Network Working Group F. Dupont, Ed.
Internet-Draft Point6
Expires: April 24, 2006 October 21, 2005

Dynamic Home Agent Address Discovery (DHAAD) Considered Harmful
draft-dupont-mip6-dhaadharmful-01.txt

Abstract

Dynamic Home Agent Address Discovery (DHAAD) mechanism of Mobile IPv6 is nearly impossible to make secure. As the service itself is useful, this document shows the security problems of the current mechanism and promotes an alternative solution.

1. Introduction

Mobile IPv6 specifications [RFC3775] contains a mechanism where a

home agent can help mobile nodes to discover the addresses of the home agents named the Dynamic Home Agent Address Discovery (DHAAD). This mechanism uses two ICMP message types:

Home Agent Address Discovery Requests which are sent by mobile nodes to the Home Agents anycast addresses for their home subnet prefixes.

Home Agent Address Discovery Replies which are sent by home agents in response.

A 16-bit identifier aids in matching requests and replies.

The main security issue is in the anycast destination of requests, and as the mechanism is the first step of bootstrapping, there is no way to add reasonable security to it.

So a solution is to change for a completely different mechanism providing the same service. One is developed in the Mobile IPv6 bootstrapping framework [ID-mip6-bootsplit]: it is based on the "Microsoft-style" for service discovery: DNS SRV Resource Records [RFC2782].

Security is provided by the DNSSEC [RFC4033] framework. The needed pre-configured data on the mobile node for this mechanism is the domain name of the mobile service provider, which marginally better than the home subnet prefix. For the security, a trust anchor which dominates the domain is needed.

The mechanism can be extended to the Network Mobility (NEMO [RFC3963]) with "nemo" as the service name.

2. ICMP Issue

Specification of ICMP to carry DHAAD incurs a certain deployability risk. Many ISPs are blocking ICMP on all links except the first hop, because ICMP is known to be a vehicle for DoS attacks and other sorts of threats. It is theoretically possible to block ICMP types selectively, and therefore it would be possible to allow DHAAD messages through firewalls and still block those DHAAD messages that are a known threat. However, because DHAAD is initiated from outside the firewall, the risk of a crude flooding DoS attack is unchanged since the firewall must allow any DHAAD message through. The ISP could deploy some kind of authentication mechanism to validate that a DHAAD message comes from an authorized user before letting it through, but such sophisticated authentication is beyond current practice, and the advantages of deploying such a mechanism specifically for DHAAD are uncertain. It is easier from a network management standpoint to simply uniformly block ICMP except on the last hop.

3. Security Considerations

Securing the current DHAAD mechanism is a hopeless task. The DNS SRV RR mechanism is already heavily used for service discovery and the standard way to make it secure is well known even not yet deployed in a large scale.

4. Acknowledgments

The authors of [ID-mip6-bootsplit] have done the hard work and should get all the credits. Many early Mobile IPv6 operators pointed out that the current DHAAD mechanism does not provide a reasonable level of security.

Nicolas Montavont proposed to extend the document to NEMO.

James Kempf is the author of the Section 2 "ICMP issue".

5. References

5.1. Normative References

[RFC2782] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, February 2000.

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

[RFC3963] Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, January 2005.

5.2. Informative References

[ID-mip6-bootsplit] Giaretta, G., Ed., Kempf, J., and V. Devarapalli, "Mobile IPv6 bootstrapping in split scenario", draft-ietf-mip6-bootstrapping-split-00.txt (work in progress), June 2005.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

Appendix A. The new DHAAD mechanism

The text of this annex is from [ID-mip6-bootsplit].

