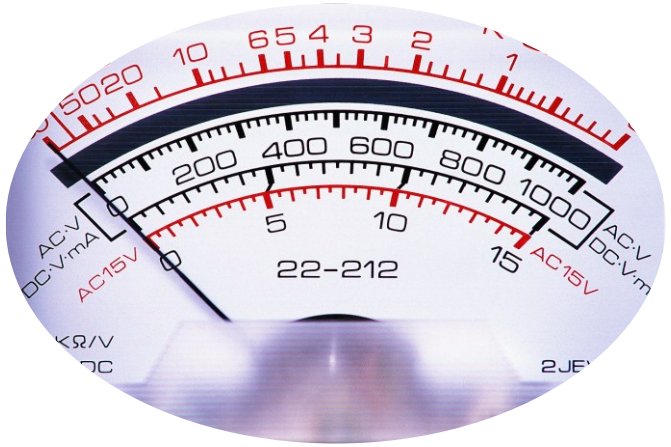
Brussels, 29 February, 2012

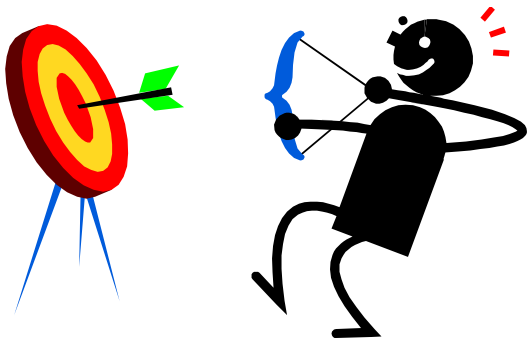


Rafał Leszczyna
Resilience and CIIP Program, ENISA

ENISA RECOMMENDATIONS ON SMART GRID SECURITY

The Aim and Scope of the Study

- SG Security „panorama”
  - Threats, risks, challenges
  - National and pan-European initiatives
- Identification of gaps
- Recommendations
- Follow-up
- Dialog between the stakeholders



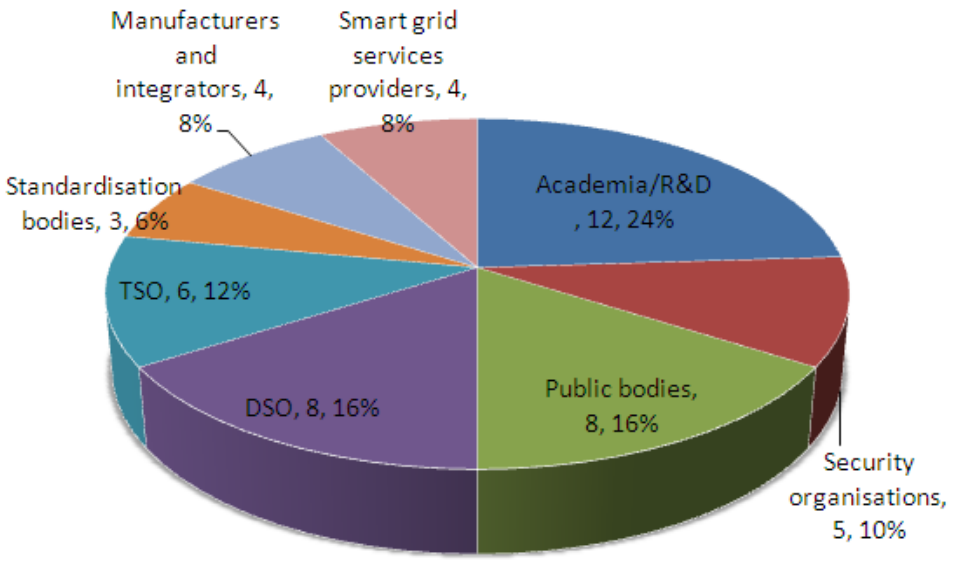
The Approach

Desktop Research

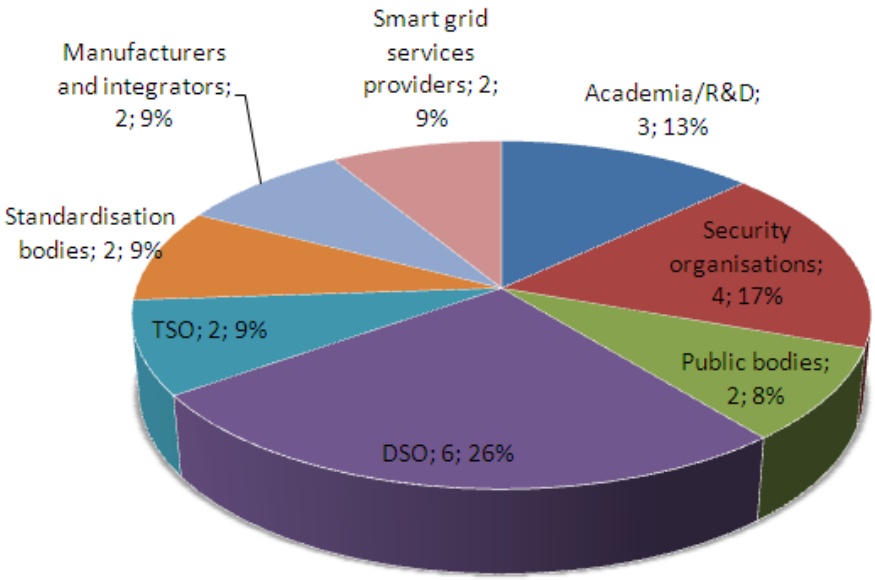
- **More than 230 documents analysed**
  - **High reputation publications: technical reports, specialised books, good practices, standards, papers.**
  - **Other technical documents: whitepapers, product/services, sheets, etc.**
  - **Latest news: forums, mailing lists, twitter, blogs, etc.**

