Internet Engineering Task Force (IETF)
Request for Comments: 6448
Category: Standards Track
ISSN: 2070-1721

R. Yount
Carnegie Mellon University

November 2011

The Unencrypted Form of Kerberos 5 KRB-CRED Message

Abstract

The Kerberos 5 KRB-CRED message is used to transfer Kerberos credentials between applications. When used with a secure transport, the unencrypted form of the KRB-CRED message may be desirable. This document describes the unencrypted form of the KRB-CRED message.

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/rfc6448.

1. Introduction

There are applications that need to transfer Kerberos credentials between them without having a prior relationship with established Kerberos keys. When transferred over a transport that provides confidentiality and integrity, the unencrypted form of the KRB-CRED message MAY be used. One application employing this method is the Kerberos attribute transport mechanism, described in Section 2.7 of the Security Assertion Markup Language (SAML) V2.0 Kerberos Attribute Profile [SAMLv2-KRB-ATTRIB].

In the SAML application, the Identity Provider (IdP) somehow obtains a Kerberos service ticket from the Kerberos Key Distribution Center (KDC) when required by the SAML system and transfers the credential to a Service Provider (SP) within an attribute statement. The SP can then use the credential to access a Kerberos protected service.

The Kerberos 5 specification as described in [RFC4120] mentions the non-standard legacy use of unencrypted KRB-CRED messages with the Generic Security Service Application Program Interface (GSS-API) [RFC1964] by the MIT, Heimdal, and Microsoft Kerberos implementations. This document provides a formal specification of the unencrypted form of the KRB-CRED message to enable its continued use in new applications.

2. Requirements Notation

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].

3. The Unencrypted Form of the KRB-CRED Message

The unencrypted form of the KRB-CRED message contains EncryptedData as defined in Section 5.2.9 of [RFC4120]. The encryption type (etype) MUST be specified as 0. The optional key version number (kvno) SHOULD NOT be present and MUST be ignored by the recipient if present. The ciphertext (cipher) is a copy of the EncKrbCredPart, which is in cleartext, as defined in Section 5.8.1 of [RFC4120].

4. Kerberos Encryption Type 0 Is Not an Encryption System

The Kerberos Encryption Type 0 is an invalid value [RFC3961]. This means that no encryption type with value 0 will ever be defined; no encryption or key management operations will use this value. Layers above the encryption layer often transport encryption types as integer values. These layers are free to use a 0 in an encryption

type integer as a flag or sentinel value, or for other context-specific purposes. For example, Section 3 of this specification defines the semantics of a 0 carried in the KRB-CRED message's encryption type field. In the context of the KRB-CRED message, it is a message-specific indicator to be interpreted as the message is not encrypted. This approach was chosen due to existing Kerberos implementations that conform to this specification.

5. Security Considerations

The KRB-CRED message contains sensitive information related to Kerberos credentials being transferred, such as their secret session keys, client and server principal names, and validity period. Possession of this information, along with the ticket itself, would allow an attacker to impersonate the client named in the ticket. The possibility of modification of the KRB-CRED message enables the attacker to substitute the credentials. This can result in the recipient using the credentials of a client that was not intended. As a result, the KRB-CRED message must be carefully safeguarded.

The use of an unencrypted form of the KRB-CRED message MUST only be used with a transport where sender and recipient identities can be established to be known to each other. The transport MUST also provide confidentiality, integrity, and mutual authentication. Examples of transports that MAY be securely used to transport an unencrypted KRB-CRED message would include Transport Layer Security (TLS) [RFC5246], where mutual authentication has been established, or the use of messages where the KRB-CRED is encoded within an encrypted and signed SAML 2.0 [OASIS-SAMLv2] statement.

6. Acknowledgements

The following individuals have contributed to the development of this specification.

Thomas Hardjono, Massachusetts Institute of Technology

Josh Howlett, Individual

Jeffrey Hutzelman, Carnegie Mellon University

7. IANA Considerations

The reference for Kerberos Encryption Type 0 has been updated to point to this document.

8. References

8.1. Normative References

[OASIS-SAMLv2]
Cantor, S., Ed., Kemp, J., Ed., Philpott, R., Ed., and E. Maler, Ed., "Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0", OASIS Standard saml-core-2.0-os, March 2005.

[RFC1964] Linn, J., "The Kerberos Version 5 GSS-API Mechanism", RFC 1964, June 1996.

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

[RFC4120] Neuman, C., Yu, T., Hartman, S., and K. Raeburn, "The Kerberos Network Authentication Service (V5)", RFC 4120, July 2005.

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

8.2. Informative References

[RFC3961] Raeburn, K., "Encryption and Checksum Specifications for Kerberos 5", RFC 3961, February 2005.

[SAMLv2-KRB-ATTRIB]
Howlett, J., Ed., and T. Hardjono, Ed., "SAML V2.0 Kerberos Attribute Profile Version 1.0", sstc-saml-attribute-kerberos.odt, August 2011.

Author's Address

Russell J. Yount
Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh, Pennsylvania 15213
US

Phone: +1 412 268 8391
EMail: rjy@cmu.edu