

Security challenges for F.I.

Comments on the paper **“The Future Internet: A Services and Software Perspective”**

Pedro Soria-Rodriguez
pedro.soria@atosorigin.com

Atos Research & Innovation
2008-04-01 - Bled

Security challenges for F.I.

- **Increasing scale =>**
 - large number of devices/terminals
- **Short communication =>**
 - Authentication, integrity, confidentiality, required in spontaneous, short-lived connections
- **Large number of devices =>**
 - which can be trusted? How to assign trust in large universe?
- **No central control and governance =>**
 - security of applications and services may not have to rely on infrastructure; end-to-end

Privacy, Trust challenges for F.I.

- **Ubiquity** of the Future Internet:
- User community will include non-tech-savvy users:
 - Responsibility: people
 - Security awareness education necessary for such users.
 - Responsibility for user's own privacy must be on users themselves.
 - Decisions on trust
 - Assistance: technology
 - Helping users understand security implications
 - Can attempt to help protect privacy
 - Can help support the decision to trust a service / provider

Security challenges for Services

Applications offered under software-as-a-service (SaaS) paradigm:

- Application providers: require secure environment to **deploy** applications (e.g. secure virtualizers)
- Availability of applications: users and providers alike will seek to have **high availability**.
- Applications imply data manipulation: confidentiality, integrity, authentication likely to be required from users in SaaS.
- Service composition results in new services and applications. Security of the **composition** operation will be necessary.
- **Security engineering**: weaving-in of security into SaaS, Services, iterated service chains.
- **Compliance + auditing** of security in SaaS, iterated outsourcing scenarios.