MIP6
Internet-Draft
Expires: July 6, 2006

A. Patel, Ed.
Cisco
G. Giaretta, Ed.
TILAB

January 2, 2006

Problem Statement for bootstrapping Mobile IPv6
draft-ietf-mip6-bootstrap-ps-04

Status of this Memo

Copyright Notice

Abstract

A mobile node needs at least the following information: a home address, home agent address and a security association with home agent to register with the home agent. The process of obtaining this information is called bootstrapping. This document discuss the issues involved with how the mobile node can be bootstrapped for Mobile IPv6 and various potential deployment scenarios for mobile node bootstrapping.

Table of Contents

1. Introduction

Mobile IPv6 [RFC3775] specifies mobility support based on the assumption that a mobile node has a trust relationship with an entity called the home agent. Once the home agent address has been learned (for example via manual configuration, anycast discovery mechanisms, or DNS lookup), Mobile IPv6 signaling messages between the mobile node and the home agent are secured with IPsec or with the authentication protocol as defined in [RFC4285]. The requirements for this security architecture are created with [RFC3775] and the details of this procedure are described in [RFC3776].

In [RFC3775] there is an implicit requirement that the MN be provisioned with enough information that will permit it to register successfully with its home agent. However, having this information statically provisioned creates practical deployment issues.

This document serves to define the problem of bootstrapping. Bootstrapping is defined as the process of obtaining enough information at the mobile node so that it can successfully register with an appropriate home agent.

The requirements for bootstrapping could consider various scenarios/ network deployment issues. It is the basic assumption of this document that certain minimal parameters (seed information) are available to the mobile node to aid in bootstrapping. The exact seed information available differs depending on the deployment scenario. This document describes various deployment scenarios and provides for a set of minimal parameters that are available in each deployment scenario.

This document stops short of suggesting the preferred solutions for how the mobile node should obtain information. Such details will be available from separate documents.

1.1. Overview of the Problem

Mobile IPv6 [RFC3775] expects the mobile node to have a static home address, home agent address (which can be derived from an anycast address) and a security association with a home agent (or multiple home agents).

This static provisioning of information has various problems as discussed in Section 5.

The aim of this draft is to:

- Define bootstrapping.
- Identify sample deployment scenarios where MIPv6 will be deployed, taking into account the relationship between the subscriber and the service provider.
- Identify the minimal set of information required on the Mobile Node and in the network in order for the mobile node to obtain address and security credentials, to register with the home agent.

1.2. What is Bootstrapping?

Bootstrapping is defined as obtaining enough information at the mobile node so that the mobile node can successfully register with an appropriate home agent. Specifically, this means obtaining the home agent address and home address, and for the mobile node and home agent to authenticate and mutually construct security credentials for Mobile IPv6.

Typically, bootstrapping happens when a mobile node does not have all the information it needs to setup the Mobile IPv6 service. This includes, but is not limited to, the mobile node (MN) not having any information when it boots up for the first time (out of the box), it does not retain any information during reboots, etc.

Also, in certain scenarios, after the MN bootstraps for the first time (out of the box), subsequent bootstrapping is implementation-dependent. For instance, the MN may bootstrap every time it boots, bootstrap everytime on prefix change, bootstrap periodically to anchor to an optimal (distance, load etc) HA, etc.

1.3. Terminology

General mobility terminology can be found in [RFC3753]. The following additional terms are used here:

Trust relationship

In the context of this draft, trust relationship means that two parties in question, typically the user of the mobile host and the mobility or access service authorizer , have some sort of prior contact in which the mobile node was provisioned with credentials. These credentials allow the mobile node to authenticate itself to the mobility or access service provider and to prove its authorization to obtain service.

Infrastructureless relationship

In the context of this draft, an infrastructureless relationship is one in which the user of the mobile node and the mobility or access service provider have no previous contact and the mobile node is not required to supply credentials to authenticate and prove authorization for service. Mobility and/or network access service is provided without any authentication or authorization. Infrastructureless in this context does not mean that there is no network infrastructure, such as would be the case for an ad-hoc network.

Credentials

Data used by a mobile node to authenticate itself to a mobility or access network service authorizer and prove authorization to receive service. User name/passwords, one time password cards, public/private key pairs with certificates, biometric information, etc. are some examples.

