FAQs on "Priorities for Research on Current and Emerging Network Technologies"

1. Why did ENISA write a report on this topic?

This report is expected to contribute to the process of identifying research topics for projects on a European level by, on the one hand, offering knowledge of industry needs to potential research institutions and, on the other hand, drawing the attention of decision-makers to the most relevant areas of network and information security where research is much needed over the next three to five years.

2. What is the goal of the report?

This report has two main goals:

- to identify recent networking trends and their impact in terms of networking resilience as well as network and information security,
- to identify research priorities in the areas of information security relating to network resilience.

To achieve these aims, several areas of current and emerging technologies that have an impact on network resilience (both positive and negative) were identified and an analysis of the threats they may present to a network was conducted.

As a final result, several areas where research is much needed over the next three to five years were identified.

3. What does the ENISA report say?

Five areas have been assessed in the report as presenting the biggest need for research within a window of three to five years:

- cloud computing
- real-time detection and diagnosis systems
- future wireless networks
- sensor networks
- supply chain integrity

These areas are analysed and described in detail in the core of this report.

4. What is *cloud computing* and why is there a need to research this area?

Cloud computing denotes a computing paradigm and associated set of business models and technologies used to provide network-based services that are accessible by a variety of platforms for numerous types of operations. Different types of popular services, such as on-line email, social networking services, on-line enterprise CRM, or outsourced on-line employee benefits services could be considered 'cloud computing'; however, the term is more frequently used in conjunction with distributed enterprise services with a broader scope that include business process automation and office application suites. Platform (client and server) virtualization is a part of some of the cloud offerings, but is generally not considered a defining trait of cloud computing.

All the components of the design of a particular service need to be secure and managed in a secure and transparent fashion in order for the service to be secure and resilient. Everything, from network design, operations and services development process, to the configuration of the receiving devices, the behaviours of users, and the responsibilities of providers and their relationships with customers, has a role in improving the resilience of a system. This complexity requires active collaboration among all the interdependent components of the solution. This is especially important for cloud computing since it changes the required approach to security and resilience.

5. What are *real-time detection and diagnosis systems* and why is there a need to research this area?

The aim of detection and diagnosis systems is to detect faults, disruptions or decreases in the services provided due to intentional or unintentional actions, and to respond accordingly without severely deteriorating the network or system performance and reliability.

Given the increasing velocity of malware spread through networks, detection is becoming insufficient if corrective action cannot be taken very rapidly – this raises the opportunity to explore machine-aided response (ie, enabling the operators to respond faster) and eventually autonomic response. This is closely related to the accuracy of the detection systems, raising the bar significantly. The optimal detection and diagnosis system would take accurate decisions in real-time and respond promptly. Employing efficient real-time fault detection and diagnosis systems is of substantial importance to guarantee the resilience of the protected system.

6. What is meant by *future wireless networks* and why is there a need to research this area?

Resilience has become an important concern in the design and architecture of of future wireless networking architectures such as mobile ad-hoc networks (MANETs) and wireless mesh networks (WMN).
While typical approaches to protection are focusing on proactive security architecture mechanisms such as authentication, access control, cryptographic algorithms and protocols for protecting the wireless communications, they are proven to be not sufficient enough, since new attack methods appear and exploit the proactive measures taken. In real world environments, where security attacks take place often, the goal is to build resilient architectures through reactive mechanisms that will be able to adapt and resist at an acceptable level, based on predefined requirements for the security levels.

Unlike the wire-line networks, the unique characteristics of future wireless networks pose a number of nontrivial challenges to resilience and security design, such as an open peer-to-peer network architecture, a shared wireless medium, stringent resource constraints and a highly dynamic network topology. These challenges clearly make a case for building a second line of defence of cross-layer resilience solutions that achieve both broad protection and
desirable network performance, in the situation where proactive security mechanisms either fail or are not sufficient to defend the networks against attacks. Research is much needed in the area of fundamental resilience mechanisms for protecting the

multi-hop network connectivity between nodes in MANETs and WMNs in terms of increasing the robustness of the reactive networking mechanisms and of detecting and recovering from attacks or failures.

7. What are *sensor networks* and why is there a need to research this area?

Sensor networks are widely installed around the world in urban, suburban and rural locations – on the ground and on various airborne platforms, including balloons, high-altitude platforms (HAPs), unmanned airborne vehicles (UAVs) and satellites. At present, few of them have a purpose that involves real-time interaction with human beings. The Internet of Things will change this, and make sensors and actuators, first class devices, fully visible with end-to-end connectivity. We will depend on their capabilities and the data they provide for healthcare, energy management, monitoring the environment, transportation, homeland security and many other aspects of life.

Our assumption accordingly is that they are inevitably becoming a part of critical infrastructure. We describe how we will depend on them and explore the nature of, and challenges to, the processes that measure and control this dependency. The resilience of these systems will become a key discriminator in assessing their quality and performance and in generating a positive or negative perception of our reliance on them.

8. What is *supply chain integrity* and why is there a need to research this area?

Supply chain integrity in the ICT industry is an important topic that receives attention from both the public and private sectors (ie, vendors, infrastructure owners, operators, etc). Currently, it is addressed separately in different industries. Important solutions have been developed in various ICT segments in this context. These solutions have led to considerable progress and need to be studied in a comprehensive research study dealing with supply chain integrity.

A common framework for supply chain integrity would help identify linkages across various industries that would magnify the impact of those solutions. It needs to include technologies, best practices and innovative business models. All the constituencies need to work together to improve risk management, which is related to anti-counterfeiting and the security of critical systems and services.