A.1. Component of the solution

HA address discovery. The Mobile Node needs to discover the address of its Home Agent. The main objective of a bootstrapping solution is to minimize the data pre-configured on the Mobile Node. For this reason, the DHAAD defined in [RFC3775] may not be applicable in real deployments since it is required that the Mobile Node is pre-configured with the home network prefix and it does not allow an operator to load balance by having Mobile Nodes dynamically assigned to Home Agents located in different subnets. This document defines a solution for Home Agent address discovery that is based on Domain Name Service (DNS), introducing a new DNS SRV record [RFC2782]. The unique information that needs to be pre- configured on the Mobile Node is the domain name of the MSP.

A.2. Home Agent Address Discovery

Once a Mobile Node has obtained network access, it can perform Mobile IPv6 bootstrapping. For this purpose, the Mobile Node queries the DNS server to request information on Home Agent service. As mentioned before in the document, the only information that needs to be auto- configured on the Mobile Node is the domain name of the Mobility Service Provider.

The Mobile Node needs to obtain the IP address of the DNS server before it can send a DNS request. This can be pre-configured on the Mobile Node or obtained through DHCPv6 from the visited link. In any case, it is assumed that there is some kind of mechanism by which the Mobile Node is configured with a DNS server since a DNS server is needed for many other reasons.

Two options for DNS lookup for a Home Agent address are identified in this document: DNS lookup by Home Agent Name and DNS lookup by service name.

While this document specifies a Home Agent Address Discovery solution based on DNS, when the ASP and the MSP are the same entity DHCP may be used. See "DCHPv6 option for home agent discovery in MIPv6" for details.

A.2.1. DNS lookup by Home Agent Name

In this case, the Mobile Node is configured with the Fully Qualified Domain Name of the Home Agent. As an example, the Mobile Node could

be configured with the name "ha1.example.com", where "example.com" is the domain name of the MSP granting the mobility service.

The Mobile Node constructs a DNS request, by setting the QNAME to the name of the Home Agent. The request has QTYPE set to 'AAAA', so that the DNS server sends the IPv6 address of the Home Agent. Once the DNS server replies to this query, the Mobile Node knows its Home Agent address and can run IKEv2 in order to set up an IPsec SA and get a Home Address.

Additionally, it could be useful to provide an ability for the Mobile Node to discover a Home Agent placed in a particular location (e.g. on the visited link). In order to achieve this, the Mobile Node must be able to construct a DNS request such that the DNS server will be able to reply with a Home Agent from the requested location. This can be accomplished by using a specific naming convention for the FQDNs of the Home Agents. As an example, an operator might assign the FQDN "ha.locationA.operator.com" to the Home Agent located in "location A" and the FQDN "ha.locationB.operator.com" to the Home Agent located in "location B". If the Mobile Node wants to use a Home Agent located in "location A", it will set the QNAME to "ha.locationA.operator.com" in the DNS request.

A.2.2. DNS lookup by service name

[RFC2782] defines the service resource record (SRV RR), that allows an operator to use several servers for a single domain, to move services from host to host, and to designate some hosts as primary servers for a service and others as backups. Clients ask for a specific service/protocol for a specific domain and get back the names of any available servers.

[RFC2782] describes also the policies to choose a service agent based on the preference and weight values. The DNS SRV record may contain the preference and weight values for multiple Home Agents available to the Mobile Node in addition to the Home Agent FQDNs. If multiple Home Agents are available in the DNS SRV record then Mobile Node is responsible for processing the information as per policy and for picking one Home Agent. If the Home Agent of choice does not respond for some reason or the IKEv2 authentication fails, the Mobile Node SHOULD try other Home Agents on the list.

The service name for Mobile IPv6 Home Agent service as required by [RFC2782] is "mip6" and the protocol name is "ipv6". Note that a transport name cannot be used here because Mobile IPv6 does not run over a transport protocol.

The SRV RR has a DNS type code of 33. As an example, the Mobile

constructs a request with QNAME set to "mip6.example.com" and QTYPE to SRV. The reply contains the FQDNs of one or more servers, that can then be resolved in a separate DNS transaction to the IP addresses. However, it is RECOMMENDED that the DNS server also return the IP addresses of the Home Agents in AAAA records as part of the additional data section in order to avoid requiring an additional DNS round trip to resolve the FQDNs, if there is room in the SRV reply.

