15 March 2012

Work Package 4.2

Awareness Stakeholders

Expert Group on the security and resilience of Communication networks and Information systems for Smart Grids

Version 1.0

Table of contents

1. Introduction

1.1. Mission, vision and goals

The mission of this Team is to contribute to a coherent and increased effort to improve the cyber security for smart grids. In particular, it consists in identifying and exploring policy issues related to raising awareness on (data) security of all the stakeholders involved in designing, manufacturing, system integration and operating and using the European Smart Grids. Securing the (data) in smart grids is not only the responsibility of the asset owners and the critical infrastructure operators. It is a combined effort of these two sets of actors with suppliers (system vendors and integrators, component suppliers, 3rd parties delivering services, IT and Telecom providers), research and knowledge institutes (research institutes, universities, education & training, standardisation bodies), industry (branch associations, industry organisations), government at the strategic policy-level (departments at policy level; regulators) and at the tactical/operational level (police, intelligence services and CERTs) and consumers/prosumers.

Awareness of the cyber and other risk factors related to the application of Smart Grids, the possible business impact and the possible impact on specific clients and society as a whole is the starting point for taking the right actions. A right level of awareness at all organisational levels combined with a sound knowledge of possible controls and measures to mitigate the risk will give these organisations the opportunity to make the right risk assessments and take appropriate actions.

In consistency with the overall mission of the Expert Group, the Team's objective is to address all relevant stakeholders with concrete, actionable guidance and recommendations for defining and implementing appropriate cyber security policies and measures upfront when developing and deploying smart grid infrastructures in the European Union.

1.2. Strategy

To achieve its mission, the Team adopted a systematic approach:

1. It has identified proper sources of information
2. It has gathered relevant materials already developed in the fields covered by the scope below.
3. It has critically assessed the material collected, evaluating its relevance in the context of the Expert Group
4. It has extracted, aggregated and organized valuable contents, pointed to appropriate external references.
5. It has identified possible gaps in available prior work and suggests below further directions for research and development as appropriate.

1.3. Scope

Stakeholders should be aware of the risk factors that the Smart Grids face. Unfortunately, Smart Grids priorities regarding security are not easily defined. Looking at them from an "industrial and operational" perspective (e.g. considering for example the ICS environment), an **AIC** (availability, integrity and confidentiality) perspective is normally followed. In higher contexts the priorities are obviously reverted (i.e. CIA). The identification of the right tradeoff between these priorities is part of the risk assessment and mitigation challenge. What matter, however, is the fact that attention should be paid to all these domains: Confidentiality, Integrity and Availability (including performance and timeliness) as well as data privacy (combination of organisation, integrity and confidentiality) and non-repudiation (e.g., electronic contracts). So the scope is broader then only data security, since data security is only one of the security aspects (though important) while implementing the smart grids in Europe. Stakeholders should be aware of the cyber security risk for the smart grids.

They also need to know their responsibility to contribute to achieving the primary protection goals of the Smart Grids like keeping up energy supply with a very high reliability and protecting consumer data to the necessary very high degree – taking into account the aforementioned risks. In order to raise this awareness, initiatives should be proposed to motivate stakeholders to take appropriate security measures to mitigate both the overall risk and risk in their own (business) scope.

1.4. Team

Team leader:

- **Auke Huistra, CPNI.NL, Netherlands:** Project manager for the Cybercrime Information Exchange and the National Roadmap for Secure Process Control Systems within CPNI.NL, the Dutch public-private platform for Cybersecurity. Main objective of CPNI.NL is to raise the resilience of the critical (information) infrastructure in the Netherlands. Auke is member of the EuroSCSIE, MPCSIE, 'EU-US Working Group on Cyber-Security and Cyber-Crime, Expert Team on Public-Private Partnership', ERNCIP Thematic Area on ICS and Smart Grids and the European FI-ISAC. He works in the field of (public) security for more than 15 years now. Before his assignment at CPNI.NL, he was amongst others cluster leader Public Security at a big international consultancy firm and CIO at a regional police force in the Netherlands.

