W. Haddad
M. Naslund
Ericsson Research
C. Vogt
Ericsson Research Nomadic Lab

July 1, 2007

# Enabling Source Address Verification via Prefix Reachability Detection
# draft-haddad-sava-prefix-reachability-detection-00

## Status of this Memo



This Internet-Draft will expire on January 2, 2008.

## Copyright Notice

Abstract

In this memo, we introduce an approach called "Prefix Reachability Detection", which aims to address certain man-in-the middle misbehavior problems and enable a location-based authentication.

Table of Contents

## 1. Introduction

In this memo, we introduce an approach called "Prefix Reachability Detection (PRD)", which aims to address certain man-in-the middle (MiTM) misbehavior problems on the IP layer and enable a location-based authentication. A direct consequence of applying the PRD approach is a source address verification mechanism, which can also be used in a mobile and multihomed environment.

The main components for applying the PRD protocol are a secure and trustable "prefix routing lookup" mechanism and a secure on-demand query/response between the communicating endpoints and their first hop routers.

## 2. Conventions used in this document

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 [TERM].

## 3. Motivation and Assumptions

The motivation behind this work stems from the need for an efficient and scalable solution to thwart MiTM misbehavior. In fact, a MiTM misbehavior can manifest itself in different aspects, which include unwanted traffic, impersonation, identity theft, denial-of service (DoS). All these aspects can target a network and/or a particular node but they share the same disruptive and destructive goals. They also have one common feature reflected by the alarming and steadily increasing frequency of their occurrence. Consequently, there is an urgent need to address this problem to avoid what could be (very) unpleasant real-world side-effects.

Our goal is to provide a solution, which can protect against these different aspects by enabling a source address verification mechanism and at in parallel, offer a set of attributes which can significantly improve the security and the overall efficiency of different types of new and existing solutions. These attributes can be seen as consequences, which fall beyond addressing the SAVA problem statement described in [SAVA].

In order to achieve our goal, we make the following assumptions:

- Existence of a secure and trustable mechanism, which enables at least a particular set/class of routers to fetch security credentials (i.e., using a third entity) of other routers belonging to the same set. Such mechanism can be based for example, on the ongoing work on [SIDR].

- Existence of secure and trustable links between each endpoint and the first hop router. Note that this does not really impose new requirements and has already been addressed in [SeND].

## 4. Protocol Overview

The suggested approach enables one endpoint to check the topological location of the other endpoint, which maps correctly to the prefix claimed in their IP address. Such procedure is also referred to by "location authentication".

The PRD protocol is performed in parallel with running a key exchange protocol, e.g., [IKEv2] or [HIP]. In the following, we consider the classic scenario where a client (C) is establishing an IKEv2 session with a server (S) and we delegate to (S) the task of triggering the PRD protocol.

In its most generic form, the PRD protocol consists on executing (in order) the following steps:

1. After completing the IKEv2 exchange, (S) requests from its first hop router (we call it AR(S)) to perform a prefix reachability detection, i.e., location authentication, on (C)'s IP address. For this purpose, (S) sends a "Prefix_Reachability_Request (PRR)" message to AR(S), which carries a secret (called Ksh) and (C)'s IP address. Ksh is derived from the hash of IKEv2 session key (Ks) and a hint (H). The PRR message MUST be signed with (C)'s CGA private key (as described in [CGA]) and the option carrying Ksh MUST be encrypted with AR(S) public key.

   Note that an optimized version of the SeND protocol (described in [OpSeND]) enables (S) and AR(S) to authenticate all messages exchanged between them by using a shared secret, which in turn eliminates the burden of using private/public key to sign (and encrypt) the PRR message.

   (C) and (S) MUST use the same method to derive Ksh. This method SHOULD be:

   Ksh = First[ 128, Hash[ Hash(Ks) | IID(C) | IID(S) ]]

   Where:

   - First(X,Y) indicates a truncation of "Y" data so that only the first "X" bits remain to be used.
   - Hash is a secure cryptographic function.
   - Ks is IKEv2 session key.
   - IID(C) = (C)'s IP address interface identifier
   - IID(S) = (S)'s IP address interface identifier
   - "|" (concatenation): indicates bytewise concatenation, as in A | B. This concatenation requires that all of the octets of the datum A appear first in the result, followed by all of the octets

of the datum B.
- IID(C) | IID(S) = Hint (H)

2. Upon receiving a valid PRR message, AR(S) starts its mission by performing a "prefix lookup" using (C)'s 64-bit prefix, in order to learn the corresponding IP address and public key of AR(C) (denoted Kpc). It follows that the result of a prefix lookup MUST return the public key and the IP address of the router, which is advertising the queried prefix. Note that it may be useful for AR(S) to store AR(C) parameters for a limited amount of time.

3. After retrieving AR(C)'s IP address and public key, AR(S) sends an "On_Link_Presence_Request" (OLPR) message to AR(C), which carries (C)'s 64-bit interface identifier (IID), (S)'s 64-bit prefix and a 64-bit nonce. The IP destination address used in the OLPR message is the one sent to AR(S) in response to its query related to (C)'s prefix. The OLPR message MUST be authenticated with Ksh and signed with AR(S) private key.

