Workgroup: RADEXT Working Group
Internet-Draft: draft-dekok-radext-tls-psk-00
Published: 3 March 2023
Intended Status: Informational
Expires: 4 September 2023
Authors: A. DeKok
FreeRADIUS

RADIUS and TLS-PSK

Abstract

This document gives implementation and operational considerations for using TLS-PSK with RADIUS/TLS (RFC6614) and RADIUS/DTLS (RFC7360).

About This Document

This note is to be removed before publishing as an RFC.

Status information for this document may be found at https://datatracker.ietf.org/doc/draft-dekok-radext-tls-psk/.

Discussion of this document takes place on the RADEXT Working Group mailing list (mailto:radext@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/radext/.

Source for this draft and an issue tracker can be found at https://github.com/freeradius/radext-tls-psk.git.

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 https://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 4 September 2023.

Table of Contents

1. Introduction

[RFC6614] and [RFC7360] define TLS and DTLS transports for RADIUS [RFC2865]. However, neither of those documents discuss how to use TLS-PSK. This document gives implementation and operational considerations for using TLS-PSK with RADIUS.

2. 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.

TBD

3. History

Certificates are hard to manage, but there is no guidance in [RFC6614] and [RFC7360] for using TLS-PSK.

4. Guidance for RADIUS clients

TLS uses certificates in most common uses. However, we recognize that it may be difficult to fully upgrade client implementations to allow for certificates to be used with RADIUS/TLS and RADIUS/DTLS. Client implementations therefore MUST allow the use of a pre-shared key (TLS-PSK). The client implementation can then expose a flag "TLS yes / no", and then a shared secret (now PSK) entry field.

Any shared secret used for RADIUS/UDP or RADIUS/TLS [RFC6613] MUST NOT be used for TLS-PSK.

Implementations MUST support PSKs of at least 32 octets, and SHOULD support PSKs of 64 octets. Implementations MUST require that PSKs be at least 16 octets in length. That is, short PSKs MUST NOT be permitted to be used.

Administrators SHOULD use PSKs of at least 24 octets, generated using a source of secure random numbers. The script given above can again be used.

We also incorporate by reference the requirements of Section 10.2 of [RFC7360] when using PSKs.

The issue of using PSKs in multiple TLS versions is discussed in [RFC8446] Section E.7, which notes:

Implementations can ensure safety from cross-protocol related output by not reusing PSKs between TLS 1.3 and TLS 1.2.

It would be unnecessarily complex for management interfaces and administrators to manage multiple PSKs depending on the TLS version. Therefore, we mandate that when TLS-PSK is used, TLS 1.3 or later MUST be used in RADIUS/TLS and RADIUS/DTLS.

Implementations MUST use ECDH cipher suites:

*TLS_ECDHE_PSK_WITH_CHACHA20_POLY1305_SHA256

*TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256

*TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA384

*TBD: other TLS ECDH PSK suites

4.1. PSK Identities

[RFC6614] is silent on the subject of PSK identities, which is an issue that we correct here. Guidance is required on the use of PSK identities, as the need to manage identities associated with PSK is a new requirement for NAS management interfaces, and is a new requirement for RADIUS servers.

RADIUS systems implementing TLS-PSK MUST support identities as per [RFC4279] Section 5.3, and MUST enable configuring TLS-PSK identities in management interfaces as per [RFC4279] Section 5.4.

A RADIUS client implementing TLS-PSK MUST update their management interfaces and application programming interfaces (APIs) to label the PSK field as "PSK" or "TLS-PKS, and MUST NOT label the PSK field as "shared secret".

Where dynamic server lookups [RFC7585] are not used, RADIUS clients MUST still permit the configuration of a RADIUS server IP address.

5. Guidance for RADIUS Servers

The following section(s) describe guidance for RADIUS server implementationas and deployments.

5.1. Identifying and filtering clients

When a RADIUS server implements TLS-PSK, it MUST use the PSK identity as the logical identifier for a RADIUS client instead of the IP address, as was done with RADIUS/UDP. That is, instead of associating a source IP address with a shared secret, the RADIUS server instead associates a PSK identity with a pre-shared key. In effect, the PSK identity replaces the source IP address of the connection as the client identifier.

