

Priorities for NIS research

ENISA perspective

Sławomir Górniak

European Network and Information Security Agency

30th TF-CSIRT Meeting
Heraklion, 21st May 2010

Activities for 2008-2010

- ★ Multi-annual Thematic Programmes
 - ★ Strategic priorities for ENISA
 - ★ Implemented through a number of Work Packages
- ★ Current focus on:
 - ★ Improving Resilience in European e-Communication Networks
 - ★ Developing and Maintaining co-operation between Member States
 - ★ Identifying Emerging Risks for creating trust and confidence
 - ★ Privacy and Trust in the Future Internet

Resilience

★ Perspectives

- ★ Availability
- ★ Performance

★ Risks

- ★ Flash crowd events
- ★ Cyber attacks
- ★ Outages to other services, affecting the network
- ★ Natural disasters
- ★ System / Logical failings

★ Mitigation



PROCENT: Cloud computing

★ Research challenges

- ★ Trusted cloud computing models
- ★ Data protection in the cloud paradigm
- ★ Cloud assurance (guidelines and standards)
- ★ Standardised data format
- ★ Service availability

PROCENT: Real-time detection and diagnosis systems

★ Research challenges

- ★ Effective mechanisms
- ★ Adaptability to emerging network architectures
- ★ Evaluation of performance and effectiveness
- ★ Human-Computer Interaction
- ★ True real-time monitoring
- ★ Privacy issues

PROCENT: Future wireless networks

★ Research challenges

- ★ Robust networking mechanisms
 - ★ Protecting route discovery
 - ★ Reactive distance vector routing
 - ★ Proactive link-state routing
 - ★ Protecting resource reservations
 - ★ Error recovery mechanisms
- ★ Intrusion detection and recovery

PROCENT: Sensor and actuator networks

★ Research challenges

★ Assumptions

- ★ low memory
- ★ low CPU usage
- ★ low power

★ Authentication and access control

★ Effective protection against intrusion

★ Protection of data and key management

PROCENT: Supply chain integrity

★ Supply chain attacks

- ★ Insertion of malicious code
- ★ Creation of counterfeited elements

★ Challenges

- ★ Common guidelines
- ★ Tools, processes, and controls
- ★ Effective methods for end users
- ★ Easy detection of counterfeiting / overproduction
- ★ Common business model

PROCENT: Supply chain integrity

★ Opportunities for research

- ★ Improved and innovative trust models
- ★ Evaluation and integrity checking techniques
- ★ Study of good practices
- ★ Solutions to detect and prevent counterfeiting / overproduction
- ★ New approaches to security assurance
- ★ Inventory/configuration control and maintenance
- ★ Approaches for assessing policy needs on the global scale

ENISA Work Programme 2010

★ MTP1 – Improving resilience in European e-Communication networks

- ★ WPK 1.1- Underpin stakeholders' efforts to deploy ENISA's information sharing and incident reporting good practice guides
- ★ WPK 1.2 – Assist providers in enhancing the resilience of their networks
- ★ WPK 1.3 – Investigation of innovative actions
- ★ WPK 1.4 – Empower stakeholders towards the first pan-European exercise



Thank You

Sławomir Górniak,
European Network and Information Security Agency
Technical Competence Department

Email: Slawomir.Gorniak@enisa.europa.eu

★References

- ★<http://www.enisa.europa.eu/act/res/technologies>
- ★<http://www.youtube.com/user/enisasta>