Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: 5 January 2026

W. Guo
L. Xia
J. Li
Y. Li
Huawei Technologies

4 July 2025

Kerberos SPAKE with Two-Factor Authentication
draft-guo-krb-spake-2fa-00

Abstract

This document defines a new two-factor authentication mechanism for the Kerberos SPAKE pre-authentication. The mechanism uses the time-based one-time password (TOTP) as a second factor, and combines it with the password factor in a more secure way, which can prevent attackers from both impersonating Kerberos clients and obtaining TGTs' session keys in case of any factor leakage.

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 5 January 2026.

Copyright Notice

Table of Contents

1. Introduction

A password-derived long-term key is commonly used in the Kerberos [RFC4120] pre-authentication stage to protect messages exchanged between a Kerberos client and a Key Distribution Center (KDC). As noted in Section 10 of [RFC4120], an attacker can mount brute-force password attacks via eavesdropping a legitimate credential returned by the KDC or a legitimate authentication message sent by the client, which are both encrypted by the long-term key.

A Kerberos SPAKE pre-authentication mechanism is proposed in [RFC9588], it uses a simple password-authenticated key exchange (SPAKE) [RFC9382] to protect against brute-force password attacks, and additionally enables two-factor authentication (2FA). For example, the second-factor (SF) authentication may include one-time passwords, challenge/response signatures, and biometric data. As suggested in Section 1.3 of [RFC9588], the SF authentication data can be first encrypted using the key established by the PAKE and then securely transferred from the client to the KDC for verification, where the password verification happens implicitly by a successful decryption of the SF authentication data.

However, this 2FA methodology does not achieve the security of true two-factor authentication, which requires that the compromise of any factor will not affect the security of whole 2FA protocol. More

specifically, in case of password leakage, an attacker can use the leaked password to successfully perform a man-in-the-middle (MITM) attack against the Kerberos SPAKE, i.e., the client establishes a Kerberos SPAKE session A with the attacker and the attacker establishes a Kerberos SPAKE session B with the KDC. In this case, the attacker can obtain the SF authentication data in plaintext from the session A, and can use it as a valid second-factor in session B. Therefore, only the password factor allows the attacker to pass the KDC's two-factor authentication.

To remedy the above problem, this document defines a new two-factor authentication mechanism for the Kerberos SPAKE pre-authentication, which uses the widely deployed time-based one-time password (TOTP) [RFC6238] as a second factor. The mechanism combines the second factor with the password factor in the following way: the resulting TOTP value is combined with the PAKE's shared key to derive at least two encryption keys at both the client and KDC sides, then the client sends a second-factor challenge encrypted by one key to the KDC for verification and the KDC sends the TGT's session key encrypted by another key to the client for TGT issuance.

As a result, if an attacker compromises either of factors, it also needs to obtain another factor's authentication data to derive the final encryption keys, which are necessary to pass the two-factor authentication or obtain the TGT's session key. But this is hard to do if the authentication of another factor is still secure.

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.

The terms "encryption type" and "random-to-key" are defined in [RFC3961].

3. Kerberos SPAKE Pre-authentication with Second-Factor TOTP

3.1. Two-Factor Authentication Overview

The SPAKE algorithm combined with the TOTP algorithm can be generally described in the following steps:

* Calculation and exchange of the public key.

* Calculation of the shared SPAKE result (K1).

* Calculation of the shared TOTP result (K2).

* Derivation of an encryption key (K') from both the result K1 and K2.

* Verification of the derived encryption key (K').

In this mechanism, key verification happens implicitly by a successful decryption of the SF challenge data specific to the second-factor TOTP.

3.2. Introduction of the TOTP Algorithm

As defined in [RFC4226], the HOTP algorithm is based on the HMAC-SHA-1 algorithm and is computed as follows:

HOTP(K, C) = Truncate(HMAC-SHA-1(K, C))

where K and C represent the shared secret and counter value, and Truncate represents the function that can convert an HMAC-SHA-1 value into an HOTP value; see [RFC4226] for detailed definitions.

Recall that in [RFC6238], the TOTP algorithm is defined as TOTP = HOTP(K, T), where T is an integer and represents the number of time steps between the initial counter time T0 (default value is 0, i.e., the Unix epoch) and the current Unix time. Note that TOTP implementations MAY use HMAC-SHA-256 or HMAC-SHA-512 functions, please refer to Section 1.2 of [RFC6238].

