WP5 – Security and Trust

TRIPCOM Kick-off meeting.
Wien, 24-25 April, 2006

Alessandro Ghioni and Davide Cerri
{ghioni, cerri}@cefriel.it
CEFRIEL – Politecnico di Milano

WP Participants and effort

- WP Leader:
  - **CEFRIEL** - 24 person months
- WP Partners:
  - **LFUI** - 8 person months
  - **TUW** - 15 person months
  - **FUB** - 8 person months
  - **TID** - 8 person months
- 63 person-months in total.

- WP5 management team:
  - Alessandro Ghioni <ghioni@cefriel.it>
  - Jacek Kopecky <jacek.kopecky@deri.org>
  - Lyndon J B Nixon <nixon@inf.fu-berlin.de>
  - Geri Joskowicz <josko@complang.tuwien.ac.at>
  - Sara Carro-Martínez <scm@tid.es>

WP5 objective and scenario

- Objectives (from TripCom Annex I – DoW)
  - Guarantee **security and privacy of the information written** in the Triple Space.
  - Provide the theoretic foundations of a mechanism for **establishing end-to-end trust** between dynamically discovered actors.
  - Provide a **prototypical, pluggable implementation** of the above.

- Relevant triple space features impacting on security
  - The TS is a **distributed infrastructure**
  - The TS does **not have any central authority**
  - The TS is based on **asynchronous communication**
  - The TS is based on data **publication**
    - one-to-one communication
    - one-to-many communication
    - many-to-many communication

WP5 main tasks

- Requirement analysis and state-of-the-art of security and trust in distributed systems.
  - what does “security” mean for the TripCom infrastructure?
- Definition of security and trust support model for the Triple Space.
  - how to derive trust when no central authority can exist?
- Design of the distributed security model in order to support sub-spaces with individual and pluggable privacy possibilities.
  - how to meet secure interaction needs for services in the TS?
- Two-phase implementation: early (M24) and final (M36) prototype.
  - pluggable implementation: security features can be “linked” in the Triple Space, but all must be designed with security in mind (at design time, security is not an “add-on feature”. Otherwise, it can be excluded at runtime, if unnecessary).

Infrastructure security

- A distributed infrastructure is intrinsically **more vulnerable** to attacks because there's not a single enforcement point.
  - On the other side a distributed infrastructure could be more dependable than a centralized one, because there's not a single point of failure.
- In TripCom we need to secure:
  - the **communication channel**;
  - the entire **distributed infrastructure**:
    - e.g. an attacker could try to subvert the infrastructure in order to gain some advantage (it's usually a P2P topic…);
  - **data stored** in each Triple Space:
    - authentication (anonymity too?);
    - integrity;
    - confidentiality;
    - non repudiation (it deals with trust…).

Establishing trust

- […] Trusting a *person* means believing that when offered the chance, he or she is not likely to behave in a way that is damaging to us, and trust will typically be relevant when at least one party is free to disappoint the other, free enough to avoid a risky relationship, and constrained enough to consider that relationship an attractive option. (*)
- As we are dealing with “machines”, but we want to learn from the way people behave…
- …we will deal with trust in **two complementary ways**:
  - a trust model based on **reputation distribution** in order to understand “how much is an entity or a statement trustworthy”;
  - trust **negotiation mechanisms** in order to provide authentication and access control “respectful of privacy policies”.

(*) Gambetta, Diego (2000) ‘Can We Trust Trust?’, in Gambetta, Diego (ed.) Trust: Making and Breaking Cooperative Relations, electronic edition, Department of Sociology, University of Oxford, chapter 13, pp. 213-237, <http://www.sociology.ox.ac.uk/papers/gambetta213-237.pdf>.