ASA

Access Service Authorizer. A network operator that authenticates a mobile node and establishes the mobile node's authorization to receive Internet service.

ASP

Access Service Provider. A network operator that provides direct IP packet forwarding to and from the end host.

Serving Network Access Provider

A network operator that is the mobile node's ASP but not its ASA. The serving network access provider may or may not additionally provide mobility service.

Home Network Access Provider

A network operator that is both the mobile node's ASP and ASA. The home network access provider may or may not additionally provide mobility service (note that this is a slighlty different definition from RFC 3775).

IASP

Integrated Access Service Provider. A service provider that provides both authorization for network access, and mobility service.

MSA

Mobility Service Authorizer. A service provider that authorizes Mobile IPv6 service.

MSP

Mobility Service Provider. A service provider that provides Mobile IPv6 service. In order to obtain such service, the mobile node must be authenticated and prove authorization to obtain the service.

Home Mobility Service Provider

A MSP that both provides mobility service and authorizes it.

Serving Mobility Service Provider

A MSP that provides mobility service but depends on another service provider to authorize it.

2. Assumptions

- A basic assumption in the Mobile IPv6 [RFC3775] is that there is a trust relationship between the mobile node and its home agent(s). This trust relationship can be direct, or indirect through, for instance, an ASP that has a contract with the MSP. This trust relationship can be used to bootstrap the MN.

  One typical way of verifying the trust relationship is using authentication, authorization, and accounting (AAA) infrastructure. In this document, two distinct uses of AAA are considered:

  AAA for Network Access

  This functionality provides authentication and authorization to access the network (obtain address and send/receive packets).

  AAA for Mobility Service

  This functionality provides authentication and authorization for mobility services.

  These functionalities may be implemented in a single entity or in different entities, depending on the service models described in Section 6 or deployment scenarios as described in Section 7.

- Yet another assumption is that some identifier, such as an NAI, as defined in [RFC4283] or [RFC2794] is provisioned on the MN which permits the MN to identify itself to the ASP and MSP.

3. Design Goals

A solution to the bootstrapping problem has the following design goals:

- The following information must be available at the end of bootstrapping, to enable the MN to register with the HA.
  - MN's home agent address
  - MN's home address
  - IPsec SA between MN and HA, IKE pre-shared secret between MN and HA, or shared secret/security association for authentication protocol [RFC4285]
- The bootstrapping procedure can be triggered at any time, either by the MN or by the network. Bootstrapping can occur, for instance due to administrative action, information going stale, HA indicating the MN etc. Bootstrapping may be initiated even when the MN is registered with the HA and has all the required credentials. This may typically happen to refresh/renew the credentials.
- Subsequent protocol interaction (for example updating the IPsec SA) can be executed between the MN and the HA itself without involving the infrastructure that was used during bootstrapping.
- Solutions to the bootstrapping problem should enable storage of user-specific information on entities other than the home agent.
- Solutions to the bootstrapping problem should not exclude storage of user-specific information on entities other than the home agent.
- Configuration information which is exchanged between the mobile node and the home agent needs to be secured using integrity and replay protection. Confidentiality protection should be provided if necessary.
- All feasible deployment scenarios, along with the relevant authentication/authorization models should be considered.

4. Non-Goals

This following issues are clearly outside the scope of bootstrapping:

- Home prefix renumbering is not explicity supported as part of bootstrapping. If the MN executes the bootstrap procedures everytime it powers-on (as opposed to caching state information from previous bootstrap process), then home network renumbering is taken care of automatically.

- Bootstrapping in the absence of a trust relationship between MN and any provider is not considered.

5. Motivation for bootstrapping

5.1. Addressing

The default bootstrapping described in the Mobile IPv6 base specification [RFC3775] has a tight binding to the home addresses and home agent addresses.

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

5.1.1. 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 be used for 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 base specification.

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

DHCP-based address assignment

Some providers may want to use DHCPv6 or other dynamic address assignment (e.g. IKEv2) from the home network to configure home addresses.

Recovery from a duplicate address collision

It may be necessary to recover from a collision of addresses on the home network by one of the mobile nodes changing its home address.

