TOC

Network Working Group	G. Zorn
Internet-Draft	Network Zen
Intended status: Standards Track	Q. Wu
Expires: August 14, 2010	Y. Wang
	Huawei
	February 10, 2010

The Local Domain Name DHCP Option
draft-wu-hokey-ldn-discovery-01

Abstract

In order to derive a Domain-Specific Root Key (DSRK) from the Extended Master Session Key (EMSK) generated as a side-effect of an Extensible Authentication Protocol (EAP) method, the EAP peer must discover the name of the domain to which it is attached.

This document specifies a Dynamic Host Configuration Protocol (DHCP) option designed to allow a DHCP server to inform clients of the name of the local domain..

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

TOC

The EAP Re-authentication Protocol (ERP) [RFC5296] (Narayanan, V. and L. Dondeti, “EAP Extensions for EAP Re-authentication Protocol (ERP),” August 2008.) is designed to allow faster re-authentication of a mobile device which was previously authenticated by means of the Extensible Authentication Protocol (EAP, [RFC3748] (Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, “Extensible Authentication Protocol (EAP),” June 2004.). Considering that the local root key (e.g., DSRK [RFC5295] (Salowey, J., Dondeti, L., Narayanan, V., and M. Nakhjiri, “Specification for the Derivation of Root Keys from an Extended Master Session Key (EMSK),” August 2008.)) is generated using the local domain name (LDN), LDN discovery is an important part of re-authentication. As described in RFC 5296 [RFC5296] (Narayanan, V. and L. Dondeti, “EAP Extensions for EAP Re-authentication Protocol (ERP)," August 2008.), the local domain name can be learned by the mobile device through the ERP exchange or via a lower-layer mechanism. However, no lower-layer mechanisms for LDN discovery have yet been defined.

This document specifies an extension to DHCP for local domain name discovery.

2. Terminology

TOC

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.).

3. Option Format

TOC

In DHCPv6-based local domain name discovery, the LDN option is used by the DHCPv6 client (MD) to obtain the local domain name from the DHCP Server after full EAP authentication has taken place.

3.1. DHCPv6 Local Domain Name Option

TOC

The format of this option is:

```
     0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     | OPTION_LOCAL_DOMAIN_NAME      |         option-length         |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |             local-domain-name ...
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 1

option code OPTION_LOCAL_DOMAIN_NAME (TBD)

option-length

Length of the ‘local domain name’ field in octets

local-domain-name This field contains the name of the local domain and MUST be encoded as specified in Section "8 of RFC 3315 (Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, “Dynamic Host Configuration Protocol for IPv6 (DHCPv6),” July 2003.) [RFC3315]

4. Appearance of the Option

TOC

The LDN option MUST NOT appear in DHCPv6 messages other than the types Solicit, Advertise, Request, Information-Request and Reply. The option-code of the LDN option MAY be included in the Option Request Option in the DHCPv6 message types Solicit, Request and Information-Request.

5. Client Behavior

TOC

If a DHCPv6 client (MD) doesn't know the local domain name and requires the DHCP Server to provide the DHCPv6 LDN option, it MUST include an Option Request option requesting the DHCPv6 LDN option, as described in Section 22.7 of RFC 3315 [RFC3315] (Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, “Dynamic Host Configuration Protocol for IPv6 (DHCPv6),” July 2003.).
When the DHCPv6 client recieves a LDN option with the local domain name present in it, it MUST verify that the option length is no more than 256 octets (the maximum length of a single FQDN allowed by DNS), and that the local domain name is a properly encoded single FQDN, as specified in Section 8 "Representation and Use of Domain Names" of the RFC3315 [RFC3315] (Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, “Dynamic Host Configuration Protocol for IPv6 (DHCPv6),” July 2003.).

6. Relay Agent Behavior

TOC

If a DHCPv6 relay agent has pre-existing knowledge of the local domain name (for example, from a previous AAA exchange), it SHOULD include it in the DHCPv6 LDN option and forward to the DHPv6 server.

7. Server Behavior

TOC

If the option code for the LDN option is included in an Option Request option, the server SHOULD return the DHCPv6 LDN option to the client. If a DHCPv6 LDN option is received from a relay agent with a non-empty local-domain-name field, the server SHOULD extract this option and include it in the reply message.

8. Security Considerations

TOC

The communication between the DHCP client and the DHCP server for the exchange of local domain name information is security sensitive and requires authentication, integrity and replay protection. Either lower-layer security (such as link layer security established as part of the network access authentication protocol run) or DHCP security [RFC3118] (Droms, R. and W. Arbaugh, “Authentication for DHCP Messages,” June 2001.) can be used.

9. IANA considerations

TOC

IANA is requested to allocate one DHCPv6 Option code, referencing this document.

10. References

TOC

10.1. Normative References

TOC

[RFC2119]	Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[RFC3315]	Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, “Dynamic Host Configuration Protocol for IPv6 (DHCPv6),” RFC 3315, July 2003 (TXT).
[RFC5295]	Salowey, J., Dondeti, L., Narayanan, V., and M. Nakhjiri, “Specification for the Derivation of Root Keys from an Extended Master Session Key (EMSK),” RFC 5295, August 2008 (TXT).
[RFC5296]	

	Narayanan, V. and L. Dondeti, “EAP Extensions for EAP Re-authentication Protocol (ERP),” RFC 5296, August 2008 (TXT).

10.2. Informative References

TOC

[RFC3118]	Droms, R. and W. Arbaugh, “Authentication for DHCP Messages,” RFC 3118, June 2001 (TXT).
[RFC3748]	Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, “Extensible Authentication Protocol (EAP),” RFC 3748, June 2004 (TXT).

Authors' Addresses

TOC

Glen Zorn
Network Zen
1463 East Republican Street
Seattle, Washington 98112
USA
Phone: +1 206 931 0768
EMail: gwz@net-zen.net

Qin Wu
Huawei Technologies Co., Ltd.
Site B, Floor 12, Huihong Mansion, No.91 Baixia Rd.
Nanjing, Jiangsu 21001
China
Phone: +86-25-84565892
EMail: sunseawq@huawei.com

Yungui Wang
Huawei Technologies Co., Ltd.
Site B, Floor 10, HuiHong Mansion, No.91 BaiXia Rd.
Nanjing, Jiangsu 210001
P.R. China
Phone: +86 25 84565893
EMail: w52006@huawei.com