Trust
Assumptions
Trustworthiness
Assurance

Aljosa Pasic

FIA Poznan, 25/10/2011

Atos

Table of Content

Opening statements

- Service-centric view is changing the way IT infrastructure and applications will be managed and delivered
- Applications will utilise components out of different domains of control, obeying separate security policies, asking for diverse security and dependability qualities
- Components may be owned and operated by different organisations (trusted or not)
- Services will be shared between many consumers

We are all part of an experiment in FI-trust whose outcome is unclear

Many add-on security solutions are trying to ensure the continuation of the physical world trust assumptions – not promting to rethink trust in e.g. composition of services

Trust is a problem ?

- Services are not trusted due to:
  - Market pressure
  - Perception by large mass of users;
  - Information managed by a restricted group of "experts", increasing info-exclusion;
  - Information mismanaged, prompting for cyber-crime, e-frauds, cyber terrorism and sabotage
  - Lack of privacy
  - etc

Trustworthiness is a problem ?

- Services are not trustworthy because of:
  - The poor engineering/programming practices
  - Not taking security requirements from the beginning or not expressing them correctly
  - Risks were not treated properly
  - Security mechanisms is not scalable/interoperable...
  - Operational context was not taken into account…
  - etc

Real-Time End2End Super Mega Deluxe Assurance Management

- Assurance process more agile and fl
- Share security/risk informati
  stakeholders (e.g. modul
  tool
- Aut
  of a
- Find
- Def
  ope
  sha
- Ver
  ope
- ...as

n
s (
h “dy
es c
sk
of high level goals (e.g. Privacy) into
eadable policies
an factor”??

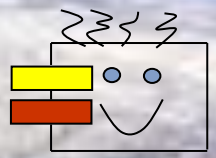
a) **b)** **c)**

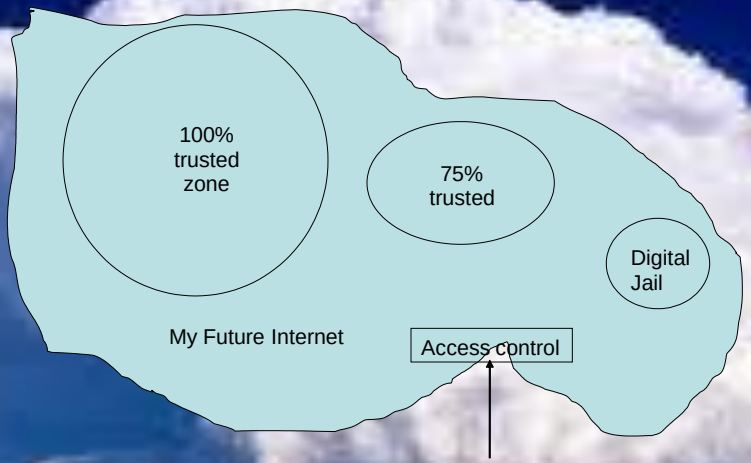
From Assurance to Assumptions Management ?

- Quality of Experience and the link between trust and trustworthiness
- A global view of service trust and trustworthiness which encompasses also socio-economical aspects
- Devising mechanisms to validate or manage assumptions including:
  - secure services architecting and engineering;
  - design- and run-time validation;
  - simulations;
  - ability to monitor, measure, test and predict the security status of a system;
  - reputation and similar mechanisms
  - LINK PHYSICAL AND REAL WORLD !!!

If computing sky is getting “cloudy”…Trust will depend on “weather conditions”…

Infrastructure view: Expanding boundary (include mobile access) and/or Contracting boundary (exclude outsourcing staff PC, external B2B server…)





Nessos research directions

- Security Requirments engineering:
  - Express higher level goals/contraints (e.g. privacy) such as social, economic and legal
  - Enable automatic verification (e.g. large scale real-life scenarios)
- Assurance and metrics
  - Assurance “case” or “profile” that include operational (e.g. outsourcing) issues
  - Automation of security model checking
  - Certification and audit frameworks
  - Link between early assurance (e.g. model check, stepwise refinement) and implementation assurance (e.g. code level testing)
- Secure service composition
  - Dynamicity of security “contracts”
  - Testbeds and risk “knowledge base”
  - Partial, inadequate, uncertain or untrusted information about service properties
- Risk and Cost aware SDLC
  - Dynamic risk allocation and sharing
  - Modularity

Atos

Thanks

For more information please contact:
T+ 34 91214 8800
M+ 34 675 639383
Aljosa.Pasic@atos.net

Atos (Spain)
Albarracín 25
E-28037 Madrid

www.atos.net