NIS plenary meeting, April 30th

WG3 Secure ICT Research & Innovation

NIS Platform WG3 Secure ICT Research & Innovation

Agenda – WG3 Secure ICT Research & Innovation

WG3 progress report - zoom in:

- **Objectives**
- **Constituency**
- **Stakeholders**
- **Subgroups timeline & state of play:**
  - **Secure ICT Research Landscape**
  - **Business cases & Innovation paths**
  - **Education & training for workforce development**
  - **Strategic Research Agenda (SRA)**

Q&A

Objectives

The main objective of WG3 is to contribute to the coordination of the European activities in Research and Innovation in connection with the European Cyber Security strategy.

WG3 should identify the **key challenges** and corresponding **desired outcomes** in terms of innovation-focused, applied but also basic research in Cyber Security, privacy and trust; and propose new ways to promote truly **multidisciplinary research** that foster collaboration among **researchers, industry and policy makers**.

WG3 should also serve as a **facilitator** for the **coordination** of, and **collaboration between, research agendas** across Europe, including **industry research roadmaps** and **national research and innovation programmes** of the **Member States**.

Objectives

Beyond the scope of **H2020**, WG3 should also help identify the elements of a **possible European industrial strategy for Cyber Security** and examine ways to **increase the impact** and **commercial** uptake of **research results** in the area of secure ICT, including via **innovative financial instruments** and **funding methods** as well as **new business models**.

Finally, WG3 is overall expected to provide input to and **elicit requirements** from the work of **both WG1 (Risk Management)** and **WG2 (Information Exchange)**.

Constituency

Members of the WG must be **qualified experts** in the field **willing to contribute** to the **achievement** of the stated **goals and objectives** of this WG3 in accordance to the **stated principles** of the WG.

Representatives from **industry, research, academia, and governmental and regulatory bodies** are sought.

Stakeholders

syssec

ECRYPT

Industry

NESSOS

CAPITAL
Cybersecurity research Agenda for Privacy and Technology chALlenges

CYSPA
EUROPEAN CYBER SECURITY PROTECTION ALLIANCE

Researchers

FIRE
Gateway to trustworthy ICT innovations in Europe

enisa
European Network and Information Security Agency

ETSI
World Class Standards

NIS WG1

Member states

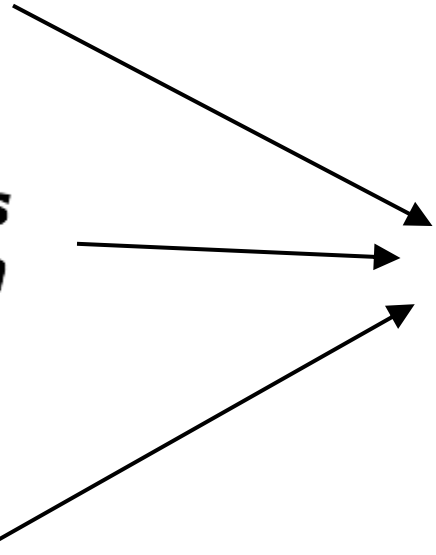
NIS WG2

Other CSAs

Policy makers

WG3 Main deliverables

- ***Secure ICT Research landscape***
- ***Business cases and innovation paths***
- ***Snapshot of education & training***



- ***Strategic Research Agenda***

Driven by the vision states (areas of interest)

Deliverables Editors

Secure ICT Research Landscape:
Bart Preneel <bart.preneel@esat.kuleuven.be>
Evangelos Markatos <markatos@ics.forth.gr>
Javier Lopez <jlm@lcc.uma.es>
Mari Kert <mari.kert@eos-eu.com>

Business cases & Innovation paths:
Paul Kearney <paul.3.kearney@bt.com>
Paul Malone <pmalone@tssg.org>
Zeta Dooly <zdooly@tssg.org>

Education & training snapshot for workforce development:
Claire Vishik <claire.vishik@intel.com>
Maritta Heisel <maritta.heisel@uni-duisburg-essen.de>

SRA Editors

SRA (Editors):
Fabio Martinelli <Fabio.Martinelli@iit.cnr.it>
Pascal Bisson <pascal.bisson@thalesgroup.com>
Raúl Riesco Granadino <raul.riesco@inteco.es>

Areas of Interest (AoI) - Leaders:

AoI#1: Individual Digital Rights and Capabilities (individual layer)
Gisela Meister <Gisela.Meister@gi-de.com>
Kai Rannenberg <Kai.Rannenberg@m-chair.net>

AoI#2: Resilient Digital Civilisation (collective layer)
Jim Clarke <jclarke@tssg.org>
Nick Wainwright <nick.wainwright@hp.com>

AoI#3: Trustworthy (Hyperconnected) Infrastructures (infrastructure layer)
Piero Corte <piero.corte@eng.it>
Steffen Wendzel <wendzel@cs.uni-bonn.de>

SRA Editors

AoI Cross-analysis sub-group:

Neeraj Suri <suri@cs.tu-darmstadt.de>
Volkmar Lotz <volkmar.lotz@sap.com>

Timeline

October 2013

Terms of Reference for WG3

June 2014

- ○
- ○Secure ICT research landscape
- ○RCV. Snapshot of Education & Training landscape for workforce development
- ○RCV. Business cases and innovation paths
- ○RCV.

Areas of Interest of Strategic Research Agenda (SRA): Individual perspective; Collective perspective; Infrastructures

September 2014

- ○Business cases and innovation paths
- ○Consolidated version:

Areas of Interest of SRA

- ○RCV. Gap analysis

March 2015

- ○The Strategic Research Agenda (SRA) of the NIS Platform

- ○*AoI 1 Individual Digital Rights and Capabilities*
- ○*AoI 2 Resilient Digital Civilisation*
- ○*AoI 3 Trustworthy (Hyperconnected) Infrastructures*
- ○*Cross analysis of AoIs*

June 2015

- ○Snapshot of Education & Training landscape for workforce development (update)

