INTERNET-DRAFT
Intended Status: Proposed Standard
Expires: June 14, 2016

Piotr Kupisiewicz
(Cisco Systems)
February 1, 2016

DNS Extension to provide Default (Preferred) Protocol
draft-pkupisie-dnsop-dprot-01

Abstract

This document defines extension to the Domain Name System to support Default Protocol. Default Protocol extension allows owners of the resources to determine which are preferred protocols to be used with their Services (i.e. https protocol to be preferred instead of http for specific servers).

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

Copyright and License Notice

Table of Contents

1 Introduction 3
1.1 State of Art 3
1.2 Terminology 4
2 Publishing 4
4 Application side implementation 4
4.1 Application implementation: Various Service Types 5
5 DNS Security Considerations 5
5 References 5
5.1 Normative References 5
5.2 Informative References 6
Authors' Addresses 6

1 Introduction

Currently applications are not able to determine what are default protocols which are used for specific Internet hosts.

Taking Web Browser as an example: It is relying on user to choose http [RFC2616] or https [RFC2818] during initial connection. If user specifies http://rfc-editor.org initial connection will be done using http on port 80, if user enters https://rfc-editor.org Browser will use https as protocol on port 443.

However, If user does not specify protocol at all (i.e. puts in the address bar of Web Browser rfc-editor.org instead of http://rfc-editor.org or https://rfc-editor.org), application needs to decide which protocol should be used. This is done based on local settings (i.e. default configuration of Web Browser) and usually is not host-specific. Most of current Web Browsers will use http:// as default protocol (with some exceptios, see chapter 1.1 "State of Art")

If specific service i.e. Online Banking wants to recommend specific protocol, it might use application layer protocol to redirect the application to different protocol. For example if initial connection is done to http://rfc-editor.org, there might be Redirect message (HTTP 302) used to redirect Browser to https://rfc-editor.org (alternatively html redirect might be used).

In that scenario redirect is done using non-secure connection (http), which allows potential man-in-the-middle attacker to redirect user to different webpage, or perform redirect using the same non-secure protocol (http://rfc.org redirecting to http://rfc.org/index.html instead of https://rfc.org/index.html).

Essentially applications are relying on user to choose proper protocol. If user does not specify protocol applications need to choose specific protocol (for user's convenience).

Aim of Default Protocol extension is to allow Service Owner i.e. Online Banking Service to specific that for that specific host given default protocol will be used. I.e. for rfc-editor.org default protocol could say that default protocol is https, allowing browser to directly attempt https as initial connection. VPN Terminator owner could say that ISAKMP protocol is preferred over SSL etc.

1.1 State of Art

One of similar solutions (limited to Web only though) is HTTP Strict Transport Security (HSTS) [HSTS]. Disadvantage of HSTS is that initial connection is still done using HTTP unless address is

statically defined, in browser, as HTTPS only (HSTS Pre-Loaded List). Since this does not scale and it is Web specific, DPROT is being proposed (not as alternative to HSTS, but more as supplement to replace HSTS Pre-Loaded List).

Taking other examples (different than HSTS limited to Web only):- One might want to suggest ISAKMP instead of SSL while connecting to VPN Gateway, not leaving decision to end-user. - One might want to suggest IMAPS to be used instead of POP3S (both might be allowed, but one might be preferred)

1.2 Terminology

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 RFC 2119 [RFC2119].

2 Publishing

Domain owners who would like to specify default protocols for specific ports MUST use TXT extensions in following format:

```
rfc-editor.org       TXT  "DPROT=https"

rfc-editor.org       TXT  "DPROT=ssh"

rfc-editor.org       TXT  "DPROT=isakmp"

192.168.10.15        TXT  "DPROT=https"
```

Protocol names should be used as defined by IANA in [RFC6335] and [IANA_PORTS]

4 Application side implementation

Implementation on the Application side queries it's DNS Server for TXT record type entries for the host that Application is about to connect to (unless protocol is specifically given by user, i.e. by using http:// specifically in the Web Browser).

For example Web Browser after user puts rfc-editor.org (without protocol) in the address bar, queries DNS Server for TXT query type with host rfc-editor.org. DNS returns entry:

```
rfc-editor.org       TXT  "DPROT=https"
```

Based on that Web Browser MUST use https://rfc.org as initial

connection attempt.

If the https connection fails Web Browser SHOULD alert the user and by default not attempt to fallback to http protocol. Fallback to different protocol SHOULD happen only after explicit customer's permission.

In case there is no DPROT entry for specific host, it's up to application's implementation on which protocol should be used.

4.1 Application implementation: Various Service Types It might happen that for specific host there will be multiple different default

protocols specified for multiple different type of services (Web/VPN/Remote Connection etc.). In example: rfc-editor.org TXT "DPROT=https"

```
rfc-editor.org       TXT  "DPROT=ssh"

rfc-editor.org       TXT  "DPROT=ipsec"
```

It's up to application to understand which protocols are relevant to the specific use cases. Web Browser SHOULD be aware that https is relevant, ignoring ssh and ipsec.

5 DNS Security Considerations

Hence original DNS design does not provide any mechanism to prevent man-in-middle attacks, DNS Security solutions like DNSSEC SHOULD be used [DNSSEC].

In addition entries in DPROT, SHOULD be specify protocol only, it SHOULD NOT contain addition protocol's specific information (like suggested ciphers).

5 References

5.1 Normative References

[KEYWORDS] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC1776] Crocker, S., "The Address is the Message", RFC 1776, April 1 1995.

[TRUTHS] Callon, R., "The Twelve Networking Truths", RFC 1925, April 1 1996.

5.2 Informative References

[DNSSEC] D. Eastlake, "Domain Name System Security Extensions", RFC 2535, March 1999

[HSTS] J. Hodges, C. Jackson, A. Barth, "HTTP Strict Transport Security (HSTS)", RFC 6797, November 2012

[IANA_PORTS] http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.txt

Authors' Addresses

Piotr Kupisiewicz

EMail: pkupisie@cisco.com