Addressing privacy

It may be desirable to establish randomly generated addresses as in [RFC3041] 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 simplify the deployment of Mobile IPv6, it is desirable to free users and administrators from the task of allocating home addresses and specifying them in the security policy database. This is consistent with the general IPv6 design goal of using autoconfiguration wherever possible.

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 [RFC3775]. Autoconfiguration in case of network renumbering is done by replacing the existing network prefix with the new network prefix.

Subsequently, the MN needs to update the mobility binding in the HA to register the newly configured Home Address. However, the MN may not be able to register the newly configured address with the HA if a security association related to that reconfigured Home Address does not exist in the MN and the HA. This situation is not handled in the current MIPv6 specification [RFC3775].

5.1.2. 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 [RFC3775].

Independent network management

An MSP may want to dynamically assign home agents in different subnets; for istance, not require that a roaming mobile node have a fixed home subnet.

Local home agents

The mobile node's MSP may want to allow the serving ASP 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

In order to simplify the deployment of Mobile IPv6, it is desirable to free users and administrators from the task of allocating home agent addresses in a static manner. Moreover, an MSP may want to have a dynamic home agent assignment mechanism to load balance users among home agents located on different links.

5.1.3. 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.

5.2. Security Infrastructure

5.2.1. Integration with AAA Infrastructure

The current IKEv1-based dynamic key exchange protocol described in [RFC3776] has no integration with backend authentication, authorization and accounting techniques unless the authentication credentials and trust relationships use certificates or pre-shared secrets.

Using certificates may require the MSP 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. This would be desirable 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 MSP 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 full AAA credentials with the mobile node. It is worthwhile to note that IKEv2 provides this feature.

5.2.2. "Opportunistic" or "Local" Discovery

The home agent discovery protocol does not support an "opportunistic" or local discovery mechanisms in an ASP'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 inter-domain service discovery in the Internet is that the client (mobile node in this case) knows the domain name of the service, and uses DNS to find the server in the visited domain. For local service discovery, DHCP is typically used.

5.3. Topology Change

5.3.1. Dormant Mode Mobile Nodes

The description of the protocol to push prefix information to mobile nodes in Section 10.6 in [RFC3775] 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 MSP 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.

Bootstrapping does not explicitly try to solve this problem of home network renumbering when MN is in dormant mode. If the MN can configure itself after it 'comes back on' by reinitiating the bootstrapping process, then network renumbering problem is fixed as a side-effect.

6. Network Access and Mobility services

This section defines some terms as it pertains to authentication and practical network deployment/roaming scenarios. This description lays the groundwork for Section 7. The focus is on the 'service' model since, ultimately, it is the provider providing the service that wants to authenticate the mobile (and vice-versa for mutual authentication between provider and the user of the service).

Network access service enables a host to send and receive IP packets on the Internet or an intranet. IP address configuration and IP packet forwarding capabilities are required to deliver this service. A network operator providing this service is called an access service provider (ASP). An ASP can, for example, be a commercial ASP, the IT department of an enterprise network, or the maintainer of a home (residential) network.

If the mobile node is not within the geographical area in which network access service is provided by its home ASP, the mobile node is roaming. In this case, the home ASP acts as the access service authorizer, but the actual network access is provided by the serving network access provider. During the authentication and authorization prior to the mobile node having Internet access, the serving network access provider may simply act as a routing agent for authentication and authorization back to the access service authorizer, or it may require an additional authentication and authorization step itself. An example of a roaming situation is when a business person is using a hotspot service in an airport, and the hotspot service provider has a roaming agreement with the business person's cellular provider. In that case, the hotspot network is acting as the serving network access provider, while the cellular network is acting as the access service authorizer. When the business person moves from the hotspot network to the cellular network, the cellular network is both the home access service provider and the access service authorizer.

Mobility service using Mobile IPv6 is conceptually and possibly also in practice separate from network access service, though of course network access is required prior to providing mobility. Mobile IPv6 service enables an IPv6 host to maintain its reachability despite changing its network attachment point (subnets). A network operator providing Mobile IPv6 service is called a mobility service provider (MSP). Granting Mobile IPv6 service requires a host to authenticate and prove authorization for the service. A network operator that authenticates a mobile node and authorizes mobility service is called a mobility service authorizer (MSA). If both types of operation are performed by the same operator, that operator is called a home mobility service provider. If authentication and authorization is provided by one operator and the actual service is provider by

another, the operator providing the service is called the serving mobility service provider. The serving MSP must contact the mobile node's mobility service authorizer to check the mobile node's authorization prior to granting mobility service.