RCV: release candidate version

NIS WG3 Meeting

Secure ICT Landscape Deliverable

Mari Kert, Javier Lopez
Evangelos Markatos, Bart Preneel

NIS Platform WG3 Secure ICT Research & Innovation

8 April 2014

Version 1 uploaded

Secure ICT landscape

- Home
- Article 13a
- Electronic Communications Reference Group
- NIS Platform
  - Shared Documents
  - WG1 - Risk management, Information Assurance, Risks Metrics, Awareness Raising
  - WG2 - Information Exchange, Incident Coordination, Incident Reporting, Risks Metrics
  - WG3 - Secure ICT Research and Innovation
    - WG3 - Forum
    - Shared spaces
      - Main documents
      - Meetings
      - Secure ICT landscape

by Rossella Mattioli — last modified Oct 21, 2013 10:10 — History

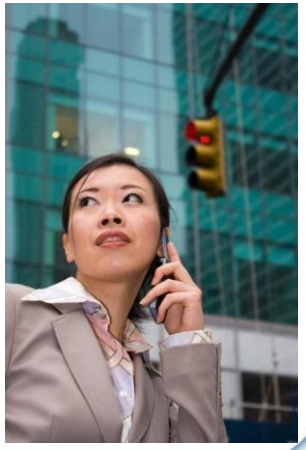
State-of-the-art of Secure ICT & Research landscape — by Rossella Mattioli — last modified Dec 06, 2013 10:17

Research Landscape Deliverable Version 1 — by Evangelos Markatos — last modified Apr 29, 2014 01:30

The Network and Information Security Platform Working Group 3 (WG3) Secure ICT: Research and Innovation aims to address the issues related to cyber security research and innovation in the context of the EU Strategy for Cyber Security. WG3 identifies the key challenges and corresponding desired outcomes in terms of innovation-focused, applied but also basic research in cyber security, privacy and trust and propose new ways to promote truly multidisciplinary research that fosters collaboration among researchers, industry and policy makers. The State-Of-The-Art of Secure ICT Landscapes deliverable is the first one among a series of other deliverables foreseen in the work program of WG3. The objective of the deliverable is to: · Map current and existing technologies in the field of cybersecurity and privacy; · Introduce and define the technologies; · Identify threats and defences to these threats; · Identify some of the outstanding research challenges; · Map existing tools that are used in each of the existing technologies; · Feed into the Strategic Research Agenda of the NIS Platform WG3.

What is it?

- Describe State of the Art
  - In Cyber Security
- What are the Treats?
  - What are the Existing Defenses for each threat?
  - What are the Research Challenges?
  - What are the Existing Tools?



Version 1 uploaded

STATE-OF-THE-ART OF SECURE ICT LANDSCAPE (DRAFT VERSION)

NIS PLATFORM

WORKING GROUP 3 (WG3)

Table of contents

Version 1 uploaded

3.2 Cloud

3.2.1 Introduction

Cloud computing is a business model that combines a multitude of technologies to provide remote, dynamic and flexible IT services. Since its emergence, there was a tendency to consider cloud computing security as the security of its technical components. However, as its initial years pass and the obstacles that prevented its proliferation are studied, it emerges that there are security considerations that are specific to cloud deployments.

Cloud computing signifies a transformation of the established ICT deployments for organizations and individuals: from an on-premise IT infrastructure to an off-premise IT service. The associated security controls and mechanisms are also migrating with the infrastructure: security is no longer in the hands of the user. What is lost in the process is the "sense of security and control of the user/IT manager", which is the most difficult to re-establish.

The above is mostly true for public clouds and hybrid clouds. Private clouds are exposed to similar threats as in-house ICT infrastructures and do not represent novel security challenges - except perhaps related to their size, which might make them attractive targets. As the level of abstraction increases and one moves from IaaS and PaaS models to SaaS models the sense of ownership, control and security gets even more damaged.

Therefore, what lies at the heart of cloud security is the matter of exerting control over ICT assets (systems, networks, data and applications). When individuals, other than the legitimate owners and users of the assets, exert this control, this creates threats and associated risks for these assets. Cloud computing makes it more difficult to assert control and cloud security tools are meant to make this process easier.

3.2.2 Current status

It was often stated that the security responsibility, which was with the in-house IT department before has now move to the cloud service provider security specialists. However, it is now seen as a joint responsibility, and tools and techniques are being developed to help both of these groups.

A significant portion of the research is being carried out to make cloud computing more transparent and accountable:

- Log and event management in the cloud,
- Monitoring, auditing, compliance and incident management,
- Data security: confidentiality, integrity and availability,
- Mitigation of insider threats,
- Cloud systems forensics tools,
- Access control technologies,
- Business continuity and disaster recovery.

Other research areas impacting cloud security are encryption technologies, physical security technologies and work related to securing hybrid and federated clouds. Users' control over their assets is also directly related to cloud vendor data formats, interoperability and portability. Although not related to security directly, these are

these companies might not always feel compelled to make their systems more transparent and accessible to users and researchers. This provides a major challenge for cloud security research as well as interoperability, not mature yet, and compliance efforts. Incentives need to be created for these companies to move to more open structures and operation models as well as the promotion of open source alternatives. Scalability (for security, compliance, data retrieval and indexing) is also needed.

- *Increased target vector:* As many services and data are concentrated in cloud service provider data centres, these become very attractive targets for attackers. While experienced security personnel run these systems, it is still a challenge where so many valuable assets and services are concentrated. Denial of Service attacks and disaster recovery become even more significant under these circumstances.
- *Insider threats*: As almost total control of data and applications and infrastructure is transferred to cloud service providers, insider threats within these providers become a major concern.
- *Cloud Model Selection:* Most companies and individuals might prefer to move to a public cloud to minimize their costs and might prefer SaaS as the least technologically demanding solution. However, a proper risk assessment needs to be carried out on the assets and targets of each company, and a proper model needs to be selected based on the threats and risks identified. A hybrid or community cloud might be less risky for some organizations. As long as organizations do not make this assessment in cloud service and model selection they place themselves and their dependents under major risks. Proper risk assessment tools need to be provided for this purpose.
- *Trust erosion:* The biggest challenge for the current clouds, however, is concerning to methods to establish presumptive trust on an evidence base, and to nurture the initially established trust relationship into one of trustworthiness are important facilitators in social and economic transactions. In dynamic systems and applications, such as in cloud computing, the sole expression of access rights is not enough. Policies for dynamic systems usually allow data providers to express which attributes may or may not be collected, but we need to allow data providers to specify provisions and obligations.
- *Privacy:* Privacy challenges in future cloud computing are related to the need to protect data on-premise and in-transit and ensure access to it by authorized parties only, including transaction histories for potential privacy-enhancing user tools as well as for compliance and forensic purposes.
- *Software and hardware architecture used by cloud providers:* Current cloud computing relies on virtualization technologies to isolate client data and applications, which carry new technical controls with implications on privacy and security. Providers also rely on client-side, perimeter, and web browser security. It is important to understand all the technologies used by cloud providers for their services. This translates into an expanded attack surface and, consequently, new risks and threats. Just recently new vulnerabilities have been found in virtualization solutions, which give an idea of the challenges with respect to the underlying architecture used in cloud offerings.
- *Authorization and Authentication*: data protection, federated identity management issues

3.2.3 Existing tools

There is an explosion of tools and services for cloud computing security. Many EU projects and private companies are generating tools to secure the cloud. Available tools and services can be found on the link provided for EU projects above: www.cloudwatchhub.eu/Projects as well as through the CSA member companies.

