BETTY WG2: Security

Ilaria Castellani & Hugo Torres Vieira

(INRIA Sophia Antipolis & University of Lisbon)

BETTY meeting

Rome, March 24, 2013

WG2 composition

- 29 members
- Countries: Croatia (1), Denmark (1), France (3), Germany (1), Italy (8), Lithuania (1), Macedonia (1), Portugal (5), Romania (2), Serbia (4), UK (2)
- Provisional chair & vice-chair: I. Castellani (F) & H. Torres Vieira (P)
- Existing collaborations on BT + security:
  - within BETTY: France-Italy, France-UK, Italy-Portugal, Italy-Serbia.
  - outside BETTY: Portugal-USA, Denmark-Japan.
- Well-balanced: F/M = 11/18, 5 Eastern Europe countries ⇒ good gender and East-West balances (F/Total = 38%, East/Total = 31%).

WG2 Focus and Questions

Questions

- Which existing security properties are relevant for sessions?
- Are there new security issues that are specific to sessions?

Thesis

Behavioural types *by themselves* should contribute to improve security: in a well-typed session, the world is not “as wild” as in an open network.

Classical BT’s help but do not suffice ⇒ need for security-enhanced BT’s.

Goal

Cover large spectrum of protocols from “general-purpose” sessions, where security is not the primary goal (but need for protection of private data), to security protocols and cryptographic protocols, which are specifically designed to ensure some security property.

State of the Art

Existing work (selection):

- Confidentiality → **Talk 1**
  Secure information flow, ensured statically by security-enhanced session types, or dynamically by a monitored semantics.
- Integrity → **Talk 2**
  Ensured by security-preserving session type compilation, using cryptographic primitives in target language.
- Role-based Access Control for data on the Web → **Talk 3**
  Ensured by “static” tree descriptions (similar in structure to BT’s), policies and role capabilities.
- Proof-carrying code in session calculi → **Talk 4**
  Exploits dependent types to guarantee properties about the session-exchanged values.

Short talks

1. Sara Capecchi
   Information flow control and reputation in multiparty sessions
2. Pierre-Malo Deniélou
   Multi-party sessions as a security protocol abstraction
3. Svetlana Jaksic
   Security Types for Dynamic Web Data
4. Bernardo Toninho
   Proof-carrying code in session calculi

Open questions/Tracks for future work

Future work:

- Unified approach to confidentiality and integrity
- Role of “role assignment” for security properties
- Internal attacks (by participants) vs external attacks (by environment)
- Security in one session vs security across related sessions
- Vulnerability of “distributed sessions” wrt “local sessions”
- Security-preserving translations between session calculi/languages
- Logics and verification tools for security properties in sessions

WG2 workplan and interaction with other WG's

Workplan for year 1

- State-of-the-art report
- First annual WG report
- Consolidate existing collaborations, spur new ones (target 3-4 STSM)
- Contact with EU FP7 project ANIKETOS

Interaction with other WG's

- Closely intertwined with WG1, from the start
- Interaction with WG3 and WG4 expected to increase in final years