Network Working Group
Internet-Draft
Intended status: Informational
Expires: April 23, 2007

M. Bagnulo
UC3M

October 20, 2006

Privacy Analysis for the SHIM6 protocol
draft-bagnulo-shim6-privacy-01

Status of this Memo

Copyright Notice

Abstract

This note presents a privacy analysis for the SHIM6 protocol for IPv6 site multihoming support and the failure detection extensions for the SHIM6 protocol.This note does not attempt to provide a solution for providing SHIM6 protocol privacy.

Table of Contents

1. Introduction 3
2. Privacy of the ULID-pair context establishment exchange 3
3. Payload packets 6
4. Other Signalling messages 6
5. Conclusion 7
6. Security considerations 7
7. References 7
Author's Address 8
Intellectual Property and Copyright Statements 9

1. Introduction

This note presents a privacy analysis for the SHIM6 protocol as defined in [1] and the failure detection extensions for the SHIM6 protocol defined in [2].

The scenario considered is the following: two nodes are communicating using the SHIM6 protocol to achieve enhanced fault tolerance capabilities. The potential attackers are located along the path and their goal is to obtain relevant information by observing the exchanged packets. In particular, we consider that information harvesters may be interested in determining whether a set of addresses belongs to a single host or if a set of packets exchanged using different address pairs belong to the same communication. In the following sections we will analyze the information contained in the SHIM6 protocol messages that can be used to obtain such information.

It should be noted that this analysis is limited to malicious third parties that are located along one or several of the available paths between the communication parties and that it is out of the scope of the analysis the case where the potential attacker is one of the parties involved in the communication i.e. the goal is not to avoid the disclosure of locator information from the peer.

The remaining of this note is structured as follows: in the next section we will perform a privacy analysis of the SHIM6 4-way exchange to establish ULID-pair contexts. Next, we will analyze the privacy aspects of the payload packet exchange and finally we consider the privacy implications of other protocol messages, including the failure detection protocol for the SHIM6 protocol.

2. Privacy of the ULID-pair context establishment exchange

The ULID-pair context establishment exchange consists of 4 messages: I1, R1, I2 and R2. We will next analyze the privacy implications of each of them.

The I1 message is exchanged using a valid locator pair in the IPv6 address fields. In addition, the I1 message contains the Initiator context tag and nonce. Besides it can carry additional options. In particular, in case that the locator pair used differs from the ULID pair for the context, an ULID-pair option must be carried in the I1 message.

Among the information carried in the I1 message we consider that the following may have privacy implications if it can be observed by a

third party:

- o The binding between a locator pair and ULID pair if the ULID-pair option is carried in clear text
- o The Context Tag information can be used by an attacker in order to correlate different packets containing different locator pairs. Through this mean, the attacker can learn that multiple locators belong to the same endpoint and that the different packets carrying different address pairs belong to the same communication.

In order to achieve privacy protection, it is required to conceal all this information.

The next message to be exchanged is R1. This message contains a pair of valid locators in the IPv6 address fields and in the message itself, it contains the Initiator nonce and the Responder nonce. In addition, the R1 message support the Validator option, which contain cryptographic information.

The disclosure of any of these elements doesn't seems to raise any privacy concerns, so there does not seem to be any requirement to conceal the information carried in the R1 message.

After the R1 message the ULID-pair context establishment continues with the I2 message. The I2 message is carried in a packet containing again a valid locator pair in the IPv6 header address fields and, in the I2 message itself the Initiator context tag, the Initiator and Responder nonces are conveyed. The I2 message can carry also the following options: ULID pair, Forked Instance Identifier, Locator list, Locator Preferences, CGA Parameter Data Structure and CGA Signature.

Of all the aforementioned information conveyed in the I2 message, we identify the following items that may imply privacy concerns:

- o The Initiator Context tag, for the same reasons than in the I1 message
- o The ULID-pair option, for the same reasons than in the I1 message
- o The locator list option, since it carries the list of locator which disclosure would clearly result in allowing the attacker to identify the multiple locator associated with a single endpoint
- o The CGA parameter data structure option. In this case, it depends of which information is carried in the data structure. If a multiprefix extension is carried i.e. HBA are used, then the information is critical from a privacy perspective, since the information about multiple prefixes and hence about multiple locators is included in the data structure. If the multiprefix extension is not included, then the CGA parameter data structure could be used by an attacker to obtain identifier information (since there is enough information in the data structure to re-

create the associated CGA). So if the CGA is being used as locator in the packet (and no multiprefix extension is being used), then the CGA parameter data structure is not critical from a privacy perspective.

The other information carried in the I2 message is not considered to be critical for preserving the privacy. In particular, the Forked Instance Identifier could be used to correlate different packets, but without knowing the Context tag, the attack seems not very practical. The Locator preference option may inform about the number of locators available and the relative preference between them, but without knowing the actual locators, this information does not seem to be very relevant neither. Finally, the CGA signature information does not seem to provide any useful information for an attacker.