Example Section: Intrusion Detection Systems

- Introduction
  - Rule-based, Anomaly-based
- Current Status
- Research Challenges
  - The Changing Security Paradigm
    - No more perimeter security
  - Speed
  - Whole System Image
    - Not only network image
  - New models for attack patterns
    - String matching and automata are not enough

NIS WG3 Meeting

Business cases & innovation paths

Paul Kerney, Paul Malone, Zeta Dooly

Outline uploaded

Business Cases and Innovation Paths

Table of Contents

Business cases & innovation paths

- Introduction and problem definition
- Methodology for the study
- Business cases
  - Initial sample market and industry analysis
  - Identification of stakeholder requirements
  - Selection and analysis of high impact use cases
  - Cost-benefit analysis of research topics in relation to use cases
  - Initial economic incentive analysis
- Process Definition & Innovation Models
  - Survey of best practices in innovation
  - Technology and research analysis link with ‘Secure ICT landscape’ deliverable
  - Recommendations to H2020 on innovation processes
- Summary of recommendations

Methodology - demand driven research

- Define a model and an approach
- Identify stakeholders
  - Describe concerns from their viewpoints
  - Impact of not meeting X requirement
- Identify E2E business processes in which X plays role
  - Identify steps where security is critical and describe challenges
- Derive set of research topics from above plus external info (SRA etc)
  - Analyse them from the viewpoints: investment, impact, likelihood of success, route to market, dependencies (e.g. on regulation)
- Go back and repeat this process ??

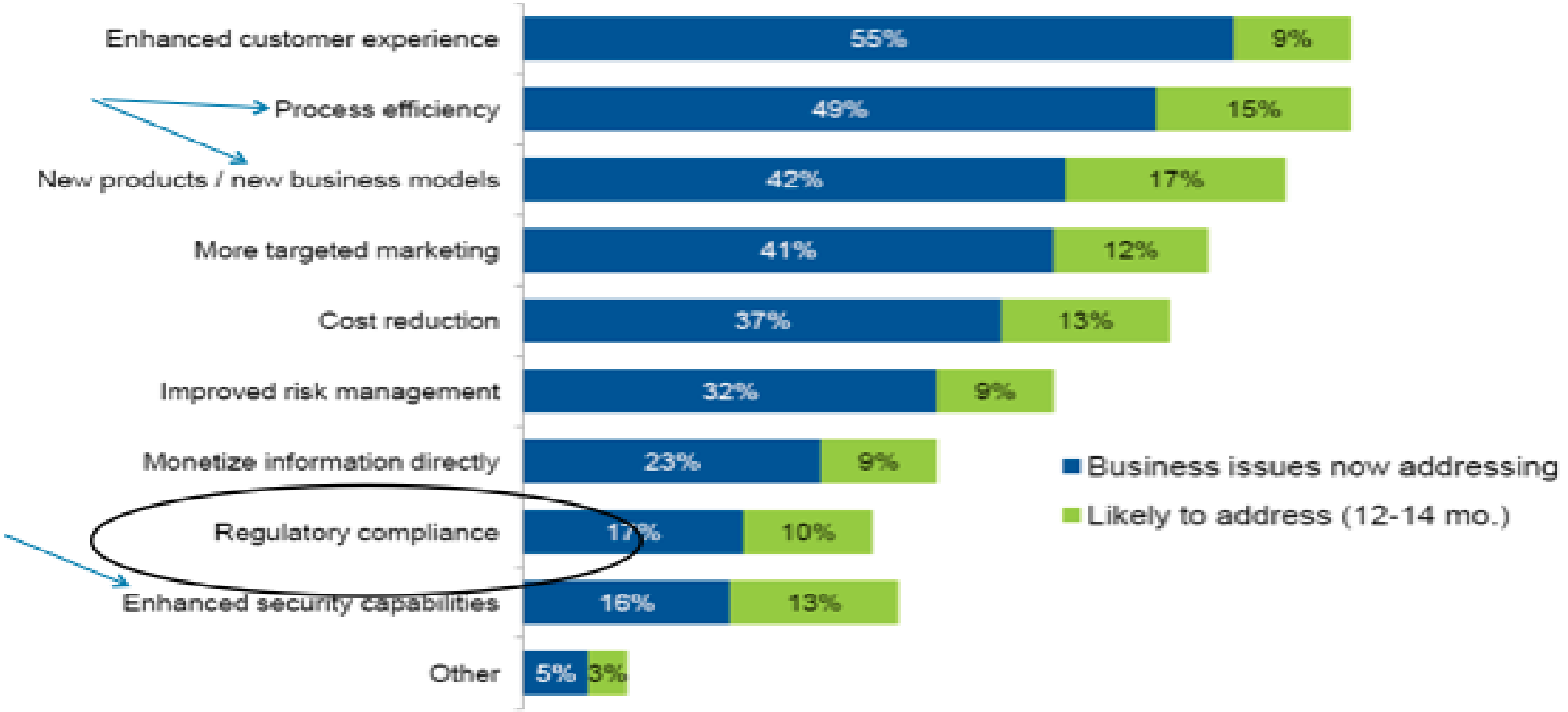
Market - initial segmentation

1. Global demand model with security sub segmentations
   - a)Defence and national security
   - b)Government and other public sector
     - Strong requirements, e.g. tax collection
     - Low impact/requirements, e.g. local school
   - c)Corporate
     - Strong needs/requirements (e.g. sector regulations) e.g. finance
     - Medium
   - d)SMEs
   - e)Citizens
2. Security topic specific demand model
   - End user: in-house, outsourced, in cloud
   - Software company: tailor made, product, components
   - Existence of S-SDL? Existence of service based software?

