SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

状態更新を含むプロトコルに対する Tamarin Prover を用いたリプレイ攻撃の検証に向けて

Towards Verification of Replay Attacks against Protocols Containing State Updates using Tamarin Prover

佐藤瑞己 * 米山一樹 *
Mizuki Sato Kazuki Yoneyama

キーワード 形式検証, リプレイ攻撃, Tamarin Prover

あらまし

多くの認証プロトコルでは、リプレイ攻撃を防ぐ目的でカウンタや状態の更新を含んでいる。Noguchi らは、そのようなステートフルなプロトコルとして、IEEE802.21 のグループ鍵共有（GKM）プロトコル [1] と Group Domain of Interpretation（GDOI） [2] の形式化を行い、自動検証ツール ProVerif を用いて秘匿性やリプレイ攻撃を含む認証性の検証を行った。しかし、ProVerif はステートフルなプロトコルの記述をサポートしていないため、リプレイ攻撃については特定の回数の実行の場合しか検証できていないという問題があった。特定の複製回数によらない一般的な状況でのリプレイ攻撃に対する安全性検証が望ましい。

本稿では、Tamarin Prover [4] の自動化モードによる自動検証を用いてそれらの状態更新を含むプロトコルにおける一般のリプレイ攻撃に対する安全性検証を行う。Tamarin Prover はマルチセット書き換え規則を用いてプロトコルをモデル化ことによって、ステートフルなプロトコルを記述することができる。さらに、論理式によって様々な安全性を定義することが可能であり、これにより、柔軟な安全性の形式化を行うことができる。例えば、カウンタの更新を含む Yubikey プロトコルの Tamarin Prover による形式化とリプレイ攻撃の検証事例 [3] が知られている。

我々は、GKM プロトコルについて Yubikey プロトコルの形式化手法を応用し、グループ管理木の深さ 2 と 3 の場合におけるシーケンス番号の更新を形式化する。GDOI についてはカウンタ更新に加え、一部の鍵の更新を形式化する。結果として、それぞれのプロトコルが一般的なリプレイ攻撃に対して安全であることを示す。

* 茨城大学, 〒 316-8511 茨城県日立市中成沢町 4-12-1, Ibaraki University, 4-12-1 Nakanarusawa-cho, Hitachi-shi, Ibaraki, 316-8511, Japan.

参考文献

[1] Ryoga Noguchi, Yoshikazu Hanatani, Kazuki Yoneyama. Verification of Group Key Management of IEEE 802.21 using ProVerif. APKC 2020，pp 19-27, 2020.

[2] 野口 凌雅, 花谷 嘉一, 米山 一樹. ProVerif による Group Domain of Interpretation プロトコルの検証. SCIS 2020, 2020.

[3] Robert Künnemannm, Graham Steel, YubiSecure? Formal Security Analysis Results for the Yubikey and YubiHSM. STM2012，pp 257-272, 2012.

[4] Benedikt Schmidt, Simon Meier, Cas Cremers, David Basin, Automated Analysis of Diffie-Hellman Protocols and Advanced Security Properties. CSF2012，pp 78-94, 2012.