The service model defined here clearly separates the entity providing the service from the entity that authenticates and authorizes the service. In the case of basic network access, this supports the traditional and well-known roaming model, in which inter-operator roaming agreements allow a host to obtain network access in areas where their home network access provider does not have coverage. In the case of mobility service, this allows a roaming mobile node to obtain mobility service in the local operator's network while having that service authorized by the home operator. The service model also allows mobility service and network access service to be provided by different entities. This allows a network operator with no wireless access, like, for example, an enterprise network operator, to deploy a Mobile IPv6 home agent for mobility service while the actual wireless network access is provided by the serving network access providers with which the enterprise operator has a contract. Here are some other possible combinations of ASPs and MSPs:

- The serving ASP might be the home ASP. Similarly, the serving MSP might be the home MSP.
- The home ASP and the home MSP may be the same operator, or not. When they are the same, the same set of credentials may be used for both services.
- The serving ASP and the serving MSP may be the same operator, or not.
- It is possible that serving ASP and home MSP are the same operator.

Similarly the home ASP and serving MSP may be the same. Also, the ASA and MSA may be the same.

These entities and all combinations that are reasonable from a deployment perspective must be taken into consideration when solving the Mobile IPv6 bootstraping problem. They impact home agent discovery, home address configuration, and mobile node to home agent authentication aspects.

7. Deployment scenarios

This section describes the various network deployment scenarios. The various combinations of service providers as described in Section 6 are considered.

For each scenario, the underlying assumptions are described. The basic assumption is that there is a trust relationship between mobile user and the MSA . Typically, this trust relationship is between the mobile user and AAA in the MSA's network. Seed information needed to bootstrap the mobile node is considered in two cases:

- AAA authentication is mandatory for network access
- AAA authentication is not part of network access. The seed information is described further in Section 8.

7.1. Mobility Service Subscription Scenario

Many commercial deployments are based on the assumption that mobile nodes have a subscription with a service provider. In this scenario the MN has a subscription with an MSA , called also the home MSP, for Mobile IPv6 service. As stated in Section 6, the MSP is responsible of setting up a home agent on a subnet that acts as a Mobile IPv6 home link. As a consequence, the home MSP should explicitly authorize and control the whole bootstrapping procedure.

Since the MN is assumed to have a pre-established trust relationship with its home provider, it must be configured with an identity and credentials, for instance an NAI and a shared secret by some out-of-band means (i.e. manual configuration) before bootstrapping.

In order to guarantee ubiquitous service, the MN should be able to bootstrap MIPv6 operations with its home MSP from any possible access location, such as an open network or a network managed by an ASP, that may be different from the MSP and may not have any pre-established trust relationship with it.

7.2. Integrated ASP network scenario

In this scenario, the ASA and MSA are the same entity. The MN has security credentials for access to the network and these credentials can be used to bootstrap MIPv6. This bootstrapping can be done during the same phase as access authentication/authorization or at a later time (probably based on some state created during access authentication/authorization).

Figure 1 describes an example AAA design for integrated ASP scenario.

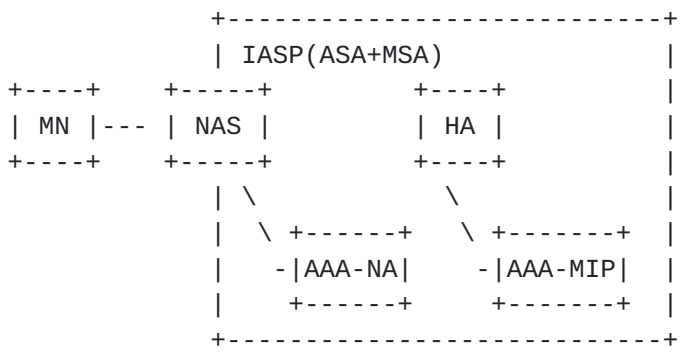

Figure 1: Integrated ASP network

7.3. Third party MSP scenario

Mobility service has traditionally been provided by the same entity that authenticates and authorizes the subscriber for network access. This is certainly the only model support by the base Mobile IPv6 specification.