Survey and Interviews

- 304 experts contacted
- 50 answered, 23 interviewed



Received questionnaires



Interviews

Key Findings

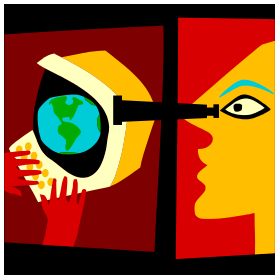
Categories

- The biggest challenges of the SG
- The SG business case
- Basic components of the SG
- SG pilots and cyber security
- Basic aspects for a secure SG
- SG cyber security challenges
- Current SG initiatives on cyber security
- Risk assessments in SG
- Certifications and the role of NCAs
- Measuring cyber security in the SG
- Managing cyber attacks
- Research topics in SG security

Around 90 Key Findings

Key Findings

- **Cyber security, privacy and fraud prevention – crucial for the success of the smart grid**
- **Cyber security and privacy addressed independently**
- **Security addressed more as an overlay than as part of the design phase**



- **Defence in depth + security by design = guiding principles**
- **Integration of the end user property + intensive use of ICT + the use of Internet and public networks → much higher attack exposure**

Key Findings

- **Reliability and resiliency – key factors driving the smart grid busines**
- **Lack of the definition of the smart grid: "*Are added-value services (e.g. demand-side management) included? Is the smart home/industry/building part of the grid?*"**
- **Lack of a standard reference architecture**
- **Cyber security – only a second-line issue in smart grid pilots and is tested in massive deployments**
- **Necessary to train and raise awareness among operators, manufacturers and consumers**

Key Findings

- **Security efforts should not only focus on smart meters but also on substation automation, micro grids, SCADA, telecommunication networks, etc.**
- **Infrastructures at consumer's premises should be fool-proof since they are out of the control of the DSO or the service provider**
- **Lack of expertise and budget limits in the root causes for dismissing cyber security**
- **Some technical challenges: 1) integration of legacy systems, 2) secure devices, 3) activity monitoring**

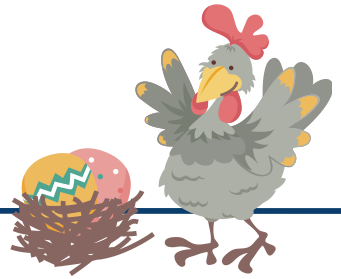
Key Findings

- **Inexistent/incomplete regulations can have security consequences (e.g. too quick start of meter roll-outs; risks of integrating gas, heat and electricity)**
- **Security initiatives: duplicity of topics, lack of visibility, same experts in all initiatives, …**
- **Need for a coordinating entity on smart grid cyber security and privacy initiatives**
- **DSOs and TSOs should undertake mandatory risk assessments**
- **Need for a specific risk assessment methodology**

Key Findings

- **NCAs should certify the security of SG product/set-up and organisations**
- **Today, standards-driven security certifications can be a burden because of immaturity of SG technology**
- **Alternative: quick tests (e.g. white box and code audits)**
- **Cyber security must be measured in terms of robustness, reliability and resiliency**
- **Regulatory pressures – in case of incompliance**
- **(In)compliance results to be public if not revealing sensitive information**

Key Findings



- **TSOs and DSOs used to dealing with incidents**
- **DSOs and TSOs in charge of cyber incident detection (IRRIS FP7 project)**
- **Operators to be obliged to report cyber incidents**
- **Controversy on the need for a pan-European entity in charge of coordinating large scale cyber security incidents**
- **Central coordination prone to slaw reacting; Alternative: decentralized approach by improving procedures**
- **CERTs not to be the central entity; To be active in incident management: advising the normal crisis management structures in place at the EU and MS**

