Network Working Group
Internet-Draft
Intended status: Informational
Expires: April 30, 2009

B. Patil
Nokia
C. Perkins
WiChorus
H. Tschofenig
Nokia Siemens Networks
October 27, 2008

Issues related to the design choice of IPsec for Mobile IPv6 security
draft-patil-mext-mip6issueswithipsec-00.txt

Status of this Memo

Abstract

Mobile IPv6 as specified in RFC3775 relies on IPsec for security. An IPsec SA between the mobile node and the home agent provides security for the mobility signaling. Use of IPsec for securing the data traffic between the mobile node and home agent is optional. This document analyses the implications of the design decision to mandate IPsec as the default security protocol for Mobile IPv6 and recommends revisiting this decision in view of the experience gained from implementation and adoption in other standards bodies.

Table of Contents

1. Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. Introduction

Mobile IPv6 as specified in RFC3775 [RFC3775] requires an IPsec security association between the mobile node (MN) and home agent (HA). The IPsec SA protects the mobility signaling messages between the MN and HA. The user data may be optionally protected by the IPsec SA but is not required.

The use of IPsec and IKE (v1 and v2) with Mobile IPv6 are specified in RFCs 3776 [RFC3776] and 4877 [RFC4877]. The Mobile IP and MIP6 working groups in the IETF chose to mandate IPsec as the default security protocol for Mobile IPv6 based on various criteria and discussions between the years 2000 and 2004. Implementation experience with Mobile IPv6 and the security variants with which it has been specified in some SDOs indicates a need to revisit the design choice for MIP6 signaling security.

This document discusses the issues and concerns with the use of IPsec for MIP6 security and proposes revisiting the security design for MIP6 protocol.

3. Terminology

This document refers to [RFC3775][RFC4877] for terminology.

4. Background

IP mobility support in IPv6 was considered to be an integral feature of the IPv6 stack based on the experience gained from developing mobility support for IPv4. The design of Mobile IPv6 was worked on by the Mobile IP WG in the late 90s and by the MIP6 WG until its publication as [RFC3775] in 2004.

IPsec was also intended to be a default component of the IPv6 stack and was the preferred protocol choice for use by any other IPv6 protocols that needed security. Rather than design security into every protocol feature the intent was to reuse a well-defined security protocol to meet security needs. Hence Mobile IPv6 has been designed with a direct dependency on IPsec.

The Mobile IPv6 specification [RFC3775] was published along with the companion specification "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents", [RFC3776]. The establishment of the IPsec SA between the MN and HA as per RFC 3776 is based on the use of IKE. The use of IKE in the context of Mobile IPv6 for IPsec SA establishment did not gain traction because of factors such as complexity of IKE and the IETF transitioning to IKEv2. The MIP6 WG completed the specification, Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture [RFC4877] in April 2007. This [RFC4877] is considered as the default security protocol solution for MIP6 and updates [RFC3776].

5. Problem Statement

Mobile IPv6 is encumbered by its reliance on IPsec from an implementation and deployment perspective. As a protocol solution for host based mobility, MIP6 can be simpler without the IPsec baggage. The issues with IPsec are even more exacerbated in the case of dual-stack MIP6 [DSMIP6].

IPsec SAs between the MN and HA are established either manually or by the use of IKEv2. Manual SA configuration is not a scalable solution and hence MIP6 hosts and Home agents rely on IKEv2 for establishing dynamically IPsec SAs. As a result MIP6 depends on the existence of IPsec and IKEv2 for successful operation.

The problem in summary for MIP6 is the dependence on IPsec and IKEv2 for operation.

6. Issues with the use of IPsec

This section captures several issues with the use of IPsec by MIP6.

(1) The design of Mobile IPv6 emphasized on the reuse of IPv6 features such as IPsec. IPsec for IPv4 was a bolt-on solution. With the increasing need for security, IPv6 designers chose to incorporate IPsec as a default feature. There existed an assumption in the MIP6 working group that every IPv6 host would have IPsec capability as a standard feature. While this is true in many host implementations today, the existence of IPsec in every IPv6 stack is not a given. Hence a host which needs to implement Mobile IPv6 must ensure that IPsec and IKEv2 are also available. As a result of this dependence, MIP6 is no longer a standalone host-based mobility protocol. A good example of a host based mobility protocol that works as a self-sufficient module is Mobile IPv4. The security associated with MIP4 signaling is integrated into the protocol itself. MIP4 has been successfully deployed on large scale in several networks.

