Chapter XIV
Trustworthy Networks, Authentication, Privacy, and Security Models

Yacine Djemaiel
University of the 7th of November at Carthage, Tunisia

Slim Rekhis
University of the 7th of November at Carthage, Tunisia

Noureddine Boudriga
University of the 7th of November at Carthage, Tunisia

ABSTRACT

Wireless networks are gaining popularity that comes with the occurrence of several networking technologies raising from personal to wide area, from centralized to distributed, and from infrastructure-based to infrastructure-less. Wireless data link characteristics such as openness of transmission media, makes these networks vulnerable to a novel set of security attacks, despite those that they inherit from wired networks. In order to ensure the protection of mobile nodes that are interconnected using wireless protocols and standards, it is essential to provide a depth study of a set of mechanisms and security models. In this chapter, we present the research studies and proposed solutions related to the authentication, privacy, trust establishment, and management in wireless networks. Moreover, we introduce and discuss the major security models used in a wireless environment.

INTRODUCTION

Wireless networks are gaining popularity. Such popularity comes with the occurrence of several networking technologies raising from personal to wide area, from centralized to distributed, and from infrastructure-based to infrastructure-less. However wireless data link characteristics such as openness of transmission media, make these networks vulnerable to a novel set of security attacks. In order to protect such networks, multiple security solutions were proposed for the authenticating of users, ensuring privacy, and establishing trust. Deploying wireless networks without considering the threats associated to this technology may lead to the compromise of the interconnected resources and also the loss of security.

To ensure the protection of mobile nodes that are interconnected using wireless protocols, several security mechanisms and security models have

been provided. The solutions were made to cope with the features of the wireless environment and the mobile nodes. In this chapter, we present the research work and security solutions related to authentication, privacy, and trust management. Moreover, we introduce and discuss the major security models used in a wireless environment.

The first section of this chapter takes interest to the concept of trust, which can be defined as the firm belief in the competence of an entity to act dependably, securely and reliably within a specified context. Starting from this definition, it is significant that trust implies a level of uncertainty and judgment. This may depend on many factors due to risks associated to wireless networks. In this section, we define the trust in wireless context and discuss its models.

The second section discusses the authentication, which is a crucial mechanism that ensures that a resource is used by the appropriate entities. Actors, architecture, and issues related to authentication in wireless environment are discussed.

The third section discusses authentication models and protocols in wireless LAN (WLAN), cellular, ad hoc, wireless mobile access networks (WMAN) networks. As Mobile IP is becoming a unifying technology for wireless networks, allowing mobile nodes to change their point of attachment without loosing their connections, a particular interest is also given to authentication in Mobile IP.

The fourth section of this chapter discusses privacy regarding location and transaction in wireless environment. The fifth section presents two aspects regarding security modeling in wireless environments. The first is related to the specification of trust, modeling, and verification. The second addresses the specification and verification of security policies that take into consideration wireless threats.

TRUST MANAGEMENT

Trust management represents the skeleton of any network security framework. The absence of a centralized entity, for example, in ad hoc networks makes trust management a challenging problem to address.

Trust Establishment Basis

Trust describes a set of relations among entities engaged in various protocols, which are established based on a body of assurance evidence. A trust is established between two different entities further to the application of an evaluation metric to trust evidence. The established relations may be composed with other trust relations to generate new relations. Trust may influence decisions including access control. To clarify the process of trust establishment, we consider the following example. Assume two trust relations *A* and *B*. Relation *A* states that "*a certification authority CA1 accepts entity X's authentication evidences*" and is established off-line upon delivery of some evidences (e.g., identity, employment card) by X to B. Upon the establishment of A, the certification authority *CA1* issues a certificate binding a public key to X. Then, it stores the relation in its trust database registering X with its certificate. Relation *B* states that "*a certification authority CA2 accepts CA1's authentication of any entity registered by CA1*". To establish *B*, certification authority *CA2* may ask *CA1* to deliver some evidences such as: (1) *CA1*'s authentication of entities is done using satisfactory mechanism and policy; and (2) certification authority *CA1*'s trust database is protected using satisfactory security mechanisms and policies. The establishment of such trust relation leads to the publication of a certificate signed by *CA2*, associating *CA1*'s public key. The relation is then stored in *CA2*'s trust database. The composition of the two trust relations leads to the acceptance of *CA1*'s authentication of *X* by *CA2*.

One of the main properties that need to be handled during trust establishment techniques is transitivity. To decide whether a trust relation is transitive or not, evidences used to establish trust should ensure (1) availability, meaning that evidences can be evaluated at any time by the entities wishing to establish trust; (2) uniformity, meaning that evidences satisfy the same global metrics of adequacy, (3) stability, which means that authen-