User Agent Connection Security  
draft-ietf-ua-conn-sec-00.txt

**Abstract**

The user agent to server transaction has many attack surfaces which have been defended by various recommendations such as Content Security Policy. An attack vector that is currently exploited is the open connection policy to first, second- and third-party resources.

A breach of the origin website or other connected resource could require the client to load resources from a malicious network. This document provides a framework which allows authors to publish authorized connectable second- and third-party resources that a user agent should or must follow depending on configuration of that user agent.

**Status of this Memo**

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/ietf/1id-abstracts.txt

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

This Internet-Draft will expire on September 13 2023.

Copyright Notice

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 carefully, as they describe your rights and restrictions with respect to this document.

Table of Contents

[1 Introduction 2](#__RefHeading___Toc258322660)

[1.1 Terminology 3](#__RefHeading___Toc425_245583736)

[1.2 Applicability 3](#__RefHeading___Toc427_245583736)

[2 Conventions used in this document 3](#__RefHeading___Toc2583226761)

[2.1 DNS Entries published 3](#__RefHeading___Toc429_245583736)

[2.1.1 Single site and domain example 3](#__RefHeading___Toc431_245583736)

[2.1.2 Multiple sites and domain example 4](#__RefHeading___Toc433_245583736)

[2.1.3 Wildcards 4](#__RefHeading___Toc435_245583736)

[3 Security Considerations 5](#__RefHeading___Toc258322676)

[4 IANA Considerations 6](#__RefHeading___Toc258322677)

[5 References 6](#__RefHeading___Toc258322679)

[5.1 Normative References 6](#__RefHeading___Toc258322680)

[5.2 Informative References 7](#__RefHeading___Toc258322681)

[6 Acknowledgments 7](#__RefHeading___Toc258322682)

# **Introduction**

The traditional website model for distributing information has been one of open resource connections. Website authors are in control as to how the published resource connections draw upon other resources. This model leaves end-users and administrators who require higher connection security to either trust the site author implicitly or profile a website and provide connection security through other means.

Establishing a trust model where all connections are approved by both parties, is an additional step in providing a model where users and administrators can be assured the website they are using is making author-verified connections to second- and third-parties.

This document covers an implementation for website authors to indicate a validation method of second- and third-party resources and a strict or compatible model for browser owners to enforce depending on their security requirements.

# **1.1 Terminology**

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

# **1.2 Applicability**

This document covers a method of actions user-agents and website authors should implement to enhance security.

# **Conventions used in this document**

First-party connections are those created to the same host listed in the URL.

Second-party connections are those created to other hosts using the same top level domain

Third-party connections are those to a host with a different host listed in the URL

# **2.1 DNS Entries published**

The DNS entry is a TXT record. The format of the record begins with uacs=1; and an optional host= identifier, if the domain serves multiple hostnames which require user-agent connection security.

Every semi-colon separated entry after it must be a RFC1123 or RFC2732 formatted host identifier.

# **2.1.1 Single site and domain example**

An example record for a single website hosted from a domain:

uacs=1;host.example1.com;\*.example2.com;zzzzzzz.example-cloud-network.net

# **2.1.2 Multiple sites and domain example**

If a domain serves multiple websites requiring user-agent connection security, these records MUST be broken up into separate TXT records with an identifying host tag:

uacs=1;host=website1.example.com;host.example1.com;\*.example2.com

uacs=1;host=website2.example.com;host.example1.com;\*.example2.com

Hostname entries are separated by semicolons and no spaces. Where characters have case representations, all characters should be in lower case versions.

# **2.1.3 Wildcards**

Wildcards are allowed to reduce record sizes and client processing time, for example a website hosted at example1.com can include resources from \*.example2.com in order to accommodate changes example2.com may publish to their service.

The wildcard MUST be interpreted as meaning 0 or more characters.

Caution should be used when using wildcards with services that publish random hostnames for customers since site authors may not intend for data from other customers to be referenced. For example, a content distribution network may create content access URIs such as 123456.example.net for every customer. A wildcard against this network would grant resource load opportunities for any non-related customers of that service.

Only one uacs= and one host= are allowed per TXT record.

