Kerberos with ticket caching 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 with ticket caching

- ✧ 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。特徴はサーバが認証情報に含まれる情報をキャッシュしてリプレイ攻撃を検出すること。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 with ticket caching は Kerberos のオプションの１つ。プロトコル仕様のシーケンスを図 1 に示す。アプリケーションサーバ（S）が認証情報（Acs）に含まれる情報をキャッシュしてリプレイを検出することによる、強固な認証機能の実現を目的とする。

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）

- ➢ 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サーバの認証。
- ➢ サーバとクライアントが共有した鍵 K_CS の秘匿性。

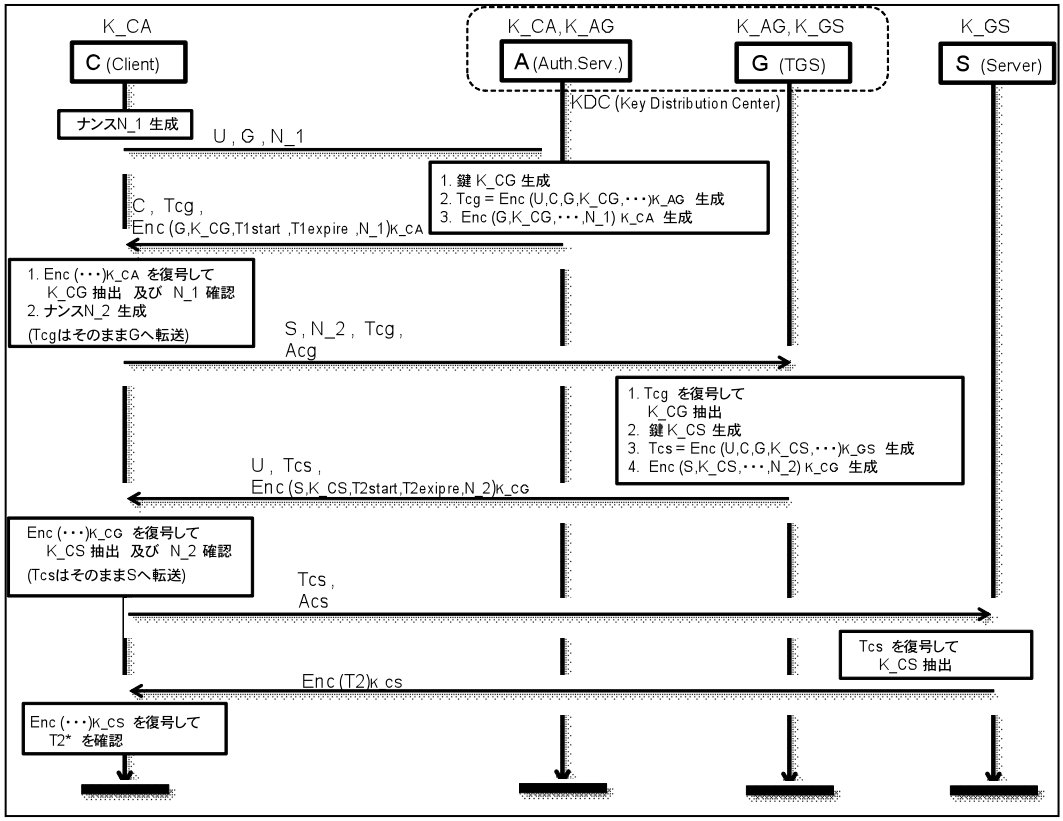

図 1. シーケンス図

5. 安全性に関して知られている結果

5.1. 制限

第三者によるチケットの受取が可能であること。

5.2. 脅威/脆弱性

K_CG の機密性。

5.3. 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-Ticket-Cache.html

に掲載されている。

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。