10

Formal verification of the QUIC and TLS protocols

次世代webの安全性がより確かなものに

～フォーマルメソッドによるQUIC・TLS1.3の検証～

どんな研究

インターネット上の通信の安全性は認証や暗号化の方法を定めたセキュリティ・プロトコルに従って守られていますが、その欠陥が近年多く発見されています。セキュリティ・プロトコルの安全性を、その仕様に基づいて自動的かつ厳密に検査する研究です。

どこが凄い

計算機を用いて攻撃を効率的・網羅的にチェックします。次世代web認証・暗号化プロトコルTLS1.3の安全性を確認するとともに、Googleによって策定されたweb認証・暗号化プロトコルQUICが従来研究で“証明”された安全性を満たさないことを発見しました。

目指す未来

現在はプロトコル仕様が策定されて広く利用されるようになってから欠陥が発見されるため、対策に多大な労力と時間を費やしています。また、その間は安全でない状態が続きます。本研究によって仕様を決める段階で安全性を検査し、利用前に欠陥を発見・修正できるようになります。

セキュリティ・プロトコルの策定と欠陥

プロトコル仕様の策定

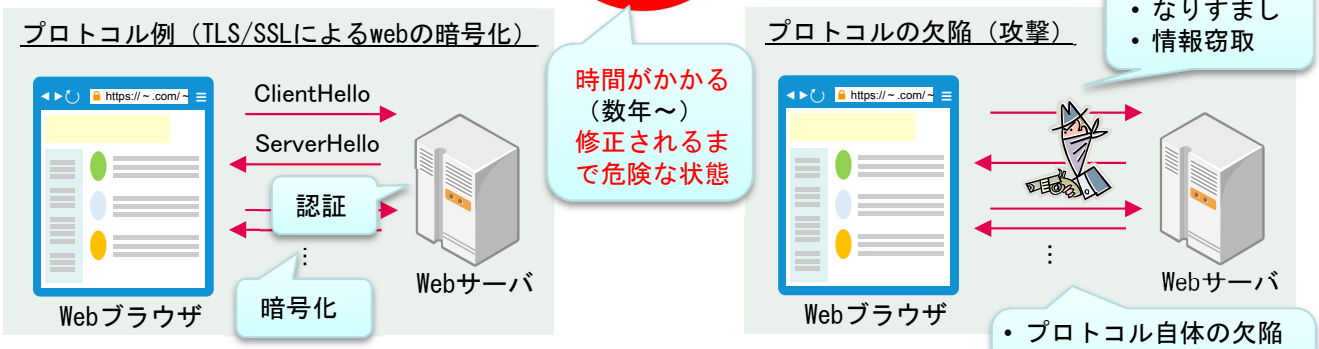
- 認証（通信相手の確認）の手順
- 部品として利用する暗号技術（暗号・署名）

実装・展開

修正

プロトコルの利用

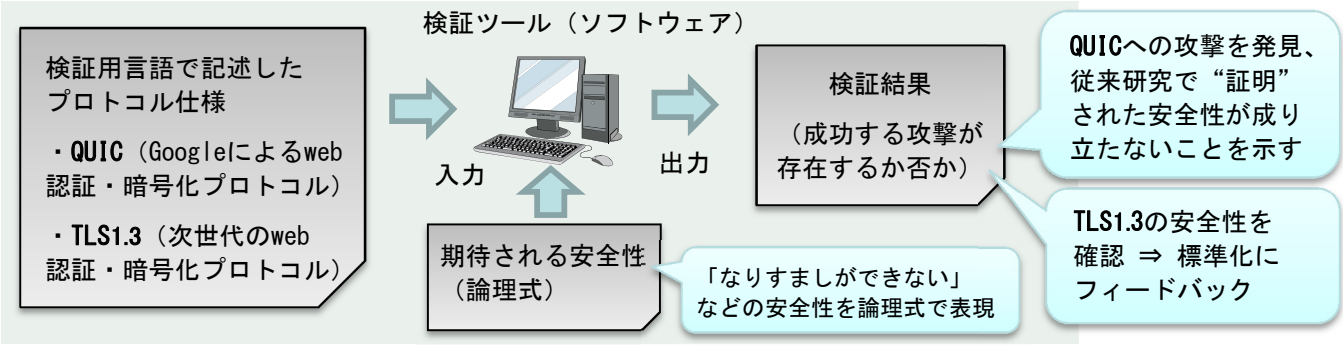
近年、広く利用されているプロトコルに欠陥が多く発見される



フォーマルメソッドによる安全性検証

目標：プロトコルの仕様を決める段階で、プロトコルの安全性を厳密に検査

- プロトコル仕様を入力として安全性を検査することで、実装・利用前の検査を可能に
- 数理論理学に基づくフォーマルメソッドにより、安全性を論理式で記述し、これに反する攻撃を網羅的に検査することで、専門家でも見逃してしまうような欠陥も発見可能に



【関連文献】

[1] 櫻田英樹, 米山一樹, 吉田真紀, 花谷嘉一, “形式検証に向けたQUICの安全性定義の検討,” *日本応用数理学会2015年度年会*, 2015.
[2] 荒井研一, 徳重佑樹, 櫻田英樹, “ProVerifによるTLS 1.3ハンドシェイクプロトコルの形式検証（その2）,” *2016年暗号と情報セキュリティシンポジウム*, 2016.

【連絡先】

櫻田 英樹 (Hideki Sakurada)　メディア情報研究部 情報基礎理論研究グループ
E-mail：sakurada.hideki(at)lab.ntt.co.jp