This requirement does not prevent the server from using source IP addresses for filtering or client identification. Instead, it says that servers are no longer required to use solely the source IP address for client identification and filtering.

RADIUS servers MUST be able to look up PSK identity in a subsystem which then returns the actual PSK.

RADIUS servers MUST support IP address and network filtering of the source IP address for all TLS connections. There is rarely a reason for a RADIUS server to allow connections from the entire Internet, and there are many reasons to limit permitted connections to a small list of networks.

RADIUS servers SHOULD be able to limit certain PSK identifiers to certain network ranges or IP addresses. This filtering can catch configuration errors. That is, if a NAS is known to have a dynamic IP address within a particular subnet, the server should limit use of the NASes PSK to that subnet.

Note that as some clients may have dynamic IP addresses, it is possible for a one PSK identity to appear at different source IP addresses over time. In addition, as there may be many clients behind one NAT gateway, there may be multiple RADIUS clients using one public IP address. RADIUS servers MUST support multiple PSKs at one source IP address, and MUST support a unique PSK identity for each unique client which is deployed in such a scenario.

RADIUS servers SHOULD tie PSK identities to a particular permitted IP address or permitted network, as doing so will lower the risk if a PSK is leaked. RADIUS servers MUST permit multiple clients to share one permitted IP address or network.

A RADIUS server which accepts TLS-PSK MUST support a unique PSK identifier per RADIUS client. There is no reason to use the same identifier for multiple clients. A RADIUS server which accepts TLS-PSK MUST have a unique PSK per RADIUS client.

6. Shared Secrets

Any shared secret used for RADIUS/UDP or RADIUS/TLS MUST NOT be used for TLS-PSK.

It is RECOMMENDED that RADIUS clients and server track all used shared secrets and PSKs, and then verify that the following requirements all hold true:

*no shared secret is used for more than one RADIUS client

*no PSK is used for more than one RADIUS cleint

*no shared secret is used as a PSK

*no PSK is used as a shared secret

7. Privacy Considerations

We make no changes over [RFC6614] and [RFC7360].

8. Security Considerations

The primary focus of this document is addressing security considerations for RADIUS.

9. IANA Considerations

There are no IANA considerations in this document.

RFC Editor: This section may be removed before final publication.

10. Acknowledgements

TBD.

11. Changelog

12. References

12.1. Normative References

[BCP14] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

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

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, DOI 10.17487/RFC2865, June 2000, <https://www.rfc-editor.org/info/rfc2865>.

[RFC4279] Eronen, P., Ed. and H. Tschofenig, Ed., "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)", RFC 4279, DOI 10.17487/RFC4279, December 2005, <https://www.rfc-editor.org/info/rfc4279>.

[RFC7585] Winter, S. and M. McCauley, "Dynamic Peer Discovery for RADIUS/TLS and RADIUS/DTLS Based on the Network Access Identifier (NAI)", RFC 7585, DOI 10.17487/RFC7585, October 2015, <https://www.rfc-editor.org/info/rfc7585>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

12.2. Informative References

[RFC6613] DeKok, A., "RADIUS over TCP", RFC 6613, DOI 10.17487/RFC6613, May 2012, <https://www.rfc-editor.org/info/rfc6613>.

[RFC6614] Winter, S., McCauley, M., Venaas, S., and K. Wierenga, "Transport Layer Security (TLS) Encryption for RADIUS", RFC 6614, DOI 10.17487/RFC6614, May 2012, <https://www.rfc-editor.org/info/rfc6614>.

[RFC7360] DeKok, A., "Datagram Transport Layer Security (DTLS) as a Transport Layer for RADIUS", RFC 7360, DOI 10.17487/RFC7360, September 2014, <https://www.rfc-editor.org/info/rfc7360>.

Author's Address

Alan DeKok
FreeRADIUS

Email: aland@freeradius.org