TRAM
Internet-Draft
Intended status: Standards Track
Expires: April 20, 2015

M. Petit-Huguenin
Impedance Mismatch
O. Johansson
Edvina AB
G. Salgueiro
Cisco Systems
October 17, 2014

Using DNS-based Authentication of Named Entities (DANE) to validate TLS certificates for the Session Traversal Utilities for NAT (STUN) protocol

draft-petithuguenin-tram-stun-dane-02

Abstract

This document defines how DNS-based Authentication of Named Entities (DANE) can be used to validate TLS certificates with the Session Traversal Utilities for NAT (STUN) protocol.

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 April 20, 2015.

Copyright Notice

Table of Contents

1. Introduction

This document defines how DNS-based Authentication of Named Entities [RFC6698] (DANE) can be used to validate TLS certificates with the Session Traversal Utilities for NAT [RFC5389] (STUN) protocol.

STUN [RFC5389] uses Transport Layer Security [RFC5246] (TLS) as a secure transport and [RFC7350] subsequently added Datagram Transport Layer Security [RFC6347] (DTLS) as a secure transport more suited for the originally intended purpose of STUN, which is to support multimedia sessions. Both transports require to have the certificate presented by the server validated following the rules established by [RFC2818]. Additionally [RFC5389] provides rules on how to use DNS SRV Resource Records [RFC2782] to resolve a domain name to a list of host name for the purpose of load balancing and increased reliability. These rules were subsequently enhanced to support S-NAPTR Resource Records [RFC5928] to add the possibility of selecting the preferred transport and redirect between domains.

DANE [RFC6698] improves the mechanism established by [RFC2818] by enabling the administrators of domain names to specify the public keys (either in an X.509 certificate or in a SubjectPublicKeyInfo structure [RFC5280]) used by the secure servers in their domains. The benefits of this approach encompass increasing flexibility, getting less reliance on trust anchors, enabling Perfect Forward Secrecy (PFS) and much more.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119] when they appear in ALL CAPS. When these words are not in ALL CAPS (such as "must" or "Must"), they have their usual English meanings, and are not to be interpreted as RFC 2119 key words.

"Source Domain" and "Host Name" are defined in [I-D.ietf-dane-srv].

3. Operations

STUN clients that are conform with this specification, and that are using one or more DNS lookups to find the server, and that have established that all DNS Resource Records from the Source Domain to the Host Name are secure according to DNSsec [RFC4033] (i.e. that the AD bit is set in all the DNS answers), and that have selected a secure protocol (e.g. TLS or DTLS) MUST lookup for a TLSA Resource Record for the protocol, port and Host Name selected. If the TLSA Resource Record is secure then the STUN client MUST use it to validate the certificate presented by the STUN server. If there is no TLSA Resource Record or if the Resource Record is not secure, then the client MUST fallback to the validation process defined in [RFC5389] and [RFC7350].

Note that only STUN Usages where the connection is the result of a DNS lookup are to be used with DANE which, for the list of STUN Usages listed in [RFC7350], means these:

NAT Discovery Usage

NAT Behavior Discovery Usage

TURN Usage

4. Security Considerations

Using DANE as (D)TLS certificate validation mechanism does not introduce any specific security considerations beyond those for STUN over TLS detailed in [RFC5389] and those for STUN over DTLS detailed in [RFC7350].

5. IANA Considerations

This document has no IANA actions.

6. References

6.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, 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.

[RFC2782] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, February 2000.

[RFC2818] Rescorla, E., "HTTP Over TLS", RFC 2818, May 2000.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC5389] Rosenberg, J., Mahy, R., Matthews, P., and D. Wing, "Session Traversal Utilities for NAT (STUN)", RFC 5389, October 2008.

[RFC5928] Petit-Huguenin, M., "Traversal Using Relays around NAT (TURN) Resolution Mechanism", RFC 5928, August 2010.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, January 2012.

[RFC6698] Hoffman, P. and J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", RFC 6698, August 2012.