4. Upon receiving an OLPR message, AR(C) starts the validation procedure by performing an (S)'s prefix look up in order to fetch the corresponding IP address(es) and public key(s) (we call it Kps). After that, AR(C) checks the validity of the IP source address used in the OLPR message. This is followed by checking the requested IID presence on the link. For this purpose, AR(C) SHOULD use the neighbor discovery protocol (described in [NDP]) and SHOULD insert the hint (H) in the corresponding message (i.e., in a new option). Finally, AR(C) MUST authenticate (or sign) the ND message before sending it (note that the message may be sent only to (C) and in this case, it can be authenticated with the shared secret obtained from running OptiSeND between AR(C) and (C)).

5. When (C) detects the hint in the ND message, it replies by sending Ksh to AR(C). For this purpose, Ksh is inserted in an encrypted option carried by an authenticated ND message sent to AR(C).

6. After receiving a valid ND message from (C), AR(C) decrypts Ksh and uses it to check the authenticity of the OLPR message. If the message is valid, then AR(C) proceeds to check the signature using AR(S)'s Kps, then sends back an "On_Link_Presence_Confirmation (OLPC)" message to AR(S). The OLPC message SHOULD carry (H) and the nonce sent in the OLPR message. In addition, the OLPC message MUST be authenticated with Ksh and signed with AR(C) private key.

However, if AR(C) does not get any valid reply (i.e., a message from (C) carrying Ksh), then it MUST send an "On_link_Prefix_Denial (OLPD)" message to AR(S). It follows that the OLPD message cannot be authenticated and in this case, it MUST carry the hint and the nonce sent in the OLPR message and MUST be signed with AR(C) private key only.

7. After checking the validity of OLPC/OLPD, AR(S) notifies (S) about the success/failure of its PRR message. This is done by sending a "Prefix_Reachability_Acknowledgment (PRA)" message to (S). The PRA message MUST be signed with AR(S) private key or authenticated with a shared secret between AR(S) and (S). The OLPD message is reflected in the PRA message by setting the "Alert" (A) bit.
   Following receipt of a valid PRA message, (S) can decide whether to pursue or not the data exchange with (C).

The PRD procedure can be repeated periodically during the data exchange between the two endpoints and/or upon receiving a mobility signaling message indicating a switch made by (C) to another network or when switching to another interface. For this purpose, refreshing Ksh is required in each location authentication procedure. To this end, one way would be to add a counter in the formula used to generate Ksh. For instance, we could do:

Ksh = First[ 128, Hash[ Hash(Ks) | IID(C) | IID(S) | COUNT ] ]

Where COUNT is equal to zero on the first PRD, then its value is increased by 1 (or more) for each new run. This also means that the new value SHOULD be sent in the signaling.

## 5. New Options and Messages Formats

The PRD protocol introduces 4 new messages and one new option which are TBD.

## 6. Security Considerations

This memo introduces a new protocol, which aims to detect and thwart certain MiTM misbehavior. Hence, the main goal is to improve the detection and defense capabilities on both sides of the two communicating endpoints. If implemented correctly, in its current form and to the best of our knowledge, the PRD protocol does not introduce nor increase any new/existing security threats. It should be noted however, that the presence of a nonce in the OLPD message is highly recommended in order to avoid launching a DoS attack on AR(S).

## 7. Acknowledgments

Authors would like to thank Pekka Nikander, Rolf Blom, Andras Mehes and Yuri Ismailov for their valuable input.

# 8. References

## 8.1. Normative References

[CGA] Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3792, March 2005.

[HIP] Moskowitz, B., Nikander, P., Jokela, P., and T. Henderson, "Host Identity Protocol", Internet Draft, draft-ietf-hip-base-07.txt, February 2007.

[IKEv2] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

[NDP] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP Version 6 (IPv6)", Internet Draft, draft-ietf-ipv6-2461bis-11.txt, March 2007.

[SeND] Arkko, J., Kempf, J., Sommerfield, B., Zill, B., and P. Nikander, "Secure Neighbor Discovery (SEND)", RFC 3971, March 2005.

[TERM] Bradner, S., "Key Words for Use in RFCs to Indicate Requirement Levels", RFC 2119, BCP , March 1997.

## 8.2. Informative References

[OpSeND] Haddad, W., Krishnan, S., Choi, J., and J. Laganier, "Secure Neighbor Discovery (SeND) Optimizations: The OptiSeND Protocol", Internet Draft, draft-haddad-optimizing-send-00.txt, July 2007.

[SAVA] Wu, J., Bonica, R., Bi, J., Li, X., Ren, G., and M I. Williams, "Source Address Verification Architecture Problem Statement", Internet Draft, draft-sava-problem-statement-00.txt, February 2007.

[SIDR] Barnes, R. and S. Kent, "An Infrastructure to Support Secure Internet Routing", Internet Draft, draft-ietf-sidr-arch-00.txt, January 2007.

Authors' Addresses

Wassim Haddad
Ericsson Research
Torshamnsgatan 23
SE-164 80 Stockholm
Sweden

Phone: +46 8 4044079
Email: Wassim.Haddad@ericsson.com

Mats Naslund
Ericsson Research
Torshamnsgatan 23
SE-164 80 Stockholm
Sweden

Phone: +46 8 58533739
Email: Mats.Naslund@ericsson.com

Christian Vogt
Ericsson Research Nomadic Lab
Jorvas FI-02420
Finland

Phone: +358 9 299 1
Email: Christian.Vogt@ericsson.com

## Full Copyright Statement



## Intellectual Property



## Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).