Network Working Group
Internet Draft
draft-keromytis-ike-id-00.txt

A. D. Keromytis
Columbia University
Bill Sommerfeld
Sun Microsystems

The "suggested ID" extension for IKE

Status of this Memo

Abstract

This document describes an extension to IKE Phase 1 exchanges that increases its usefulness in certain scenarios.

1. Introduction

In the IKE key negotiation protocol [RFC2409], the Responder in a Phase 1 exchange picks their Phase 1 identity based on the IP address of the remote host, the local IP address used in the negotiation, and the identity of the Initiator.

There are some circumstances where the Initiator wishes to establish a security association with a specific identity that the Responder has. For example, when IPsec [RFC2401] is used for protecting user-to-user traffic, it is desirable to inform the Responder's IKE daemon which Identity (and, by extension, authentication material) to use.

The proposed extension to IKE is to allow the Initiator to send a suggested Responder ID in the 5th message of main mode, along with the Initiator ID normally sent. The Responder should treat this as a hint; the Responder may return a different Phase 1 ID. The

Initiator should verify that the returned Phase 1 ID is the same as the suggested and, if not, whether the returned Phase 1 ID is acceptable. The suggested ID is included in all encryption and authentication operations; for the HASH computation, HASH_I is computed over both the Initiator's identity and the suggested Responder identity. Following the notation in [RFC2409]:

```
HASH_I = prf(SKEYID, g^xi | g^xr | CKY-I | CKY-R | SAi_b | IDii_b |
                     IDir_s )
```

where IDir_s is the "suggested" Responder ID.

2. Security Considerations

This documents discusses an extension to the IKE protocol that extends its functionality. The extension has no security implications: the Responder's identity is privacy-protected in the same way the Initiator's identity is.

3. IANA Considerations

No actions by IANA are required.

References:

[RFC2401] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

Authors' addresses:

Angelos D. Keromytis
Columbia University, CS Department
515 CS Building
1214 Amsterdam Avenue, Mailstop 0401
New York, New York 10027-7003

Phone: +1 212 939 7095
Email: angelos@cs.columbia.edu

Bill Sommerfeld
1 Network Drive, UBUR02-212
Burlington, MA 01803

Phone: +1 781 442 3458
Email: sommerfeld@eng.sun.com

Expiration and File Name

This draft expires in March 2002

Its file name is draft-keromytis-ike-id-00.txt