MIP6
Internet-Draft
Expires: August 13, 2004

J. Kempf
DoCoMo Communications Labs USA
J. Arkko
Ericsson

February 13, 2004

The Mobile IPv6 Bootstrapping Problem
draft-kempf-mip6-bootstrap-00.txt

Status of this Memo

Copyright Notice

Abstract

This document discusses the creation of a security association between a mobile node and a home agent that is previously unknown to it. This problem is called the bootstrapping problem. The document discusses several different usage scenarios, as well as related issues involving informing the mobile node of changes in the home network topology and mobility management service. Limitations of the base Mobile IPv6 protocol in dealing with the scenarios are outlined.

Table of Contents

1. Introduction

The bootstrapping problem for Mobile IPv6 [4, 5] is one of the issues the MIP6 WG is chartered to solve. The text in the charter says:

> "A bootstrap mechanism for setting up security associations between the mobile node and home agent that would enable easier deployment of Mobile IPv6. This bootstrap mechanism is intended to be used when the device is turned on the very first time and activates MIPv6. The WG should investigate and define the scope before solving the problem."

In addition to easier deployment, reasons for bootstrapping include the following:

- Resilience to network renumbering, provisioning of new home agents, and other network management operations.
- Increasing the efficiency of communications through the selection of an appropriate home agent.
- Load balancing.
- Hiding the topological location of the mobile node.

The current Mobile IPv6 procedure for establishing an IPsec security association between the Mobile Node and home agent requires either manual keying or IKEv1 [2]. With manual keying, the security associations have to be bound to specific home addresses and home agent addresses. With IKEv1, the mobile node needs to have a statically defined home address in order that the home agent can make an authorization decision and identify the credentials during the IKE Phase 1 ISAKMP exchange. In this document, we discuss why these constraints may be problematic in some deployment scenarios.

In addition, Mobile IPv6 defines mechanisms for dynamic home agent and home prefix discovery. While these mechanisms are not specifically related to security, changes in the home agent address and mobile node home address also imply changes in authorization information related to security policies. As a result, the discovery mechanisms might not be as easily deployed as would be desirable.

This document defines the bootstrap problem. In Section 2 we review the Mobile IPv6 mechanisms for configuration and security association establishment; bootstrapping issues related to addressing, infrastructure, and topology changes are discussed in Section 3. Some scenarios for possible use of a bootstrapping mechanism are outlined in Section 4. Finally, some conclusions are presented in

Section 5.

1.1 Requirements language

In this document, the key words "MAY", "MUST, "MUST NOT", "optional", "recommended", "SHOULD", and "SHOULD NOT", are to be interpreted as described in [1].

2. Mobile IPv6 Configuration

The Mobile IPv6 protocol needs no configuration or security set-up mechanisms for its route optimization functionality. However, it requires that mobile nodes and home agents have been assigned to each other via configuration.

All mobile node - home agent communications are protected by IPsec, as described in Section 5.1 of [4] and [5]. In order to protect messages exchanged between the mobile node and the home agent with IPsec, appropriate security policy database entries are needed. A mobile node must be prevented from using its security association to send a message on the behalf of another mobile node using the same home agent. This is achieved through the use of the security policy database, and via an authorization check in IKEv1 when dynamic keying is used.

Sections 10.6 and 11.4 of [4] describe the operation of a protocol by which an mobile node that is away from home can discover it's home agent and by which the home agent can push prefix changes to the mobile node. The protocol is an extension of ICMPv6.

Prefix information propagation is envisioned as a way for network renumbering events in the home network to be propagated to the mobile node so that the mobile node can form a new home address. Home agent discovery is envisioned as a way for the mobile node to find a home agent given the prefix of its home network. While not strictly involved in the mobile node - home agent IPsec security relation, this protocol is required for bootstrapping the mobile node - home agent connection.

3. Issues in Bootstrapping

3.1 Addressing

In this section, we discuss the problems caused by the currently tight binding to home addresses and home agent addresses.

3.1.1 Dynamic Home Address Assignment

Currently, the home agent uses the mobile node's home address for authorization. When manual keying is used, this happens through the security policy database, which specifies that a certain security association may only use a specific home address. When dynamic keying is used, the home agent ensures that the IKE Phase 1 identity is authorized to request security associations for the given home address. Mobile IPv6 uses IKEv1, which is unable to update the security policy database based on a dynamically assigned home address. As a result, static home address assignment is really the only home address configuration technique compatible with the current specification.

However, support for dynamic home address assignment would be desirable for the following reasons:

Prefix changes in the home network

The Mobile IPv6 specification contains support for a mobile node to autoconfigure a home address based on its discovery of prefix information on the home subnet [4].

DHCP-based address assignment

Some ISPs may want to use DHCPv6 from the home network to configure home addresses [7].

Addressing privacy

It may be desirable to establish randomly generated addresses as in RFC 3041 [3] and use them for a short period of time. Unfortunately, current protocols make it possible to use such addresses only from the visited network. As a result, these addresses can not be used for communications lasting longer than the attachment to a particular visited network.

