BIC, WG1 – Topic: Trust management and secure software

Fabio Martinelli

Institute for Informatics and Telematics

National Research Council

(IIT-CNR)

Outline

- On trust management
- On secure software
- Topics/issues of interest for cooperation

Many meanings for trust

- Trust is a generic keyword
  - Used in many communities with different meanings
    - E.g. Herbig et al., "*The **estimation** of the consistency over time of an attribute or entity*"
    - E.g. Gambetta et al.: "*a particular level of the **subjective** probability with which an agent assesses that another agent or group of agents will perform a particular action, both before he [i.e. the trustor] can monitor such action (or independently of his capacity ever to be able to monitor it) and in a context in which it affects his [i.e. the trustor's] own action*"
    - E.g. Dimitrakos et al.: "*Trust of a party A in a party B for a service X is the measurable **belief** of A in B behaving dependably for a specified period within a specified context in relation to X...*"
    - …

Trust

- Trust is declined in several dimensions:
  - We can trust a system for correctly functioning: *System trust*
  - We might wish to model trust relationships **inside** our system because those are necessary for its behaviour: *Identity trust, Access trust, Delegation trust, …*
- However, we *trust* something/someone for a *purpose* in a given context
- We need mechanisms to evaluate, analyze, use, negotiate …
  - Interoperable mechanisms to represent it
  - Trust is central notion for certification of software
- Trust may be based on several aspects:
  - verifiable evidence:
    - E.g. proof methods, rigorous design&analysis techniques, …
  - direct experience:
    - E.g., previous interaction history (monitoring the target entity behaviour is the main tool)
  - indirect experience:
    - Third party recommendation (then you need to trust someone to recommend others and so on …)
  - and represented, combined, monitored and negotiated in several ways
    - Some computational models of trusts based have been proposed on social networks, probability theory, formal semantics and logic, game theory …

Security and trust

- Traditional "trust management" is used for access control in security
  - Credentials, policies, access and delegation rules
- On the relationships between security and trust:
  - Application of Trust management concepts in Security, e.g.:
    - trust-based service provisioning,
      - trust-based routing, …
    - trust-based access control,
    - exploiting trust and reputation information as anomaly detection mechanism
    - Security flaws reporting by users
    - …
  - Application of Security concepts in Trust management, e.g:
    - secure and reliable trust/reputation/recommendation mechanism (fully decentralized systems)
    - privacy issues in trust negotiation,
    - Monitoring contractual behaviour
    - …

Some approaches in secure software engineering

- Security mechanisms
- Design principles available
- Standards for sofware certification
- Vulnerabilities reduction techniques
- Static code analyis
- Penetration tests adopted
- Secure mantainance and configuration
- Security metrics (not yet satisfactory)
- Integration of security requirements in secure software engineering (e.g., Secure UML)
- Model-based Design
  - Model checking, model refinement, model based testing
- Language based security
  - Type systems, …
- Run-time support
  - Run time monitoring
- Policy-based system management
- Design-by-contract (a.k.a security-by-contract)
- …