3. **<u>Now calculate market size: 1+ c + ii + service based = ???</u>**

Business problems

Business problems companies are addressing



"Survey Analysis: Big Data Adoption in 2013 Shows Substance Behind the Hype" G00255160, Sep 2013

Identify research topics

- Integration of early and late assurance
- Risk driven development
- Socio technical multi stakeholder requirements elicitation…

- Prioritisation according to:
  - investment, impact, likelihood of success, route to market, dependencies (e.g. on regulation
  - NESSoS SecEval +CBK , OWASP CIO Guide

NIS WG3 Meeting

Education & Training snapshot for workforce development in Cybersecurity

Claire Vishik, Maritta Heisel

NIS Platform WG3 Secure ICT Research & Innovation

8 April 2014

Data Collection

- Education: data from UK, Germany, Italy, Cyprus, France, Ireland, Greece, Spain, Luxembourg, Turkey, France, Austria, Finland
- Other countries: Portugal, Ireland, Bulgaria, Latvia, Lithuania, Estonia, Czech Republic, Slovakia, Poland, Romania, several other countries are not covered
- Incomplete coverage, but provides an idea of the general direction and focus
- Data collection on training initiated
- Widely available in organizations, mostly beginning level

Summary of Collected Data

Country	Entries	Course Level	Disciplines
Austria	5	Graduate (3), Undergraduate (2)	Computer Science
Cyprus	5	Graduate (3), MSc/PhD pathway Graduate (1), Undergraduate (1)	Economics, Business, Computer Science, Computer Engineering, Information Systems, Communication Systems
Finland	7	Graduate (6?) Undergraduate (1?)	Information Security and Cryptography, ...
France	5	Graduate (5)	Computer Science
Germany	143	Graduate (69), Undergraduate (43) (course level is not given for all entries)	Computer Science, Software Systems Engineering, IT Security/ Information Technology, Data Science, …
Greece	2	Graduate (2)	Computer Science, Computer Engineering, Information Systems, Communication Systems

Summary of Collected Data

Country	Entries	Course Level	Disciplines
Italy	8	Graduate (6), Undergraduate (2)	Computer Science, Computer Science-Security, Computer Science, Computer Engineering, Law
Luxembourg	1	Graduate	Computer Science
Spain	14	Graduate (13), Undergraduate (1)	Economics, Business, Computer Science, Law
Sweden	5	Graduate (5)	Computer Science
UK	81	Graduate (81)	Computer Science, Information Systems, Technology Management, Law, Business Studies

Analysis

- Data still insufficient for direct analysis, but offers good insights echoed in reports
- Secondary materials – reports and analysis of adjacent fields – will be useful to draw conclusions

Early Insights

- Few courses and programs dedicated to cybersecurity; topic teaching fundamental concepts of general security stand as a proxy cybersecurity concentration

- Most programs we are aware of are graduate
  - While there are many jobs available at the beginner level that would benefit from the undergraduate degree preparation
- Most programs are not multi-disciplinary
  - While the requirements are for multi-disciplinary training including security, privacy, usability, economics, law, policy, etc.
- Global nature of most cybersecurity topics is not reflected in curriculum

NIS WG3 Meeting

Strategic Research Agenda (SRA)

Fabio Martinelli, Raúl Riesco

State of play, the case of 3x AoIs (Areas of Interest)

NIS Platform WG3 Secure ICT Research & Innovation

8 April 2014

AoI's job uploaded

Areas of Interest (AoI)

- Home
- Article 13a
- Electronic Communications Reference Group
- NIS Platform
  - Shared Documents
    - WG1 - Risk management, Information Assurance, Risks Metrics, Awareness Raising
    - WG2 - Information Exchange, Incident Coordination, Incident Reporting, Risks Metrics
    - WG3 - Secure ICT Research and Innovation
      - WG3 - Forum
      - Shared spaces
        - Main documents
        - Meetings
        - Secure ICT landscape

by Rossella Mattioli — last modified Dec 19, 2013 11:41 — History

Title	Author	Type	Modified
Citizen Digital Rights and Capabilities (tentative title)	Rossella Mattioli	Folder	Dec 19, 2013 11:41
Resilient Digital Civilisation (tentative title)	Rossella Mattioli	Folder	Dec 19, 2013 11:41
Trustworthy (Hyperconnected) Infrastructures (tentative title))	Rossella Mattioli	Folder	Dec 19, 2013 11:41
CleanReportBreakOutSessions-WG3-Sept13-v1	Rossella Mattioli	File	Dec 19, 2013 11:41
Results of the Breakout Session of GroupB Version 1.1 20130930	Kai Rannenberg	File	Dec 19, 2013 11:41

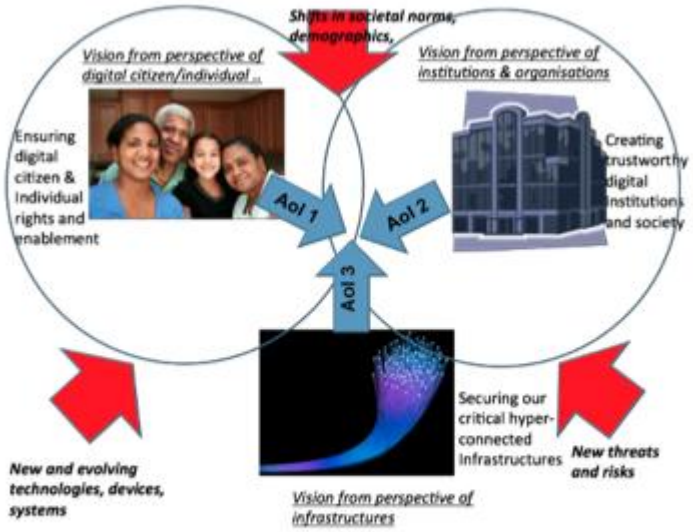
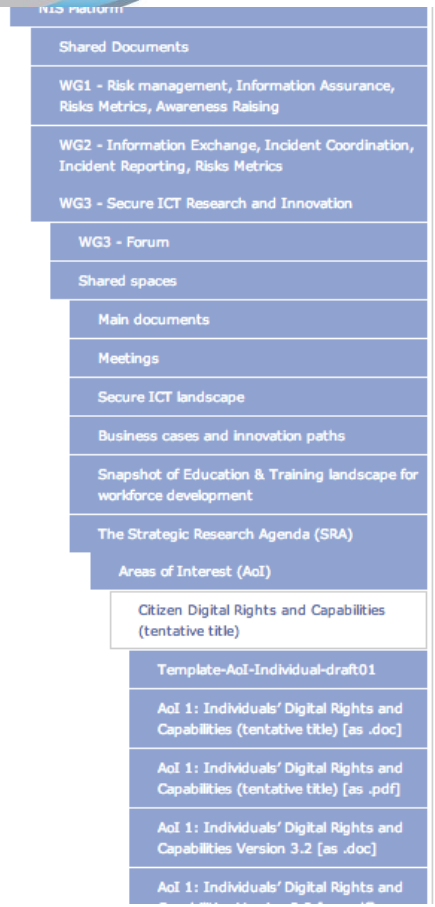


Figure 1. Areas of Interest coverage areas

AoI # 1 (individual layer) v3.2 uploaded



AoI 1: Individuals' Digital Rights and Capabilities (tentative title) [as .doc] — by Kai Rannenberg — last modified Apr 02, 2014 03:39

AoI 1's vision is that individuals' needs and fundamental rights are placed at the very centre of how we design, manage, and control network and information and communications technologies. Networks and ICT should be designed to take into account each of the following from the perspective of the individual: diversity, control (e.g. user empowerment), privacy, fairness, democracy, freedom of expression, safety. The concept of individuality includes being able to 'individualise' according to the differences of people; Individual Rights (and duties) of e.g. citizens and consumers must be respected and transparency (without intrusiveness) must be provided at all times.

