ALTO	M. Stiemerling	
Internet-Draft	NEC Europe Ltd.	
Intended status: Standards Track	H. Tschofenig	
Expires: January 28, 2011	Nokia Siemens Networks	
	July 27, 2010	

TOC

A DNS-based ALTO Server Discovery Procedure
draft-stiemerling-alto-dns-discovery-00.txt

Abstract

The Application-Layer Traffic Optimization (ALTO) provides guidance to applications having to select one or several hosts from a set of candidates that are able to provide a desired resource.
This document specifies the U-NAPTR based resolution process.

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 28, 2011.

Copyright Notice

Table of Contents

1. Introduction

TOC

Networking applications today already have access to a great amount of Inter-Provider network topology information. For example, views of the Internet routing table are easily available at looking glass servers and entirely practical to be downloaded by clients. What is missing is knowledge of the underlying network topology from the ISP or Content Provider (henceforth referred as Provider) point of view. In other words, what a Provider prefers in terms of traffic optimization -- and a way to distribute it.

The ALTO Service provides information such as preferences of network resources with the goal of modifying network resource consumption patterns while maintaining or improving application performance. This document describes a protocol implementing the ALTO Service. While such service would primarily be provided by the network (i.e., the ISP), content providers and third parties could also operate this service. Applications that could use this service are those that have a choice in connection endpoints. Examples of such applications are peer-to-peer (P2P) and content delivery networks.

This document specifies the U-NAPTR based resolution process. To start the U-NAPTR resolution process a domain name needs to be obtained first. One mechanism to obtain such a domain name is via DHCP, as described in [I-D.ietf-geopriv-lis-discovery] (Thomson, M. and J. Winterbottom, “Discovering the Local Location Information Server (LIS),” March 2010.).

2. Terminology

TOC

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and

"OPTIONAL" are to be interpreted as described in RFC 2119 [RFC2119] (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.).

---

3. U-NAPTR Resolution

TOC

ALTO servers are identified by U-NAPTR/DDDS (URI-Enabled NAPTR/Dynamic Delegation Discovery Service) [RFC4848] (Daigle, L., “Domain-Based Application Service Location Using URIs and the Dynamic Delegation Discovery Service (DDDS),” April 2007.) application unique strings, in the form of a DNS name. An example is 'altoserver.example.com'.
Clients need to use the U-NAPTR [RFC4848] (Daigle, L., “Domain-Based Application Service Location Using URIs and the Dynamic Delegation Discovery Service (DDDS),” April 2007.) specification described below to obtain a URI (indicating host and protocol) for the applicable ALTO service. In this document, only the HTTP and HTTPS URL schemes are defined. Note that the HTTP URL can be any valid HTTP URL, including those containing path elements.
The following two DNS entries show the U-NAPTR resolution for "example.com" to the HTTPS URL https://altoserver.example.com/secure or the HTTP URL http://altoserver.example.com, with the former being preferred.

```
example.com.

IN NAPTR 100  10   "u"    "ALTO:https"
     "!.*!https://altoserver.example.com/secure!"  ""

IN NAPTR 200  10   "u"    "ALTO:http"
     "!.*!http://altoserver.example.com!"  ""
```

End host learn the ALTO's server host name by means beyond the scope of this specification, such as DHCP.

---

4. IANA Considerations

TOC

This document registers the following U-NAPTR application service tag:

> **Application Service Tag:** ALTO
>
> **Defining Publication:** The specification contained within this document.

