Tcpcrypt

The case for ubiquitous transport level encryption

Andrea Bittau, Mike Hamburg,
Mark Handley, David Mazieres, Dan Boneh.

UCL and Stanford.

What would it take to encrypt the vast majority of TCP traffic?

Performance

- Fast enough to enable by default on almost all servers.

Authentication

- Leverage certificates, cookies, passwords, etc., to give best possible security for any given setting.

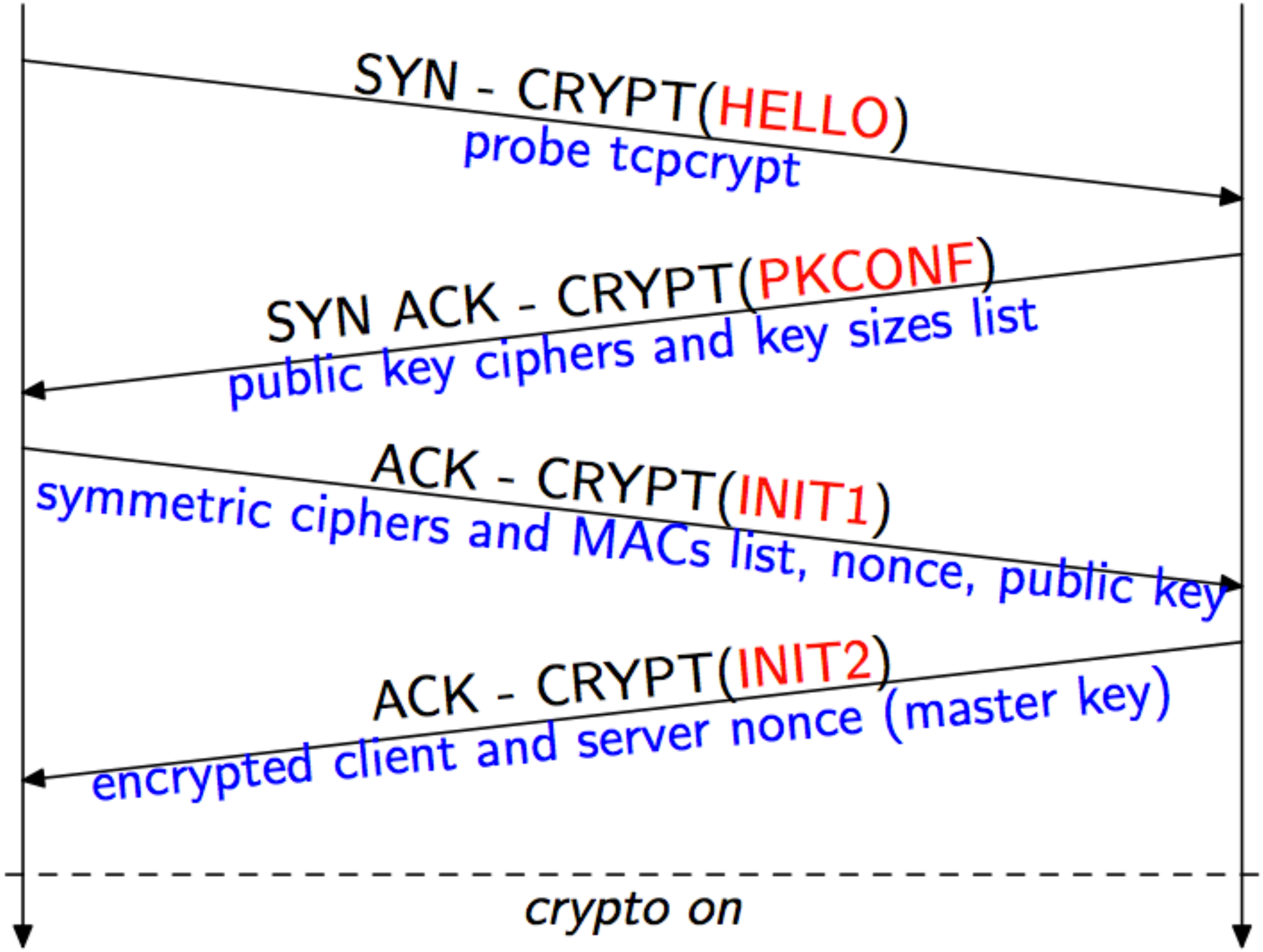
Compatibility

- Works in existing networks
- Works with unmodified legacy applications

Tcpcrypt uses TCP options to provide deployable transport-level encryption.

- High server performance - push complexity to clients
- Allow applications to authenticate endpoints.
- Backwards compatibility: all TCP apps, all networks, all authentication settings.