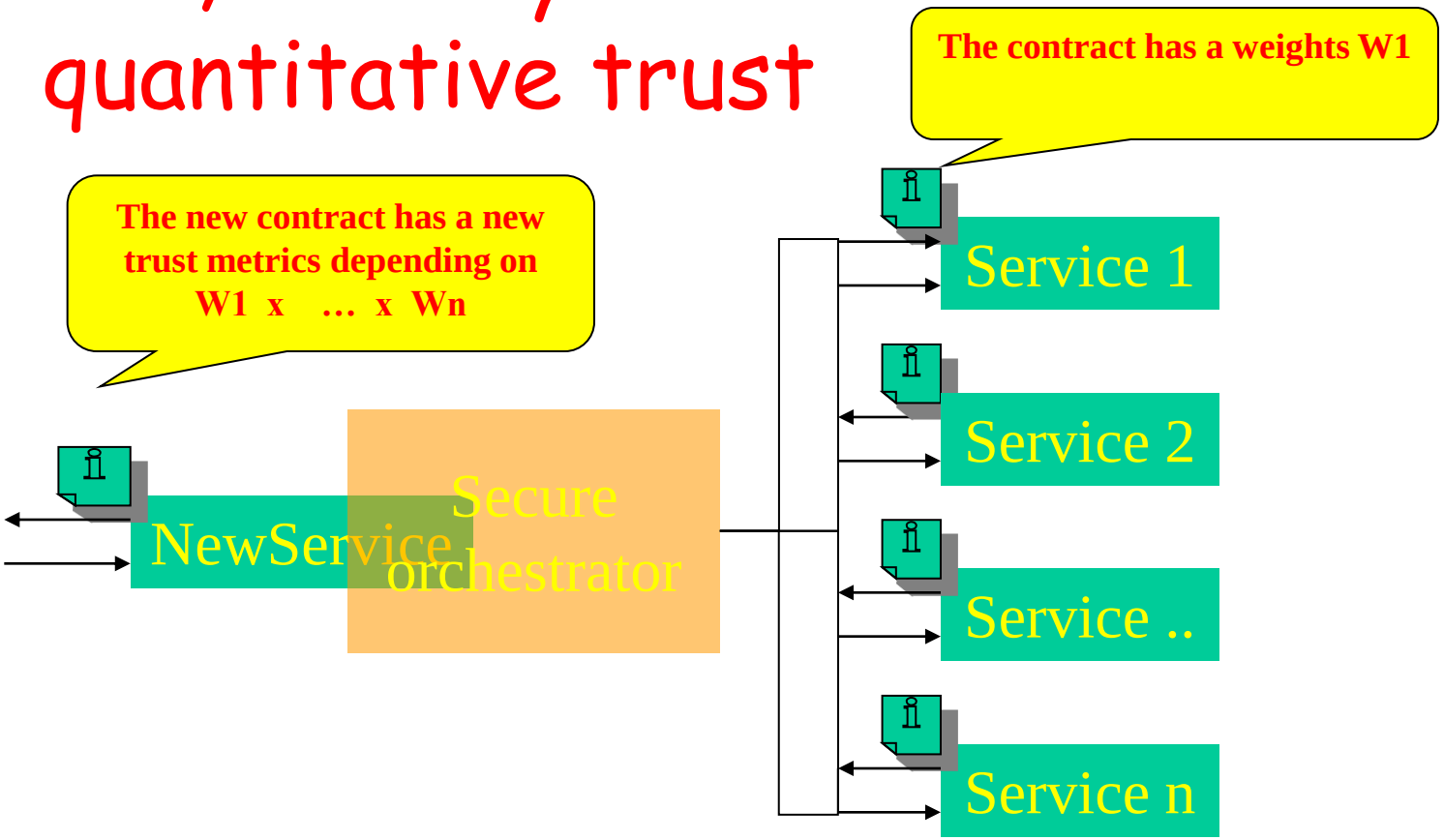
Towards assurance

- Assurance needs to ability to rigorously prove that a software meets its security requirements:
  - The proof could be also conducted by others, still with similar results
- However, you cannot be always in the position to control everything necessarily for the performing the proof:
  - There are intrinsic theoretical limitations
  - There are limits in what you can know and able to use in the proof of assurance
- In reality, often you have to rely (trust) on others, considering on subjective statements rather than objective facts …

The user in the loop

- Some examples of user perspective:
  - Needs for assurance / certification for software to increase user confidence and adoption on software/services
  - Active role on receiving trust information and produce trust information
    - E.g. reputation systems for mobile application market
  - Need for perceiving trustworthiness on software
    - Consider the iPhone "Kill Switch" or location tracking issues on the media
      - Much of the criticisms are from the lack of declaration of the existence of such control mechanism
  - …

An example: Secure service composition ,security contracts and quantitative trust



Topics/issues of interest?

- No specific order:
  - Models for trust formation, evolution, delegation, dissolution
  - Social models of trust
  - Trust models for secure software/service composition
  - **Certification models for software (producers, vendors, testers, etc.)**
  - Integrated assurance/trust techniques
  - Security level prediction of software based on recommendations
  - Trust models for application market
  - Usability of trust and security metrics
  - Empirical studies relating trust perception and trustworthiness
  - User perception of software trustworthiness
  - Role of *trusted* computing for secure software
    - Btw, trusted by whom?
  - …
  - …

Possible cooperation with

- EU projects:

- International WGs:
  - Security and Trust Management WG of the European Research Consortium in Informatics and Mathematics (ERCIM)
  - IFIP WG on Trust management
  - …