Network and Information Security (NIS) Platform

WG3 Secure ICT Research & Innovation

Fabio Martinelli – CNR
Raul Riesco Granadino – INCIBE
(Chairs)

Outline

WG3 Main deliverables

- **Secure ICT landscape**
- **Business cases and innovation paths**
- **Education and training**
- **Strategic research agenda (SRA)**

WG3 next steps

WG3 Main deliverables

- **Secure ICT Research landscape**

(**Second public version available**)

https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents

Technology driven

- **Business cases and innovation paths**

(first public release Dec. 2014)

https://resilience.enisa.europa.eu/nis-platform/wg3-secure-ict-research-and-innovation/shared-spaces/business-cases-and-innovation-paths/business-cases-and-innovation-paths-interim-version/view

- **Snapshot of education & training**

(first public release Dec. 2014)

https://resilience.enisa.europa.eu/nis-platform/wg3-secure-ict-research-and-innovation/shared-spaces/snapshot-of-education-training-landscape-for-workforce-development/Education-Training.pdf/view

- **Strategic Research Agenda**

Driven by the vision states (areas of interest)

(draft version Jan 2015/ first public release March 2015)

https://resilience.enisa.europa.eu/nis-platform/wg3-secure-ict-research-and-innovation/shared-spaces/the-strategic-research-agenda-sra/SRA-draft-2.05.pdf/view

WG3 Steering Committee

Secure ICT Landscape (Editors):
Mari Kert, EOS
Javier Lopez, U. Malaga
Evangelos Markatos, FORTH
Bart Preneel, KU Leuven

Business cases (Editors):
Zeta Dooly, WIT
Paul Kearney, BT

Education and training (Editors):
Maritta Heisel, U. Duisburg Essen
Claire Vishek, INTEL

Strategic Research Agenda (Editors):
Pascal Bisson, Thales
Fabio Martinelli, CNR,
Raúl Riesco Granadino, INCIBE

Area of Interest (AoI) - Leaders:
AoI#1: Citizen Digital Rights and Capabilities (individual layer)
Kai Rannenberg, Goethe University
Gisela Meister, GI-DE

AoI#2: Resilient Digital Civilisation (I) (collective layer)
Nick Wainwright, HP
Jim Clarke, TSSG

AoI#3: Trustworthy (Hyperconnected) Infrastructures (infrastructure layer)
Steffen Wendzel, U. Bonn
Piero Corte, Engineering

AoIs Cross analysis leaders:
Volkmar Lotz, SAP
Neeraj Suri, TU Darmstadt

Work methodology and meetings

Work in the Platform is carried out with the following principles in mind:

- Be results-oriented and focused on impact
- Be of value to the stakeholders
- Follow a bottom-up and consensus building approach
- Sharing of work load/ownership

Several F2F WG3 meetings (usually each 4 months since the end of 2013)

Deliverable: Secure ICT Landscape

Goal:

- Describe Current State of the Art in Cyber Security Technologies and application domains
- Identify the current treats and corresponding short term Research Challenges

Structure:

Basic technologies

Metrics in cybersecurity, Authentication, Authorization and Access Control, System integrity - Antivirus – Antispyware, Cryptology, Audit and monitoring, Configuration Management and Assurance, Software security and secure software development, Hardware and platform security, Network and mobile security, Cybersecurity threat technologies/ Offensive technologies, Information Sharing technologies, Big data, Data Protection, PET

Focus on Cloud/Internet of Things (IoT):

Models, current approaches and projects, open challenges

Application Domains:

e-Government, Energy-GRIDS, Smart transport/Automotive, Banking and finance, Smart cities, Telecommunications/ICT services, Dual use technologies, Food, Drinking water and water treatment systems, Agriculture, Cyber security awareness and training

The Strategic Research and Innovation Agenda (SRA)

NIS Platform WG3 Secure ICT Research & Innovation

Goal

- Define a strategic research and innovation agenda on cyber security
- Start from the desired vision states (or Areas of Interest) we wish to achieve in 2020
- Consider not just technological, but also social, legal, business, and educational aspects

SRA's Areas of Interests (AoIs)

- ***Several concepts emerged during the meetings:***
  - Citizen and people centric computing
  - Interconnected and vulnerable society
  - Privacy, security and civilization
  - Resilient infrastructure and services heavily depending on ICT
  - Multi-disciplinary skills, knowledge and awareness

- ***Eventually summarized in 3 main areas of interest:***
  - Individuals' Digital Rights and Capabilities (**Individual** layer)
  - Resilient Digital Civilisation (**Collective** layer)
  - Trustworthy (Hyperconnected) Infrastructures (**Infrastructure** layer)

Process

Each area of interest has been investigated separately for

- Identifying challenges, enablers/inhibithors (technical, policy, organizational) and research gaps
- Those elements are useful to stakeholders mainly interested to one perspective

After a cross analysis has been performed in order identify common emerging themes and possible divergences.

