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

セキュアチャネル上の認証プロトコルの形式検証
Formal Verification of Authentication Protocol on Secure Channel

中林 美郷 *　　奥田 哲矢 *
Misato NAKABAYASHI　　Tetsuya OKUDA

キーワード TLS，認証プロトコル，形式検証，ProVerif

あらまし

一般的なセキュリティプロトコル検証ツールでは，公開通信路における秘匿性および認証を安全性要件として，公開通信路では攻撃者が盗聴・改ざんを行える想定として，安全性の検証を行う．一方，Web サービスのユーザ認証プロトコルにおいては，サーバ認証済の TLS（セキュアチャネル）を利用することが一般的である．

そこで本研究では，セキュアチャネルの存在を前提としたセキュリティプロトコルの検証手法について検討を行った．第一かつ最重要点として，不正に認証を要求する端末を表現するために，端末内に公開通信路を仮想的に設定することで，不正な端末を形式的に表現可能とした．第二に，認証を要求する端末を，正規端末（認証前／認証済）と不正端末（認証前）に分類することで，認証前の端末が，認証済の他端末の通信の盗聴・改ざんが困難であることを表現した．第三に，サーバからのすべての通信に署名を付与することで，サーバ認証済のセキュアチャネルを表現した．本研究の提案により，TLS などのセキュアチャネルを前提とした Web サービスの認証プロトコルに対する攻撃を検知可能な形式検証システムが実現可能になると期待される．

本論文で想定するネットワーク構成と信頼/脅威モデルを図 1 に示す．クライアントとサーバ間にはサーバ認証済みのセキュアチャネルが張られており，サーバは信頼できると仮定する．攻撃者はセキュアチャネル上の情報（他のクライアントのセッションの情報）を盗聴・改ざんできないものとし，不正なクライアントが正規のクライアントとして受理されることを狙って，サーバに対して任意のリクエストを送信できるものとする．

* NTT 社会情報研究所 〒 180–8585 東京都武蔵野市緑町 3-9-11. NTT Social Informatics Laboratories, 3-9-11, Midori-cho Musashino-shi, Tokyo 180–8585, Japan. {misato.nakabayashi.mu, tetsuya.okuda.uy}@hco.ntt.co.jp.

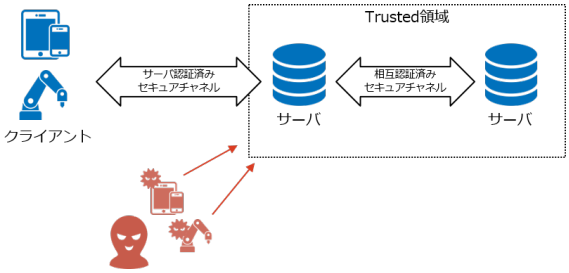

図 1: 本論文で想定するネットワーク構成と信頼/脅威モデル．クライアントとサーバ間にはセキュアチャネルが張られているため，攻撃者は他のクライアントのセッション情報を盗聴・改ざんすることができない．

Feng らは，同様のネットワーク構成を仮定して，形式検証ツール ProVerif を用いた FIDO UAF 認証プロトコルの安全性検証を行った [1]．Feng らの研究では，セキュアチャネル上の認証を表現するために同じエンティティを並行して動かす必要があり，そのためには ProVerif 自体の改良が必要であった．我々のアプローチでは ProVerif 自体の改良は不要であるため，実装や検証が容易になる．また，Feng らの研究では，FIDO 端末の内部構成に特化した脅威を想定して，FIDO 端末内部の特定のエンティティ間に公開通信路を規定しているが，我々のアプローチでは一般の認証クライアント内部に “仮想的に” 公開通信路を設定しているため，FIDO 以外の一般的な認証クライアントについて，不正な認証要求を行う攻撃者，“端末攻撃者” の表現が ProVerif で可能となる．

参考文献

[1] Haonan Feng, Hui Li, Xuesong Pan, and Ziming Zhao. A formal analysis of the FIDO UAF protocol. *Proceedings of 28th Network And Distributed System Security Symposium (NDSS)*. 2021.