In the 3rd party mobility service provider scenario, the subscription for mobility service is made with one entity (MSA for instance a corporate network), but the actual mobility service is provided by yet another entity (such as an operator specializing on this service, the serving MSP). These two entities have a trust relationship. Transitive trust among the mobile node and these two entities may be used to assure the participants that they are dealing with, are trustworthy peers.

This arrangement is similar to the visited - home operator roaming arrangement for network access.

Figure 2 describes an example network for third party MSP scenario.

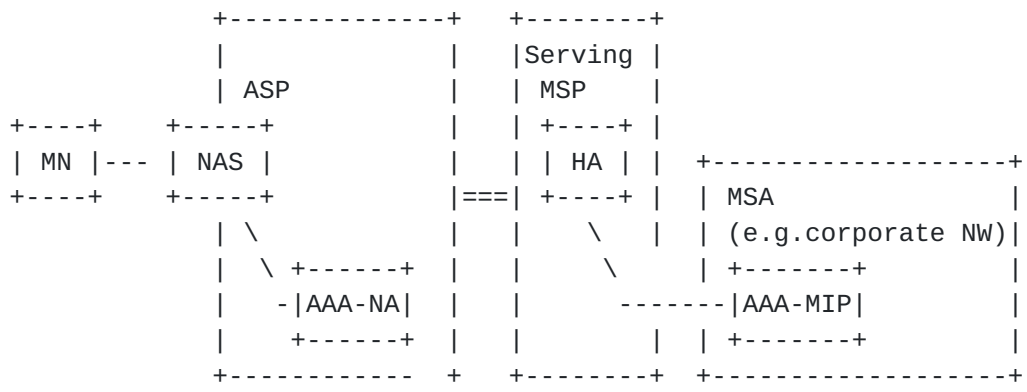

Figure 2: Third Party MSP network

7.4. Infrastructure-less scenario

Infrastructure refers to network entities like AAA, PKI, HLR etc. Infrastructure-less implies that there is no dependency on any elements in the network with which the user has any form of trust relationship.

In such a scenario, there is absolutely no relationship between host and infrastructure.

A good example of infrastructure-less environment for MIP6 bootstrapping is the IETF network at IETF meetings. It is possible that there could be MIP6 service available on this network (i.e a MIPv6 HA). However there is not really any AAA infrastructure or for that matter any trust relationship that a user attending the meeting has with any entity in the network.

This specific scenario is not supported in this document. The reason for this is described in Section 9.

8. Parameters for authentication

The following is a list of parameters that are used as the seed for the bootstrapping procedure. The parameters vary depending on whether authentication for network access is independent of authentication for mobility services or not.If different client identities are used for network access and mobility services, authentication for network access is independent of authentication for mobility services..

o Parameter Set 1

In this case, authentication for network access is independent of authentication for mobility services.

If the home agent address is not known to the mobile node the following parameter is needed for discovering the home agent address:

* The domain name or FQDN of the home agent

This parameter may be derived in various ways such as (but not limited to) static configuration, use of the domain name from the network access NAI (even if AAA for network access is not otherwise used) or use of the domain name of the serving ASP where the domain name may be obtained via DHCP in the serving ASP.

If the home agent address is not known but the home subnet prefix is known, Dynamic Home Agent Address Discovery of Mobile IPv6 may be used for discovering the home agent address and the above parameter may not be used.

When the home agent address is known to the mobile node, the following parameter is needed for performing mutual authentication between the mobile node and the home agent by using IKE:

* IKE credentials(*)

In the case where the home agent does not have the entire set of IKE credentials, the home agent may communicate with other entity (for example a AAA server) to perform mutual authentication in IKE. In such a case, the IKE credentials include the credentials used between the mobile node and the other entity. In the case where a AAA protocol is used for the communication between the home agent and the other entity during the IKE procedure, AAA for Mobile IPv6 service may be involved in IKE.

If authentication protocol [RFC4285] is used, the shared key based security association with home agent is needed.

- Parameter Set 2

  In this case, some dependency exists between authentication for network access and authentication for mobility services in that a security association that is established as a result of authentication for network access is re-used for authentication for mobility services.

