Overview of the Technology Transfer Potential of EU Security and Trust R&D Projects
6th Sept 2012

WP2 - Foundations and Analysis

Martina de Gramatica – Fabio Massacci
University of Trento
Document Analysis

- Publishable reports, Deliverables, Web sites.

Ethnographic Research

- Interviews with project officers, project coordinators, technical leaders;
- More than 70 interviews to Call 1, Joint Call and Call 5 projects.

Why not just documents?

- At beginning projects only have DoW and this is confidential;
- At the end they have hundreds of deliverables and many are just stepping stones.
- Call 1 and Joint Call: Hubs role of software and integrators
- Call 5: Same structure but more Telcom
WP2 - High Level View

Why Constituency Changed?
- Call 1 - stronger focus on privacy and identity management
  - More software integrators
- Joint Call on critical infrastructure
  - More “non-IT” partners
- Call 5 - stronger focus on Infrastructures and platforms
  - More Telcos

Why some Universities are big hubs?
- Diverse groups participate
  - E.g KUL: crypto, software security, legal aspects
Potential Marketable Results also outside consortium

- some projects have results directly usable by citizens
  - biometrics and privacy;

- most projects have innovations in tools and methods for ICT specialists (from consultants on IT governance to IT administrators) that are widely usable beyond the project’s consortium.
  - Mostly in area of command, control and compliance (of networks and IT systems)

- Some projects have knowledge based contribution

Other contributions

- Mostly in terms of architecture and policy languages result
  - Harder to market outside consortium
Sample Example – Call 1

- Citizen’s Potential Innovation
  - (car) driver authentication module – ACTIBIO

- ICT Specialists
  - Confidentiality preserving methods for market data aggregation (applied to supply-chain information systems) – SECURESCM
  - Integrated packages for trusted operating systems – TECOM
  - Model checking tool for security protocols - AVANTSSAR

- Knowledge Base
  - Development of databases of vulnerabilities - INTERSECTION & SHIELDS
Sample Example – Call 5

- **Citizen’s Potential Innovation**
  - Reliability of the biometric systems – TABULA RASA

- **ICT Specialists**
  - Process isolation for embedded platform – SEPIA
  - Model checking and run time analysis for services – SPACIOS

- **Knowledge Base**
  - Software repository for secure software engineering - NESSOS
WP2 – Innovation Missing Gaps

- **Few projects run PILOT** (ABC4TRUST – U-TRUST IT– PICOS - ACTIBIO):
  - More time/resources for user trials needed
  - Lots of development effort, research-wise not so valuable

  «there is never enough time for user-trials»

- **Often research projects deliver their results and then there is no time to pilot them, unless running new projects:**
  - Lots of instruments exists (CIP, Pre-Commercial Procurement) but they are “new projects”
  - What’s missing is “follow-up” measure for the most promising part = (PRIME, PRIMELIFE, ABC4TRUST)
  - Possible solution: the EC to support streamlined measures for subset of consortium to explore trial
Lack of structured and documented relations with product groups within the industry partners

Open issue: should EC push projects to establish a structured and visible relationship with the product group from the very start?

Lack of a good and innovative business model for security: lack of awareness about security and privacy issues by the critical mass:

- “The point in security is not to make money but to avoid losing money”
- “security is often perceived as an extra cost”
Many projects claim to create a community: this is not really clear how successful and measurable in the short term this is.

Secretive approach to disclosure of security problems

Possible solution: an European-wide regulatory initiative to mandate the controlled disclosure of security incidents