AoI 1: Individuals' Digital Rights and Capabilities (tentative title) [as .pdf] — by Kai Rannenberg — last modified Apr 02, 2014 03:42

AoI 1's vision is that individuals' needs and fundamental rights are placed at the very centre of how we design, manage, and control network and information and communications technologies. Networks and ICT should be designed to take into account each of the following from the perspective of the individual: diversity, control (e.g. user empowerment), privacy, fairness, democracy, freedom of expression, safety. The concept of individuality includes being able to 'individualise' according to the differences of people; Individual Rights (and duties) of e.g. citizens and consumers must be respected and transparency (without intrusiveness) must be provided at all times.

AoI 1: Individuals' Digital Rights and Capabilities Version 3.2 [as .doc] — by Kai Rannenberg — last modified Apr 25, 2014 02:21

AoI 1's vision is that individuals' needs and fundamental rights are placed at the very centre of how we design, manage, and control network and information and communications technologies. Networks and ICT should be designed to take into account each of the following from the perspective of the individual: diversity, control (e.g. user empowerment), privacy, fairness, democracy, freedom of expression, safety. The concept of individuality includes being able to 'individualise' according to the differences of people; Individual Rights (and duties) of e.g. citizens and consumers must be respected and transparency (without intrusiveness) must be provided at all times. Social, legal and regulatory aspects of security and privacy need to be investigated in an interdisciplinary research context.

AoI 1: Individuals' Digital Rights and Capabilities Version 3.2 [as .pdf] — by Kai Rannenberg — last modified Apr 25, 2014 02:23

AoI 1's vision is that individuals' needs and fundamental rights are placed at the very centre of how we design, manage, and control network and information and communications technologies. Networks and ICT should be designed to take into account each of the following from the perspective of the individual: diversity, control (e.g. user empowerment), privacy, fairness, democracy, freedom of expression, safety. The concept of individuality includes being able to 'individualise' according to the differences of people; Individual Rights (and duties) of e.g. citizens and consumers must be respected and transparency (without intrusiveness) must be provided at all times. Social, legal and regulatory aspects of security and privacy need to be investigated in an interdisciplinary research context.

AoI # 1 (individual layer) v3.2 uploaded

AoI 1: Individuals' Digital Rights and Capabilities

V 3.2, 2014-04-25

Description of the AoI 1's vision

AoI 1's vision is that individuals' needs and fundamental rights are placed at the very centre of how we design, manage, and control network and information and communications technologies. Networks and ICT should be designed to take into account each of the following from the perspective of the individual: diversity, control (e.g. user empowerment), privacy, fairness, democracy, freedom of expression, safety. The concept of individuality includes being able to 'individualise' according to the differences of people; Individual Rights (and duties) of e.g. citizens and consumers must be respected and transparency (without intrusiveness) must be provided at all times. Social, legal and regulatory aspects of security and privacy need to be investigated in an interdisciplinary research context.

Description of the issues and challenges

- Technical challenges
  - Interoperability issues: Technical standards have to be improved, e.g. to properly protect
    - seamless (contactless) communication by mobile phone
    - applications being transferred data from one to another device across boundaries
  - Individual communication between citizens of different countries;
  - Scaling (up & down) of storage and how it relates to interoperability
  - User friendliness (interoperable user interface)
  - Security / Privacy by design,
  - Privacy by default so that the end user does not need to be aware and familiar with the security measures but that the system ensure security and privacy related properties;
  - Derived data protection, avoid users spreading their identity all over the web, instead enable use of derived credentials
  - Classification of security levels with a basic provable interoperable level for all communications devices
  - Avoid correlation of data so that individuals' data cannot be correlated or subsequently analysed (Big Data problem)
- Societal challenges
  - Influences of social content on privacy requirements must be addressed;
  - Digitalization of citizens (individuals should have freedom not to use all technology and still be able to live a normal not restricted life
    - Digital divide/inclusion:
      - Everything can be "googled";
      - Technology concentration leads to the digital divide and to exclusion.
      - Awareness (tangible means such as secure tokens) to identify if what they are doing is safe;
      - Opting-out of technologies and applications or to choose one's own preferences in applications need to be guaranteed (for example filling tax forms by hand and returning paper copies should continue to be available for citizen who prefer this, as the state should not raise the burdens for citizens, who want to communicate with the state).
  - Derived data protection, avoid users spreading their identity all over the web; instead enable use of derived credentials.
  - A balance needs to be found between anonymity and trust and security requirements.
  - Cross-border data protection: Citizens of one country may find their data stored in data centres located in another country.
  - User friendliness (well -known handling of devices, no device specific supplies)
  - Users need to have control (including ownership and usage rights) over their ICT assets (personal devices, networks, data, and applications).
- Political and governance challenges
  - Preserve rights and societal values of the physical world in the digital world, where appropriate
    - Consider, that concepts like "ownership"," means of production", and "copyright" may be different in the digital world compared to the physical world.
    - Understand the potential effect on digital rights
    - Consider the impacts of public goods, creative commons, open source and crowd sourcing
  - Trust in governance of surveillance systems
    - Personal data and information will not be captured/analysed without the knowledge and consent of lawful citizens;
    - Technology, that is inherently able to perform permanent surveillance (such as computers and networks with storage capabilities including Internet, pervasive computing, mobiles, apps, sensors and CCTV) is to be built in a way, that it helps people and does not harm people.
- Educational challenges
  - Responsibility for continuous education and raising awareness campaigns
  - Bringing Massively Open Online Courses (MOOCs) to the same level as real-life in-class courses is a challenge from quality and certification perspectives.

AoI # 2 (collective-org layer) v2.0 uploaded

Resilient Digital Civilisation (tentative title)

- Home
- Article 13a
- Electronic Communications Reference Group
- NIS Platform
  - Shared Documents
  - WG1 - Risk management, Information Assurance, Risks Metrics, Awareness Raising
  - WG2 - Information Exchange, Incident Coordination, Incident Reporting, Risks Metrics
  - WG3 - Secure ICT Research and Innovation

by Rossella Mattioli — last modified Dec 19, 2013 11:41 — History

AoI 2 - Collective draft01-1.doc — by Fabio Martinelli — last modified Mar 05, 2014 04:08

AoI2 Resilient Digital Civilisation V2.0 — by James Clarke — last modified Apr 26, 2014 12:17

This is the current version of the document for the AoI2 Resilient Digital Civilisation. It is intended to obtain inputs from the workshop on 29th April, 2014.

