Dispatch
Internet-Draft
Updates: 5922 (if approved)
Intended status: Standards Track
Expires: January 11, 2014

O. Johansson
Edvina AB

July 10, 2013

TLS sessions in SIP using DNS-based Authentication of Named Entities (DANE) TLSA records
draft-johansson-dane-sip-00

Abstract

Use of TLS in the SIP protocol is defined in multiple documents, starting with RFC 3261. The actual verification that happens when setting up a SIP TLS connection to a SIP server based on a SIP URI is described in detail in RFC 5922 - SIP Domain Certificates.

In this document, an alternative method is defined, using DNS-Based Authentication of Named Entities (DANE). By looking up TLSA DNS records and using DNSsec protection of the required queries, including lookups for NAPTR and SRV records, a SIP Client can verify the identity of the TLS SIP server in a different way, matching on the SRV host name in the X.509 PKIX certificate instead of the SIP domain. This provides more scalability in hosting solutions and make it easier to use standard CA certificates (if needed at all).

This document updates RFC 5922.

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 11, 2014.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

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. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction 2
2. Terminology and Conventions Used in This Document 3
3. Using DNS in the SIP protocol 4
4. Why DNSsec is important for SIP 4
5. Secure delegation is required for DANE to apply 4
6. TLSA record name 5
7. Procedures for DANE-capable SIP implementations 5
8. X.509 certicate validation 5
9. Backward Compatibility with RFC 5922 5
10. Examples on certificate content 6
10.1. Example 1: johansson.example.com 6
10.2. Example 2: lundholm.example.com 6
11. Security Considerations 7
12. IANA Considerations 7
13. Acknowledgements 7
14. References 7
14.1. Normative References 7
14.2. Informative References 8
Appendix A. Appendix A. Implementation notes 8
Author's Address 9

1. Introduction

RFC 3261 [RFC3261] defines how to use TLS in the SIP protocol, but doesn't describe the actual verification between a SIP request and a TLS server certificate in detail. RFC 5922 [RFC5922] updates RFC 3261 with a definition of how a SIP client matches a PKIX X.509 [RFC5280] certificate provided by a TLS-enabled SIP server with the domain of a SIP request that caused the connection to be set up. Verification is done using the domain part of the SIP URI and the X.509 SubjectAltName extension of type dNSName or uniformResourceIdentifier. This is called "domain verification" as opposed to "host verification" in RFC 5922.

Including all domains hosted by a server in a server's certificate doesn't provide for a scalable and easy-managed solution. Every time a service adds a domain, a new certificate will need to be provided, unless TLS Server Name Identification (SNI) is used, where each domain can have it's own certificate. Having one certificate per domain and subdomain adds to the administration of a service. In addition, no known commercial CA offers certificate services with SIP URI's in the certificates.

Using DNSsec and DNS-based Authentication of Named Entities (DANE)[RFC6698] the chain from a SIP uri to a TLS certificate changes, as outlined in this document. With DNSsec, the DNS lookups are authenticated and can be verified and trusted. [I-D.ietf-dane-srv] describes a DANE-based chain of trust, matching the SRV host name with the contents of the certificate.

This document describes how a SIP implementation can use DANE to set up a secure connection to a SIP server with TLS support. In addition, we describe how a server can provide support for RFC 5922-style clients with the same certificate, if needed.

This document updates RFC5922 so that SIP implementations supporting DANE can validate a SIP domain identity using secure DNS queries and the identity of the SIP host by verifying the certificate using the SRV host name found in a SubjectAltName extension of type DNSName in the certificate. The domain verification will now happen based on DNSsec and the TLS verification will be based on host names (host verification in RFC 5922).

In order to learn about DANE and the different ways a TLSA record can be constructed, readers of this document needs to also read RFC 6698 [RFC6698].

2. Terminology and Conventions Used in This Document

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].