Ease of deployment

In order to make deployment of Mobile IPv6 easy, it would be desirable to free users and administrators from the task of

allocating home addresses and specifying them in the security policy database.

3.1.2 Dynamic Home Agent Assignment

Currently, the address of the home agent is specified in the security policy database. Support for multiple home agents requires the configuration of multiple security policy database entries.

However, support for dynamic home agent assignment would be desirable for the following reasons:

Home agent discovery

The Mobile IPv6 specification contains support for a mobile node to autoconfigure a home agent address based on a discovery protocol [4].

Independent network management

An ISP may also want to dynamically assign home agents in different subnets, that is, not require that a roamed mobile node have a fixed home subnet.

Local home agents

The mobile node's home ISP may want to allow a local roaming partner ISP to assign a local home agent for the mobile node. This is useful both from the point of view of communications efficiency, and has also been mentioned as one approach to support location privacy.

Ease of deployment

ISP may want to allow "opportunistic" discovery and utilization of its mobility services without any prearranged contact. These scenarios will require dynamic home address assignment.

3.1.3 Management requirements

As described earlier, new addresses invalidate configured security policy databases and authorization tables. Regardless of the specific protocols used, there is a need for either an automatic system for updating the security policy entries, or manual configuration. These requirements apply to both home agents and mobile nodes, but it can not be expected that mobile node users are

capable of performing the required tasks.

3.2 Security Infrastructure

3.2.1 Integration with AAA Infrastructure

The current IKEv1-based dynamic key exchange protocol described in [5] has no integration with backend authentication, authorization and accounting techniques unless the authentication credentials and trust relationships use certificates.

Using certificates may require the ISP to deploy a PKI, which may not be possible or desirable in certain circumstances. Where a traditional AAA infrastructure is used, the home agent is not able to leverage authentication and authorization information established between the mobile node, the foreign AAA server, and the home AAA server when the mobile node gains access to the foreign network, in order to authenticate the mobile node's identity and determine if the mobile node is authorized for mobility service.

The lack of connection to the AAA infrastructure also means the home agent does not know where to issue accounting records at appropriate times during the mobile node's session, as determined by the business relationship between the home ISP and the mobile node's owner. Presumably, some backend AAA protocol between the home agent and home AAA could be utilized but IKEv1 does not contain support for exchanging the right kind of information, primarily the NAI [6], with the mobile node.

3.2.2 "Opportunistic" or "Local" Discovery

The home agent discovery protocol does not support "opportunistic" or local discovery mechanisms in a roaming partner's local access network. It is expected that the mobile node must know the prefix of the home subnet in order to be able to discover a home agent, it must either obtain that information through prefix update or have it statically configured. A more typical pattern for interdomain service discovery in the Internet is that the client (mobile node in this case) knows the domain name of the service, and uses DNS in some manner to find the server in the other domain. For local service discovery, DHCP is typically used.

3.3 Topology Change

3.3.1 Dormant Mode Mobile Nodes

The description of the protocol to push prefix information to mobile nodes in Section 10.6 has an implicit assumption that the mobile node

is active and taking IP traffic. In fact, many, if not most, mobile devices will be in a low power "dormant mode" to save battery power, or even switched off, so they will miss any propagation of prefix information. As a practical matter, if this protocol is used, an ISP will need to keep the old prefix around and handle any queries to the old home agent anycast address on the old subnet, whereby the mobile node asks for a new home agent as described in Section 11.4, until all mobile nodes are accounted for. Even then, since some mobile nodes are likely to be turned off for long periods, some owners would need to be contacted by other means, reducing the utility of the protocol.

3.3.2 Use of ICMP

Many ISPs now routinely block ICMP at firewalls as a blanket security measure, to remove the possibility of ping attacks, etc. Requiring them to pass the Mobile IPv6 prefix update and home agent discovery messages is likely to meet with a skeptical response.

While the ICMP messages associated with the prefix update are required to be sent within the mobile node - home agent IPsec security association, the home agent discovery message is sent to an anycast address. Securing anycast messages is, however, difficult with IPsec. As a result, at least some of the ICMP messages have to be processed in the clear. While the specific threats relating to the discovery of home agent addresses are not that significant, it is at least necessary for the ICMP messages to pass firewalls.

4. Bootstrapping Scenarios

In this section, we discuss four different scenarios involving bootstrapping.

The simplest bootstrapping scenario involves the creation of the security association "from thin air", i.e., without any pre-existing relationship. This could be achieved using, for instance, SSH-style leap-of-faith or other weak authentication mechanisms [9]. Unfortunately, as discussed in Section 6, some of the assumptions of the base Mobile IPv6 protocol rely on there being at least some administrative relationship between the mobile node and its home agent. As a result, either this approach should be ruled out, or the assumptions of the base protocol removed through extensions.

Another scenario involves turning an existing security association in the user's home network for a different purpose into a new security association suitable for protecting Mobile IPv6. For instance, an existing security association for a VPN service could be used to generate suitable Mobile IPv6 security associations, on a first-come-first-served home address basis.