AoI2 Resilient Digital Civilisation V2.0 pdf version — by James Clarke — last modified Apr 26, 2014 12:23

AoI # 2 (collective-org layer) v2.0 uploaded

Resilient Digital Civilisation (I) (collective layer)

Co-Chaired by Nick Wainwright (HP Labs <nick.wainwright@hp.com> and Jim Clarke (Waterford IT <jclarke@tssg.org>

Context

The pervasiveness of information and communication technology and ubiquity of digital infrastructures means that the Digital civilization is now a fact of Life. Some examples illustrate this: digital Media, digital social relations, critical infrastructures, services, surveillance, industrial control, government, intelligent transport systems, smart cities, amongst others.

A Digital Civilisation is desirable to society at large due to a number of key drivers such as: ease, convenience, economisation, speed, information access, optimisation, proximity, and others. However, the Digital Civilisation is exposed to new threats as the exposure of the digital interconnected society to this digital infrastructure, which is continuous evolving, can have issues related to accessibility, invisibility, profiling, connectivity, complexity, and others. Coupled with the trust issues arising from a constant concern of surveillance and/or potential loss of personal data could eventually diminish the digital infrastructure's image, and consequently change the future architecture of the infrastructure by necessity of barriers, filters and inspections at all stages of usage and operation. Moreover, an architecture based on shared platforms and infrastructures increase the impact of incidents on civilization.

Resilience is key for a functional digital civilization, and civilization must be empowered to manage and balance their own risks according to their requirements, similar to how it is done in the physical form of civilization. These concepts and solutions must also be addressed in a fashion that is not localized in pockets, but can it translate to a "world scale" taking into account the different aspects of civilization as it will be in 2025.

Terms of reference

The main focus of this **AoI Resilient Digital Civilisation (I) (collective layer)** is the protection of the groups/society/organizations (we will call this 'Digital Interconnected society') as it represents the collective interest of the organized citizens, institutions, business, etc. This can be thought of as the 'supply side' of the digital civilisation.

These groups and organisations operate under a whole series of obligations – regulation, contracts, societal norms, and to manage risks, ensure security, and handle information securely and respecting fundamental rights of the customers/citizens.

The AoI will focus on ensuring that digital institutions of society will be trusted and secure, as trusted in their digital forms as they would be in physical form - if indeed it would be possible to translate the digital institutions of 2025 back to what they were 15 or 25 years previously, such is the nature and scale of the transformation to a Digital Interconnected Society.

Challenges (4 types):

1. Technology:
   - Resilience and security of ICT systems
   - Including Cloud / Data centers
   - Resilient Governmental ICT systems
   - Preventing Cyber crime/cyber terrorism
   - Fostering Trust in the Digital Society
   - Interoperability
   - Adaptation
   - Security metrics
   - Trust & assurance
   - Security engineering
   - Security & privacy by design, and others.
2. Political / Societal:
   - Policy & regulation - Digital civilization should ensure an 'digital interconnected society' that is (Fair, Democratic, Safe, Transparent, avoid Censorship, balance the citizen rights and duties)
   - Control - individual vs. collective - ensuring that individuals can manage their individual digital presence in a way that's balanced with collective needs form business, state, society, community
   - Allow (digital) diversity - not treating everyone the same, enabling differences, supporting the different cultures, approaches perspectives online.
   - International aspects
   - Values and rights
   - European view
   - Data protection principles
   - Framework (certification etc.), and others.
3. Economical:
   - Grant business and service continuity (lack of security breaches/failures leading to damages/loss)
   - Economic value of security
   - Large-scale coordination
   - Transparency of business models
   - Taking into account the full spectrum of industry e.g. Big players – SMEs
   - Complexity
4. Educational:
   - Raising Awareness,
   - Multi-disciplinarity
   - Risk perception
   - Ease of use
   - Simplicity.

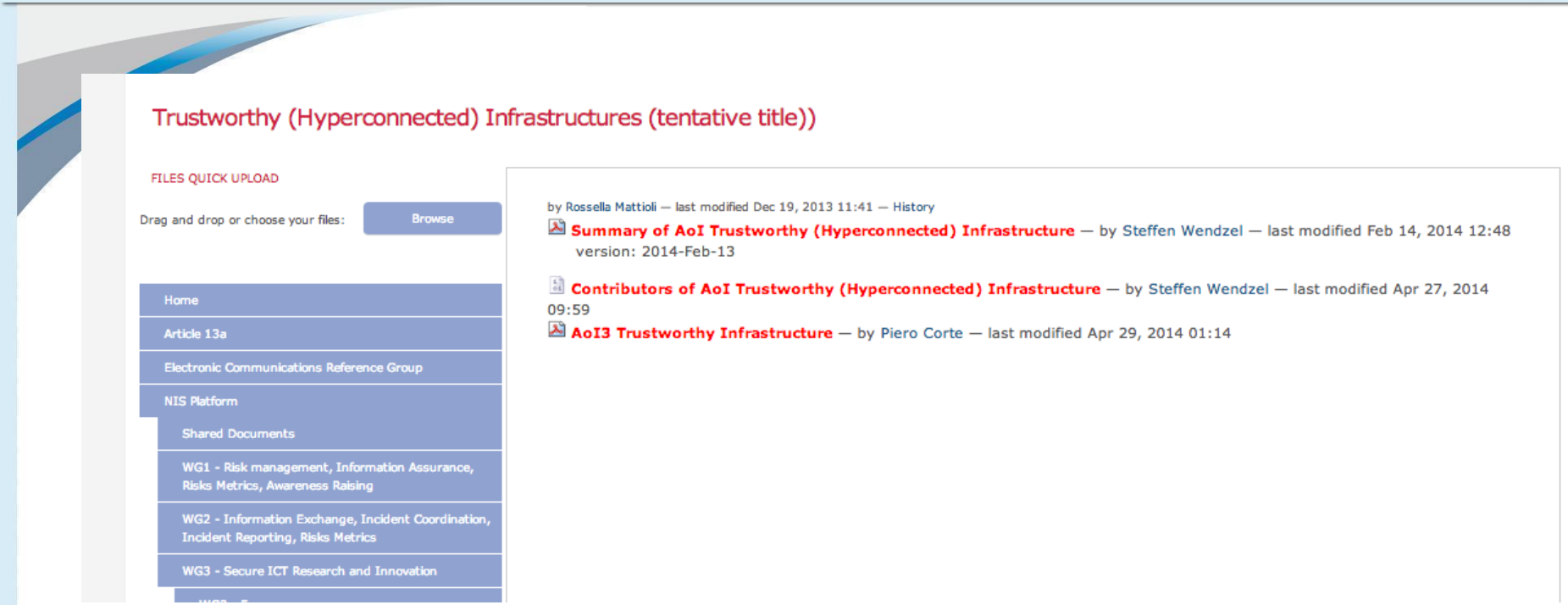
AoI # 2 (collective-org layer) v2.0 uploaded

One way to consider the future barriers to secure and trustworthy institutions is to project forward the technology enablers of the digital future and consider what threats or barriers are introduced at the same time that prevent the institutions of society being secure or trusted.