  All required information including IKE credentials are bootstrapped from the following parameter:

  * Network access credentials(*)

(*) A pair of a NAI and a pre-shared secret is an example set of credentials. A pair of an NAI and a public key, which may be provided as a digital certificate, is another example set of credentials.

9. Security Considerations

There are two aspects of security for the Mobile IPv6 bootstrapping problem:

1. The security requirements imposed on the outcome of the bootstrapping process by RFC 3775 and other RFCs used by Mobile IPv6 for security.

2. The security of the bootstrapping process itself, in the sense of threats to the bootstrapping process imposed by active or passive attackers.

Note that the two are related; if the bootstrapping process is compromised, the level of security required by RFC 3775 may not be achieved.

The following two sections discuss these issues.

9.1. Security Requirements of Mobile IPv6

The Mobile IPv6 specification in RFC 3775 requires the establishment of a collection of IPsec SAs between the home agent and mobile node to secure the signaling traffic for Mobile IP, and, optionally, also to secure data traffic. The security of an IPsec SA required by the relevant IPsec RFCs must be quite strong. Provisioning of keys and other cryptographic material during the establishment of the SA through bootstrapping must be done in a manner such that authenticity is proved and confidentiality is ensured. In addition, the generation of any keying material or other cryptographic material for the SA must be done in a way such that the probability of compromise after the SA is in place is minimized. The best way to minimize the probability of such a compromise is to have the cryptographic material only known or calculable by the two end nodes that share the SA -- in this case, the home agent and mobile node. If other parties are involved in the establishing the SA, through key distribution for example, the process should follow the constraints [I-D.ietf-eap-keying-08] designed to provide equivalent security.

RFC 3775 also requires a trust relationship as defined in Section 1.3 between the mobile node and its home agent(s) . This is necessary, for instance, to ensure that fradulent mobile nodes which attempt to flood other mobile nodes with traffic can not only be shut off but tracked down [I-D.rosec]. An infrastructureless relationship as defined in Section 1.3 does not satisfy this requirement. Any bootstrapping solution must include a trust relationship between mobile node and mobility service provider. Solutions that depend on an infrastructureless relationship are out of scope for

bootstrapping.

Another requirement is that a home address is authorized to one specific host at a time. RFC 3775 requires this in order to that misbehaving mobile nodes can be shut down. This implies that, in addition to the IPsec SA, the home agent must somehow authorize the mobile node for a home address. The authorization can be either implicit (for example, as a side effect of the authentication for mobility service) or explicit. The authorization can either be done at the time the SA is created or dynamically managed through a first come, first served allocation policy.

9.2. Threats to the Bootstrapping Process

Various attacks are possible on the bootstrapping process itself. These attacks can compromise the process such that the RFC 3775 requirements for Mobile IP security are not met, or they can serve to simply disrupt the process such that bootstrapping cannot complete. Here are some possible attacks:

- An attacking network entity purporting to offer the mobile node a legitimate home agent address or bootstrapping for the IPsec SAs may, instead, offer a bogus home agent address or configure bogus SAs that allow the home agent to steal the mobile node's traffic or otherwise disrupts the mobile node's mobility service.

- An attacking mobile node may attempt to steal mobility service by offering up fake credentials to a bootstrapping network entity or otherwise disrupt the home agent's ability to offer mobility service.

- A man in the middle on the link between the mobile node and the bootstrapping network entity could steal credentials or other sensitive information and use that to steal mobility service or deny it to the legitimate owner of the credentials. Refer to Section 7.15 in [2284bis] and [I-D.mariblanca-aaa-eap-lla-00] for further information.

- An attacker could arrange for a distributed denial of service attack on the bootstrapping entity, to disrupt legitimate users from bootstrapping.

In addition to these attacks, there are other considerations that are important in achieving a good security design. As mobility and network access authentication are separate services, keys generated for these services need to be cryptographically separate, separately named, and have separate lifetimes, including if the keys are generated from the same authentication credentials This is necessary

because a mobile node must be able to move from one serving (or roaming) network access provider to another without needing to change its mobility access provider. Finally, basic cryptographic processes must provide for multiple algorithms in order to accommodate the widely varying deployment needs.

10. IANA Considerations

No new protocol numbers are required.

