Authentication-only Mode for Secure DHCPv6
draft-templin-dhc-authonly-sedhcpv6-02.txt

Abstract

Secure DHCPv6 includes mechanisms for encryption and authentication, where encryption is currently mandated due to concerns for pervasive monitoring in the Internet. The Secure DHCPv6 specification states that the mechanisms are applicable in any environment where physical security on the link is not assured and attacks on DHCPv6 are a concern. However, this document presents a reference use case where physical and/or link-layer security are already assured. This document therefore proposes an authentication-only application of Secure DHCPv6 when there is already sufficient protection against pervasive monitoring.

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 March 12, 2017.

Copyright Notice

Copyright (c) 2016 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents.
1. Introduction

DHCPv6 [RFC3315] is the stateful autoconfiguration protocol for IPv6 [RFC2460]. Secure DHCPv6 [I-D.ietf-dhc-sedhcpv6] includes mechanisms for encryption and authentication, where encryption is currently mandated due to concerns for pervasive monitoring in the Internet.

The Secure DHCPv6 specification states that the mechanisms are applicable in any environment where physical security on the link is not assured and attacks on DHCPv6 are a concern. However, this document presents a reference use case where physical and/or link-layer security are already assured. This document therefore proposes an authentication-only application of Secure DHCPv6 when there is already sufficient protection against pervasive monitoring.

Encryption avoidance becomes important when information sharing between DHCPv6 clients, relays and servers is required and/or when an application of an additional layer of encryption would be redundant and would result in poor performance. The document therefore proposes an authentication-only mode for specific use cases where pervasive monitoring is already mitigated through other means, but a means for authenticating the source of the DHCPv6 message is still required.

2. Use Case for Authentication-only Secure DHCPv6

Figure 1 depicts a reference use case for an authentication-only mode for Secure DHCPv6, where the link between the DHCPv6 client and relay is protected by link-layer encryption and the DHCPv6 service infrastructure is protected by physical security:
In this reference use case, the link between the client and relay is secured against pervasive monitoring through the application of link-layer encryption. (The link itself also may or may not be secured at the physical layer.) No information is therefore available in plain text over the link that connects the client and relay. The DHCPv6 service infrastructure (i.e., all DHCPv6 relay agents and servers) is further secured against pervasive monitoring through physical security and the application of network-layer securing mechanisms such as IPsec.

In the reference use case, therefore, no opportunity for pervasive monitoring exists and the use of DHCPv6 application layer encryption would be unnecessary, inefficient and would interfere with client/relay/server information sharing. An example where this use case applies is in the AERO protocol [I-D.templin-aerolink].

This document therefore recommends an amendment of the Secure DHCPv6 specification to permit an authentication-only application of the
protocol when pervasive monitoring is already mitigated through other means.

3. IANA Considerations

This document introduces no IANA considerations.

4. Security Considerations

Security considerations are discussed in the DHCPv6 and Secure DHCPv6 specifications [RFC3315][I-D.ietf-dhc-sedhcpv6]. This document notes that, in addition to protection against pervasive monitoring of DHCPv6 messages, a means for authenticating the sources of DHCPv6 messages may still be necessary in some environments to mitigate insider attacks such as spoofing and theft of service.

5. Acknowledgements

TBD

6. References

6.1. Normative References

[I-D.ietf-dhc-sedhcpv6]


6.2. Informative References

[I-D.templin-aerolink]
Templin, F., "Asymmetric Extended Route Optimization (AERO)", draft-templin-aerolink-71 (work in progress), September 2016.
Author’s Address

Fred L. Templin (editor)
Boeing Research & Technology
P.O. Box 3707
Seattle, WA  98124
USA

Email: fltemplin@acm.org