Multidomain Virtual Security Negotiation over the Session Initiation Protocol (SIP)

Daniel J. Martínez-Manzano, Gabriel López, and Antonio F. Gómez-Skarmeta

Department of Information and Communications Engineering
University of Murcia, Spain
{dani,gabilm,skarmeta}@dif.um.es

Abstract. When organizations need to exchange critical information they need to rely on dependable and resilient channels, which define a trusted overlay network over the underlying IP infrastructure. Today, secure information sharing in these scenarios has become a main concern for domain administrators. To solve this problem, current research initiatives are focused on the establishment of (usually static) trust relationships and security services among such organizations. This paper analyzes the usage of the standard Session Initiation Protocol (SIP) for performing a multidomain virtual negotiation, in order to dynamically protect the exchange of critical data from the security risks of the public networks. As an example of this proposal, a prototype is presented in the context of secure overlay networks. This prototype shows also the integration of the virtual negotiation process with a Policy Based Network Management infrastructure (PBNM), in order to provide the security policies required by each organization.

Keywords: Secure Information Sharing, Overlay, Virtual Negotiation, SIP.

1 Introduction

When two or more organizations need to share critical information over their communication networks, either protected information among companies or simple end user data, they need to rely on trusted channels able to offer properties such as confidentiality, integrity, information assurance, etc. These secure channels between organizations define a secure overlay network upon the physical communication infrastructure.

The concept of overlay network is associated with the definition of resilient and secure logical communication infrastructures deployed over an underlying physical network. Overlays are used to solve management and scalability problems in nowadays common services such as peer-to-peer [12] or multicast [16] networks, or even to deal with problems of dependability and resilience in communication networks [1]. Needless to say, security is a key issue in those scenarios. Several research works have been carried out to add security mechanisms to these infrastructures. For example, we can find works about how to protect routing protocols in peer-to-peer networks [3] or how to protect overlays from DDoS (Distributed

J. Lopez (Ed.): CRITIS 2006, LNCS 4347, pp. 249–261, 2006.

Denial of Service) attacks [10]. Other proposals try to define a generic security framework to protect any kind of high level services running in the overlay, such as [17].

However, the security requirements imposed by those solutions are often static, usually through the definition of either preconfigured secure tunnels between nodes, or access control mechanisms for reaching the infrastructure. The establishment of such a secure overlay network has to be maintained by each domain which is a part of it, which normally requires defining:

- The security requirements for protecting internal communications and services, that is, required levels of confidentiality, integrity, authentication, etc.
- How end users and internal devices will deal with these security requirements.
- How these security requirements will be mapped to specific security technologies.
- How those security requirements will be agreed among other organizations to provide interdomain secure communications.

This work does not try to answer all of the above questions, and it focuses on the last one. That is, we propose a virtual negotiation process able to allow organizations to agree on security requirements and technologies to be applied along the path between them. The starting point is a scenario where several domains want to communicate securely making use of preestablished security requirements, for example, by means of an off-line Service Level Agreement (SLA). Each security domain has its own mechanism to allow end users or systems to specify security levels such as *low*, *medium* or *high*, and has its own method to translate those levels into security parameters (for example, a *medium* security level could mean strong authentication but weak encryption).

This paper proposes a way to define a dynamic secure overlay network among such organizations by means of a negotiation protocol. The Session Initiation Protocol (SIP) will be used for this, allowing domains to agree on a common set of security requirements and technologies, which respects the internal policies of them all.

This paper is structured as follows: section 2 briefly describes the SIP protocol as the base protocol used in the virtual negotiation, and then section 3 presents the proposed design for it. Detailed implementation is described in section 4, including how the proposed protocol has been integrated with a Policy Based Network Management (PBNM) infrastructure. Section 5 presents some related work and finally section 6 gives some conclusions.

2 The SIP Protocol

SIP (Session Initiation Protocol, [6]) is an application-layer signaling protocol for creating, modifying, and terminating data sessions of whatever kind. SIP allows the participants to agree on session parameters, a feature which can be useful for conveying on compatible requirements resulting from the intersection of each peer's own requirements plus any other constraints that could be imposed administratively. SIP can also make use of entities called proxy servers,