Thales Communications
Perspectives to the Future Internet
2\textsuperscript{nd} June 2010 - Luxembourg
Challenges of Future Internet

- Internet as a starting point…
  - Was defined for asynchronous services (web pages, file transfer …)
  - Designed as a best effort (no security, no guarantee, no priority…)
    and static network (no reconfigurability, no mobility, no wireless…)

- … But the current Internet as we know it
  - is reaching a saturation point to face increasing user expectations
    (video on demand, gaming, social networks, P2P, streaming …)
  - is showing inability to efficiently respond to new socio-economical challenges in terms of security, scalability, mobility, availability, and manageability

Future Internet is now a business platform,
the future heart of the Economy
that links social life of users as well as critical activities such as
Communications (telephone, Internet), Energy & fluids (electricity, gas, water),
Transportation (railways, airlines, road) & Health and emergency response
As a world leader in critical mission information systems, Thales Communications develops a common base of technologies to serve a single objective:

The security of people, property and nations.

The Group offers security solutions for large critical infrastructures as system integrator, security expertise and product & services supplier.

Thales proposes to foster the development the Future Internet as critical information system environment with native:

Trust, Dependability and security
Why Trusted systems?

Security by design not sufficient
- For complex and large systems
- For dynamic systems
- For multi-players services providers

Security and Trust tradeoffs
Imposing a single common model/framework limitations

Trust as a BUSINESS enabler
We need to equip system evaluation tools with both:
- Internal probes/actuators to ensure security assurance
- External, non intrusive, trust evaluation engines
Distributing Trust

Trust is made of:
- Belief in reliability, honesty, good faith in the intend of another party
- Belief of proof that the means used to conduct the deal cannot be misused

Distributing trust:
- All the parties and medium involved maintain trustworthiness

Trust and security:
- Confidentiality of information
- Network termination
- Secured users & machines
- Authenticated sources
- Service access

Answers:
- Network/link protection
- Application/web protection
- Signature & time stamping
- Trusted identity & role-based rules
- ID federation, delegation of authority and resource provisioning
“Internet can only be evaluated by Internet”

Service Consumers (SC)

Trusted Third Party B

Trusted Third Party F

Users Community Z

Experts Federation A

Trusted Advisors (Single, or federation, or social network)

Users Community C

Experts Federation N

Trust metrics consultation

Trust metrics assessment

Service Providers (SP)

Trust Increase

Business Increase
Thales aims to increase the dependability of critical open and interconnected systems by a multi-disciplinary and coordinated effort:

- Combined breakthroughs in
  - Modelling,
  - Fault analysis,
  - Performance simulation,
  - Symptomatic scenarios detection,
  - Decision aid tools
  - Reconfiguration
Critical system management

Autonomic computing background knowledge

- **Self-configuration**
  - To speed up the configuration dedicated to new client according to negotiated SLAs
  - To make sure previous SLAs are still correctly answered

- **Self-healing**
  - To recover when critical incidents occurs (e.g. hardware failure)

- **Self-organisation**
  - To dynamically adapt the management resources and processes to the actual usage

- **Self-protection**
  - To organize back-ups
  - To early detect intrusion
  - To perform security audits
Introduction of self* capabilities

- self* actions implemented within bounds of high level policies

With an aim to

- improve the deployment of heterogeneous systems with formal validation of policy introduction

To increase resilience of critical systems by providing faster self-healing capabilities
Cyber-security: a FI priority

Cyber-Threats:

- **Cyber-crime**: breach of the law via Internet,
- **Cyber-terrorism**: Internet as a vector for destabilisation, disinformation, propaganda or to target critical infrastructures,
- **Cyber-war**: Attacks against military computer systems and/or critical civilian assets (power, telecoms, financial institutions, Airlines)

Main kinds of attacks:

- Distributed denial of service targeting Internet or an information system
- Intrusion in order to steal or to modify data
Vulnerabilities assessment

System vulnerabilities audit
- Criticality analysis
- Attacks models evaluation

Framework based on the combination of several technologies
- Topology and services discovery
- Knowledge representation
- Inference engines

Used to secure SCADA & Information systems

Key capabilities to ensure an information system surveillance, decision making and anticipation
Thales Interest to PPP FI

Transport
Dependable
Multimodal transportation system (SOA, ETSI ITS/ISO CALM architectures, V2X)
Multi-services networks (Virtual Network, Opportunistic network)
Smart Cities

Content
Content network aware
Content-based routing
Content Based Information security (traceability, identity federation, anonymisation, multilevel cyphering)
Distributed caching

Smart Grid
Distributed Security
Reliable distributed Scada
Integration of small, long life-cycle devices
Monitoring the overall integrated system

Core Platform
Security & Trust
Internet of Things (M2M, Embedded Sensors)
Reliable and dependable

Needed partners:
- Living labs & User
- Academic partners with prototyping skills and testbed for scalability assessment
- SME with knowledge on
  - virtualisation; trust management, sensors integration ...