There is general agreement across industries and other stakeholders about the need to identify and appropriately share good practices and advanced research in the area of ICT supply chain integrity. Because of its complexity and industry-specific technology and business issues, studying this subject is challenging for researchers. A good model for such joint studies needs to be defined.

9. What are ENISA's conclusions regarding *cloud computing*?

Establishing a clear chain of trust from the client application to the server application and/or data involves new challenges. The hardware-software chain of trust needs to be adapted to the cloud environment. The defence-in-depth practices employed in protecting data need to be scaled and adapted to protect cloud services. Research is also needed to identify gaps and effective solutions to increase the levels of assurance that can be provided through the cloud computing environment.

Aspects of data protection in the cloud environment pose new challenges that may benefit from focused research. In addition to the technical issues, policy and law enforcement challenges are also areas of considerable interest. Cloud computing models can benefit greatly from the international harmonization of data protection, retention and privacy regulations. Research is also needed to better understand the best practices and policies that will facilitate effective incident handling.

Research and industry collaboration is needed to develop guidelines and standards that will allow meaningful and unambiguous evaluation and certification of the assurance of cloud-based services. New business and policy mechanisms are required to provide incentives for implementing the effective levels of protection.

There has not been any significant standardization activity that has led to proprietary application programming interfaces (APIs). Making service and data migration easier would allow users easier migration between the traditional data centre model and the cloud.

10. What are ENISA's conclusions regarding *real-time detection and diagnosis systems*?

Although RTDDS have already received much attention, there are many important challenges and open issues that demand additional investigation. Researchers, developers and vendors should be encouraged to undertake additional research and to develop safer, more accurate RTDDS.

The effective development of a detection and diagnosis system that combines the advantages of *misuse* and *anomaly detection*, and is thus able to minimize false alarms while detecting unknown attacks, is a challenging task.

The interconnection of small embedded devices with limited power makes the problems of measurement and detection harder. Scalable solutions and technologies are therefore needed. A trend in networking architectures is the collapse of backbone networks into Layer 2 networks. This change deeply impacts the management and monitoring capabilities of RTDDS. The increasing use of wireless communications has enabled the development of some intrusion detection approaches specifically tailored for these transmission media, but the research remains in its initial stages. An explosive uptake of the cloud computing paradigm creates a demand for RTDDS that are suitable for cloud service providers.

Other relevant areas for research in the field of RTDDS include the performance and effectiveness of detection and diagnosis systems, human-computer interaction issues, management and update issues, vulnerabilities assessment and true real-time monitoring.

11. What are ENISA's conclusions regarding *future wireless networks*?

Protecting future wireless networks in a reactive manner is a complex issue.

The majority of the secure routing protocols proposed for mobile ad hoc networks do not support the protection of QoS-aware routing metrics, while intrusion and misbehaviour detection and recovery mechanisms proposed for wired networks and for mobile ad hoc networks are not optimized for mesh networks; they should be adapted to the characteristics of mesh networks to increase their performance in terms of effectiveness and reliability.

Research should focus on the requirements for resilience in wireless networks robust networking mechanisms, and intrusion detection and recovery mechanisms.

12. What are ENISA's conclusions regarding *sensor networks*?

The present and future Internet and sensor networks are increasingly being integrated. This implies significant change and innovation to ensure that they converge successfully. The Internet must evolve to support a massive number of additional end-points that are aggregated in various ways into overlapping sub-networks and that are of relatively poor capability in energy, processing power, communications links and storage. The sensor networks must evolve to be able to participate fully in a network architecture where they appear as secure devices.

A great deal of recent research has been done on the assumption that the poor capabilities of small wireless connected sensor nodes will remain a constraint. It has focused on the innovations in architectures and protocols at various layers but not on issues that will affect resilience and attack. These are articulated as design choices, including, among others, fault tolerance to inevitable errors and losses of data and connectivity; scalability, ie, a wide range of variability in dimension, range, and population of the nodes and in their interactions in time and space; and topology, as pervasive access to a wide range of communications pathways will allow more ad-hoc, transient connectivity and mobility with consequences on routing.

As well as addressing the negative impacts of resilience vulnerabilities, it is necessary to make sure that sensor network applications operating over critical infrastructure are protected effectively as well as being thoroughly tested and correctly planned and deployed. Research should focus on the issues of authentication, access control, security of data and key management, and effective mechanisms of protection against intrusions.

13. What are ENISA's conclusions regarding *supply chain integrity*?

In the world where almost all aspects of life rely on electronic equipment, the subject of the integrity and safety of the supply chain seems to be crucial for maintaining trust and confidence in the infrastructure and in the digital economy. The area is ready for new research challenges that will result in a new generation of technologies and approaches to ICT supply chain integrity, in areas ranging from supply chain management and execution to preserving system authenticity and building new integrity assessment tools.

Research in this area can also provide a foundation for a common framework for addressing the key issues in the ICT supply chain that need to be endorsed and adopted by all the stakeholders. There are significant opportunities for research to define new models, mechanisms and techniques addressing multiple areas of the ICT supply chain. The subject should be treated on an international level, as the integrity of ICT supply chains is an issue crucial to all constituencies building, configuring and using ICT systems, including the private sector, academia, governments and international organizations.

The full report:
http://www.enisa.europa.eu/act/res/technologies/procent

The press release see:
http://www.enisa.europa.eu/media/press-releases/future-eu-research-it-security-priorities-identified-always-online-availability-in-focus

For further details contact:
Ulf Bergström, Spokesman, ENISA press@enisa.europa.eu,
Mobile: +30 6948 460143
Slawek Gorniak, Security Expert, slawomir.gorniak@enisa.europa.eu