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

Alexandra Boldyreva (Georgia Tech), Cristina Nita-Rotaru (Northeastern University)
http://nds2.ccs.neu.edu/uframe.html

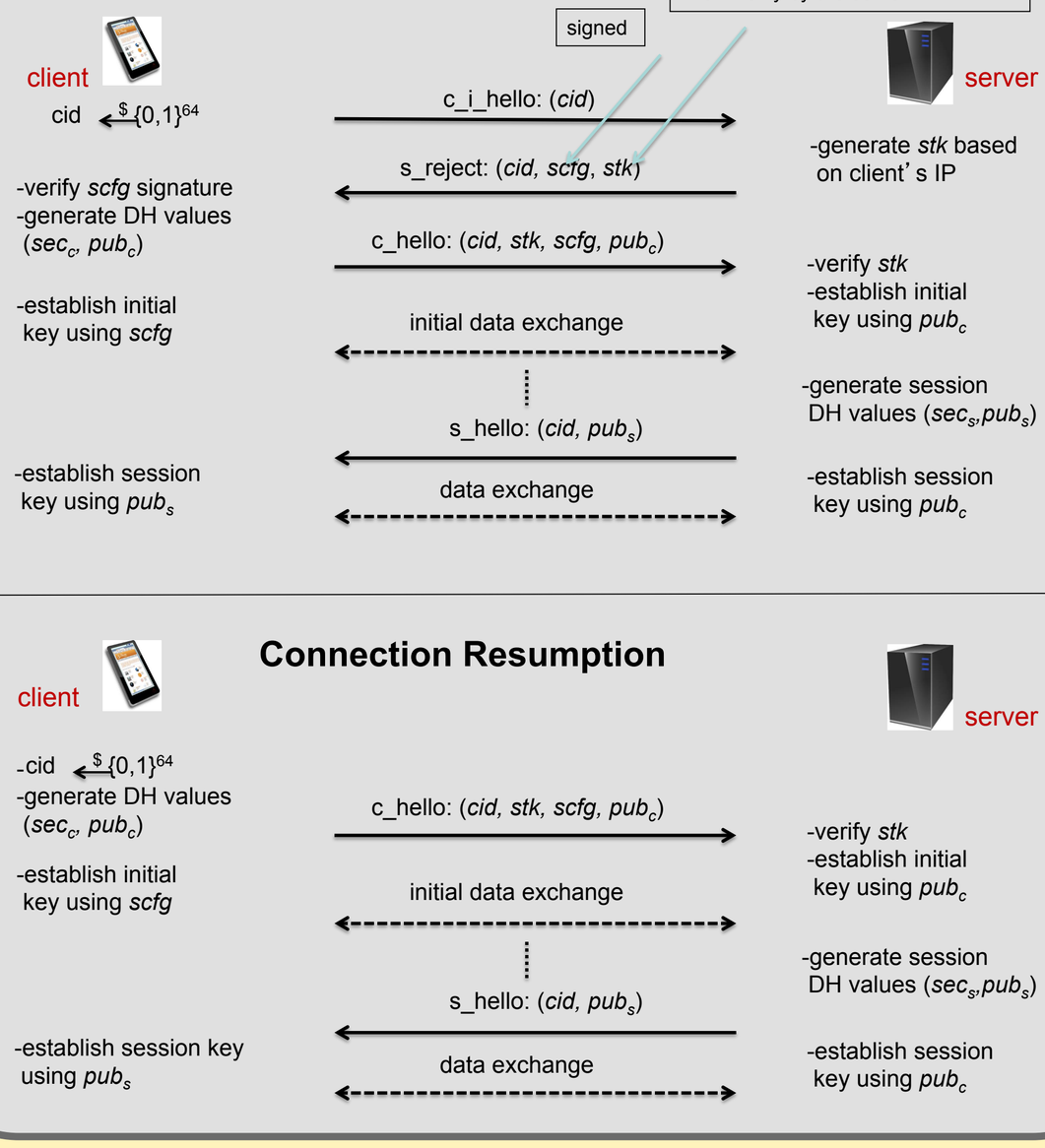
Objective

This project bridges the gap between protocol design, implementation, deployment, and security guarantees by developing a novel general security framework that facilitates the provable-security analyses of practical networking protocols.

Problem

- Many network protocols are deployed without a formal security analysis resulting in attacks discovered after deployment.
- 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.

QUIC

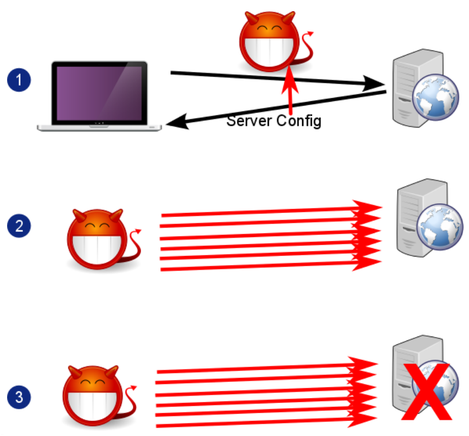


Approach

- 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 and performance.
- 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.

Progress

- Security analysis of QUIC, a secure protocol developed by Google and integrated with Chrome.
- QUIC meets our notion of QACCE-security if
  - Underlying signature scheme is *suf-cma*
  - Associated AEAD is *ind-cpa* and *auth-secure*
  - SCDH Problem is hard
  - In the random oracle (RO) model



Current Work

- TCP Fast Open and TLS False Start promise similar properties to QUIC:
  - Authenticate and encrypt a connection
  - Similar latency promises
  - Key exchange complete after first phase
  - Provided optionally by several browsers
- Analyze security properties for TCP Fast Open + TLS False Start and compare them with QUIC security and performance properties

Interested in meeting the PIs? Attach post-it note below!

National Science Foundation
WHERE DISCOVERIES BEGIN

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9-11, 2017
Arlington, Virginia