Chapter XXIX
Trust Management and Context-Driven Access Control

Paolo Bellavista
University of Bologna, Italy

Rebecca Montanari
University of Bologna, Italy

Daniela Tibaldi
University of Bologna, Italy

Alessandra Toninelli
University of Bologna, Italy

ABSTRACT

The increasing diffusion of wireless portable devices and the emergence of mobile ad hoc networks promote anytime and anywhere opportunistic resource sharing. However, the fear of exposure to risky interactions is currently limiting the widespread uptake of ad hoc collaborations. This chapter introduces the challenge of identifying and validating novel security models/systems for securing ad hoc collaborations, by taking into account the high unpredictability, heterogeneity, and dynamicity of envisioned wireless environments. We claim that the concept of trust management should become a primary engineering design principle, to associate with the subsequent trust refinement into effective authorization policies, thus calling for original and innovative access control models. The chapter overviews the state-of-the-art solutions for trust management and access control in wireless environments by pointing out both the need for their tight integration and the related emerging design guidelines, that is, exploitation of context awareness and adoption of semantic technologies.

INTRODUCTION

Wireless telecommunication systems and the Internet are converging towards an integrated distributed environment that permits users to access/share services and to collaborate anytime and anywhere even when they are on the move. The increasing diffusion of portable devices with wireless connectivity and the emergence of mobile ad hoc networks (MANET) further promote opportunistic and temporary resource sharing by enabling mobile users in physical proximity of each other to spontaneously form ad hoc communities without the need to rely on the availability of a fixed network infrastructure. Mobile file sharing, mobile e-campus, emergency response, and vehicle coordination are just few collaborative application examples that illustrate the novel opportunities leveraged by envisioned and converged wired-wireless networks of the future. Hereinafter we will indicate this integrated network computing scenario formed by fixed Internet hosts, wireless terminals and wireless access points in between, as well as by collections of wireless mobile hosts forming MANET without the aid of any established fixed infrastructure, with the comprehensive term of *wireless Internet*.

However, the fear of exposure to risky interactions (possibly compromising confidentiality, availability, and integrity of both data and services) is currently limiting the widespread uptake of anywhere and anytime collaboration. To some extent, the above risk is present in any traditional distributed collaborative setting, but the wireless Internet exacerbates the perception of that risk because of the complex security challenges arising from the increased degree of openness and dynamicity of the scenario. Collaborating participants often cannot be statically preidentified; they usually change frequently due to high mobility and/or occasional failures, forming continuously varying ad hoc coalitions with entities entering and leaving groups dynamically. At the same time, roaming participants are often interested in establishing opportunistic collaborations with dynamically discovered partners, without having previous knowledge or long-term pre-established relationships with them. One of the most difficult security challenge in these environments is how to decide who to trust in the plethora of opportunistically discovered entities. In addition, MANET introduce a further level of complexity to secure collaborative applications: differently from traditional fixed networks where dedicated nodes support basic networking functions, for example, routing, in MANET these functions are carried out by available peers in the network, and there is no reason to assume that these peers will all cooperate uniformly. For instance, because network operations consume energy, some nodes may exhibit a selfish behavior and deny their cooperation, thus leading to severe degradation of network performance and functioning.

To protect and/or provide incentives for anywhere and anytime collaborations, there is the need for appropriate security models/systems that should follow novel design guidelines to take into account the high unpredictability, heterogeneity, and dynamicity of wireless Internet environments. In those scenarios where identities/roles of collaborating entities are difficult to be a-priori established, we claim that the concept of trust should become a primary design principle for the engineering of secure collaborative applications (Cahill, Gray, Seigneur, Jensen, Yong, Shand, *et al.*, 2003; Capra, 2004; Kagal, Finin, Joshi, 2001; Ruohomaa & Kutvonen, 2005). Trust provides a means to reduce the exposure to risky transactions in unfamiliar environments with no possibility to offer absolute protection against potential dangers. Trust solutions allow entities to decide whether to accept or refuse the dangers presumably associated with interactions with other entities. How to access resources and to whom to grant permissions should depend on the trust degree that collaborating entities mutually have.

Using trust as the basis to support secure ad hoc collaborations requires the design of novel trust management frameworks that enable entities to form, maintain, and evolve trust opinions in highly dynamic wireless environments. In fact, the wireless Internet deployment scenario poses complex issues to trust management and requires rethinking traditional solutions based