Host Identity Protocol	D. Lagutin
Internet-Draft	Helsinki Institute for Information
Intended status: Experimental	Technology
Expires: January 4, 2011	July 3, 2010

TOC

Packet Level Authentication (PLA) Extensions for Host Identity Protocol (HIP)
draft-lagutin-hip-pla-00

Abstract

This document defines extensions to provide Packet Level Authentication (PLA) functionality for the HIP protocol. PLA provides strong hop-by-hop security features that allow intermediate nodes to detect the hostile traffic quickly, and drop the traffic before it reaches the destination and can consume resources in the target network.
Unlikely other similar solutions, PLA does not require excessive signaling or state in verifying nodes, and is path-independent, making it suitable for dynamic environments, such as ad-hoc networks.

Requirements Language

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 (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.) [RFC2119].

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.
Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.
Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as “work in progress.”
This Internet-Draft will expire on January 4, 2011.

Table of Contents

TOC

1. Introduction

Packet Level Authentication (PLA) [LAG08] (Lagutin, D., “Redesigning Internet - The Packet Level Authentication architecture, Licentiate's thesis,” Jun 2008.) is a novel security solution that aims to provide availability and integrity protection on the network layer. PLA offers hop-by-hop authentication: any intermediate node has the ability to independently verify authenticity and integrity of the traffic, without pre-established trust relationships with the sender or other nodes that handled the traffic. The good analogy to PLA is a paper currency: anyone can verify validity of the paper bill using built-in security measures such as watermark and hologram, there is no need to contact the bank that has issued the bill.

Similarly, PLA allows intermediate nodes to detect modified, delayed, and duplicated packets simply by looking at the packet's contents. This protects the recipient from denial-of-service attacks, since such packets can be dropped immediately before they can reach the destination, and cause a load to the recipient or the recipient's network. Furthermore, strong security mechanisms offered by PLA have additional uses. They can be used to implement simple and secure user authentication, since there is often no need for puzzle mechanisms or to contact external authentication servers.

PLA achieves it goals by adding a cryptographic signature and other fields to the packet's header. PLA utilizes elliptic curve cryptography (ECC) due to its compact key and signature sizes, but can also work with other cryptographic solutions. While the public key signature verification is resource intensive operation, it can be performed at wire-speed with a dedicated hardware acceleration [FOR08] (Forsten, J., “Packet Level Authentication - Hardware Subtask Final Report, Technical report,” May 2008.).

We feel that combining PLA with HIP is advantageous, since both technologies are based on cryptographic operations and provide different sets of features. PLA offers hop-by-hop authentication and integrity protection, and depending on local policies it can make the HIP base exchange unnecessary in some cases. While HIP provides end-to-end confidentiality and security.

---

2. PLA-HIP Protocol Overview

TOC

Packet Level Authentication (PLA) Extensions for Host Identity Protocol (HIP) basically add PLA's features, such as a hop-by-hop integrity protection, to HIP using a new HIP parameter (PLA_HIP).

TOC

2.1. Security Mechanisms

Following PLA's security mechanisms are included in the PLA-HIP extensions, and MUST be added to the PLA_HIP parameter by the sender:
1. The sender's cryptographic identity (public key) and the signature over the packet. The signature protects packet's integrity and should be calculated over the whole packet ignoring the fields that may change during the lifetime of the packet. If the signature verification fails, the packet MUST be dropped.
While PLA-HIP can utilize any public key algorithms including RSA and DSA, using Elliptic Curve Digital Signature Algorithm (ECDSA) is recommended due to its low key and signature sizes.
2. Timestamp. The aim of the timestamp is provide protection against replay attacks that use delayed packets. Efficient usage of the timestamp field requires loosely synchronized clocks in the network. Network's policy decides how strictly the timestamp is enforced. For example, in a public network differences of several seconds can be tolerated.
3. The sequence number is a monotonically increasing number that allow intermediate nodes to detect duplicated packets, and packets that are significantly out-of-order.
It is important to note that performing signature and other above mentioned checks is optional. The recipient and intermediate nodes can decide which checks to perform. For example, some nodes may opt to verify only the timestamp and sequence number fields, ignoring the signature field. Therefore PLA-HIP can also be supported by devices with a limited computing power.
PLA also offers additional security mechanisms, such as trusted third parties that act as certificate authorities (CAs) and authorize nodes in the network. For simplicity, they have been omitted from this version of the draft.

