Building a Trust Framework for Future Internet Services and Infrastructures

Title of the workshop: “Building a Trust Framework for Future Internet Services and Infrastructures”

Format of the workshop: An introductory presentation, which will set the scene and raise key questions/challenges, will be followed by several position statements and a panel discussion.

Problem Statement and Objectives of the workshop:
Every day we can witness how communication technologies become more pervasive and ubiquitous in our close environment and make an impact on our personal life and work. In addition, communication networks and services are increasingly being considered as an integral part of the so-called critical infrastructures such as power grids, transportation networks, etc...

With the advent of Future Internet, communication networks, systems and services will become more dynamic (adaptive and autonomous), more scalable, and will include a myriad of actors (machines, sensors), and will be highly distributed. In this context, the notions of Trust and Trustworthiness of services and infrastructures play a vital role in the enablement of the Future Internet vision and the challenges of dynamicity, heterogeneity, scalability, automation also apply to these notions. While trust is considered today mainly as a bilateral relationship, the so-called end-to-end trust spans from the end-user, making usage of the applications, services, systems or devices, to the technology and solution operators, service providers and software developers. End-to-end trust is thus composed on multiple relationships with multi-facet elements, crossing usage areas, services, systems and infrastructures.

Trustworthiness is an attribute of a person, organization, component or devices that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities. Determination of trustworthiness is based on the assurance or grounds for confidence that the functionality has been implemented correctly and operates effectively. Today many trust frameworks tend to equate assurance with trustworthiness, characterizing trusted systems in a way that dissociates the system from those that use, operate, or access it.

In this workshop we look at the holistic trust framework that includes determination of trustworthiness properties, their publication, discovery, composition and management, as well as association of these properties with usage and operational issues. Given the fact that same components and communication networks might be used in a critical infrastructure, there is also an issue of multiple Levels of Assurance (LoA) for different end-to-end environments and application scenarios.

Trust mechanisms, trust management and assurance will certainly have high impact on the design, development, and deployment of the networks of the future, encompassing both services and infrastructures. The different definitions, requirements and technologies of trust are intrinsically linked and have to be considered altogether to deliver a continuum and total trust management.

In particular, the following dimensions or viewpoints of trust, sharing an evolution toward more assisted, autonomous, distributed and de-materialized decision and control processes, are considered and will be highlighted during the session:

- Network-centric trust, dealing with autonomic networks and their behavioural models, in terms of compliance/conformance to operator and service strategies. This level comprises a synthetic view and evaluation of the operations of cooperating software and hardware components. What are the main issues in ensuring trustworthiness of autonomous behaviours, what are the key evaluation criteria to comfort operator’s trust in self-managing networks, especially in the context of critical service demands mandating stricter and more complex trust assurance and management.
Component-centric trust, dealing with software components, services and their respective security aspects. Issues such as robustness, reliability, operational compliance enforcement, privacy by design, secure coding, requirements engineering etc are some of the topics to deal with. Enabling methodologies and technologies to enhance FI component-centric trust framework will be introduced based on the following three pillars: trustworthy service engineering which aims at novel engineering methodologies to guarantee secure service behavior and validation of the security requirements on a variety of Future Internet system environments involving multiple autonomous stakeholders; trustworthy service composition and evolution which aims at the integration and interoperability of end-to-end trusted services by adapting the service interfaces, modelling and composition techniques to enable a better modularity, reconfiguration and dynamic adaptation; and trust assurance as an integral constituent of the Future Internet system development process, relying on a broad range of assurance methods that jointly offer full development cycle support, rigorous development and verification techniques such as stepwise refinement, theorem proving, and model checking. Other aspects to consider include assessing the trustworthiness of composition of services as well as composing end-to-end metrics.

User-centric trust, dealing with authentications, identity management, operational issues, socio-economic and psychological factors, vendors, end-user, etc. In FI more stakeholders with different trust levels are involved in a typical service and network system composition and a variety of potentially harmful content sources are leveraged to provide value to the end user. This also creates more vulnerabilities and risks as the number of trust domains in an application gets multiplied, the size of attack surfaces grows and so does the number of threats. The challenges that dynamicity, scalability, heterogeneity or automation pose to user-centric trust are including the adaptive level of authentication assurance, connection between dynamicity of trust and dynamicity of “private information”, multi-organisational context, risk allocation across service chain, user environment (legal, cultural...) etc. End-to-end trust of specific applications dealing with personal data need to be designed to protect this data all the time according to the EU privacy requirements, while other environments might need to comply with other legislative compliance requirements (e.g. EU directive on Critical Infrastructure).

Of course, interplay between these three views on trust framework (e.g. in multilateral requirement analysis) is also included in the goal of this session. The session will debate the following questions through synthetic position statements presenting different viewpoints and a panel discussion:

**Question 1** – Which is the failure/threat/attack model that should be considered in designing an autonomous infrastructure, system or service targeting “trust erosion”? What needs to be protected?

**Question 2** – What is the end-to-end trust model? How is “transitive” or “modular” trust modelled, designed and which trust mechanisms are applied in your domain? (To address/solve Q1) – Are there agreed or useful metrics or characteristic information on the current reliability and assurance level of a specified service and infrastructure component? Are these different for critical and non-critical environments?

**Question 3** – How to describe/communicate/discover/translate trust framework elements or what to communicate to enable end-to-end trust interworking and interoperability (e.g. across user/application/service/network)?

**Question 4** – Is trust and trustworthiness an element to consider only at the design-time or run-time?

**Question 5** – What actions should be taken towards certification, standardization or regulation, which research directions or seeds should be fostered?

**Question 6** – What is new, unsolved, changed by the introduction of software and autonomic systems (less human in the loop) in telecommunication infrastructures and processes? Which introduction/migration/transition path(s), and technical/business incentives should be considered and developed?
Statement – Please indicate in one slide what action(s) your organization/project/initiative is planning to develop trust in future networks infrastructure and service.

Session organisers: Henning Arendt (@bc, Germany), Laurent Ciavaglia (Alcatel-Lucent, France), Samir Ghamri-Doudane (Alcatel-Lucent, France), Fabio Martinelli (CNR, Italy), Aljosa Pasic (Atos, Spain)

Steering Committee representative: Nancy Alonistioti (NKUA, Greece)

Target audience: Future Internet researchers, designers and architects. Standardization bodies representatives and participants. Scientists and engineers with interest in trust, security, conformance, testing, etc.

Build on previous FIA sessions:
- FIA Budapest – Standardization session
- ETSI Future Network Technologies workshop

Draft Agenda
Workshop chair: Laurent Ciavaglia (Alcatel-Lucent)

15 min – Introduction
  Armadeo Sarma (NEC – TDL Consortium)

60 min – Position statements
  Aljosa Pasic (ATOS – FP7 project NESSOS)
  Armadeo Sarma (NEC – TDL Consortium)
  Laurent Ciavaglia (Alcatel-Lucent – FP7 project UNIVERSELF)

45 min - Panel discussion
Panel Moderator: Henning Arendt (@BC)

Position statements will be debated based on the 6 questions and interactions with the audience. Panelists will comprise speakers of the position statements

References: