Chapter 14

Security, Privacy and Trust

Federico Bergenti

14.1 Introduction

The literature about trust in multiagent systems collects a huge number of works that analyse almost any facets of this concept from nearly every point of view. Nevertheless, an accepted and stable formal model of trust in agent societies is still missing. In this chapter, we address this remarkable flaw of the current research by reporting the main contributions of the CASCOM project on this topic: (i) a stochastic model of trust that measurably captures trust in two-party interactions, and (ii) a general-purpose framework that the CASCOM platform provides to enable the realization of secure, privacy-aware and trust-aware multiagent systems.

Interaction is a key feature of agenthood (“the” key feature, we may say) and secure, trusted and privacy-aware interactions are what we truly want from real-world multiagent systems. While it is easy to identify a minimum set of requirements capable of providing guarantees for security in multi-party interactions, e.g., authorization and authentication, we are not yet ready to identify similar requirements for trusted and privacy-aware interactions.

The work done in the CASCOM project on these problems is along the lines of the research that is trying to identify a set of abstractions and mechanisms to guarantee trust- and privacy-awareness in multi-agent interactions. In particular, the final objective of our work is about providing the CASCOM platforms with a set of facilities to allow developers to easily and intuitively create not only secure but also privacy- and trust-aware multiagent systems. In order to achieve our goal, we developed a stochastic model of trust capable of formally showing that interactions mediated by a trusted third party, that we call guarantor, are rationally convenient over direct interactions. This result ensures that privacy- and trust-awareness can be obtained by mediated interactions and it provides a solid base for the design of the framework for privacy and trust awareness that we integrated in the CASCOM platform.
This chapter is organized as follows: next section frames the problem that we address in order to focus on the ideas and the abstractions behind our stochastic model. Section 14.3 provides the foundations of our model and it quantifies the increment of the utility that agents perceive because of the mediation of a guarantor. Then, Section 14.4 deals with the decision-making strategies of rational agents and it shows a worst-case specialization of our model that justifies why agents are more likely to choose guarantor-mediated over direct interactions. Section 14.5 reports on how our stochastic model is concretized into the CASCOM platform by means of a framework that facilitates the realization of trust- and privacy-aware multiagent systems. This framework relies on secure messaging within the CASCOM platform and Section 14.5 also gives some technical details on this. Finally, Section 14.6 summarizes the lessons learned from this work.

### 14.2 Two-Party Interactions

Most of the work reported in this chapter is about the study of the interaction between two agents only, $X$ and $Y$. This study is very generic and its results can be applied in many situations. In any case, we needed to focus our work on a special case of general interest in order to devise a formal framework for our study. This is the reason why we take the assumption that, from the point of view of security, trust and privacy, we can always reduce any two-party interaction to the special case of two agents mutually signing a contract. With no loss of generality, from now on we will always refer to the joint act of signing a contract as a means to study any other form of two-party interaction.

Having said this, we can state our working scenario as follows: $X$ is interested in signing a contract with $Y$ and it is in the process of deciding whether to do it directly or through the mediation of a trusted third party, the guarantor $G$, that can act as a middleman for transactions. We take a rational standpoint and we assume that $X$ discriminates between direct and mediated interaction on the basis of its utility function. Moreover, we assume incomplete information and we say that $X$ cannot take a fully-informed decision; rather, it has to face some risks.

This scenario models some interesting properties of real-world interactions and it provides a sufficiently simple case to allow for a formal analysis. Moreover, we believe that many interactions that are possibly occurring in nowadays multiagent systems can be approximated with acceptable accuracy to a network of two-party interactions. The comprehensive study of scenarios involving many jointly interacting agents is still in progress and it is subject of a future work.

The two-party scenario that we use to define our stochastic model of trust relies on an underlying assumption that is worth some discussion. In particular, we always assume that agents exchange the terms of the contract under negotiation using individuals of a known and shared ontology, which is described in some known and shared logic formalism, e.g., OWL [14]. This assumption allows agents to manage the information contained in the contract in a friendly way and to