We intend to use the opportunity of the April 29th workshop to start populating the following table:

<2025 technology>	**Enables <Gov I Biz I Civil Soc> to [goal]**	**Significance 1-5**	**Provided <trust / security barriers> are addressed**	**Priority 1-5**
Pervasive monitoring of cities and public areas	Provide security to citizens		Ensuring citizens privacy rights can be guaranteed	
	Manage the environment		Controlling data use who can use what for what purpose	
Track everything all the time	…	…	…	

AoI # 3 (Infrastructures layer) uploaded



AoI # 3 (Infrastructures layer) uploaded

Area of Interest (AoI) "Trustworthy (Hyperconnected) Infrastructure"

Document Version: 2014-Apr-27

EARLY DRAFT VERSION FOR INTERNAL DISCUSSION

Editors:

Steffen Wendzel, Fraunhofer FKIE, steffen.wendzel@fkie.fraunhofer.de

Piero Corte, Engineering, piero.corte@eng.it

Contributors (preliminary; names listed under the condition of actual contribution):

Kristian Beckers, University of Duisburg-Essen

Ruth Breu, UIBK

Charles Brookson, ETSI / Zeata

Philippe Bonnet, IT University of Copenhagen

Piero Corte, Engineering

Hervé Debar, Télécom SudParis

Leonardo Fiocchetti, Selex

Maritta Heisel, University of Duisburg-Essen

Seudie Herve, Bossh

Nigel Jefferies, Huwai

Paul Kearney, British Telecom

Mari Kert, European Organisation ofr Security

Mika Lauhde, SSH

Evangelos Markatos, ICS Forth

General Aspects

Description of the AoI's vision

Participants see future infrastructure processes and resources as adaptive, de-central, collaborative and efficiently controlled. ICT infrastructure must be reliable, predictable and always available, it must operate confidentially and in a privacy protecting way, it should be capable to react to cyber threats in real time. Users should additionally be provided with permanent access to information that allows the confirmation of the trustworthiness of the infrastructure and its services (even if partly compromised). A key aspect in the development of trustworthy infrastructure will be the surrounding of citizens by network devices in the context of ubiquitous computing. Ubiquitous computing brings changes (e.g. ambient assisted living, AAL) but also challenges (e.g. privacy threats). Future cities for European citizens depend on CI and compete for human resources as each city must be optimized to use its CI in order to motivate skilled people to stay in the city/to move to the city. The participants expect failure of critical infrastructure to cause catastrophic consequences.

Issues and Challenges

The AoI contributors highlighted a number of challenges during both plenary meetings held in September and December and via e-mail. The major aspects mentioned are the integration of privacy and security by design in infrastructure (incl. cars, trains, buildings, Internet infrastructure, ...); realizing achievable solutions/engineering of more secure infrastructure environments; incident/vulnerability handling; providing trust for partly compromised infrastructure components; the communication between stakeholders (e.g. industry and research) as well as the education of end-users; the migration of legacy systems and protocols; the scalability increase of infrastructure and its data; the handling of a rapid growth in the sophistication of threats across the whole spectrum of the cyber ecosystem and the linked increase of the risk of disruption; the decreasing available time to respond to attacks; the global competition (-> establish a security industry for the necessary products in Europe); the creation of ways to measure security; the creation of user-friendly/user-tailored security solutions; secure inter-connectivity of infrastructure components; and the introduction of improved standards.

Identification of Technology, Policy and Regulation enablers/inhibitors

Enablers (Technology, Policy and Regulation)

Key aspects mentioned multiple times serving as enablers are the education of users/companies, the implementation of constructive security/privacy regulations and standards on different levels (also governmental / cross border), the improvement of security features on different levels of security; the integration of security by design, improvement/utilization of formal methods, empirical studies, privacy enhancing global PKI, and machine learning to improve security, the presence of an un-fragmented and compact research community in Europe (on trusted devices). A forum with research institutions and industry on industrial themes could also serve as an enabler.

AoI # 3 (Infrastructures layer) uploaded

ICT Infrastructure

Associated Contributors: Mika Lauhde, Hervé Debar, Paul Kearney, Charles Brookson, Piero Corte, Steffen Wendzel, Nigel Jefferies

Issues and Challenges

Input 1 (Mika Lauhde):

Currently the EU is not competing any more with ICT high tech players, but newcomers like China, India, etc. The current mass surveillance can be seen as a wake-up, what will be lost when dependency and legislations are misused towards EU.

We see that there are three challenges which are needed to overcome:

build European assets for ICT and ICT security

protect European ICT assets and ICT security instruments from unfair competition

allow European member states to build their ICT protection according their own foreign policy

Shortly:

a) we have clear shortage with European ICT assets which means that EU is heavily depending from foreign ICT components. We need to improve this situation by Horizon2020 program in the way that this funding is targeted to European companies which will then also build the ecosystem competences in this area for European utilization.

b) as we have seen, European ICT players are needing similar support as US companies when building their ICT security and business. In EU we have been concerned from unfair competition which we have seen in passenger plane and shipyard industry. However EU focus should be broadened also to cover ICT and ICT security industry. When Google has been under investigation here in EU, NSA has been taken immediate actions to influence and mitigate this kind of investigation which is targeted to US ICT industry players. This means in other words that EU need to protect similar way ICT industry as we need to protect Shipyards and passenger plane industry.

c) Part of the NIS work is risk assessments (WG1), which happens only if real information is available to make risk assessment. This information to make justified decisions from Risk area cannot be done only trough political or commercial justifications. WG3 should take in agenda, how in long run EU could make security assessments to ICT components (Hardware or Software) used in EU networks. In this we should perhaps look to US as well, while they have already a working program on how to utilize foreign ICT components in their networks.

Input #2 (Hervé Debar).

