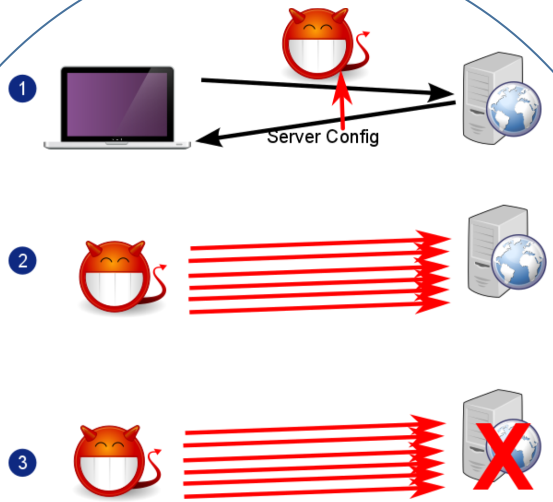
A Unifying Framework For Theoretical and Empirical Analysis of Secure Communication Protocols

Challenge:

- Many network protocols are deployed without a formal security analysis.
- Many existing security specifications and analyses do not take into account such goals as performance and interoperability with other protocols that are already deployed in practice.

Solution:

- Develop a novel security framework that will facilitate the provable-security analyses of practical networking protocols.
- Understand the tradeoffs between the level of complexity of a theoretical model and the extent of empirical evaluations needed to perform to capture security, performance, and deployability issues.



A QC protocol Π is QACCE-secure if its advantage $\mathrm{Adv}_{\Pi}^{QACCE}(A)$, defined as $\mathrm{Adv}_{\Pi}^{s\text{-}imp}(A) + \mathrm{Adv}_{\Pi}^{ips}(A) + \mathrm{Adv}_{\Pi}^{ch\text{-}corr}(A)$, is negligible (in λ) for any polynomial-time adversary A.

Scientific Impact:

- New security model that captures multi-key exchange and network-level attacks.
- New security model that captures properties of layered protocols.
- Analysis of QUIC, TCP Fast Open, TLS False Start, TLS 1.3.

Broader Impact:

- Combine provable security with network protocol design to yield a novel unifying security framework and analyses of specific networking protocols.
- Increase security and availability of Internet communication.

CNS- 1421815, Georgia Tech, PI Alexandra Boldyreva (sasha@gatech.edu)
Northeastern University, PI C. Nita-Rotaru (c.nitarotaru@neu.edu)