Kerberos PKINIT 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

  Public Key Cryptography for Initial Authentication in Kerberos (PKINIT)

- ✧ 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。特徴は公開鍵暗号を利用し、最初のリクエスト時にデータの一部に署名を付与すること。

- ✧ 関連する標準

  RFC4556 (https://tools.ietf.org/html/rfc4556)

2. プロトコル仕様

Kerberos PKINIT のプロトコル仕様のシーケンスを図 1 に示す。公開鍵暗号を利用し、最初のリクエスト時に、データの一部に署名を付与し、認証サーバがこれを検証する。これにより、攻撃者がリクエストを大量に送りつけてクライアントの長期鍵を解読することを防止できる。特にクライアントの鍵がパスワードから生成される場合に有用。

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。

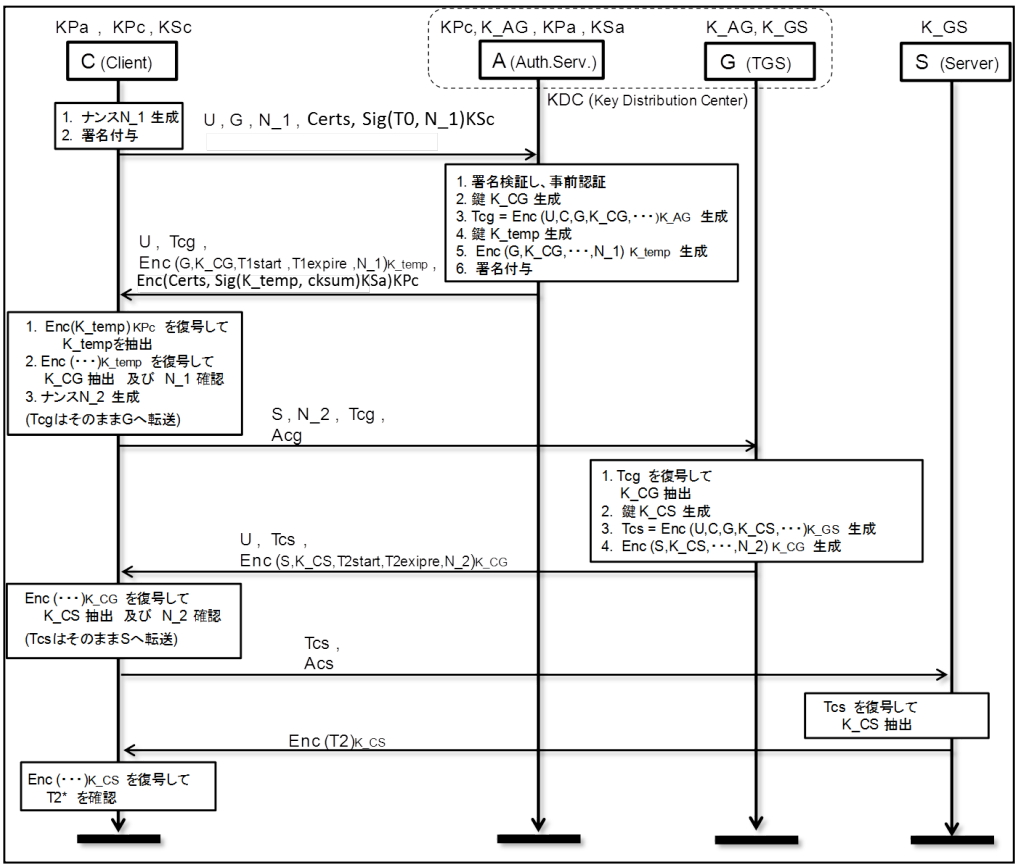

図 1. シーケンス図

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-PKINIT.html に掲載されている。

また、Cervesato らによって、旧バージョンの評価結果が http://dx.doi.org/10.1016/j.ic.2007.05.005 で発表されている。

- Iliano Cervesato, Aaron D. Jaggard, Andre Scedrov, Joe-Kai Tsay, and Christopher Walstad, “Breaking and fixing public-key Kerberos,” Inf. Comput., 206(2-4), pp.402-424 (2008).

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。