Chapter VI

Two-Layer Models for Managing Distributed Authenticity and Trust

Rolf Haenni, University of Berne & Berne University of Applied Sciences, Switzerland

Jacek Jonczy, University of Berne, Switzerland

Reto Kohlas, University of Berne, Switzerland

Abstract

This chapter describes the difficulty of managing authenticity and trust in large open networks. Participants of such networks are usually unknown to each other. Questioning somebody’s authenticity and trustworthiness is thus a natural reflex and an important security prerequisite. The resulting problem of properly managing authenticity and trust is an emerging research topic. The chapter proposes a common conceptual framework and compares it to several existing authenticity and trust models. The goal is to increase the awareness that authenticity and trust are not separable and to promote the corresponding two-layer requirement.
Introduction

The past few years have seen a remarkable growth of computer networks. This development is driven by many new groundbreaking applications such as electronic mail, online auctions, peer-to-peer file sharing, electronic commerce, VoIP phoning, online banking, electronic voting, virtual discussion groups, chat rooms, online dating, and many more. Most of these applications run on open networks, most notably on the Internet or on corresponding subnetworks thereof. These networks are mostly characterized by a large and dynamic group of geographically widespread participants, who often stay anonymous or use pseudonyms or nicknames. The large size and the anonymity of such networks imply that most participants do not know each other in person. This is a fundamental source of many severe security problems, and it raises the important question of trust relative to a potential communication partner. In the context of open networks and with respect to an unknown network participant $X$, trust has at least two facets:

- **Identity trust**: Is $X$ the person (s)he claims to be?
- **Reliability trust**: Will $X$ be a reliable service provider, business partner, customer, etc.?

Identity trust is particularly important if the transmitted information is confidential, for example in electronic mails. Confidentiality is usually achieved by means of cryptographic techniques such as public-key encryption, but it is only guaranteed as long as authentic public keys are used. The problem of establishing identity trust is thus closely related to the problem of public-key authentication. In this chapter, we will refer to it as the *authenticity problem*. Authentic public keys are also a prerequisite for achieving data integrity by means of digital signatures.

Reliability trust is not primarily related to the transmitted information between two network participants, but rather to the commercial or interpersonal transaction that comes afterwards. The winner of an online auction, for example, is interested in promptly receiving the auctioned item from the seller. His primary concern is the quality of the service offered; the seller’s identity is secondary. The seller has a similar view, as the main concern is receiving a prompt payment, independently of the buyer’s identity. These views are typical for most electronic commerce relationships between a seller and a buyer. Similar views have the users of peer-to-peer networks, where not revealing the identity (i.e. to stay anonymous) is even a desirable property. In this chapter, reliable network participants will be called *trustworthy*, and the problem of judging somebody’s trustworthiness is simply the *trust problem*.

Network participants, who know each other in person or from dealing with each other in the past, may have a direct basis to judge themselves authentic and/or trustworthy. This is what we call *direct authenticity* and *direct trust*, respectively, which is based on their first-hand experience. In general, that is, between unknown network participants without mutual first-hand experience, the only way to establish authenticity and trust is by means of direct statements from third parties. The most prominent examples of such third-party statements are *certificates*, *recommendations*, and *ratings*. A certificate approves the authenticity of somebody’s public key. Recommendations and ratings are similar, but they usually refer to
Related Content

Evaluating the Effects of Service Quality, Customer Satisfaction, and Service Value on Behavioral Intentions with Life Insurance Customers in India

A Novel QoS-Based Framework for Cloud Computing Service Provider Selection
www.igi-global.com/article/a-novel-qos-based-framework-for-cloud-computing-service-provider-selection/113807?camid=4v1a

On the use of the Hybrid Cloud Computing Paradigm
www.igi-global.com/chapter/use-hybrid-cloud-computing-paradigm/66234?camid=4v1a
E-Government Service Research Development: A Literature Review
www.igi-global.com/article/e-government-service-research-development/120724?camid=4v1a