RFC 3261 [RFC3261] defines additional terms used in this document that are specific to the SIP domain such as "proxy"; "registrar"; "redirect server"; "user agent server" or "UAS"; "user agent client" or "UAC"; "back-to-back user agent" or "B2BUA"; "dialog"; "transaction"; "server transaction".

This document uses the term "SIP Server" that is defined to include the following SIP entities: user agent server (UAS), registrar, redirect server, a SIP proxy in the role of user agent server, and a B2BUA in the role of a user agent server.

This document uses the term "SIP client" that is defined to include the following SIP entities: user agent client(UAC), a SIP proxy in the role of user agent client, and a B2BUA in the role of a user agent client.

3. Using DNS in the SIP protocol

RFC 3263[RFC3263] describes how a SIP implementation use DNS to find the next hop server. The first step is to look up a DNS NAPTR record for the domain part of the URI. NAPTR records are used by the target domain to indicate reachability using different transports. NAPTR may be used to indicate a preference for TLS/TCP connections.

The result of the NAPTR lookup is a DNS name used to query for DNS SRV records. The list of DNS SRV records indicate host names that are queried for to find A or AAAA records with IP addresses.

SIP SRV records for TLS/TCP are using the prefix _sips._tcp, as in the DNS name _sips._tcp.example.com.

A SIP implementation with no support for NAPTR may, based on configuration or URI scheme, choose to set up a TLS session to the target domain.

> In rare cases, no SRV lookup is done. This means that the implementation lacks capability to do load balancing and failover based on the information in the DNS. These type of clients are not considered in this document.

4. Why DNSsec is important for SIP

DNS relies on DNS lookups not only to find the next hop server, but also for server administrators to provide failover and to load balance clients. The result of querying for one domain may need to SRV records or host names in another domain. Without DNSsec, an attacker can forge DNS replies and issue bogus DNS records, directing traffic to a bad server. This applies to calls as well as instant messaging, chat and presense.

5. Secure delegation is required for DANE to apply

It is important for implementors to understand the concept of "secure" DNSsec validation according to RFC 4033[RFC4033]. For this

specification to take effect, all DNS RRsets in the chain from SIP URI to IP address and TLSA record must be secure. (This corresponds to the A.D. bit being set in the responses).

If any RRset is not secure, this specification doesn't apply and the implementation should fall back to RFC 5922[RFC5922] behaviour. If any of the responses are "bogus" according to DNSsec validation, the client MUST abort the connection.

6. TLSA record name

For the SIP protocol DANE usage, TLSA records are to be found in accordance with [I-D.ietf-dane-srv]. If the domain example.com's TLS SRV records points to sip01.example.com port 5042 then the corresponding TLSA record will be found using the name _5042._tcp.sip01.example.com.

7. Procedures for DANE-capable SIP implementations

DANE capable SIP implementations follow the procedures above to find a SRV host name and look for a TLSA record. If no TLSA record is found, the client should fall back to RFC 5922 behaviour.

If a TLSA record is found, the client should never fall back to RFC 5922 behaviour. If TLSA-based validation fails, the client MUST abort the connection attempt.

8. X.509 certicate validation

When using DANE-based validation the client validates the SRV hostname with the certificate using RFC 5922 rules. A DANE-capable SIP implementation looks for the SRV hostname in the list of SubjAltName DNSName extension fields. Only if there are no SubjAltName extension fields may the client look in the CN of the X.509 certificate (according to RFC 5922).

If the SRV host name is not found in the certificate, DANE validation fails and the client MUST abort the connection.

Using the SRV host name for validation of a SIP domain identity is an update to RFC 5922

9. Backward Compatibility with RFC 5922

RFC 5922[RFC5922] implementations with no DANE support will be able to connect with the matching described in that document. SIP Servers can use certificates that are compatible with both this specification and RFC5922.

[I-D.ietf-dane-srv] requires use of the TLS Server Name Indication (SNI) extension [RFC6066]. This is not a requirement in this document, since SIP certificates can support both RFC 5922 style validation and DANE-based validation with the same certificate.