AoI#1 Individuals' Digital Rights and Capabilities (Individual layer)

Scope:

"Citizen centric view " incorporating

- how to design, manage, and control network and information and communications technologies
- respecting privacy, freedom of expression, safety
- enhancing technical aspects by social, legal and regulatory aspects of security and privacy

Individuality includes

- respect for citizens and consumers
- and transparency (without intrusiveness) to be provided at all times

Focus on:

Technology:

- **Secure computing** in untrusted platforms
- Provision of a **secure personal device** based on a secure core
- **Personal Identity Management**
- Sufficiently advanced **security and privacy** enablers together with **user friendliness**
- Technologies, that reduce the chances and the impact of **users giving up their privacy**
- **Policy-based** technologies for improving **compliance**
- Easing engineering of complex systems

From a social, policy, regulatory point of view

- Demand and support **user friendliness** of technical and IT security interfaces
- Provide **Privacy** in a heavily **controlled** world
- **Control of surveillance**
- **Assurance** in the digital world
- Support for open source technology production and evaluation tools
- Research on "trustworthiness/trust"

AoI#2 – Resilient Digital Civilisation (collective layer)

Scope:

Ensure trust in the digital form of (social) institutions/organizations.

- Organizations operate under a whole series of obligations that include:

➢ regulation, contracts, societal norms, risk management, security, secure handling of information and respect of fundamental rights of the customers/citizens.

Focus on:

Technology

•**Cryptography** with high strength
•**Privacy protecting**, yet **trustworthy identification technologies**
•**Transparency** about who has data at all times and knowledge of what it is being used for;
•New forms of **fraud protection** for digital currency;
•**Cyber forensics** that will provide the user with strong security
•**Secure data channels**
•**Secure shared computation environments**
•**Security and dependability** of Critical Information Infrastructure protection **(CIIP)**

From a social, policy, regulatory point of view

•**Balancing the societal needs**
•Stronger **coordination and cohesion** of the stakeholders groups:
•**R&I undertakings and results catch up with the faster requirements** of the **industry**
•**Standardization**

AoI#3 Trustworthy (Hyperconnected) Infrastructures (Infrastructure layer)

Scope:

- ICT as pervasive enabler in a world that is more and more highly interconnected
- Provision of cyber security in order to avoid ICT as weaker point in the security chain
- Study of the overall relationships among infrastructures

Focus on:

Global Hyperconnected vision, with main focus on:

- ICT
- Energy/Smart Grids
- Transportation
- Civil administration
- Smart Cities
- Automotive
- Control systems for water, food
- Healthcare
- Finance (Cyber Insurance)
- …

Common relevant themes (I)

Assurance

- Security Engineering
  - Architecture and design
  - Secure Coding and programming
  - Testing and Verification
  - Security metrics
  - …
- Certification
  - Automated certification schemas
  - Standards for certification
  - …
- Cyber Insurance
  - Risk assessment
  - Cost models
  - Economic models for cyber insurance
  - …

Focus on data

- Data protection
  - Data centric policies
  - User empowerment over personal data
  - Accountability and provenance
  - Operations on encrypted data
  - Economic value of personal / business data
  - …
- Data processing for security
  - Highly scalable data processing for situation awareness
  - Privacy aware big data analytics
  - …

Secure execution environments for everybody

- Secure devices for everybody
  - Trustworthy personal devices eco systems
  - Mobile devices operative system security
  - intrusion resilient systems
  - Human computer interface security
  - …
- Secure execution environments
  - Trusted cloud/IoT/network services
  - Crypto for cloud (e.g. homomorphic encryption) as well as for low resources devices
  - Secure communication
  - Secure virtualization
  - …

Common relevant themes (II)

Privacy issues

- Privacy preserving technologies
  - Anonymous credentials
  - Secure multiparty computation
  - Flexible privacy policies
  - Privacy risk management controls
  - …
- Privacy aware security mechanisms
  - Privacy preserving authentication
  - Privacy aware IDS
  - …
- ID management

Manging and assessing risks

- Dynamic risk assessment
- Composable risk metrics and indicators
- Managing complexity and system evolution
- Legal aspects
- …

Increasing trust

- Trust computational models
- Dynamic trust assessment
- Trust for on-line communities
- Trusted information management
- Economic models of trust
- …

Common relevant themes (III)

User-centricity

- Focus on user centric technologies (individuals)
  - Engineering methodologies that are user centric
  - Reduce possibilities for user misbehaviour
  - Reduce digital divide
  - …
- Usability
  - Usability of security mechanisms
  - E.g., authentication, usable secure public key algorithms
  - Proper visualization techniques for security alerts
  - …

Standardization and Interoperability

- Crypto
- Policy frameworks
- Assurance, risk, security metrics/indicators
- Security certification
- Information sharing
- IoT/Networks/Cloud frameworks
- …

Education and awareness

- Education
  - Multi-disciplinary focus
  - Responsiveness to changes in technology and societal environment
  - End-to-end skill development
  - Alignment of curricula and training with demand for skills
  - Using appropriate methodologies for teaching cybersecurity at all levels, from awareness to focused expertise
  - Bring all Member States to agree upon baseline with regard to cybersecurity indicators
  - …
- Awareness
  - Promote continuous awareness
  - Raising user awareness on privacy, big data collection, etc.
  - …

Comments/suggestions are very welcome!

NIS Platform
WG3 Secure ICT Research & Innovation