Trust management in secure software

BIC Discussion Paper **22-June-2012**

Fabio Martinelli[1]

1 National Research Council of Italy, Italy

This project is supported within the portfolio of the European Commission's DG-CNECT Unit H.4, Trust and Security, and has received funding by European Commission's Seventh Framework ICT Programme under grant number 25258655 for the period January 2011 to December 2013.

Introduction

The scale of the emerging global infrastructure, combined with the need for fully autonomous operation, surpass the usefulness of existing security infrastructures such as authorization services, certificate issuance and validation services. Having a certified identity (maybe granted using sloppy/undocumented procedures) in a dynamic and open environment does not *a priori* guarantee an acceptable behaviour and performance of software and services.

In particular, it is not enough for informed decisions on access restrictions and control, the selection among potential candidates for interaction. Entities need to be distinguished not only based on their static (certified) identities but also based on their (un)expected, dynamically varying qualities that are relevant to the specific interaction context. Decisions are often based on directly verifiable evidence, but in a highly open system could be also based on indirect evidence reported by other entities. In these cases, the notion of trust becomes central.

Trust

Trust is a very general and wide-ranging concept, with different meanings in different communities and contexts. Usually, trust is concerned with several dimensions: We can trust a system for correctly functioning (system trust), we can trust a *persona* to act in our behalf (delegation trust), etc. In general, we trust something/someone for a purpose in a given context or environment, and such interpretation is often used in computer science where several trust management models have been developed (initially for modelling access control issues, and more recently to model relationships in social computing). Indeed, in modern pervasive ICT systems, trust is a first-class object that need to be evaluated, analyzed, used, negotiated.

Trust may therefore be based on several features:

- verifiable evidence: e.g. ,proof methods, rigorous design & analysis techniques, …
- direct experience: e.g., previous interaction history (monitoring the target entity behaviour is a main tool …)
- indirect experience: e.g., third party recommendation (then you need to trust someone to recommend others and so on …)

These must be 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, etc.

Trust is also used when we certify software. Basically, we trust a third party to assess properties of software installations produced by another party. In addition, trust management aspects are necessary in usual Service Level Agreements (SLA) in service oriented architectures/infrastructures and in particular for secure service composition. Indeed, several stakeholders with different trust levels are involved in a typical service composition and a variety of potentially harmful content/service sources. This is attractive in terms of degrees of freedom in the creation of service offerings and businesses. Yet this also creates more vulnerabilities and risks as the number of trust domains in an application gets multiplied, the size of attack surfaces grows and so does the number of threats. Furthermore, the Future Internet will be an intrinsically dynamic and evolving paradigm where, for instance, end users are more and more empowered and therefore decide (often on the spot) on how content and services are shared and composed. This adds an extra level of complexity, as both risks and assumptions are hard to anticipate.

Research challenges

There are several technical areas that need further development in the trustworthy ICT research community (in no specific priority 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 information/metrics
- Empirical studies relating trust perception and trustworthiness
- User perception of software trustworthiness
- Role of trusted computing for secure software
- And, BTW, trusted by whom?

International cooperation aspects

From an international cooperation perspective, we can highlight:

- Commonly agreed trust models for service interaction;
- The standardization of the software and service certification process, including the necessary interoperability and automation information;
- The standardization of interoperable Service Level Agreeements (SLAs) among services;
- From a policy based perspective, there is clearly the need to define certification standards with which high-level assurance services need to conform in several scenarios and fields of application.

Recommendations

Because of the global nature of ICT, and hence the trust and security challenges, the overall interpretation of, and dependence on *trust* – what do we mean by …? – must be developed in this international environment.

To be effective, the search for, and development of general solutions is only going to be meaningful if addressed across national and regional boundaries.

About the Author

Fabio Martinelli is a senior researcher in the security group at Security Group at the Istituto di Informatica e Telematica - IIT; National Research Council - C.N.R. He is the Project Coordinator of the EU Project NESSoS Network of Excellence on Engineering Secure Future Internet Software Services and Systems and responsible for the CNR Interdipartimental Security Project.