**Session Title: How far do we have to go to make the Internet secure?**

**Session organiser(s):** Jim Clarke (Waterford Institute of Technology – WIT), Carmen Fernandez Gago (University of Malaga), Fabio Martinelli (CNR), Paul Malone (WIT), Nick Wainwright (HP)

**Purpose & Audience**

The main purpose of the session was to bring together stakeholders across FIA domains in order to identify the priorities for new research designed to make the Internet secure in the H2020 timeframe for the uprising of the Future Internet. The session was designed to capture the views from the research and industry communities across three main streams:

- Secure networks and infrastructures;
- Security and big data;
- Trustworthy software and services.

**Key message(s):**

We can highlight one sentence key message from each of the streams of the session:

- Controlled ways to deal with the security threats and challenges that will rise having as starting point the architectures of the systems.
- Governance and organisation's responsibilities are the key issues to be considered in big data security.
- We need to find good and adequate metrics to determine how trustworthy services and systems are and what is the balance between trust and trustworthiness.

The architectures of the systems should be the starting point of where to address the security challenges, such as dealing with emerging threats, identity management, privacy, and trust in a reactive way. We cannot only concentrate on user's needs. Big data and governance are issues to work on especially on the organisations' side. On the users side, determining how trustworthy services are will become essential. Therefore, we need to define good metrics for that.

**Summary**

The following contains a summary of the three streams of the session.

1. **Secure networks and infrastructures.** The two speakers considered two different approaches. Dirk Kuhlmann reviewed the main weaknesses in networks security: top perceived threats (on the customers side), top observed problems (operators). His main idea is that security has to be

built in a reactive way, paying special attention to whether this way will make adding security to the systems sustainable at all.

Rubén Rios introduced the challenges that a new type of systems will raise for the FI, the so-called Internet of Things (IoTs). He presented the type of security architectures that will fit into this paradigm. Special focus was paid to privacy, identity management and trust.

This topic raised a very interesting discussion from the audience about what is the most convenient to deal with security threats in a controlled way.

2. **Security and big data.** The speakers for this stream were Henning Arrendt and Seamus Galvin. Both of them emphasised on the fact that governance and the way organisations deal with their responsibilities is of paramount importance as well as privacy. Issues related to data such as their characteristics, requirements of the data and the right to be forgotten (privacy by default) need to be paid attention to. The questions raised from the audience were about the cost of implementing data governance in the cloud. The notion of provable deletion of data was pointed out by the audience as a complement of the right to be forgotten. In order to aid the achievement of these two issues, we need tools to ensure that users are well informed before making decisions on their data.

3. **Trustworthy services and systems.** Hisain Elshaafi and Mike Surridge where the speakers of this session. Their talks focused mainly on how to make sure that a service is secure. We need suitable metrics for security attributes. Mike Surridge pointed out the importance of engineering trustworthiness and engineering user trust, making clear the difference between trust and trustworthiness by, for example, matching user behaviour to trust levels.


**Recommendations**

We believe that the three streams in this session are the key topics that should be considered as research trends for Europe when dealing with securing the Future Internet in the coming years. Inside each of these topics, we are highlighting as of paramount importance considering networks security having as a starting point the type of architecture of the system. Governance and organisations' responsibilities are key topics when considering big data. From the trustworthy services perspective, we need suitable metrics that aid us ensure how trustworthy a service is and defining the process of engineering trustworthiness taking into account the user perspective.