Available online at www.sciencedirect.com
ScienceDirect
Computers and Electrical Engineering 34 (2008) 173–191
Computers and Electrical Engineering
www.elsevier.com/locate/compeleceng

Secure overlay networks for federated service provision and management

Gregorio Martínez Pérez *, Félix J. García Clemente, Manuel Gil Pérez, Antonio F. Gómez Skarmeta

Departamento de Ingeniería de la Información y las Comunicaciones, University of Murcia, Campus de Espinardo, s/n 30.071 Murcia, Spain

Received 31 May 2006; received in revised form 1 February 2007; accepted 13 March 2007
Available online 8 June 2007

Abstract

This paper presents the components and formal information model enabling the dynamic creation and management of secure overlay networks. Special attention will be paid to the solution provided to two important open issues: the definition of a certificate path building and validation algorithm (to ease the trust establishment and negotiation processes) and the definition and negotiation of SLAs in inter-domain secure overlay scenarios. Given a set of already existing domains with certain trust relationships, each overlay network allows the secure sharing of some (or all) of its services. For this, the administrator of each administrative domain will define using a formal information model which services he wants to share with any other domain, and which ones is he expecting from these other domains. Time and other networking conditions can also be indicated allowing secure overlay networks to be dynamically and automatically established and managed.

Keywords: Secure overlay networks; Trust establishment and negotiation; Cross-certification; Federated services; Policy-based management; Service level agreement; Inter-domain security

1. Introduction

Overlay networks are virtual networks formed by a set of cooperating nodes that share an underlying physical network. They represent a flexible method for deploying distributed services without having to modify the underlying network protocols. Such deployment requires security and dynamicity to be really effective and useful in current communication systems.

However, the abstraction introduced by overlay networks usually entails a number of security problems. Most of them have been related to the fact that the additional layer of abstraction makes it more likely for certain attacks, such as man-in-the-middle and eavesdropping, especially when the overlay network is composed by systems belonging to different administrative domains.

* Corresponding author. Tel.: +34 968 367646; fax: +34 968 364151.
E-mail addresses: gregorio@dif.um.es (G. Martínez Pérez), fgarcia@dif.um.es (F.J. García Clemente), manuel@dif.um.es (M. Gil Pérez), skarmeta@dif.um.es (A.F. Gómez Skarmeta).

0045-7906/$ - see front matter
doi:10.1016/j.compeleceng.2007.03.001

Another challenge that needs to be faced by the overlay network approach is dynamicity, where the current use of automatic self-organizing methods and protocols seems to mitigate it, but just in part.

This paper, which results from a research work mainly intended to address these two issues, presents the architecture, protocols, middleware components, and formal information model enabling the dynamic creation and management of secure overlay networks (SON). It is based on technologies and concepts, such as public-key cryptography, peer-to-peer cross-certification, policy-based networking (PBN), and service level agreements (SLA).

1.1. Motivation

This research line was initially identified as an objective of the VPN Workshop Initiative [1], although work in this forum was finally reduced to design and develop an inter-domain secure military overlay network over a certain number of military and civil subnetworks. Each of these "low level" subnetworks (i.e., autonomous systems) was identified with one private network taking part of a "high level" secure military coalition network, thus providing one clear example of dynamic and secure overlay network as presented in [2].

However, this work was able to create and manage just one single dynamic secure overlay network, which presents serious limitations when trying to deploy federations of services in medium and large-scale scenarios. In fact, it was considered as a first step towards the final objective to identify and provide the elements required for developing and managing dynamic secure overlay networks. It provides "virtual" sets (also known as federations) of services with common requirements, and usually belonging to different networks or administrative domains.

As it was defined in this research, each secure overlay network may represent different kind of services regarding different criteria, such as the required level of access control (i.e., which users and/or services can access to them) or the requirements for managing them (i.e., who can manage and monitor these services and how).

One example of this is a federation of services belonging to a set of networks that can be accessed by everybody (e.g., Web portals and FTP servers), another federation of services existing in the same set of networks that can only be accessed by the intranet/extranet users (e.g., videoconferencing and VPNs), and a third federation of services that can only be accessed by network administrators (e.g., monitoring services and DNS servers for updating data operations). This example provides three different secure overlay networks grouping different services with common requirements (in this case access control requirements) and belonging to the same set of networks.

The same set of services from a different perspective could be grouped into different overlay networks. For example, regarding availability network administrators could define these other groups (i.e., federations): low level for the FTP servers and videoconferencing, medium level for the Web portals and VPNs, and high level for monitoring services and DNS servers.

Such secure overlays can also be used in scenarios where services should be kept private unless offered to users or services belonging to the same coalition of networks. This can be the case aforementioned of military and tactical environments. A set of services, from a given communication network, will only be offered to others belonging to the same coalition (helicopters, submarines, or troops, for example) in a particular location and time previously defined by the administrators of such networks [2].

This research has been mainly undertaken as part of the SEINIT (Security Expert INITiative) EU IST project. SEINIT [3] has among its objectives to define innovative security models to address the new issues of the pervasive computer world, being the proposed scenarios a clear example of them.

1.2. Issues under consideration

To create and manage this kind of secure overlay networks several issues were identified early during this research. Some of them are now presented together with their motivation and the main technologies and concepts used to address them. The first three ones are related with the provision of security and with the trust establishment and negotiation processes in overlay networks, whereas the other three are related with the dynamic creation and management of such secure overlay networks.