PROSEARCH: A Protocol to Simplify Path Discovery in Critical Scenarios

Cristina Satizábal[1,2], Rafael Páez[1], and Jordi Forné[1]

[1] Telematics Engineering Department. Technical University of Catalonia
C/Jordi Girona 1-3, C3, 08034 - Barcelona (Spain)
{isabelcs,rpaez,jforne}@entel.upc.edu
[2] Engineering and Architecture Department. Pamplona University
Km 1 via a Bucaramanga, Pamplona (Colombia)

Abstract. Authentication is a strong requirement for critical information systems, and Public Key Infrastructure (PKI) is widely used to provide this service. Peer-to-peer PKIs are quite dynamic and certification paths can be built although part of the infrastructure is temporarily unreachable, which is quite common after disasters or network attacks. However, certification path discovery is one of the main drawbacks of peer-to-peer PKIs that strongly affects their scalability. We propose a protocol to build a virtual hierarchical PKI from a peer-to-peer PKI, since certification path construction in hierarchical PKIs is straightforward. Our protocol does not require to issue new certificates, facilitates the certification path discovery process and it is adaptable to the characteristics of users with limited processing and storage capacity. Results show that the execution time of this protocol is short in critical scenarios.

Keywords: Public Key Infrastructure (PKI), hierarchical trust model, peer-to-peer trust model, certification path discovery, critical information systems.

1 Introduction

As communication networks have increased their importance in our daily lives, our dependency upon their underlying infrastructure has grown too. Unfortunately, at the same time, hostile attacks on the infrastructure have increased in number and impact. Thus, networks become increasingly vulnerable and it is essential to guarantee the security of information which is considered of critical importance, from a political, economic, financial or social standpoint.

Secure connectivity is a requirement of communication networks in many critical scenarios. Some critical information systems require the rapid deployment of a secure connected network, in which each node has a path to every other node in the network and they can authenticate each other. Hierarchical Public Key Infrastructures (PKIs)[1] are widely used in distributed applications to provide the authentication service because are scalable and certification path construction is straightforward. Nevertheless, there are many situations where a static hierarchical PKI cannot operate, because part of the infrastructure is not available. On the other hand, peer-to-peer PKIs are quite dynamic and certification paths can be built although part of the

J. Lopez (Ed.): CRITIS 2006, LNCS 4347, pp. 151 – 165, 2006.

infrastructure is temporarily unreachable, which is quite common after disasters or network attacks. However, certification path discovery is difficult in peer-to-peer PKIs because there can be multiple certification paths between two entities and all the options do not lead to the target entity.

In this paper, we propose a protocol to establish a virtual hierarchy among the CAs of a peer-to-peer PKI called PROSEARCH (Protocol to Simplify the Certification Path Discovery Constructing a Hierarchy). Thus, we take advantage of the efficiency in the path discovery process offered by hierarchical architectures, where trust relationships are unidirectional and paths are easy to find. Using this protocol, nodes of critical information systems can find easy and rapidly the certification paths to the other nodes and in case that some node fails due to a disaster or attack, it is possible to establish a new hierarchy in a short time.

Unlike the previous works, our protocol does not require to generate new certificates to establish a hierarchy among the entities of the PKI. In addition, PROSEARCH sets a maximum certification path length to be adaptable to users with limited capacities.

This paper is divided into six sections. Section 2 gives the concept of certification path and the characteristics of peer-to-peer and hierarchical PKIs. Also, it explains the certification path discovery process and some solutions to increase its efficiency in decentralized architectures. In section 3, we describe how our protocol establishes a hierarchical architecture in a peer-to-peer PKI. Section 4 contains a practical example of PROSEACH in a critical scenario. In section 5, we show the obtained results in the simulation of our protocol. Finally, section 6 concludes.

2 Background

2.1 PKI Trust Models and Certification Paths

PKI uses Trust Third Parties (TTPs), known as Certification Authorities (CAs), to digitally sign data structures called Public Key Certificates (PKCs). A PKC binds a particular public key with the identity of a certain user. Thus, certificates, and the keys they contain, give the communicating parties information about the owner of the certificate and the entity that issued it.

Before trusting the content of a certificate, the user must check its signature. When the same CA issues the certificates of communicating parties, one can easily verify the signature of the other's certificate using the public key of this authority. However, to verify the signature of a certificate issued by another CA, it is necessary a continuous chain of trust points between the two parties. These chains of trust are called certification paths.

A *certification path* [2] is a chain of public key certificates through which a user can obtain the public key of another user. Paths are traced from the trusted CA of the verifier to the target entity's certificate. Therefore, the certification path length is equal to the number of CAs in the path plus one: a certificate for each CA and the target entity's certificate.

Certification architectures or trust models describe how the trust relationships among the entities of a PKI and the necessary rules to find and to cross the certification