Internet Engineering Task Force (IETF)
Request for Comments: 7686
Category: Standards Track
ISSN: 2070-1721

J. Appelbaum
The Tor Project, Inc.
A. Muffett
Facebook

October 2015

The ".onion" Special-Use Domain Name

Abstract

This document registers the ".onion" Special-Use Domain Name.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7686.

Table of Contents

1. Introduction

The Tor network [Dingledine2004] has the ability to host network services using the ".onion" Special-Use Top-Level Domain Name. Such names can be used as other domain names would be (e.g., in URLs [RFC3986]), but instead of using the DNS infrastructure, .onion names functionally correspond to the identity of a given service, thereby combining location and authentication.

.onion names are used to provide access to end to end encrypted, secure, anonymized services; that is, the identity and location of the server is obscured from the client. The location of the client is obscured from the server. The identity of the client may or may not be disclosed through an optional cryptographic authentication process.

.onion names are self-authenticating, in that they are derived from the cryptographic keys used by the server in a client-verifiable manner during connection establishment. As a result, the cryptographic label component of a .onion name is not intended to be human-meaningful.

The Tor network is designed to not be subject to any central controlling authorities with regards to routing and service publication, so .onion names cannot be registered, assigned, transferred or revoked. "Ownership" of a .onion name is derived solely from control of a public/private key pair that corresponds to the algorithmic derivation of the name.

In this way, .onion names are "special" in the sense defined by Section 3 of [RFC6761]; they require hardware and software implementations to change their handling in order to achieve the desired properties of the name (see Section 4). These differences are listed in Section 2.

Like Top-Level Domain Names, .onion names can have an arbitrary number of subdomain components. This information is not meaningful to the Tor protocol, but can be used in application protocols like HTTP [RFC7230].

Note that .onion names are required to conform with DNS name syntax (as defined in Section 3.5 of [RFC1034] and Section 2.1 of [RFC1123]), as they will still be exposed to DNS implementations.

See [tor-address] and [tor-rendezvous] for the details of the creation and use of .onion names.

1.1. Notational Conventions

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].

2. The ".onion" Special-Use Domain Name

These properties have the following effects upon parties using or processing .onion names (as per [RFC6761]):

1. Users: Human users are expected to recognize .onion names as having different security properties (see Section 1) and also as being only available through software that is aware of .onion names.

2. Application Software: Applications (including proxies) that implement the Tor protocol MUST recognize .onion names as special by either accessing them directly or using a proxy (e.g., SOCKS [RFC1928]) to do so. Applications that do not implement the Tor protocol SHOULD generate an error upon the use of .onion and SHOULD NOT perform a DNS lookup.

3. Name Resolution APIs and Libraries: Resolvers MUST either respond to requests for .onion names by resolving them according to [tor-rendezvous] or by responding with NXDOMAIN [RFC1035].

4. Caching DNS Servers: Caching servers, where not explicitly adapted to interoperate with Tor, SHOULD NOT attempt to look up records for .onion names. They MUST generate NXDOMAIN for all such queries.

5. Authoritative DNS Servers: Authoritative servers MUST respond to queries for .onion with NXDOMAIN.

6. DNS Server Operators: Operators MUST NOT configure an authoritative DNS server to answer queries for .onion. If they do so, client software is likely to ignore any results (see above).

7. DNS Registries/Registrars: Registrars MUST NOT register .onion names; all such requests MUST be denied.

Note that the restriction upon the registration of .onion names does not prohibit IANA from inserting a record into the root zone database to reserve the name.

Likewise, it does not prevent non-DNS service providers (such as trust providers) from supporting .onion names in their applications.

3. IANA Considerations

This document registers ".onion" in the registry of Special-Use Domain Names [RFC6761]. See Section 2 for the registration template.

4. Security Considerations

The security properties of .onion names can be compromised if, for example:

- The server "leaks" its identity in another way (e.g., in an application-level message), or
- The access protocol is implemented or deployed incorrectly, or
- The access protocol itself is found to have a flaw.

Users must take special precautions to ensure that the .onion name they are communicating with is the intended one, as attackers may be able to find keys that produce service names that are visually or semantically similar to the desired service. This risk is magnified because .onion names are typically not human-meaningful. It can be mitigated by generating human-meaningful .onion names (at considerable computing expense) or through users using bookmarks and other trusted stores when following links.

Also, users need to understand the difference between a .onion name used and accessed directly via Tor-capable software, versus .onion subdomains of other top-level domain names and providers (e.g., the difference between example.onion and example.onion.tld).

The cryptographic label for a .onion name is constructed by applying a function to the public key of the server, the output of which is rendered as a string and concatenated with the string .onion. Dependent upon the specifics of the function used, an attacker may be able to find a key that produces a collision with the same .onion name with substantially less work than a cryptographic attack on the full strength key. If this is possible the attacker may be able to impersonate the service on the network.

A legacy client may inadvertently attempt to resolve a .onion name through the DNS. This causes a disclosure that the client is attempting to use Tor to reach a specific service. Malicious resolvers could be engineered to capture and record such leaks, which might have very adverse consequences for the well-being of the user. This issue is mitigated if the client's software is updated to not leak such queries or updated to support [tor-rendezvous], or if the client's DNS software is updated to drop any request to the .onion special-use domain name.

5. References

5.1. Normative References

[Dingledine2004]
Dingledine, R., Mathewson, N., and P. Syverson, "Tor: The Second-Generation Onion Router", August 2004, <https://svn.torproject.org/svn/projects/design-paper/tor-design.html>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC6761] Cheshire, S. and M. Krochmal, "Special-Use Domain Names", RFC 6761, DOI 10.17487/RFC6761, February 2013, <http://www.rfc-editor.org/info/rfc6761>.

[tor-address]
Mathewson, N. and The Tor Project, "Special Hostnames in Tor", 2006, <https://spec.torproject.org/address-spec>.

[tor-rendezvous]
The Tor Project, "Tor Rendezvous Specification", April 2014, <https://spec.torproject.org/rend-spec>.

5.2. Informative References

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, DOI 10.17487/RFC1034, November 1987, <http://www.rfc-editor.org/info/rfc1034>.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <http://www.rfc-editor.org/info/rfc1035>.

[RFC1123] Braden, R., Ed., "Requirements for Internet Hosts - Application and Support", STD 3, RFC 1123, DOI 10.17487/RFC1123, October 1989, <http://www.rfc-editor.org/info/rfc1123>.

[RFC1928] Leech, M., Ganis, M., Lee, Y., Kuris, R., Koblas, D., and L. Jones, "SOCKS Protocol Version 5", RFC 1928, DOI 10.17487/RFC1928, March 1996, <http://www.rfc-editor.org/info/rfc1928>.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, <http://www.rfc-editor.org/info/rfc3986>.

[RFC7230] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing", RFC 7230, DOI 10.17487/RFC7230, June 2014, <http://www.rfc-editor.org/info/rfc7230>.

Acknowledgements

Thanks to Roger Dingledine, Linus Nordberg, and Seth David Schoen for their input and review.

This specification builds upon previous work by Christian Grothoff, Matthias Wachs, Hellekin O. Wolf, Jacob Appelbaum, and Leif Ryge to register .onion in conjunction with other, similar Special-Use Top-Level Domain Names.

Authors' Addresses

Jacob Appelbaum
The Tor Project, Inc. & Technische Universiteit Eindhoven

Email: jacob@appelbaum.net

Alec Muffett
Facebook

Email: alecm@fb.com