ICT infrastructures have become pervasive in our modern life. We rely on them for services that have become intensely critical for many aspects of our modern life, such as obtaining basic services (energy, water, transportation, ...) or easing our activities (computing faster routes on the road, entertaining ourselves everywhere, etc.). Yet, there are many security issues that remain at bay:

Understanding and visibility of risk and security measures. In many cases, security imposed in ICT infrastructures is seen as a constraint and a loss of functionality. For example, we have

Transportation

Associated Contributors: Paolo Venturoni, Paul Kearney, Steffen Wendzel, Leonardo Fiocchetti, Paolo Roccetti (from CYSPA project)

Issues and Challenges

Before introducing issues and challenges it is worth identifying the context of Transport Critical Infrastructures in the transport domain, i.e. define what is part of a Transport Critical Infrastructure, and what is not.

A Transport Critical Infrastructure (T-CI) is a transport system (for people and freights) whose failure may have a macroscopic effect on critical sectors at National and/or European level.

It's worth noticing that the definition applies differently to the different transport modes (road, rail, air, etc.). As a sample, the malfunctioning of a train on the RailRoute2050[1] backbone could have a relevant effect on the tourism sector at European level, so in this case trains running on the rail backbone are part of the T-CI itself. On the other hand, malfunctioning of all traffic lights on a small town would not impact significantly any critical sector, so that particular traffic light system shouldn't be part of a T-CI.

Moreover, we define each T-CI as subject to a single controlling entity (either alone or composed by a consortium). As a sample, Italian and French highways are two different T-CI, as they're subject to different controlling entities.

For the purpose of this document, T-CIs are analyzed from the point of view of the ICT systems governing them. In particular, we foresees that, in the next years, the T-CIs will greatly increase reliance on ICT systems. This is also reflected by the aim of creating a Single European Transport Area, thus easing "the movements of citizens and freight, reduce costs and enhance the sustainability of European transport."[2]. The major challenge in the creation of a single transport area at the European Level is the interoperation of ICT systems governing the existing T-CIs, that cannot be easily replaced. Interoperation does not only refers to technical aspects related to the interconnection of existing systems, but primarily refers to the definition of policies and procedures enabling an extensive collaboration of systems that govern every T-CIs.

In the transport sector there are significant strategic challenges in which ICT can play a vital role. Among the most important challenges, it is interesting to mention:

- minimization of CO2 emission by promoting the use of cleaner means of transport such as electric vehicles
- increase of road safety with particular attention on reducing significantly the number of deaths caused by road accidents
- creation of the Single European Sky, to address the forecasted 50% increase in air traffic in the next 20 year

[1] Rail Route 2050: http://www.errac.org/wp-content/uploads/2013/11/D9-SRRA-RAILROUTE2050.pdf

[2] Single European Transport Area: http://ec.europa.eu/transport/themes/strategies/2011_white_paper_en.htm

AoI # 3 (Infrastructures layer) uploaded

Smart Grids

Associated Contributors: Kristian Beckers, Philippe Bonnet, Maritta Heisel, Erkuden Rios Velasco, Paul Kearney

Issues and Challenges

Input #1 (Beckers):

A smart grid provides energy on demand from distributed generation stations to customers. The grid intelligently manages the behavior and actions of its participants using information and communication technologies (ICT). A novelty compared to existing energy networks is the two-way communication between consumers and electric power companies. The benefits of the smart grid are envisioned to be a more economic, sustainable and reliable supply of energy. However, significant security concerns have to be addressed for this scenario, due to the possible dangers of missing availability of energy for customers, as well as threats to the integrity and confidentiality of customer's data. These concerns are of particular relevance, because energy grids have a significantly longer lifespan than telecommunication networks (Aloula, Al-Alia, Al-Dalkya, Al-Mardinia, & El Hajj, 2012). In addition, privacy concerns have risen, such as the possibility of creating behavioral profiles of customers if their energy consumption is transmitted over the smart grid in small time intervals (Lin & Fang, 2014). In particular, the attack surface is increasing over time in the smart grid for two reasons. Firstly, an increased amount of private sensitive customer data is available to service providers, utility-, and third party partners. Secondly, new data interfaces such as new and improved meters, collectors, and other smart devices cause new entry points for attackers (Cuellar, 2014).

Input #2 (Bonnet):

Smart Grid can be defined as a process, rather than a product. Smart Grid is the digitalization of the electricity infrastructure. Smart Grid is the transition from a closed, centralized, analog infrastructure to an open, largely decentralized, digital infrastructure. Smart Grid is the transition from a system where generation, based on fossil fuel, adapts to users consumption, to a system where user consumption must be flexible enough to adapt to the fluctuations of the renewable based generation. Finally Smart Grid is a system where electricity is traded as a commodity on international marketplaces.

Resilience has always been the prime goal for the operators in charge of the generation, transmission and distribution infrastructures. In Europe, these operators have a long track record of success in containing accidents, avoiding black outs, and mitigating the effects of natural disasters. With the Smart Grid, cyber-security is now at the core of their efforts to provide a resilient infrastructure.

The issues linked to cyber-security follow from the very nature of the Smart Grid transition. It should be assumed that all software components could be compromised either because they are exposed to the Internet, or because physical security can be bypassed. It should be assumed that all components of the Smart Grid, from smart meters, to power plants, or relays could be targets for cyber attacks, as well as the SCADA systems used to monitor these software components. Users privacy should be enforced, and the mechanisms of trading marketplaces should be resilient.

The fact that all components might be compromised is commonplace on the Internet. The obvious solution is to rely on encryption whenever data is transmitted or stored. The problem then is (i) to secure encryption keys, (ii) to secure encryption and decryption and (iii) to secure the computation that takes place on decrypted data. The existing hardware protection techniques (e.g., trusted execution environments or hardware secure modules) can be used to guarantee confidentiality and integrity (as the sensitive data is protected in hardware that can provide tamper-resistance and tamper-evidence), but they cannot guarantee

WG1 inputs for Research - Risk management

Thanks to all WG1 and chairs

1. Research to identify the barriers to adoption of Best practices

1. Research to gauge Risk Management penetration into “hard to research” organisations and SMEs establish the best means of communications to raise awareness

2. Research to help to solve the lack of information to perform statistical / predictive risk analysis

3. Research into dynamic risk analysis for cyber threats

4. Research on risks metrics

Wrap up & next steps

- *Planning going as expected (WIP)*
- *Active+ contributions needed*
- *Landscape final version very soon*
- *Business & education Deliverables release candidate version (WIP)*
- *Processing of AoI priorization results for SRA + start creation of SRA document*
- *Taking care of NIS WG1, WG2 research gaps as well as stakeholders recommendations into SRA AoIs.*
- ***…***

Thank you.

NIS Platform
WG3 Secure ICT Research & Innovation