Towards a global dependability and security framework

Jacques Bus
Head of Unit “ICT for Trust and Security”-
European Commission
Directorate-General Information Society
jacques.bus@cec.eu.int
A comprehensive EU approach to security

<table>
<thead>
<tr>
<th>Economic, business and social aspects of security in Information Society</th>
<th>Cyber-crime, Internal security</th>
<th>External security / defence</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Electronic Signature</td>
<td>• Framework Decision on attacks against information systems</td>
<td>• Pilot action with DG RTD</td>
</tr>
<tr>
<td>• Data protection in elect. com.</td>
<td>• Lawful interception</td>
<td>• Dual use technology research</td>
</tr>
<tr>
<td>• Network &amp; information security</td>
<td>• G8 CIP</td>
<td>• Crisis management</td>
</tr>
<tr>
<td>• Culture of security</td>
<td>• e-identification/e-authentication</td>
<td></td>
</tr>
<tr>
<td>• ENISA</td>
<td>• biometrics in visas and residence permit</td>
<td></td>
</tr>
<tr>
<td>• digital right management, biometrics, smart card, IPv6, open source software</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• critical infrastructure protection</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Preparatory Action on Security Research

Research and Technology
Information and Communication Technologies

• network security, dependability, cryptography, biometrics, identity management, watermarking, ...
Driving the future in ICT

CONVERGENCE OF:

MEDIA

PROCESSES

NETWORK (IP)
The down side?

COMPLEXITY & VULNERABILITY

LACK OF TRUST & SECURITY

CYBERCRIME

RESILIENCE, TRUST and LAW ENFORCEMENT
Highly vulnerable, complex and interconnected infrastructures and utilities.

September 28, 2003 Italian electricity grid collapse: ~50 million people without electricity for one day
October 31, 2004 Part of France Telecom IT infrastructure collapse: ~15 million people without telephone for two days

EU research needed on:
  • dependability and resilience of ICT infrastructures against faults and attacks
  • capabilities to manage and control large scale dependable systems
Pervasiveness of ICT in our daily life risks privacy, abuse personal data and digital assets, and identity theft and undermines trust in the Information Society.

EU research needed on:

- Identity and privacy management
- Secure access and authentication for networks and services
- Protecting digital assets of business and consumers
- Control and transparency of handling personal and enterprise digital assets
Biometric identification must provide secure access; protection, integrity and security of identity and data; without compromising trust and privacy.

EU research needed on:
- Multi modal biometrics
- Usability of biometrics
- Biometrics for privacy protection
- User control on his/her biometric data
Curing pathological aspects of digital electronic networks

Computer hacking, viruses, spy/malware, phishing, spoofing …

‘Always-on’ and mobility increase risks and scale, hence costs

EU research needed on:

• Architectures, models components for nomadic, pervasive, multi-players communicating world

• Auditing, reporting, logging for forensics and law enforcement

Win32 viruses & worms
(source: Symantec corporation)

- **Objectives:**
  - Improve EU-citizen security
  - Reinforce European technological and industrial potential and encourage cross sector interaction
  - Prepare a European Security Research Programme (ESRP) to be launched in 2007 as part of FP7

- **Budget:** 55 Mio€ for the 3 years – 1 call per year

- **Activities:** Multi-disciplinary, mission-oriented projects and supporting activities
Call 2005

- Publication in January
- Deadline April
- Budget 15 Mio€
- 6-8 Projects, some SA

Projects priorities

- Networked systems
- Protection against terrorism
- Crisis management
- Interoperability and integrated systems
- Situation awareness
The IST Priority funds five sorts of project

- **Integrated Projects (IPs) and Specific Targeted Research Projects (STREPs)** are aimed at generating, demonstrating and validating new knowledge by means of research and development.

- **Networks of Excellence (NoEs)** are aimed at the durable integration of the participants’ activities/capacities.

- **Coordination Actions (CAs) and Specific Support Actions (SSAs)** are aimed at supporting collaboration and coordination, and other activities such as conferences and studies.
Instruments in IST

For more information on instruments:

- Brochure – the FP6 in Brief
- The Guides for proposers
General financial regime

• Community support will be in the form of a “grant to the budget”
• Paid as a contribution to actual costs
  – that are necessary and economic for the project
  – that are recorded in the accounts of the participants
    • or, when provided for in the contract, in the accounts of third parties
      – that exclude indirect taxes, duties, interest…
• Annually, each participant to provide a summary cost statement supported by:
  – certification of total costs by an independent auditor
  – management-level justification of costs
  – corresponding activity report
• Rolling advance scheme throughout duration
Where are we in FP6?