A.3. HA Address Discovery Security

Use of DNS for address discovery carries certain security risks. DNS transactions in the Internet are typically done without any authentication of the DNS server by the client or of the client by the server. There are two risks involved:

1) A legitimate client obtains a bogus Home Agent address from a bogus DNS server. This is sometimes called a "pharming" attack,

2) An attacking client obtains a legitimate Home Agent address from a legitimate server.

The risk in Case 1 is mitigated because the Mobile Node is required to conduct an IKE transaction with the Home Agent prior to performing a Binding Update to establish Mobile IPv6 service. According to the IKEv2 specification, the responder must present the initiator with a valid certificate containing the responder's public key, and the responder to initiator IKE_AUTH message must be protected with an authenticator calculated using the public key in the certificate. Thus, an attacker would have to set up both a bogus DNS server and a bogus Home Agent, and provision the Home Agent with a certificate that a victim Mobile Node could verify. If the Mobile Node can detect that the certificate is not trustworthy, the attack will be foiled when the Mobile Node attempts to set up the IKE SA.

The risk in Case 2 is limited for a single Mobile Node to Home Agent transaction if the attacker does not possess proper credentials to authenticate with the Home Agent. The IKE SA establishment will fail when the attacking Mobile Node attempts to authenticate itself with the Home Agent. Regardless of whether the Home Agent utilizes EAP or host-side certificates to authenticate the Mobile Node, the authentication will fail unless the Mobile Node has valid credentials.

Another risk exists in Case 2 because the attacker may be attempting to propagate a DoS attack on the Home Agent. In that case, the attacker obtains the Home Agent address from the DNS, then propagates the address to a network of attacking hosts that bombard the Home

Agent with traffic. This attack is not unique to the bootstrapping solution, however, it is actually a risk that any Mobile IPv6 Home Agent installation faces. In fact, the risk is faced by any service in the Internet that distributes a unicast globally routable address to clients. Since Mobile IPv6 requires that the Mobile Node communicate through a globally routable unicast address of a Home Agent, it is possible that the Home Agent address could be propagated to an attacker by various means (theft of the Mobile Node, malware installed on the Mobile Node, evil intent of the Mobile Node owner him/herself, etc.) even if the home address is manually configured on the Mobile Node. Consequently, every Mobile IPv6 Home Agent installation will likely be required to mount anti-DoS measures. Such measures include overprovisioning of links to and from Home Agents and of Home Agent processing capacity, vigilant monitoring of traffic on the Home Agent networks to detect when traffic volume increases abnormally indicating a possible DoS attack, and hot spares that can quickly be switched on in the event an attack is mounted on an operating collection of Home Agents. DoS attacks of moderate intensity should be foiled during the IKEv2 transaction. IKEv2 implementations are expected to generate their cookies without any saved state, and to time out cookie generation parameters frequently, with the timeout value increasing if a DoS attack is suspected. This should prevent state depletion attacks, and should assure continued service to legitimate clients until the practical limits on the network bandwith and processing capacity of the Home Agent network are reached.

Explicit security measures between the DNS server and host, such DNSSEC or TSIG/TKEY can mitigate the risk of 1) and 2), but these security measures are not widely deployed on end nodes. These security measures are not sufficient to protect the Home Agent address against DoS attack, however, because a node having a legitimate security association with the DNS server could nevertheless intentionally or inadvertently cause the Home Agent address to become the target of DoS.

Security considerations for discovering HA using DHCP are covered in draft-jang-dhc-haopt-01.

Author's Address

Francis Dupont (editor)
Point6
c/o GET/ENST Bretagne
2 rue de la Chataigneraie
CS 17607
35576 Cesson-Sevigne Cedex
France

Fax: +33 2 99 12 70 30
Email: Francis.Dupont@enst-bretagne.fr

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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