**2.2 User-Agent Requests**

User-Agents SHOULD include the TXT record request at the time of the DNS request to resolve the host name, should subsequently send the request to retrieve the uacs= TXT record prior to processing any further connection requests other than the initial resource request.

**2.3 Caching**

User-Agents SHOULD follow their normal caching rules for the TXT records request.

**2.4 User-Agent Enforcement Modes**

Compatible, Compliant, Strict

**2.4.1 Compatible mode**

Compatible mode is included as a transition option. This mode indicates the user-agent SHOULD NOT enforce any uacs entries

**2.4.2 Compliant mode**

Compliant mode indicates the user-agent MUST process and follow the rules identified by a website author.

**2.4.3 Strict mode**

Strict mode indicates the user-agent should not connect to any resources beyond the domain.

**2.5 Record Size**

Published records SHOULD be limited to fit within the 512 octet limit. If not, it could exceed the DNS protocol limit. For further details on the technical details, please see RFC4408 section 3.1.4 entitled Record Size. It is RECOMMENDED to follow these directions.

# **Security Considerations**

3.1 Sensible initial defaults

The initial compatible user agent mode was chosen as a lead in order to provide a path for adoption due to this RFC requiring changes from both website operators and developers of user-agents.

**3.2 DNS TXT versus a text file**

The DNS TXT entry was chosen after working through a model with a plain text file, similar to security.txt or a robots.txt file. After consideration, one of the defensive tactics for UACS is to protect a client against a server compromise attack in which a text file could be replaced by an attacker. Having the approved connections list separate provides an additional layer of defense.

**3.3 Misconfigurations**

It is possible to configure the connection host entries too inclusively thereby allowing connections to unintended hosts and degrading the security posture this RFC is proposing.

**3.4 Profiling**

A profile-building model of security is prone to functional deferred deprecation upon website updates. For organizations managing security profiles, not every security administrator is willing to trust every website vendor implicitly, and not every website vendor openly discloses every third-party resource connection.

Attacks that leverage injectionable payloads from second- and third-party connections require an open connection to an attacker-controlled resource. Limiting attacks with connection restrictions such as this RFC reduces the available options an attacker may use and improves the security posture of the user agent.

# **IANA Considerations**

This draft does not require any IANA action.

# **References**

## **Normative References**

1. [RFC1034] Mockapetris, P., "Domain names - concepts and facilities", RFC 1034, DOI 10.17487/RFC1034, November 1987, <<https://www.rfc-editor.org/info/rfc1034>>
2. [RFC1035] Mockapetris, P., "Domain names - implementation and specification", [RFC 1035](https://datatracker.ietf.org/doc/html/rfc1035), November 1987.
3. [RFC1123] Braden, R., "Requirements for Internet Hosts – Application and Support", [RFC 1123](https://datatracker.ietf.org/doc/html/rfc1123), October 1989
4. [RFC2181] Elz, R., “Clarifications to the DNS Specification”, [RFC 2181](https://datatracker.ietf.org/doc/html/rfc2181), July 1997
5. [RFC2732] Hinden, R., Carpenter, B., Masinter, L., “Format for Literal IPv6 Addresses in URL’s”, , RFC 2732, December 1999
6. [RFC4343] Eastlake 3rd, D., “Domain Name System (DNS) Case Insensitivity Clarification”, [RFC 4343](https://datatracker.ietf.org/doc/html/rfc4343), January 2006
7. [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, [RFC 2119](https://datatracker.ietf.org/doc/html/rfc2119), March 1997.
8. [RFC2234] Crocker, D. and Overell, P.(Editors), "Augmented BNF for Syntax Specifications: ABNF", [RFC 2234](https://datatracker.ietf.org/doc/html/rfc2234), Internet Mail Consortium and Demon Internet Ltd., November 1997.

# **Acknowledgments**

The author would like to thank Steven Hart, Michael J. Calaletto, Yulia Slesavara and the many other team members who contributed suggestions and edits to help complete this document.

This document was prepared using 2-Word-v2.0.template.dot.

Authors’ Addresses

David Steckbeck

Email: dsteckbeck@gatech.edu