2.2. Related Solutions

TOC

The functionality provided by PLA-HIP is somehow related to HICCUPS (Camarillo, G. and J. Melen, “HIP (Host Identity Protocol) Immediate Carriage and Conveyance of Upper- layer Protocol Signaling (HICCUPS),” March 2010.) [I-D.ietf-hip-hiccups], SAVAH (Kuptsov, D. and A. Gurtov, “SAVAH: Source address validation architecture with Host Identity Protocol,” March 2009.) [I-D.kuptsov-sava-hip], and HIP certificates (Heer, T. and S. Varjonen, “HIP Certificates,” April 2010.)
[I-D.ietf-hip-cert]. The biggest difference is that PLA-HIP is a path independent solution that does not use acknowledgment messages, and does not require state for the integrity protection in verifying nodes. Since each packet can be verified independently, PLA-HIP is suitable for multihoming and dynamic network environments.

3. Packet Processing

TOC

The following diagram in Figure 1, shows an example how the PLA-HIP packet is processed in a node. The order of verification steps is not strict, and can be decided by the verifier. PLA-HIP packets are considered to be fully valid if they pass all checks, however, in some cases nodes may forward packets even though they have failed timestamp or sequence number checks.

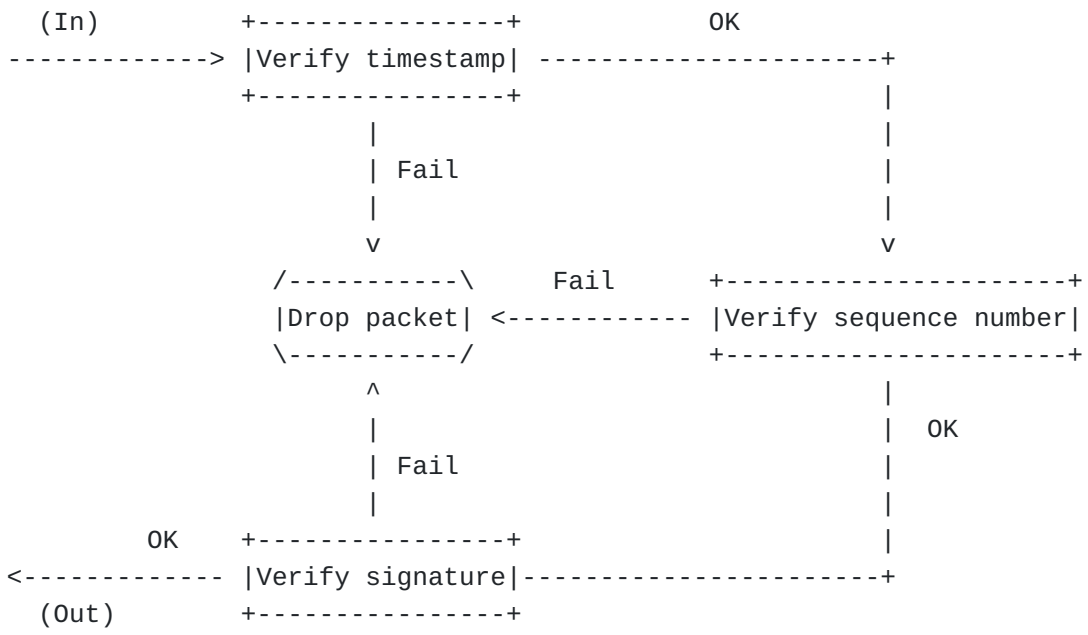

Figure 1

4. Packet Formats

TOC

In addition to the basic HIP headers, the PLA-HIP packet contains sender's public key, signature, and timestamp and sequnce number fields provided by the PLA_HIP parameter. Basically the PLA-HIP packet can be expressed as:
IP (HIP (HOST_ID, PLA_HIP, HIP_SIGNATURE) PAYLOAD)
Where HOST_ID and HIP_SIGNATURE parameters are defined in Sections 5.2.8 and 5.2.11 of [RFC5201] (Moskowitz, R., Nikander, P., Jokela, P., and T. Henderson, “Host Identity Protocol,” April 2008.). And the PLA_HIP