The last packet of the initial exchange is the R2 packet that contains the Responder context tag, and the following potential options: Locator List, Locator Preferences, CGA Parameter Data Structure, CGA Signature. Analogously to the I2 case, the following information needs to be concealed: the Responder context tag, the Locator list option, the CGA Parameter Data structure.

In addition to the four messages of the basic ULID-pair context establishment exchange, there are also two additional messages defined, that need to be analyzed also these are the R1bis packet and the I2bis packet.

The R1bis message is carried in a packet that carries valid locators in the IPv6 address fields and the message itself contains the Packet context tag and the Responder nonce. In addition, it also can carry the Validator option.

Similarly to the R1 packet, the R1bis packet does not carries any critical information from a privacy point of view.

The I2bis message is also carried in a packet that contains valid locators in the IPv6 address fields and it carries the following information in the message: Initiator context tag, the Initiator and Responder nonces and the Packet context tag. In addition it allows the following options: Responder Validator, ULID pair, Forked Instance Identifier, Locator list, Locator Preferences, CGA Parameter Data Structure and the CGA Signature.

Similarly to the previous cases, the following information needs to be concealed in order to preserve privacy: Initiator context Tag, ULID pair option, Locator List option, CGA Parameter Data Structure.

3. Payload packets

Payload packets are data packets that carry the SHIM6 header containing the Payload option. This option carries the Receiver context tag. The main privacy issue related to the Payload packets is that they may change the locator pair used while keeping the Context tag unchanged. The problem with this approach is that an attacker located along the different paths can correlate different packets carrying different locator pairs through the constant context tag included in the payload header. Through this mean, the attacker can determine different locators of the locator set and determine that different packets exchanged belong to a single communication. In order to prevent this privacy breach, it is required that different unrelated context tags are used when the locator pair is changed.

4. Other Signalling messages

In addition to the messages previously analyzed, the SHIM6 protocol also defines the Update Request and Ack messages and the Keepalive and Probe messages. We will next perform the privacy analysis for these messages.

The Update Request carries the Context tag and the request nonce and it supports the following options: Locator List, Locator Preferences, CGA Parameter Data Structure, CGA Signature.

As for the prior analysis, the critical information from a privacy perspective is the following: the context tag (if a different locator pair is being used), the Locator List option, and the CGA parameter data structure (with the considerations described above).

The Update Ack message contains the context tag and the request nonce. If different locator pair is used, the context tag and the request nonce can be used to correlate different packets with different locator pairs. In this case, the context tag and nonce information need to be concealed to protect privacy.

With respect to Keepalive and Probe messages, the critical information contained in those messages is the following: the context tag and the identifier information carried in different options available.

The considerations with respect to the context tag information are similar to the ones already discussed for other messages.

With respect to the Identifier information, this information would

allow the correlation of different Keepalive and Probe packets, allowing then to bind different locators used in different packets. In order to preserve privacy, the Identifier information need to be concealed.

5. Conclusion

It is clear that there is quite a few information included in the SHIM6 protocol that need to be concealed in order to provide privacy support for the SHIM6 protocol. However, it is likely that encrypting the critical information using a shared secret generated through a Diffie Hellman exchange would provide enough protection for most of the cases. There are however two cases that would require additional study: one is the case of the information exchanged in the I1 packet, which is the first message to be exchanged implying that no previous shared secret can possible be exchanged. In order to address this case, or additional prior message exchange is included in the protocol to provide privacy or the critical information is removed from the I1 message. Another case that would require further analysis is the case of the context tag. The context tag is used to demultiplex incoming packet. In order for this to be useful, the context tag needs to be known beforehand by both ends and in order to provide privacy support, the context tag needs to be changed when the locator pair is changed. Mechanisms for changing the context tag depending on the locator pair used can be defined, keeping in mind that the relation between the locator pair and the context tag must remain untraceable for an external observer.

6. Security considerations

This note analyzes the privacy issues of the SHIM6 protocol. Additional security considerations of the SHIM6 protocol are addressed in the protocol specification itself

7. References

[1] Nordmark, E. and M. Bagnulo, "Multihoming L3 Shim Approach", draft-ietf-shim6-l3shim-00 (work in progress), July 2005.

[2] Arkko, J. and I. Beijnum, "Failure Detection and Locator Pair Exploration Protocol for IPv6 Multihoming", draft-ietf-shim6-failure-detection-03 (work in progress), December 2005.

Author's Address

Marcelo Bagnulo
Universidad Carlos III de Madrid
Av. Universidad 30
Leganes, Madrid 28911
SPAIN

Phone: 34 91 6249500
Email: marcelo@it.uc3m.es
URI: http://www.it.uc3m.es

Full Copyright Statement

Intellectual Property

Acknowledgment

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