Mobility, Virtual identity management, Privacy
Novel crypto technologies, Digital assets protection
Dependable networks & systems, Critical infrastructure protection
Biometrics & Smart card research

Digital Assets Mgt, Critical Infrast.Prot.
Dependability / Resilience

Projects Contracted
15 + 1

Proposals from Calls 1 & 2
Total funding ~74 MEuro

three key Areas not addressed
Research Focus:

- security and dependability challenges arising from complexity, ubiquity and autonomy
- resilience, self-healing, mobility, dynamic content and volatile environments
- strategic and solid research on security and trust for new societal applications
- interoperable content and digital rights management

Key Objectives & Breakthroughs

- build on EU technical and scientific excellence on security, dependability and resilience
- meet EU demands for privacy and trust
- strengthen the interplay between research and policy

Indicative budget > 63 MEuro

The next step: IST Call 4
S.O. 2.4.3 Towards a global dependability and security framework
Priority areas

- integrated frameworks and technologies for resilience, dependability and security
- modelling/simulation techniques and synthetic environments for interdependencies, recovery and continuity
- technologies and architectures for secure computing and interoperable management and trustworthy sharing of digital assets
- secure and interoperable biometrics
- security and privacy technologies and architectures for future wireless and mobile scenarios
- security assurance and certification of complex networked systems and infrastructures

Instruments

IPs, NoEs, STREPs, CAs
IPs, NoEs, STREPs, CAs
IPs, STREPs
IPs, STREPs
STREPs, SSAs
Preparing FP7 (1)

• First Proposal FP7 by April 2005 to Council and Parliament
  – Structure
  – Content
  – Budget requirements

• Consultations and preparations ongoing
  – Web
  – Various industry consultations
  – In context of new calls of FP6
Resilience and plasticity in a complex world – Future RTD

Assured Service and Information in Information Society

- endemic vulnerabilities, auditable
- active, self-adapting
- user empowerment, digital asset control and management
- multiple virtual identity; management of roles; access control; privacy aware authentication and authorization; user empowerment of rights and obligations

Towards a dependable ICT for Information Society

- Resilience in large scale and complex systems
- Mastering scale & volume
- Miniaturization of components, ICT fabric

Dynamic security policies; epidemiological security models and mechanisms for computing and sensor networks; network awareness & disaster avoidance technologies; network assurance and forensics; assured security of service provisioning; open and interoperable management of digital assets; ...

Architecture and technologies for widely distributed attack detection systems, and cooperative recovery systems; risk management; human factor technologies; ...

INFRASTRUCTURE LEVEL

SERVICE LEVEL

PET & MULPIDE

Resilience in large scale and complex systems
“For the research actors, by the research actors”

• ETP aims to foster effective public-private partnerships
  – between the research community, industry and policy makers
  – to mobilise research and innovation efforts for achieving common goals
  – to accelerate innovation and eliminate the barriers to deployment

• it is a mechanism to bring together all interested stakeholders
  – to first develop a long-term vision,
  – create a coherent, dynamic strategy to achieve it
  – steer the implementation

• an ETP operates at a strategic level and is not directly related to any specific programme

• E.g. a GSM-like process
In which field?

- Where there are **clearly identified outcomes from RTD coordination**
  - strengthening industrial competitiveness, addressing societal challenges
  - need for consensus building e.g. to develop standards
  - need to coordinate with other research funding bodies, MSs Eureka,…

- Where coordination is feasible
  - A **well identified** research and industrial community
  - ready to collaborate in developing a roadmap
  - and to engage in its implementation

- Were industry is clearly **committed to invest** in the research roadmap
  - Involvement at the highest level.
  - ETPS are NOT just forums for discussion or advisory groups.

- Where technology progress has to be articulated with other actions
  - regulatory framework, uptake measures

- In addition in FP7, the use of Article 171 is proposed
  - Joint Technology Initiatives
In ICT field

• Major successes obtained in areas where research roadmaps have been set up:
  – In Europe and also worldwide roadmaps
  – Microelectronics, mobile,..

• So far three initiatives
  – nano electronics
  – Embedded systems
  – Mobile and wireless Technologies

• Will there be others?
  – Perhaps, but depending on Industry engagement
Preparing FP7 (2)

- Security: two broad issues
  - Technology development in: Complexity, resilience, services related to broader technology work on software, grids and knowledge-intensive (web)services
  - Technology and Society: Trust, Identity, Privacy, Management of personal and business digital assets, use of RFID and biometrics
Web sites

IST Programme:

www.cordis.lu/ist

ICT for Trust & Security

www.cordis.lu/ist/so/dependability-security/home.html