parameter is defined in Section 4.1 (Definition of the PLA_HIP Parameter).

4.1. Definition of the PLA_HIP Parameter

TOC

The following is the definition of the PLA_HIP parameter:

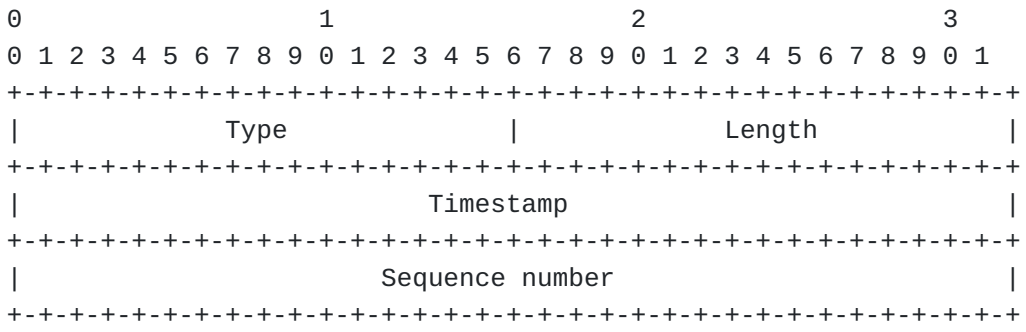

Figure 2

Both the timestamp and sequence number fields are 32 bits long.

5. Discussion

TOC

6. IANA Considerations

TOC

No IANA considerations.

7. Security Considerations

TOC

No security considerations.

TOC

8. Acknowledgements

Thanks to Miika Komu for his helpful comments and suggestions.

---

9. References

TOC

9.1. Normative References

TOC

[I-D.ietf-hip-cert]	Heer, T. and S. Varjonen, “HIP Certificates,” draft-ietf-hip-cert-03 (work in progress), April 2010 (TXT).
[I-D.ietf-hip-hiccups]	Camarillo, G. and J. Melen, “HIP (Host Identity Protocol) Immediate Carriage and Conveyance of Upper-layer Protocol Signaling (HICCUPS),” draft-ietf-hip-hiccups-02 (work in progress), March 2010 (TXT).
[I-D.kuptsov-sava-hip]	Kuptsov, D. and A. Gurtov, “SAVAH: Source address validation architecture with Host Identity Protocol,” draft-kuptsov-sava-hip-01 (work in progress), March 2009 (TXT).
[RFC2119]	Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[RFC5201]	Moskowitz, R., Nikander, P., Jokela, P., and T. Henderson, “Host Identity Protocol,” RFC 5201, April 2008 (TXT).

9.2. Informative References

TOC

[FOR08]	Forsten, J., “Packet Level Authentication - Hardware Subtask Final Report, Technical report,” May 2008.
[LAG08]	Lagutin, D., “Redesigning Internet - The Packet Level Authentication architecture, Licentiate's thesis,” Jun 2008.

Author's Address

TOC

	Dmitrij Lagutin
	Helsinki Institute for Information Technology
	Metsanneidonkuja 4
	Helsinki
	Finland

Phone:	+358 9 47001
Fax:	+358 9 694 9768
Email:	dmitrij.lagutin@hiit.fi