Kerberos cross realm version の概要

国立研究開発法人 情報通信研究機構

1. 基本情報

- ✧ 名前

  The Kerberos Network Authentication Service (V5), Kerberos cross realm version

- ✧ 機能

  信頼できる第三者機関（TTP, Trusted Third Party）の存在を前提とする、オープンなネットワークにおけるサーバ・クライアント間でのネットワーク認証・鍵交換プロトコル。特徴は異なる管理ドメイン間で認証情報を共有可能であること。暗号として共通鍵暗号を利用。

- ✧ 関連する標準

  RFC4120 (https://www.ietf.org/rfc/rfc4120.txt)

2. プロトコル仕様

Kerberos cross realm version のプロトコル仕様のシーケンスを図 1 に示す。レルム（管理ドメイン）A のサーバにより認証されたクライアントがリモートのレルム B のサーバにより認証されるための流れである。

3. 攻撃者モデル（自然言語による記述）

攻撃者として Dolev-Yao モデルを想定する。すなわち、通信の盗聴、改ざん、遮断、再送が可能とする。

4. セキュリティ要件（自然言語による記述）

- ➢ リモートサーバ（S）によるクライアント（C）の認証。
- ➢ クライアントによるリモートサーバの認証。
- ➢ リモートサーバとクライアントが共有した鍵 K_CS の秘匿性。

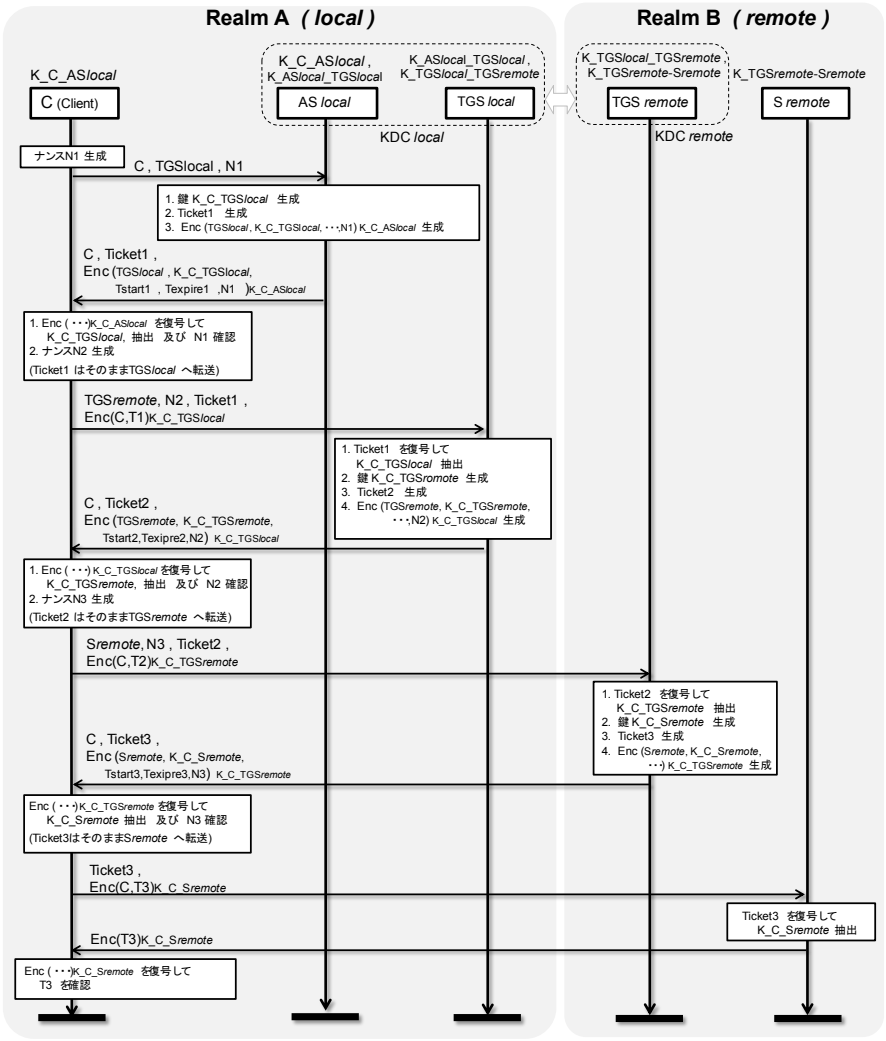

図 1. シーケンス図

5. 安全性に関して知られている結果

5.1. 脅威/脆弱性

第三者によるチケットの受取が可能であること。

5.2. 形式手法に基づく検証

AVISPA による評価結果が、

http://www.avispa-project.org/library/Kerb-Cross-Realm.html

に掲載されている。

また、Butler らによる評価結果が http://dx.doi.org/10.1016/j.tcs.2006.08.040 で発表されている。

- Frederick Butler, Iliano Cervesato, Aaron D. Jaggard, Andre Scedrov, and Christopher Walstad, “Formal analysis of Kerberos 5,” Theor. Comput. Sci.

367(1-2), pp.57-87 (2006).

6. 備考

本文書は、**総務省「暗号・認証技術等を用いた安全な通信環境推進事業に関する実証実験の請負　成果報告書」**からの引用である。