10. Examples on certificate content

This section gives examples on certificate content and how the match a given URI. The X.509 PKIX Subject field CN value is abbreviated as "CN", the SubjectAltName extension DNSName and uniformResourceIdentifier are abbreviated as "SAN-DNS" and "SAN-URI". The certificates are tested with three different clients. A DANE-aware client, a RFC 5922 client with no DANE support and a client that matches the SIP domain with the Common Name in the Subject of the certificate. The last example is not really covered by any SIP-related RFC and should be avoided.

10.1. Example 1: johansson.example.com

- Domain: johansson.example.com
- DNS SRV host for TLS: siphosting.example.net

Certificate content:

- CN: siphosting.example.net
- SAN-URI: -
- SAN-DNS: -
- Matching for DANE-aware SIP clients: Yes
- Matching for only RFC 5922 SIP clients: No
- Matching on CNAME only: No

10.2. Example 2: lundholm.example.com

- Domain: lundholm.example.com
- DNS SRV host for TLS: sipcrew.example.net

Certificate content:

- CN: randomname.example.net
- SAN-URI: sip:lundholm.example.com

- SAN-DNS: lundholm.example.com
- Matching for DANE-aware SIP clients: Yes
- Matching for only RFC 5922 SIP clients: Yes

Note: More examples is coming here.

11. Security Considerations

This document use already published solutions for providing credentials for setting up a secure connection to a SIP server. By depending on secure lookups of DNS NAPTR and SRV records as well as using TLSA records to verify a SIP servers TLS certificate it describes a secure method for making sure that a SIP request for a domain is sent to an authoritative server.

In addition to this document, many security considerations are covered in ID.ietf-dane-srv.

12. IANA Considerations

This document does not require actions by IANA.

13. Acknowledgements

The author wishes to acknowledge Jakob Schlyter for inspiration and .SE for promoting DNSsec and DANE. Victor Dubovn

14. References

14.1. Normative References

[I-D.ietf-dane-srv]
Finch, T., "Using DNS-Based Authentication of Named Entities (DANE) TLSA records with SRV and MX records.", draft-ietf-dane-srv-02 (work in progress), February 2013.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[RFC3263] Rosenberg, J. and H. Schulzrinne, "Session Initiation Protocol (SIP): Locating SIP Servers", RFC 3263, June 2002.

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

[RFC4346] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, April 2006.

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

[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.

[RFC5922] Gurbani, V., Lawrence, S., and A. Jeffrey, "Domain Certificates in the Session Initiation Protocol (SIP)", RFC 5922, June 2010.

[RFC6066] Eastlake, D., "Transport Layer Security (TLS) Extensions: Extension Definitions", RFC 6066, January 2011.

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

14.2. Informative References

[I-D.ogud-dane-vocabulary] Gudmundsson, O., "Harmonizing how applications specify DANE-like usage", draft-ogud-dane-vocabulary-00 (work in progress), June 2013.

[RFC5589] Sparks, R., Johnston, A., and D. Petrie, "Session Initiation Protocol (SIP) Call Control - Transfer", BCP 149, RFC 5589, June 2009.

Appendix A. Appendix A. Implementation notes

Developers of SIP implementations are strongly encouraged to implement RFC 5922 and this document for secure verification of a SIP domain with a TLS server. This document also encourages implementation of TLS SNI both in client and server implementations. In order to get support of this function, update to new versions of

the TLS libraries and make sure that the implementation supports new versions of TLS - TLS 1.1 [RFC4346] and TLS 1.2 [RFC5246].

Implementatinos that do support TLS are encouraged to always start with attempting TLS, even if the URI is a SIP: uri. If there are NAPTR records for the domain and the domain indicates support of TLS, use it. If there are no NAPTR records, start SRV lookup with the _sips._tcp prefix. This way, the SIP network will gradually shift to always using secure and authenticated TLS sessions.

Author's Address

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

Email: oej@edvina.net