10

Assuring the next-generation web security

～Formal verification of the QUIC and TLS protocols～

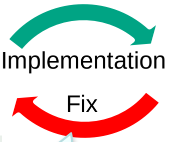
Abstract

Abstract: Communications on the Internet are often protected by using security protocols. However, many security flaws have recently been found in widely-used protocols such as TLS/SSL. Such flaws may allow attackers to impersonate yourself and/or steal your information from the communications. In this work we analyze the next-generation web security protocols by using formal methods. Formal methods based on mathematical logics allow us to rigorously verify expected security of protocols as logical formulae and to find attacks (if any) that are hard to be found even by experts. We have shown that the QUIC protocol developed by Google does not satisfy certain security that has been "proved" in previous work, and also that TLS1.3, the next version of TLS, is secure with respect to our security definitions.

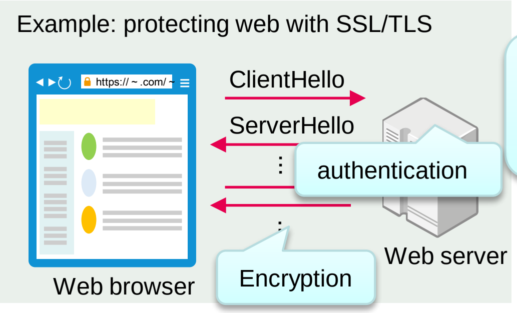
Development and Flaws of Security Protocols

Development of Security Protocols

- Authentication of participants
- Message protection (Encryption, Signature,...)

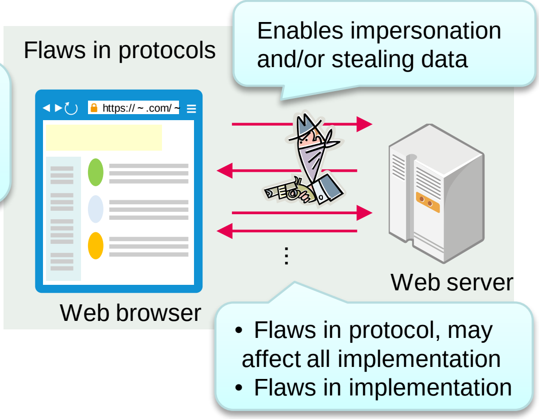


May take a long time, danger for the moment


Example: protecting web with SSL/TLS

Use of Security Protocols

Recently, many security flaws have been found in widely used protocols (e.g. SSL/TLS)


Flaws in protocols

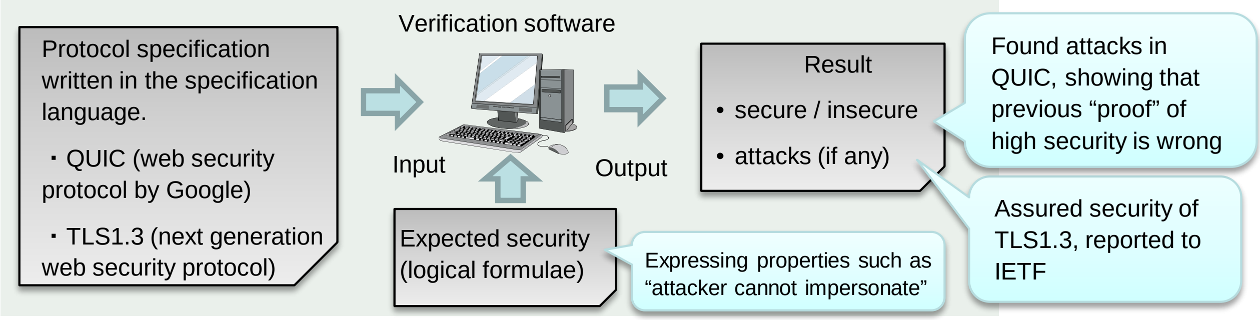
Enables impersonation and/or stealing data

- Flaws in protocol, may affect all implementation
- Flaws in implementation

Formal Verification

Goal: Rigorously verify security during the development phase, before implementation

- By using protocol specification (not implementation), enables verification before implementation.
- Using mathematical logics as a basis, enables to specify security as logical formulae and to find attacks (if any) that violate the security that are hard to be found even by experts.


Protocol specification written in the specification language.

・QUIC (web security protocol by Google)

・TLS1.3 (next generation web security protocol)

Result

- secure / insecure
- attacks (if any)

Expected security (logical formulae)

Expressing properties such as “attacker cannot impersonate”

Found attacks in QUIC, showing that previous “proof” of high security is wrong

Assured security of TLS1.3, reported to IETF

【Reference】

[1] H. Sakurada, K. Yoneyama, M. Yoshida, Y. Hanatani, “Toward the formal verification of the QUIC protocol,” Proc. *Annual conference of the Japan society for industrial and applied mathematics*, 2015.

[2] K. Arai, Y. Tokushige, H. Sakurada, “Formal Verification of TLS 1.3 Handshake Protocol Using ProVerif (Part 2),” Proc. *2016 Symposium on Cryptography and Information Security*, 2016.

【Contact】

Hideki Sakurada Computing Theory Research Group, Media Information Laboratory
E-mail：sakurada.hideki(at)lab.ntt.co.jp