07

Formal evaluation of network security

〜Verification of cryptographic protocols using formal methods〜

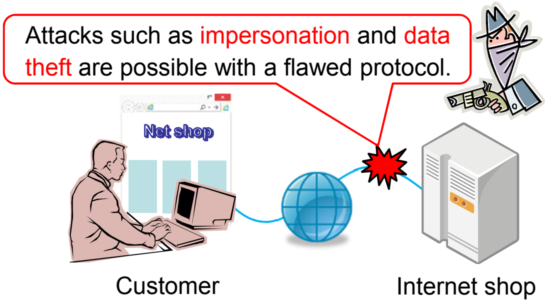
Abstract

Cryptographic protocols are often used to guarantee security in communications such as internet shopping. Such protocols are usually constructed by combining cryptographic technologies such as public-key encryption and digital signatures. However, an inappropriate combination can allow unexpected and serious attacks, and enormous efforts are required to fix and replace all the software implementing the flawed protocol. To prevent this, we have developed a method for evaluating the security of cryptographic protocols. To enable a fast evaluation, we identify and exclude a vast number of attacks that succeed only with negligible probability and test only the remaining attacks.

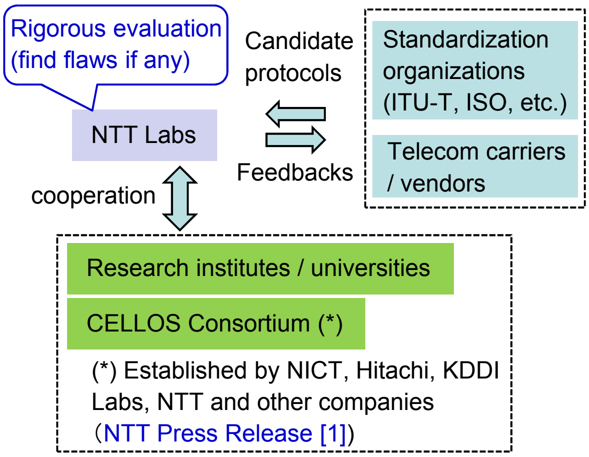
Problems with cryptographic protocols

Cryptographic protocols are used to provide security in communications. However,

- Many of them have no rigorous security guarantee.
- There is no fast and highly accurate security evaluation method.

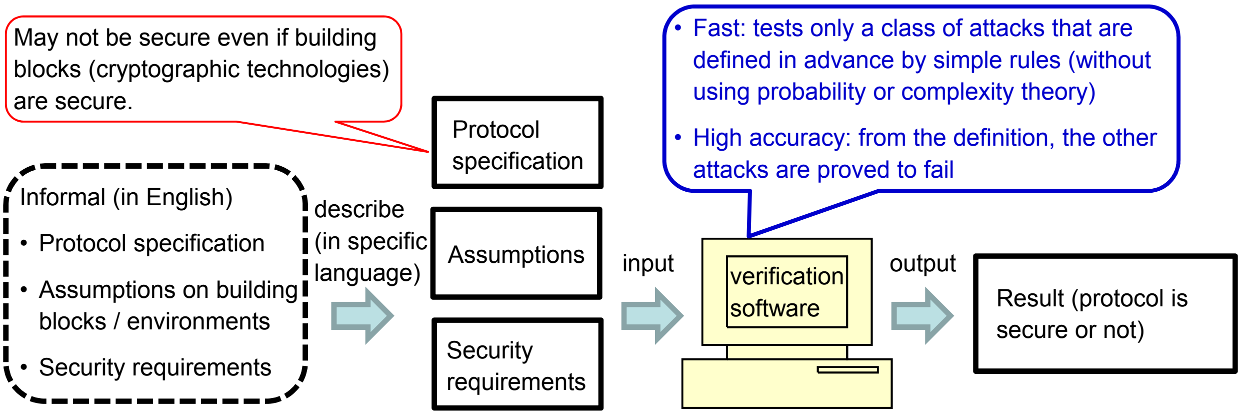

Attacks such as impersonation and data theft are possible with a flawed protocol.

Alliance for evaluating protocols


Rigorous evaluation (find flaws if any)
NTT Labs
Candidate protocols
Feedbacks
Standardization organizations (ITU-T, ISO, etc.)
Telecom carriers / vendors
cooperation
Research institutes / universities
CELLOS Consortium (*)

(*) Established by NICT, Hitachi, KDDI Labs, NTT and other companies （NTT Press Release [1])

Enabling fast and highly accurate evaluation (verification)


May not be secure even if building blocks (cryptographic technologies) are secure.

- Fast: tests only a class of attacks that are defined in advance by simple rules (without using probability or complexity theory)
- High accuracy: from the definition, the other attacks are proved to fail

Related work

[1] NICT, Hitachi, KDDI Labs, NTT, “Establishment of cryptographic protocol evaluation toward long-lived outstanding security (CELLOS) consortium,” NTT Press Release 2013.

[2] H. Sakurada, “Computational soundness of symbolic blind signatures under active attacker,” in *Proc. The Sixth International Symposium on Foundations & Practice of Security (FPS 2013)*, 2013.

Contact

Hideki Sakurada Computing Theory Research Group, Innovative Communication Laboratory
E-mail : sakurada.hideki{at}lab.ntt.co.jp (Please replace {at} with @)