Trust model

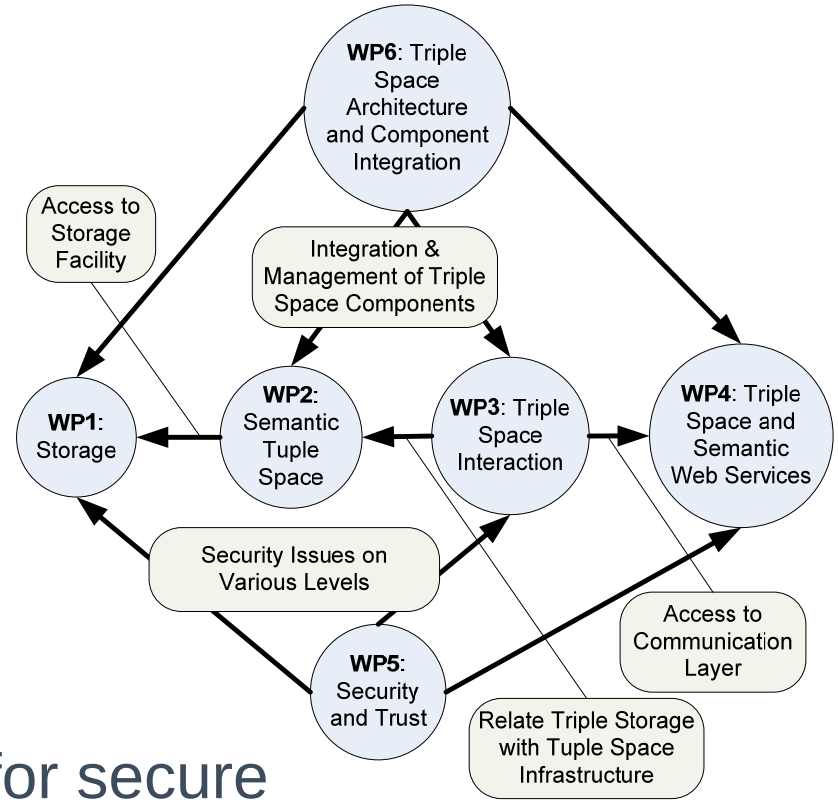
- Distributed authentication and trust model based on a sort of decentralized "**web of trust**":
  - no central authorities;
  - **subjective** trust;
  - graph-like trust relationships between participants.
- Each participant will be enabled to distinguish between "trusted" and "not trusted" **participants**.
- Each participant will be enabled to distinguish between "trusted" and "not trusted" **triples**.
- All of this will be based on **reputation** techniques:
  - participants **express** their opinion on some triples;
  - participants **aggregate** opinions in order to decide how much a statement found in the Triple Space can be considered trustworthy;
  - each participant has his **own opinion** based on his experience and on "who said what".

Trust negotiation

- As entities in the Triple Space can interact, they must decide how security is handled within the interaction.
- Participants will be able to obtain reputation information about their counterparts and statements, but…
  - they need also to express and enforce their own **subjective access control** policies;
  - they could prefer **not to disclose** their policies;
  - they could decide not to “fully” authenticate if the counterparts have not **revealed part of their identity** too;
  - they could need to interact only with particular **categories of counterparts** (and what if a participant claims to belong to a certain category, while this is not true? It’s a trust matter).
- Participants will be able to negotiate trust, privacy policies and access control for services within the Triple Space.

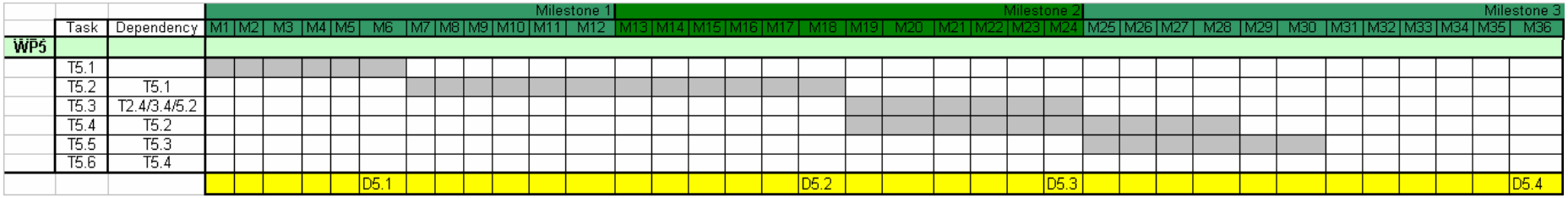
TripCom security: the “big” picture

- WP5 will give inputs to **WP1** for **storage security**
  - data authentication, integrity, confidentiality, non repudiation.
- WP5 will give inputs to **WP3** for **infrastructure security**
  - security for the entire distributed infrastructure



- WP5 will give inputs to **WP4** for secure interaction between TripCom **semantic web services**
  - trust model used by participants in order to obtain reputation information about counterparts or triples;
  - trust negotiation used by services in business processes.

Next steps



- T5.1:Requirement analysis and state-of-the-art of security and trust in distributed systems.
  - Gather requirements and analyze literature for security of distributed infrastructures (storage, communication channel, P2P).
  - Gather requirements and analyze literature for authentication, reputation distribution and trust based on “web of trust” models.
  - Gather requirements and analyze literature for trust negotiation mechanisms and policy specification.
- *T5.2:Definition of security and trust support model for the Triple Space.*
- *T5.3:First implementation: Early prototype of the security and trust components.*
- *T5.4:Definition of a distributed trust and security model that supports clustering and sub-spaces with individual and pluggable privacy possibilities.*
- *T5.5:Evaluation of initial implementation.*
- *T5.6:Second implementation: Refinement and final prototype.*

WP5 deliverables

- D5.1 - Requirement analysis and state-of-the-art
  - Lead Participant: **CEFRIEL**
  - Related to **Task 5.1**
- D5.2 - Definition of security and trust support model for the reference architecture.
  - Lead Participant: **CEFRIEL**
  - Related to **Task 5.2**
- D5.3 - Early prototype of the security and trust infrastructure.
  - Lead Participant: **TUW**
  - Related to **Task 5.3**
- D5.4 - Final prototype.
  - Lead Participant: **TID**
  - Related to **Tasks 5.4, 5.5 and 5.6**