Team members:

- **Dr. Igor Nai Fovino, GCSEC, Italy:** Igor is the Head of the Research Division of the Global Cyber Security Center. Igor holds a Ph.D. in Computer Security and a Master in computer science. He has deep knowledge in the fields of ICT Security of industrial critical infrastructure, Energy and Smart Grids, Risk Assessment methodologies, Intrusion Detection Techniques, Cryptography and Secure Network Protocols. In this context Igor is author of more than 60 scientific papers published on international journals, books and conference proceedings; moreover, he serves as reviewer for several international journals in the ICT security field and act as guest editor for IEEE Networks. In May 2010 he received the IEEE HSI 2010 award in the area of SCADA Systems. He is also an expert in European Policies (mainly in CIIP field) and in European policy support mechanism. During his career Igor worked as contractual researcher at the University of Milano in the field of privacy preserving datamining, computer security and system survivability, and as contractual professor of Operating Systems at the University of Insubria. From 2005 to 2011 he served as Scientific Officer at the Joint Research Centre of the European Commission where he led the Laboratory for ICT Security of Industrial Critical Infrastructure, providing scientific support to the EU Policies related to the EPCIIP program. In 2011 he joined the Global Cyber Security Center as Head of the Research Department. Since 2007 he is member of the IFIP 11.10 Working Group on Critical Infrastructure Protection.

- **Paul Théron MBCI, Thales, France:** Paul is Thales' Expert on Cyber Resilience and Civil C2 systems, French Area Representative of the Business Continuity Institute (BCI) since 2002, has been carrying out consulting and academic research in relation to economic and societal Resilience for the past 32 years. His research and work focuses on the dynamics of major incidents that civil, public and private organisations undergo, and on how Governmental Administrations, Military & Civil Protection Forces, Critical Infrastructure Operators, Corporations and their Supply-Chain manage to yield a dynamic, adaptive resilient response under such circumstances. After founding the French Council for Business Continuity in 2008, which organises Public - Private debates around the new Critical Infrastructure Protection regulations and issues, he has been co-opted as a member of the ENISA's Permanent Stakeholders Group, the technical council of the European Network and Information Security Agency. He is also an active member of ISO TC223 and CEN TC391 work groups on Business Continuity and Command & Control Systems. Finally, he teaches post-graduates Business Continuity Management as a regular invited lecturer in France at the Poitiers Faculty of Science (IRIAF), at the Aix-Marseille Faculty's Institute of Corporate Management (IAE), and at Mines ParisTech, as well as in a number of public and private institutions like the National Institute for Higher Studies of Homeland Security and Justice (INHESJ), the High School of War (Ecole de Guerre) and the High Committee for

Civil Defence (HCFDC). He is also the author of a large number of publications and conferences on these topics.

- **Jarkko Saarimäki, CERT-FI, Finland:** Development Manager at CERT-FI. CERT-FI is the Finnish national computer security incident response team whose task is to promote security in the information society by preventing, observing, and solving information security incidents and disseminating information on threats to information security. He is responsible of developing and coordinating the information security services that CERT-FI provides to critical infrastructure providers.

- **Eric Luiijf, TNO, The Netherlands:** M.Sc. in Mathematics at the Technical University Delft in 1975. Officer in the Royal Netherlands Navy for his duties. He joined the TNO end of 1977. Since 1995, he works as Principal Consultant Information Operations and Critical (Information) Infrastructure Protection (C(I)IP). He supports the Dutch Government on policy and technology related issues regarding C(I)IP, Cyber Operations and National Risk Assessment. He has been involved in many national and EU studies on C(I)IP including VITA, IRRIIS, DIESIS, EURACOM, and RECIPE. Eric maintains a unique database on CI disruptions, cascading effects and consequences based upon public sources. Eric is part-time employed by the Dutch Centre for Protection of National Infrastructure (CPNI.NL) as ICS and Smart Grid security expert. His SCADA Good Practices book has been translated into English, Japanese and Italian. Eric has been interviewed many times by national and international press, radio and TV, and has published many popular articles, reports, and scientific publications.

Further contributions by:

- Hans Honecker, BSI Germany (German Federal Office for Information Security)

2. Statement of Work

Awareness is the key factor to secure the smart grids. There is a clear need to raise consciousness that cyber security is a critical component in our daily life and business. We need to learn from everyday practice to identify the blind spots, educate and train stakeholders, exchange information on good practices and information gaps. Awareness about cyber security in Smart Grids is needed at all stakeholders and from their CxOs down to the youngest maintenance engineer, since there is not one organisation that can fix the security challenges for the smart grids on their own. The asset owners and critical infrastructure operators of course have a very important role, since they are responsible for implementing and operating the smart grids, but it does not stop there. The Smart Grid risk factors are not limited to single organisations. Smart Grids bring multi-organisational risk components which overarch the whole energy supply and demand chains and include manufacturers of components, system integrators, 3rd party service organisations, regulators, research and development, and so on.