The third scenario is similar to the second one, but utilizes a security association from one of the access networks to which the node is connected, if available, rather than from the home network. The network access security relationship is used in order to create a security association suitable for Mobile IPv6. For instance, when the mobile node boots and connects to the network for the first time, it could create a security association with the access operator's home agent. This home agent could then be used as the mobile node moves into a different position or even into a different access network.

The fourth scenario involves turning an existing security association with a home agent into a new one. For instance, the existing security association for one home address can be used to communicate changed addresses and home agents. Based on this the parties can modify their security policy entries and authorization tables.

5. Conclusions

The ability to bootstrap security associations for Mobile IPv6 is necessary for many purposes, and can be expected to have a significant impact on the speed with which the protocol can be deployed. New protocol mechanisms are required for this bootstrap to become possible, however, as the base Mobile IPv6 protocol does not accommodate for it.

We expect the bootstrapping mechanisms to focus on scenarios 2, 3, and 4 described in Section 4, i.e., bootstrapping based on an existing home network security association, network access security association, or the modification of an existing security association for Mobile IPv6.

The ability of the mobile node to dynamically locate a home agent impacts whether the mobile node can set up the IPsec security association, and the constraints on the ability of the mobile node to dynamically configure the IPsec security association also constrain how dynamic home agent location can be. The current mobile node - home agent IPsec SA bootstrapping procedure is constrained by the requirements of IKEv1 dynamic key exchange. These constraints, in turn, make dynamic home address assignment, dynamic home agent assignment, and proper integration with AAA infrastructure difficult. The IKEv2 design [8] is much less constrained in many of these areas, and may be a good candidate for a more flexible bootstrapping procedure.

The design intent of the prefix updating and home agent discovery protocols described in Sections 10.6 and 11.4 of [4] is to extend the same kind of subnet configuration service enjoyed by hosts and routers on a local subnet (address autoconfiguration, router discovery) to a remote mobile node, using a similar mechanism (home address autoconfiguration, home agent discovery). This basic subnet configuration mechanism is not well suited to a loose collection of perhaps millions of roaming mobile nodes. Some utilization of existing interdomain mechanisms for bootstrapping home network mobility service from a foreign domain and standard service configuration mechanisms for performing the same function within a roaming partner's network is more likely to be viable. On the other hand, IP layer mechanisms for bootstrapping Mobile IPv6 should not be bound to mechanisms specific to a particular type of access network technology, wireless technology, or ISP, in order to ease the use of the mechanism across many different kinds of access networks and ISPs.

6. Security Considerations

This document does not propose any new protocols, and therefore does not involve any security considerations in that sense. However, throughout this document there are discussions of problems with Mobile IPv6 involving the mobile node - home agent IPsec security association.

When considering different bootstrapping solutions, it is important to keep the security assumptions of the Mobile IPv6 protocol design in mind. In particular, the protocol relies on the home agent's operator to have an administrative relationship with the mobile node's user. Through this relationship, rogue mobile nodes can be tracked down. Completely automatic bootstrapping without any pre-existing relationship is thus out of the question, unless additional defenses (such as new care-of address verification) are built into the Mobile IPv6 protocol.

Normative References

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

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

[3] Narten, T. and R. Draves, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 3041, January 2001.

[4] Johnson, D., Perkins, C. and J. Arkko, "Mobility Support in IPv6", draft-ietf-mobileip-ipv6-24 (work in progress), July 2003.

[5] Arkko, J., Devarapalli, V. and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents", draft-ietf-mobileip-mipv6-ha-ipsec-06 (work in progress), July 2003.

Informative References

[6] Aboba, B. and M. Beadles, "The Network Access Identifier", RFC 2486, January 1999.

[7] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C. and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[8] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", draft-ietf-ipsec-ikev2-11 (work in progress), October 2003.

[9] Arkko, J. and P. Nikander, "How to Authenticate Unknown Principals without Trusted Parties", To appear in Proceedings of Security Protocols Workshop 2002, Cambridge, UK, April 2002.

[10] Montenegro, G., Patil, B., Arkko, J. and J. Kempf, "Thoughts on Bootstrapping Mobility Securely", Presentation in MIP6 WG in IETF-57, July 2003.

[11] Arkko, J. and C. Perkins, "Alternative (Future) Proposals for MIPv6 Security", Presentation in MIP6 WG in IETF-57, July 2003.

Authors' Addresses

James Kempf
DoCoMo Communications Labs USA
181 Metro Drive
San Jose, CA 94043
USA

EMail: kempf@docomolabs-usa.com

Jari Arkko
Ericsson

Jorvas 02420
Finland

EMail: jari.arkko@ericsson.com

Appendix A. Acknowledgements

The authors would like to thank Tom Hiller and Gabriel Montenegro for interesting discussions in this problem space. Part of this draft is based on ideas presented in [10] and [11].

Intellectual Property Statement

Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.