[RFC7350] Petit-Huguenin, M. and G. Salgueiro, "Datagram Transport Layer Security (DTLS) as Transport for Session Traversal Utilities for NAT (STUN)", RFC 7350, August 2014.

[I-D.ietf-dane-srv] Finch, T., Miller, M., and P. Saint-Andre, "Using DNS-Based Authentication of Named Entities (DANE) TLSA Records with SRV Records", draft-ietf-dane-srv-07 (work in progress), July 2014.

6.2. Informative References

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008.

[RFC7065] Petit-Huguenin, M., Nandakumar, S., Salgueiro, G., and P. Jones, "Traversal Using Relays around NAT (TURN) Uniform Resource Identifiers", RFC 7065, November 2013.

Appendix A. Examples

With the DNS RRs in Figure 1 and an ordered TURN transport list of {DTLS, TLS, TCP, UDP}, a TURN client conform to this specification and using the TURN URI [RFC7065] "turns:example.com" will try first to connect to the TURN server at address 192.0.2.1:5389 using DTLS and using DANE to verify the certificate subsequently presented by the server.

If this connection does not succeed, the client will then try to connect to the TURN server at 192.0.2.1:5000 but will not use DANE for the certificate verification even as a TLSA RR is available, because the DNSsec validation chain is broken in this case.

Using a TURN URI of "turns:example.com;transport=udp" bypasses the NAPTR lookup, but at the expense of preventing the TLS fallback.

```
example.com.
IN NAPTR 100 10 "" RELAY:turn.tls:turn.dtls "" example.net.
IN RRSIG NAPTR ...

_turns._tcp.example.com.
IN SRV   0 0 5000 a.example.net.

_turns._udp.example.com.
IN SRV   0 0 5349 a.example.net.
IN RRSIG SRV ...

example.net.
IN NAPTR 200 10 "" RELAY:turn.tcp:turn.tls "" stream.example.net.
IN NAPTR 100 10 "" RELAY:turn.udp:turn.dtls "" datagram.example.net.
IN RRSIG NAPTR ...

datagram.example.net.
IN NAPTR 100 10 S RELAY:turn.udp "" _turn._udp.example.net.
IN NAPTR 100 10 S RELAY:turn.dtls "" _turns._udp.example.net.
IN RRSIG NAPTR ...
```

```
stream.example.net.
IN NAPTR 200 10 S RELAY:turn.tcp "" _turn._tcp.example.net.
IN NAPTR 200 10 S RELAY:turn.tls "" _turns._tcp.example.net.
IN RRSIG NAPTR ...

_turn._udp.example.net.
IN SRV   0 0 3478 a.example.net.

_turn._tcp.example.net.
IN SRV   0 0 5000 a.example.net.

_turns._udp.example.net.
IN SRV   0 0 5349 a.example.net.
IN RRSIG SRV ...

_turns._tcp.example.net.
IN SRV   0 0 5000 a.example.net.

a.example.net.
IN A     192.0.2.1
IN RRSIG A ...

_5389._udp.a.example.net.
IN TLSA ...
IN RRSIG TLSA ...

_5000._tcp.a.example.net.
IN TLSA ...
IN RRSIG TLSA ...
```

Figure 1

Appendix B. Release notes

This section must be removed before publication as an RFC.

B.1. Modifications between draft-petithuguenin-tram-stun-dane-01 and draft-petithuguenin-tram-stun-dane-02

- DANE can store public keys or certificates.

B.2. Modifications between draft-petithuguenin-tram-stun-dane-00 and draft-petithuguenin-tram-stun-dane-01

- Change affiliation.
- Update STUN-DTLS reference.

- Nits

Authors' Addresses

Marc Petit-Huguenin
Impedance Mismatch

Email: marc@petit-huguenin.org

Olle E. Johansson
Edvina AB
Runbovaegen 10
Sollentuna SE-192 48
SE

Email: oej@edvina.net

Gonzalo Salgueiro
Cisco Systems
7200-12 Kit Creek Road
Research Triangle Park, NC 27709
US

Email: gsalguei@cisco.com