level.

DNSSEC:

- The consensus among service providers indicates that the deployment of DNSSEC is expected to improve network resilience and in particular network security.
- Information security policies focus on DNSSEC security guidelines, key management and recommendations are missing.
- Tools facilitating easy deployment of DNSSEC on all services that comprise the DNS are missing.
- Customers adopt easily and quickly DNSSEC after getting familiar with its improved resilience features.

Regulations:

- Regulatory intervention either at national or EU level was not considered necessary by the interviewed service providers since the existing regulatory environment is considered to be adequate.
- The need for information security policies, security practices and best practice guidelines relating in particular to IPv6 as well as DNSSEC deployment, management and operation was identified.