Abstract

A long long time ago DES was standardized. Some 30 years later (2003) it was withdrawn as a standard by NIST, today 6 years later, its time for DES to finally die. By 2008 it was possible to brute force DES keys in 6.4 days using less than USD 10k worth of hardware. So by 2008 DES had passed its sell-by date. Use in Kerberos should therefore stop.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on September 26, 2010.

Copyright Notice

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.
1. 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].
2. Background

Kerberos 5 was defined in [RFC1510] and updated in [RFC4120], the Kerberos crypto system is defined by [RFC3961] and includes support for DES encryption types. This document move all of the DES encryption and related checksum types to historic.

DES was withdrawn in [DES-Transition-Plan] by NIST. IETF have also published its the position in [RFC4772], which in the recommendation summery is made very clear: "don’t use DES".

In Kerberos GSS-API mechanism [RFC1964] and the updated version [RFC4121] the following checksum and encryption mechanism is defined: three SGN ALG: 0000 - DES MAC MD5, 0100 - MD2.5 0200 - DES MAC and one SEAL ALG 0000 - DES. With newer encryption types for Kerberos defined in [RFC4121], Microsofts ARCFOUR4-HMAC based GSS-API mech, and MITs DES3, there is no need to support the old DES based SGN/SEAL types.
3. Recommendations

This document removes the mandatory-to-implement types from [RFC4120]: Encryption: DES-CBC-MD5(3)

This document removes the mandatory-to-implement types from [RFC4120] when used in conjunction with DES-CBC-MD5: Checksums: DES-MD5(7)

Kerberos implementation and deployments SHOULD NOT implement the single DES encryption types: DES-CBC-CRC(1), DES-CBC-MD4(2), DES-CBC-MD5(3).

Kerberos implementation and deployments SHOULD NOT implement the checksum type: CRC32(1), RSA-MD4(2), RSA-MD4-DES(3), DES-MAC(4), DES-MAC-K(5), RSA-MD4-MAC-K(6), DES-MD5(7), RSA-MD5-DES(8).

Note that RSA-MD5 might be with non-DES encryption types, for example, when doing a TGS-REQ with a ARCFOUR-HMAC-MD5 some client uses RSA-MD5 for the checksum that is stored inside the encrypted part of the authenticator. This use of RSA-MD5 should probably be considered safe, so the Kerberos implementation should make sure this usage is not disabled when used with legacy system that can’t handle newer checksum types.

Kerberos GSS mechanism implementation and deployments SHOULD NOT implement the SGN ALG: DES MAC MD5(0000), MD2.5(0100), DES MAC(0200).

Kerberos GSS mechanism implementation and deployments SHOULD NOT implement the SEAL ALG: DES(0000).
4. Acknowledgements

Jeffery Hutzelman, Simon Josefsson, Mattias Amnefelt and Leif Johansson have read the document and provided suggestions for improvements.
5. Security Considerations

Removing support for single DES improves security since DES is considered to be insecure.
6. IANA Considerations

There are no IANA Considerations for this document
7. References

7.1. Normative References


7.2. Informative References


Author’s Address

Love Hornquist Astrand
Apple, Inc
Cupertino
USA

Email: lha@apple.com