Particular attention has to be paid to the necessity to meet the primary protection goals for the emerging Smart Grids – at any point of time in the continuous further development towards their final implementation. Main goals are:

- Keeping up the energy supply with the necessary – i.e. very high – overall availability, even under condition of general crises (naturals disasters, pandemia, failures or impairment of other critical infrastructures) and ICT-crises

- Keeping the data security on the necessary level (e.g. very high integrity for grid control data, very high privacy for consumer metering data)

All stakeholders should take into account the vital need for a very high availability of the supply of energy. This is mandatory in the design, implementation and operation phase of all parts of energy infrastructures that contribute to the delivery of energy, or can endanger it. Furthermore, since it will not be possible to quickly rebuild energy infrastructures under changing threats, this primary protection goal requires to choose solutions that anticipate or keep the vulnerability and susceptibility to changing threats to a minimum. Also awareness has to be built regarding the fact, that the degree of resilience and robustness already built-in in the functional view/general layer and energy-physical layers of the Smart Grids heavily influence the security and resilience necessary in the ICT-layers.

Next to the broad awareness raising activities regarding ICT security in general and the specific need for continuous robustness and resilience of Smart Grids, specific attention has to be paid to data security. A substantial part of the security that will have to be built into smart grids, especially in the smart metering segment of the value chain, is geared towards ensuring consumer data confidentiality and integrity, i.e. the basic requirements of data security. When building the inventory of implications and challenges of potential security requirements, it is important to bear in mind that the more privacy-relevant a particular data is, the higher levels of security it requires. In turn, to be able to provide the appropriate level of security, it has to be clearly known and understood exactly which data are privacy-relevant (you need to know what you are protecting in order to be able to protect it appropriately).

An example of an existing approach is the German BSI's "Schutzprofil für Smart Meter" (Smart Meter Protection Profile) which gives a fairly accurate overview of where the most privacy-relevant data reside in the smart metering infrastructure, what the related privacy risk factors are, what level of protection is warranted, and how security should be built. Moving further from the individual smart meter to the whole of the smart grid, data protection and privacy will be related to the long term data retention requirements mandated by legislation, and the policies adopted by operators accordingly. From a technical point of view, these requirements and policies should be addressed by building certain technologies into the data centres and control centres of utilities, e.g. anonymisation, backup, deduplication, etc. The technical details are discussed in other WPs. In this WP the focus will be on the ways to deliver the message to the right audience.

It is important to align the awareness raising activities with existing ones by, e.g., Smart Grids Taskforce, DG ENER's Mandate 490 on Smart Grids, ENISA with its stock-taking research on Smart Grids and ICS, the workgroup on ICS and Smart Grids within ERNCIP, the EU-US Working Group on Cyber Security and Cyber Crime: Expert Sub Group on PPP and ICS and Smart Grids, the European Network for Cyber Security (ENCS), national initiatives like, e.g., the National Roadmap for Secure Process Control Systems in the Netherlands and similar ones in de US. The private sector is also very active at this moment in organising seminars on the topic of smart grid (data) security. At the same time it is important to bring the awareness not only to stakeholders but also on the standardization bodies discussion tables, to ensure that the due attention to these topics will be paid in the delivery of the coming new international standards on the security of Energy Smart Grids.

In order to raise the awareness at all levels, initiatives should be proposed to motivate stakeholders to take action on security and privacy measures. This can be done through:

- Building and maintaining national and linked pan-European and global social network that brings experts together and cooperates in securing the smart grids.
- Facilitating the storage, dissemination and exchange of information and knowledge between public and private sector entities in Europe and around the globe.
    - Sharing of incidents, threats, vulnerabilities, good practices and policies across borders through conferences, workshops and an interactive information sharing platform.
    - Special targets are the CxO level people in the private and the public sectors. This target group is dealt with in WP 4.1
    - Creating a general inventory of key implications/challenges with regard to data & privacy security in smart grids that potential security requirements would have. This issue should be dealt with in the other Teams.
    - Involving standardization bodies (ISA, ISO, IEC, ETSI etc.) in the definition of guidelines for the definition of permanent Information Sharing groups within Smart Grids interested entities as one of the requirements for improving their security. This is also a topic to be dealt with by other Teams.
- Improving security capabilities (people, products, organisations) while ensuring compliance with industry accepted standards.
- Leveraging the skills and experience of global experts in collaborative and cooperative projects.
- Education & Training
    - Education & Training facilities in Europe for all organisation levels (up to and including the CxO-level)

The content that is produced in the other Teams can be valuable content in the awareness raising activities as mentioned above.