(2) IPsec use in most hosts is generally for the purpose of VPN connectivity to enterprises. It has not evolved into a generic security protocol that can be used by Mobile IPv6 easily. While RFC4877 does specify the details which enable only the MIP6 signaling to be encapsulated with IPsec, the general method of IPsec usage has been such that all traffic between a host and the IPsec gateway is carried via the tunnel. Selective application of IPsec to protocols is not the norm. Use of IPsec with Mobile IPv6 requires configuration which in many cases is not easily done because of reasons such as enterprise environments preventing changing to IPsec policies or other.

(3) A MIP6 home agent is one end of the IPsec SA in a many-to-one relationship. A MIP6 HA may support a very large of mobile nodes which could number in the hundreds of thousands to millions. The ability to terminate a large number of IPsec SAs (millions) requires signifiant hardware and platform capability. The cost issues of such an HA are detrimental and hence act as a barrier to deployment.

(4) The implementation complexity of Mobile IPv6 is greatly increased because of the interaction with IPsec and IKEv2. A standalone MIP6 protocol is easier to implement and deploy (such as MIP4 [RFC3344]). The complexity of the protocol implementation is even more so in the case of [DSMIP6].

(5) IPsec and IKEv2 is not implemented in every IPv6 or dual stack host. Mobile IPv6 support on such devices is not an option. Many low-end cellular hosts have IP stacks. The need for IPsec and IKEv2 in these devices is not important whereas mobility support is needed in many cases. MIP6 without any dependencies on protocols for security is easier to implement and has wider applicability.

(6) [RFC4877] which specifies the use of IKEv2 and IPsec with Mobile IPv6 essentially results in a variant of IPsec which is specific to Mobile IP. Hence this results in added complexity to implementations.

(7) Mobile IPv6 needs to be capable of being deployed in situations where alternative security mechanisms are already well-understood by the network administration. It should be possible to enable Mobile IPv6 to work in situations where alternative security mechanisms already supply the necessary authentication and privacy.

(8) IPsec has been successfully applied to VPN and other infrastructure operations, but less so for general end-to-end applications. Thus, the granularity for selectors was originally not at all sufficient for Mobile IPv6.

(9) The way that the IPsec code sits in the usual kernel, and the access mechanisms for the SA database, are not very convenient for use by straightforward implementations of Mobile IPv6. Unusual calling sequences and parameter passing seems to be required on many platforms.

(10) In certain environments the use of IPsec and IKEv2 for establishing the SA is considered as an overhead. Bandwidth constrained links such as cellular networks and air interfaces which are in the licensed spectrum tend to be optimized for user traffic. MIP6 signaling with the IPsec overhead and the IKEv2 messages are viewed negatively. It is more acceptable to have signaling without IPsec encapsulation.

The issues listed above have been a cause for MIP6 not being implemented widely or adopted by other SDOs which are considering IP mobility solutions.

7. MIP6 evolution

In order to make the Mobile Ipv6 protocol a solution that is easy to implement and available in even low-end devices, it is necessary to simplify the protocol. The design or the security architecture for MIP6 needs to be revisited and a solution that does not rely on other components developed.

8. Security Considerations

This I-D discusses the security architecture of Mobile IPv6 which is based on IPsec. The dependency on IPsec for security of MIP6 signaling is a detriment to the protocol implementation and deployment. Hence the security architecture needs to be revisited.

The experience gained over the last few years indicates that IPsec cannot necessarily be used as a generic solution for security. The design choice made for MIP6 in the initial stages no longer are valid and is hampering the implementation and use.

9. IANA Considerations

This document does not have any information which requires IANA review.

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3775] Johnson, D., "Mobility Support in IPv6", RFC 3775, June 2004.

[RFC3776] Arkko, J., "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents", RFC 3776, June 2004.

[RFC4877] Devarapalli, V., "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture", RFC 4877, April 2007.

[DSMIP6] Soliman, H., Ed., "Mobile IPv6 Support for Dual Stack

Hosts and Routers",
draft-ietf-mext-nemo-v4traversal-05.txt, July 2008.

10.2. Informative References

[RFC3344] Perkins, C., "IP Mobility Support for IPv4", RFC 3344, August 2002.

Authors' Addresses

Basavaraj Patil
Nokia
6021 Connection Drive
Irving, TX 75039
USA

Email: basavaraj.patil@nokia.com

Charles Perkins
WiChorus
3590 N. 1st Street, Suite 300
San Jose, CA 95134
USA

Email: charliep@wichorus.com

Hannes Tschofenig
Nokia Siemens Networks
Linnoitustie 6
Espoo 02600
Finland

Phone: +358 (50) 4871445
Email: Hannes.Tschofenig@gmx.net
URI: http://www.tschofenig.priv.at

Full Copyright Statement

Intellectual Property