Denial-of-Service, Address Ownership, and Early Authentication in the IPv6 World

Pekka Nikander

Ericsson Research
Pekka.Nikander@nomadiclab.com

Abstract. In the IPv6 world, the IP protocol itself, *i.e.*, IPv6, is used for a number of functions that currently fall beyond the scope of the IPv4 protocol. These functions include address configuration, neighbour detection, router discovery, and others. It is either suggested to or required that IPsec is used to secure these functions. Furthermore, IPsec is used to protect a number of functions that are considered dangerous in the IPv4 world, including mobility management and source routing. Now, the currently prominent method for creating IPsec Security Associations, the Internet Key Exchange (IKE) protocol, is both relatively heavy and requires that the underlying IP stacks are already fully functional, at least to the point that UDP may be used. As a result, the combination of the widened responsibility of IPsec and the relative heavy weight of IKE creates a vicious cycle that is a potential source of various denial-of-service attacks. Additionally, if we want to use IPsec to secure IPv6 autoconfiguration, a chicken-and-egg problem is created: fully configured IPsec is needed to configure IP, and fully configured IP is needed to configure IPsec. In this paper, we describe these problems in detail.

1 Introduction

In IPv6, security is assumed to be based on IPsec. First, IPsec is used to protect basic application traffic such as standard TCP connections and UDP packet flows. Second, IPsec may be used for protecting ICMPv6 messages [1], which are, among other things, used to configure the IPv6 stack during boot time [2]. Third, IPsec is required to be used to protect a number of message types that have various IP specific control functions. These message types include Mobile IPv6 Binding Updates and Binding Acknowledgements [3], the Routing Extension Header [1], the IPv6 Router Renumbering messages [4], and there will probably be more in the future. Since this paper *only* concerns IPv6, from here on the terms IP and ICMP are used to denote IPv6 [1] and ICMPv6 [5], unless explicitly otherwise noted.

As we show in this paper, this approach of using IP to secure IP has a number of potential security pitfalls. These problems are not necessarily exceptionally hard to solve, but their solving requires a crisp understanding of the situation. Unfortunately, based on the discussion at the IETF ipsec mailing list [6], many of the people currently involved in the IPv6 design and deployment have hard

B. Christianson et al. (Eds.): Security Protocols, LNCS 2467, pp. 12–21, 2002.

time to understand the scope and nature of these problems. In this paper, we attempt to analyse the specific nature of these problems, illustrating the underlying principles when appropriate.

To lay background for the forthcoming discussion, some understanding of the IPv6 and IPsec design is needed. We assume some familiarity with both IPsec and IPv6 from the reader, and do not discuss the technical differences between IPv4 and IPv6. On the other hand, we do illustrate the differences in the IP-internal signalling mechanisms, since they are one of the fundamental source so the security problems discussed.

In this paper, we aim to analyse a chicken-and-egg and the so called address ownership problems and propose a possible approach to alleviate them. Thus, the rest of this paper is organized as follows. First, in section 2, we discuss how the IPv6 architecture differs from IPv4 architecture, and how this, together with some already existing deficiencies, leads to a number of potential denial-of-service and authorization problems. Based on the analysis, in section 3, we outline a number of requirements for a potential protocol that could be used to alleviate the situation. In section 4 we define a number of building blocks that could be used to design such a protocol. Finally, section 5 includes a summary.

2 Security Problems in IPv6

In this section, we explain in detail an IP autoconfiguration *vs.* IPsec chicken-and-egg problem and the so called address "ownership" problem. When looking at these problems, our main focus on looking at potential denial-of-service attacks, and attacks based on improper assumptions and insufficient authorization. In sub-section 2.1, we look at the IPv6 autoconfiguration phase, discuss the chicken-and-egg problem, and also note some related phenomena. Sub-section 2.2 discusses the address "ownership" problem, mainly in the light of Mobile IPv6.

2.1 Autoconfiguration

The stateless autoconfiguration specification [2] defines a method of providing initial boot time configuration for any IP host. Since the autoconfiguration is based on solely local traffic, physical link security is often good enough to provide adequate security against potential DoS and other attacks. However, if we ever want to use stateless autoconfiguration in wireless networks, such as future ad hoc networks, some sort of security must be provided. The security measures can be either provided by some mechanism that is outside the scope of IP and autoconfiguration (*e.g.* through a layer 2 protocol), or the autoconfiguration mechanism can be enhanced to deal with the potential threats. In this paper, we focus on the latter approach.

In the basic stateless autoconfiguration process, a booting host sends a series of *Neighbor Solicitations* [9] to the local link. These messages contain a *tentative IP address* that the host would like to use at its link local IP address. If the