3.3. Definition of the Second-Factor TOTP

Recall that in Section 4.2 of [RFC9588], each second factor is represented by a SPAKESecondFactor.

```
SPAKESecondFactor ::= SEQUENCE {
  type    [0] Int32,
  data    [1] OCTET STRING OPTIONAL
}
```

The type field is a unique integer that identifies the second-factor type, and the data field contains optional challenge data.

This document defines the type as an integer 2 to identify the second-factor TOTP, and defines the data as a random nonce whose length SHOULD match the multiplier length of the negotiated group, where the multiplier length is defined in Section 12.2 of [RFC9588].

4. Key Derivation

The SPAKE result and the TOTP result are both used to derive keys K'[n] as defined in this section.

The intermediate key is produced from the SPAKE result and other relevant values, please refer to Section 7 of [RFC9588].

Unlike the computation in Section 7 of [RFC9588], the key K'[n] is computed as follows:

* A pepper string is generated by concatenating the string "SF-TOTP" and the TOTP result as an octet string.

* An octet string is derived using PRF+(initial-reply-key, pepper), where PRF+ is defined in Section 5.1 of [RFC6113].

* An update reply key is produced from the octet string using the random-to-key function, which has the same encryption type as the initial reply key.

* The key K'[n] has the same encryption type as the update reply key, and has the value KRB-FX-CF2(update-reply-key, intermediate-key, "SPAKE", "keyderiv"), where KRB-FX-CF2 is defined in Section 5.1 of [RFC6113].

5. Second-Factor Types

This document defines one second-factor type:

SF-TOTP 2

This second-factor type indicates that the TOTP second factor is used.

6. IANA Considerations

This document defines a new second-factor type "SF-TOTP" with the following contents, and requests that IANA add it to the "Kerberos Second-Factor Types" Registry defined in [RFC9588].

ID Number: 2
Name: SF-TOTP
Reference: This document (RFC XXXX).

7. Normative References

[RFC4120] Neuman, C., Yu, T., Hartman, S., and K. Raeburn, "The Kerberos Network Authentication Service (V5)", RFC 4120, DOI 10.17487/RFC4120, July 2005, <https://www.rfc-editor.org/rfc/rfc4120>.

[RFC9588] McCallum, N., Sorce, S., Harwood, R., and G. Hudson, "Kerberos Simple Password-Authenticated Key Exchange (SPAKE) Pre-authentication", RFC 9588, DOI 10.17487/RFC9588, August 2024, <https://www.rfc-editor.org/rfc/rfc9588>.

[RFC9382] Ladd, W., "SPAKE2, a Password-Authenticated Key Exchange", RFC 9382, DOI 10.17487/RFC9382, September 2023, <https://www.rfc-editor.org/rfc/rfc9382>.

[RFC6238] M'Raihi, D., Machani, S., Pei, M., and J. Rydell, "TOTP: Time-Based One-Time Password Algorithm", RFC 6238, DOI 10.17487/RFC6238, May 2011, <https://www.rfc-editor.org/rfc/rfc6238>.

[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/rfc/rfc2119>.

[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/rfc/rfc8174>.

[RFC3961] Raeburn, K., "Encryption and Checksum Specifications for Kerberos 5", RFC 3961, DOI 10.17487/RFC3961, February 2005, <https://www.rfc-editor.org/rfc/rfc3961>.

[RFC6113] Hartman, S. and L. Zhu, "A Generalized Framework for Kerberos Pre-Authentication", RFC 6113, DOI 10.17487/RFC6113, April 2011, <https://www.rfc-editor.org/rfc/rfc6113>.

[RFC4226] M'Raihi, D., Bellare, M., Hoornaert, F., Naccache, D., and O. Ranen, "HOTP: An HMAC-Based One-Time Password Algorithm", RFC 4226, DOI 10.17487/RFC4226, December 2005, <https://www.rfc-editor.org/rfc/rfc4226>.

Authors' Addresses

Wei Guo
Huawei Technologies
Email: guowei90@huawei.com

Liang Xia
Huawei Technologies
Email: frank.xialiang@huawei.com

Ji Li
Huawei Technologies
Email: liji100@huawei.com

Yong Li
Huawei Technologies
Email: Yong.Li1@huawei.com