Chapter XXVI
Trust Models for Ubiquitous Mobile Systems

Mike Burmester
Florida State University, USA

ABSTRACT

This chapter introduces the notion of trust as a means to establish security in ubiquitous mobile network systems. It argues that trust is an essential requirement to enable security in any open network environments, and in particular, in wireless ad hoc environments where there is no network topology. In such environments, communication can only be achieved via routes that have to be trusted. In general it may be hard, or even impossible, to establish, recall, and maintain trust relationships. It is therefore important to understand the limitations of such environments and to find mechanisms that may support trust either explicitly or implicitly. We consider several models that can be used to enable trust in such environments, based on economic, insurance, information flow, and evolutionary paradigms.

INTRODUCTION

Wireless mobile networks are a paradigm for mobile communication in which wireless nodes do not rely on any underlying static network infrastructure for services such as packet routing, name resolution, node authentication, or distribution of computational resources. The communication medium is broadcast. Nodes in range communicate in a direct peer-to-peer manner, while nodes out of range establish routing paths dynamically through other nodes where possible. The recent rise in popularity of mobile wireless devices and technological developments have made possible the deployment of wireless mobile networks for several applications. Examples include emergency deployments, disaster recovery, search-and-rescue missions, sensor networks, military (battlefield) operations, and more recently e-commerce. Since

the network nodes are mobile, the network topology frequently changes: Communication links are established or broken as nodes move in and out of range, and the network may get partitioned with the connectivity restricted to the partitions. As a result it may be much harder (or even impossible) to establish trust associations.

The trend in trust management is to view trust implicitly through delegation of privilege via certificates. Certificates can be chain-linked (linking à priori trust relationships) and used to propagate and distribute trust over insecure media, without the danger of being manipulated.

In this chapter, we give an overview of several models that can be used to support trust in mobile networks, based on economic, insurance, information flow, and evolutionary paradigms.

TRUST IN WIRELESS MOBILE NETWORKS

We consider environments in which there may be no fixed underlying network infrastructure, such as static base stations, for services such as packet routing, name resolution, node authentication, or the distribution of computational resources. In such environments, recalling and maintaining trust relationships is particularly challenging. Mobile systems share many of the complexities of fixed infrastructure systems. For example, nodes may have (Burmester & Yasinsac, 2004):

1. No prior relationship or common peers
2. No shared proprietary software
3. Different transmission, memory and processing capabilities
4. Different mobility characteristics
5. Different lifetime properties

Defining Trust

Trust is a highly abstract concept and it is unlikely that any simple definition can comprehensively capture all the subtleties of its essence. Informally we may define trust as a behavioral expectation of one party toward another. There are two perspectives in this definition, one in which a party *awards* trust to another (Alice trusts that Bob's public key is PK(Bob)), the other in which a party *gains* trust from another (Alice has convinced Bob that her public key is PK(Alice)).

Representing Trust: Certificates vs. Tokens

In any stateful trust model, trust must be represented by some type of persistent structure. Certificates are the de facto standard for representing trust relationships that are protected by cryptography. Certificates are portable and bind a cryptographic key (a digital string) to an entity, thus guaranteeing the authenticity of actions performed by that entity. Trust tokens are another structure that can be used to represent trust in a more direct way, analogous to the relation between checks and cash. Checks guarantee payment by tying the purchaser to some identifying information (like a certificate), while the value of cash is self-contained.

Trusted Third Parties

A trusted third party (TTP) can facilitate significantly the establishment of trust in mobile environments. For example, if two parties A and B who do not know each other have a trust relationship with a third party T, then T can be an effective intermediary for transactions between A and B.