11. Contributors

This contribution is a joint effort of the problem statement design team of the Mobile IPv6 WG. The contributors include Basavaraj Patil, Gerardo Giaretta, Jari Arkko, James Kempf, Yoshihiro Ohba, Ryuji Wakikawa, Hiroyuki Ohnishi, Mayumi Yanagiya Samita Chakrabarti, Gopal Dommety, Kent Leung, Alper Yegin, Hannes Tschofenig, Vijay Devarapalli, Kuntal Chowdury.

The design team members can be reached at:

Basavaraj Patil basavaraj.patil@nokia.com

Gerardo Giaretta gerardo.giaretta@tilab.com

Jari Arkko jari.arkko@kolumbus.fi

James Kempf kempf@docomolabs-usa.com

Yoshihiro Ohba yohba@tari.toshiba.com

Ryuji Wakikawa ryuji@sfc.wide.ad.jp

Hiroyuki Ohnishi ohnishi.hiroyuki@lab.ntt.co.jp

Mayumi Yanagiya yanagiya.mayumi@lab.ntt.co.jp

Samita Chakrabarti Samita.Chakrabarti@eng.sun.com

Gopal Dommety gdommety@cisco.com

Kent Leung kleung@cisco.com

Alper Yegin alper.yegin@samsung.com

Hannes Tschofenig hannes.tschofenig@siemens.com

Vijay Devarapalli vijayd@iprg.nokia.com

Kuntal Chowdhury kchowdhury@starentnetworks.com

12. Acknowledgments

Special thanks to James Kempf and Jari Arkko for writing the initial version of the bootstrapping statement. Thanks to John Loughney and T.J. Kniveton for their detailed reviews.

13. IPR Disclosure Acknowledgement

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

14. Informative References

[2284bis] Levkowetz, Ed., H., "Extensible Authentication Protocol (EAP)", February 2004, <draft-ietf-eap-rfc2284bis-09.txt>.

[I-D.giaretta-mip6-authorization-eap] Giaretta, G., "MIPv6 Authorization and Configuration based on EAP", draft-giaretta-mip6-authorization-eap-02 (work in progress), February 2004, <draft-giaretta-mip6-authorization-eap-02.txt>.

[I-D.ietf-eap-keying-08] Aboba et. al., B., "Extensible Authentication Protocol (EAP) Key Management Framework", draft-ietf-eap-keying-08.txt (work in progress), October 2005, <draft-ietf-eap-keying-08.txt>.

[I-D.kempf-mip6-bootstrap] Kempf, J. and J. Arkko, "The Mobile IPv6 Bootstrapping Problem", draft-kempf-mip6-bootstrap-00 (work in progress), March 2004, <draft-kempf-mip6-bootstrap-00.txt>.

[I-D.mariblanca-aaa-eap-lla-00] Mariblanca, D., "EAP lower layer attributes for AAA protocols", May 2004, <draft-mariblanca-aaa-eap-lla-00.txt>.

[I-D.rosec] Nikander, P., Arkko, J., Aura, T., Montenegro, G., and E. Nordmark, "Mobile IP version 6 Route Optimization Security Design Background", draft-ietf-mip6-ro-sec-02 (work in progress), October 2004, <draft-ietf-mip6-ro-sec-02.txt>.

[RFC2794] Calhoun, P. and C. Perkins, "Mobile IP Network Access Identifier Extension for IPv4", RFC 2794, March 2000.

[RFC3041] Narten, T. and R. Draves, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 3041, January 2001.

[RFC3753] Manner, J. and M. Kojo, "Mobility Related Terminology", RFC 3753, June 2004.

[RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

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

[RFC4283] Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Mobile Node Identifier Option for Mobile IPv6 (MIPv6)", RFC 4283, November 2005.

[RFC4285] Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Authentication Protocol for Mobile IPv6", RFC 4285, January 2006.

Authors' Addresses

Alpesh Patel
Cisco
170 W. Tasman Drive
San Jose, CA 95134
USA

Phone: +1 408 853 9580
Email: alpesh@cisco.com

Gerardo Giaretta
Telecom Italia LAB
via Reiss Romoli 274
Torino 10148
Italy

Phone: +39 011 228 6904
Email: gerardo.giaretta@telecomitalia.it

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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