2.1. Information and Knowledge Sharing

Work Package 4.2.1: Providing awareness raising activities in the European Network of experts that works to secure the smart grids. Within this network, activities for sharing of information and knowledge will be organised.

Within this work package regular physical and virtual meetings will be organised to support the network. All stakeholders will get added value through sharing of information on incidents, threats, vulnerabilities and good practices. A set of activities amongst which information exchange platforms, white papers, benchmarks, conferences, and an evidence-based database will be used to raise awareness.

Activities within this WP should be:

- Organize meetings to raise awareness and disseminate information and knowledge:
    - Regular pan-European meetings (physically and virtual). An example could be the start of an European Smart Grids Information Exchange (similar like the EuroSCSIE for ICS);
    - Two thematic conferences each year (supported by the European Commission), of which one is at CxO-level and includes top-level EC policy representatives (see also WP 4.1 and the EU-US Working Group on Cyber-Security and Cyber-Crime, Expert Team on Public-Private Partnership);
    - Several web-seminars/workshops each year on relevant topics (amongst which is data and privacy security in smart grids).
- Create a trusted digital platform though which information and knowledge can be shared Europe-wide between the stakeholders. Existing portals of ENISA may be good candidates for supplying such a function.
- Encourage the writing and dissemination of white papers based on the experience, information and knowledge stemming from the Smart Grid challenge domains (as have been highlighted by the other WPs).
- Distribute Open Source Intelligence (OSINT) on the security of smart grids towards the stakeholders. Here existing OSINT initiatives by EU-CERT and in e.g. the Netherlands can be used to build upon.
- Support the development of an evidence based database, with at first open source information about incidents and lessons identified. In a later stage also closed source information can be added. The experience from JRC and the Netherlands on this topic can be used.
- Encourage the development of authoritative white papers that inform the policy-makers of the European Commission and the individual countries, in order to influence the European political agenda in the area of cyber security of smart grids.

2.2. Education and Training

Work Package 4.2.2: Education and training of people at all levels within the organisations of the stakeholders.

Education & Training is fundamental to counteract cyber security threats on the smart grids. Stakeholders will have to be educated and trained throughout the life cycle of new security solutions for Smart Grids. The E&T programmes will have to help stakeholders to think in different, innovative ways and experience new approaches. The focus of these E&T programmes should be on:

- Enhancing (and updating) awareness;
- Providing insight and perspective into real-case scenarios;
- Developing, experimenting and experiencing new (cyber security) concepts.

In particular, senior management training (CxO-level) is key since this audience is mostly responsible for the proper functioning of the critical infrastructures they manage. This specifically includes meeting the primary protection goals like the necessary high overall reliability of energy supply and ensuring the necessary privacy of end consumer data. Senior managers will be helped to understand the challenges they face and take responsibility. They will learn to take the most effective and appropriate actions within their own organisations. Courses will be developed in collaboration with relevant partners (like universities and private organisations in Europe and INL in the US). The E&T curriculum should consist of the following products:

- C-level training course
    - Unique course for the education of top management (CxO level).
    - Gives overview regarding primary protection goals and discussion of the necessary contribution of the stakeholder

    - Gives insight into cyber threats, vulnerabilities, risk factors and the disruptive effects of cyber attacks at strategic level.
    - Give insight that the degree of resilience and robustness already built-in in the functional view/general layer and energy-physical layers of the Smart Grids heavily influence the security and resilience necessary in the ICT-layers.
    - Handles policy and executive dilemmas and will provide insight into the current perspectives for policy makers (at CxO-level).
    - Consists of one hour classroom teaching, six hours table-top exercise (learning by doing during a serious gaming exercise) and a one hour wrap-up.
    - This class can be given in-house at the company.
- Classical training (including demonstration)
    - Enhancing security awareness and providing good and tangible practices.
    - Focus on cyber security aspects at the operational and tactical levels of professional organisations.
    - Either in-house at the company location or at the training organiser location.
    - Training courses will be available.
- Hands-on training
    - Cooperation with, e.g., INL which provides for instance the advanced ICS Security Training (also known as Red/Blue team training). This training should be tweaked towards smart grids. Also companies like Red Tiger Security in the US provide similar hands-on courses.
- Web-based training
    - Modules for different target groups will be developed. Internet courses will be available.