Recommendations

- **R1: Improve the regulatory and policy framework on SG cyber security**
- **R2: Create an EU-level coordinating entity for SG cyber security initiatives**
- **R3: Foster dissemination, knowledge sharing, awareness rising and training**
- **R4: Develop a minimum set of reference standards and guidelines**
- **R5: Promote the development of security certification schemes for products and organisational security in the SG**
- **R6: Foster the creation of test beds and security assessments**
- **R7: Further discuss the creation of a European entity and the role of CERTs in the coordination of large scale cyber incidents**
- **R8: Foster research in SG cyber security leveraging existing research programmes**

R1: Improve the regulatory and policy framework on SG cyber security

- Key aspects:
  - Develop specific documents and regulations
  - To define the root principles, challenges, goals and needs of a European-wide cyber security strategy for SG

- The regulatory framework should look for:
  - Considering privacy and cyber security altogether
  - Defining security objectives for current SG deployments (e.g. smart meters roll-outs)
  - Demanding mandatory risk assessments
  - Demanding security certifications: products and organisations
  - Establishing regulatory pressures (e.g. fines) for not complying companies
  - Making public (in)compliance results
  - Asking for reporting in case of cyber security incidents

R2: Create an EU-level coordinating entity for SG cyber security initiatives

- Key aspects:
  - Establish a unique central coordinating entity at the EU-level
  - With a global vision of EU and MS's initiatives on cyber security of SG (e.g. SGIS, DG INFSO's ad-hoc EG, …)

- Objectives:
  - Avoiding duplicated work
  - Enhancing communication among task forces and work groups
  - Defining a clear and unified strategy for ongoing and new initiatives
  - Identifying synergies among national and European initiatives
  - Disseminating the work being done
  - Establishing a common dictionary of technical terms
  - Managing lobbies

R3: Foster dissemination, knowledge sharing, awareness rising and training

- Key aspects:
  - Under the umbrella of the EU-coordinating entity
  - Promoted by MS and EU
  - Targeting grid operators, electricity service providers, manufacturers and end consumers
  - Actively involve academia/R&D
  - Increase DSO/TSO leadership

- Objectives:
  - Awareness-rising of C-level staff
  - Training for manufacturers on how to build secure devices and applications
  - Training for operators on threats and risks affecting security and resiliency of the grid
  - Awareness-rising and training on fraud prevention, privacy, etc. of end consumers and service providers
  - Encouraging existing initiatives to actively disseminate their work
  - Analyse the creation of a knowledge sharing platform for DSOs and TSOs (and possibly other stakeholders) considering involving CERTs

R4: Develop a minimum set of reference standards and guidelines

- Key aspects:
  - Led by the EU in collaboration with MS
  - Leverage ongoing initiatives (e.g. DG INFSO's ad-hoc EG)
  - Should set the basis for mandatory security assessments and for developing certification schemes
- Minimum set of standards and guidelines:
  - A common reference architecture
  - A reference risk assessment methodology
  - Technical requirements for SG systems
  - Guidelines on security governance
  - Guidelines for achieving fool-proof HAN/IAN/BAN

R5: Promote the development of security certification schemes

- Key aspects:
  - Promoted by EU public authorities
  - Target product and organisational security
  - Leverage existing initiatives such as CC, ISA99 and ISO 27K
- Objective:
  - Harmonize security and resilience requirements across MS
  - Establish the base for a minimum set of auditable controls
  - Accredit NCAs for certificate issuance

R6: Foster the creation of test beds and security assessments

- Key aspects:
  - Both tasks should be promoted by MS and the EU
  - Test beds: should perform quick/agile security tests based in basic security principles (e.g. WIB's requirements for vendors)
  - Security assessments: incentivize independent security assessments and pen-tests on DSOs, TSOs and other actors
- Objective:
  - Fill the gap while certification schemes are developed
  - Once they are ready, test beds could become accredited certification evaluators

R7: Discuss the creation of a European entity and the role of CERTs in the coordination of cyber incidents

- Key aspects:
  - To be discussed by EU and MS
  - Manage large scale cyber incidents reported by operators
  - Coordinate transnational electricity infrastructures and national CIP agencies
- Envisioned characteristics of the coordinating entity:
  - To have a global overview of the situation of the European grid
  - To have direct communication with normal crisis management structures and CERTs
  - Responsible for escalating alarms
  - Act in accordance with political decisions and pre-established incident handling strategies
  - Understand and advice on the interdependencies inside the European power grid and affecting other CIs

R8: Foster research in SG cyber security leveraging existing research programmes

- Key aspects:
  - Leverage FP7 and Horizon 2020
- Proposed topics of research:
  - Protection of monitoring functionalities and automated decision making systems of the smart grid
  - Robust, secure and resilient architectures (e.g. self-healing/graceful degradation, management of cryptographic material)
  - Trust and assurance and end-to-end security (e.g. dependencies analysis, use-case modelling)
  - Security in dependable systems
  - Supply chain protection
  - Secure smart grid in the cloud
  - Legal and economic aspects of cyber security in the smart grid

Thank you!