This document registers the following U-NAPTR application protocol tags:

*Application Protocol Tag: http

Defining Publication: RFC 2616 (Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1," June 1999.) [RFC2616]

*Application Protocol Tag: https

Defining Publication: RFC 2818 (Rescorla, E., "HTTP Over TLS," May 2000.) [RFC2818]

---

5. Security Considerations

TOC

The address of a ALTO is usually well-known within an access network; therefore, interception of messages does not introduce any specific concerns.
The primary attack against the methods described in this document is one that would lead to impersonation of a ALTO server since a device does not necessarily have a prior relationship with a ALTO server.
An attacker could attempt to compromise ALTO discovery at any of three stages:

1. 1. providing a falsified domain name to be used as input to U-NAPTR
2. 2. altering the DNS records used in U-NAPTR resolution
3. 3. impersonation of the ALTO

This document focuses on the U-NAPTR resolution process and hence this section discusses the security considerations related to the DNS handling. The security aspects of obtaining the domain name that is used for input to the U-NAPTR process is described in respective documents, such as [I-D.ietf-geopriv-lis-discovery] (Thomson, M. and J. Winterbottom, "Discovering the Local Location Information Server (LIS)," March 2010.).
The domain name that is used to authenticated the ALTO server is the domain name in the URI that is the result of the U-NAPTR resolution. Therefore, if an attacker were able to modify or spoof any of the DNS records used in the DDDS resolution, this URI could be replaced by an invalid URI. The application of DNS security (DNSSEC) [RFC4033] (Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements," March 2005.) provides a means to limit attacks that rely on modification of the DNS records used in U-NAPTR

resolution. Security considerations specific to U-NAPTR are described in more detail in [RFC4848] (Daigle, L., “Domain-Based Application Service Location Using URIs and the Dynamic Delegation Discovery Service (DDDS),” April 2007.).

An "https:" URI is authenticated using the method described in Section 3.1 of [RFC2818] (Rescorla, E., “HTTP Over TLS,” May 2000.). The domain name used for this authentication is the domain name in the URI resulting from U-NAPTR resolution, not the input domain name as in [RFC3958] (Daigle, L. and A. Newton, “Domain-Based Application Service Location Using SRV RRs and the Dynamic Delegation Discovery Service (DDDS),” January 2005.). Using the domain name in the URI is more compatible with existing HTTP client software, which authenticate servers based on the domain name in the URI.

An ALTO server that is identified by an "http:" URI cannot be authenticated. If an "http:" URI is the product of the ALTO discovery, this leaves devices vulnerable to several attacks. Lower layer protections, such as layer 2 traffic separation might be used to provide some guarantees.

---

6. Acknowledgements

TOC

The authors would like to thank Martin Thomson for his feedback on this document. We would like to thank the ALTO working group for their prior discussions on discovery.

---

7. References

TOC

7.1. Normative References

TOC

[RFC2119]	Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” RFC 2119, BCP 14, March 1997.
[RFC2616]	Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, “Hypertext Transfer Protocol -- HTTP/1.1,” RFC 2616, June 1999 (TXT, PS, PDF, HTML, XML).
[RFC2818]	Rescorla, E., “HTTP Over TLS,” RFC 2818, May 2000 (TXT).
[RFC3958]	Daigle, L. and A. Newton, “Domain-Based Application Service Location Using SRV RRs and the Dynamic Delegation Discovery Service (DDDS),” RFC 3958, January 2005 (TXT).
[RFC4033]	

	Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements," RFC 4033, March 2005 (TXT).

7.2. Informative References

TOC

[I-D.ietf-geopriv-lis-discovery]	Thomson, M. and J. Winterbottom, "Discovering the Local Location Information Server (LIS)," draft-ietf-geopriv-lis-discovery-15 (work in progress), March 2010 (TXT).
[RFC4848]	Daigle, L., "Domain-Based Application Service Location Using URIs and the Dynamic Delegation Discovery Service (DDDS)," RFC 4848, April 2007 (TXT).

Authors' Addresses

TOC

	Martin Stiemerling
	NEC Laboratories Europe/University of Goettingen
	Kurfuerstenanlage 36
	Heidelberg 69115
	Germany
Phone:	+49 6221 4342 113
Fax:	+49 6221 4342 155
Email:	martin.stiemerling@neclab.eu
URI:	http://ietf.stiemerling.org
	Hannes Tschofenig
	Nokia Siemens Networks
	Linnoitustie 6
	Espoo 02600
	Finland
Phone:	+358 (50) 4871445
Email:	Hannes.Tschofenig@gmx.net
URI:	http://www.tschofenig.priv.at