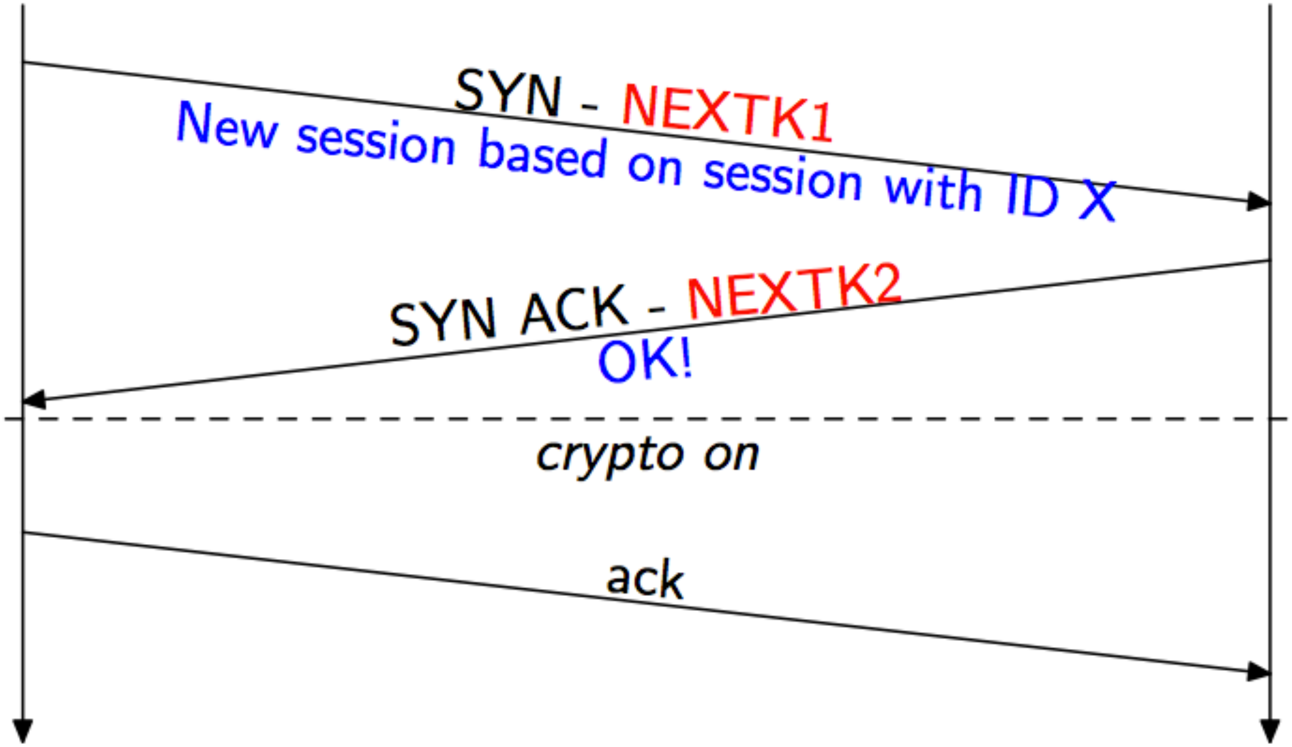
Key exchange is performed in the TCP connection setup handshake.



SYN - CRYPT(HELLO)
probe tcpcrypt
SYN ACK - CRYPT(PKCONF)
public key ciphers and key sizes list
ACK - CRYPT(INIT1)
symmetric ciphers and MACs list, nonce, public key
ACK - CRYPT(INIT2)
encrypted client and server nonce (master key)
crypto on

Crypto state can be cached.

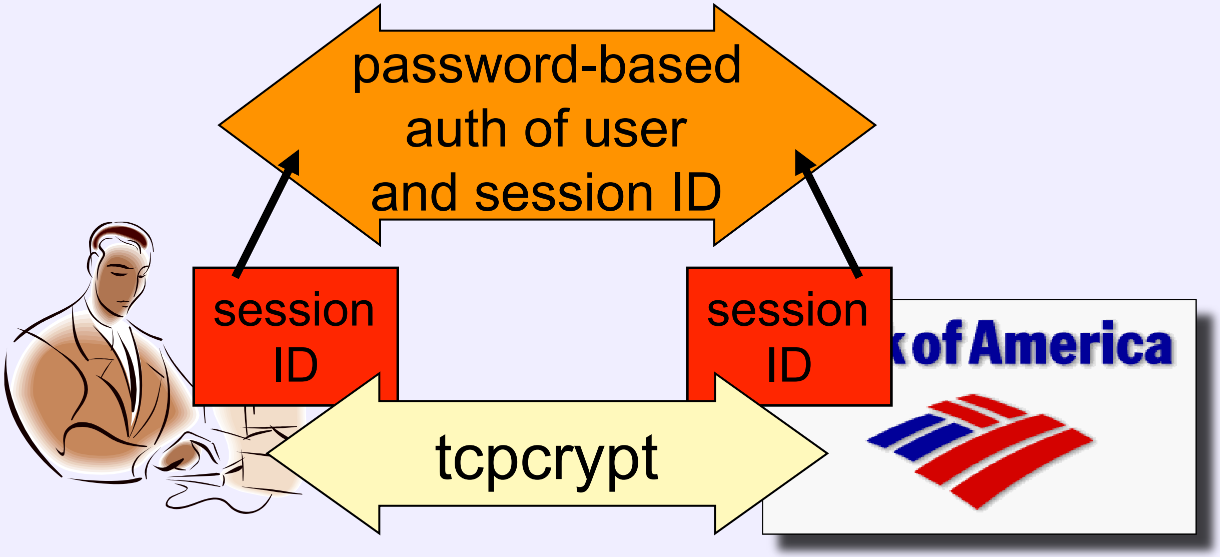
Subsequent connections between the same endpoints get similar latency to regular TCP.



After initial handshake, tcpcrypt’s Session ID provides the hook to link application authentication to the session.

- New **getsockopt()** returns non-secret Session ID value.
- Unique for every connection.
- If same on both ends, guaranteed there’s no man-in-the-middle.

Authenticating the session ID authenticates the endpoint



password-based auth of user and session ID

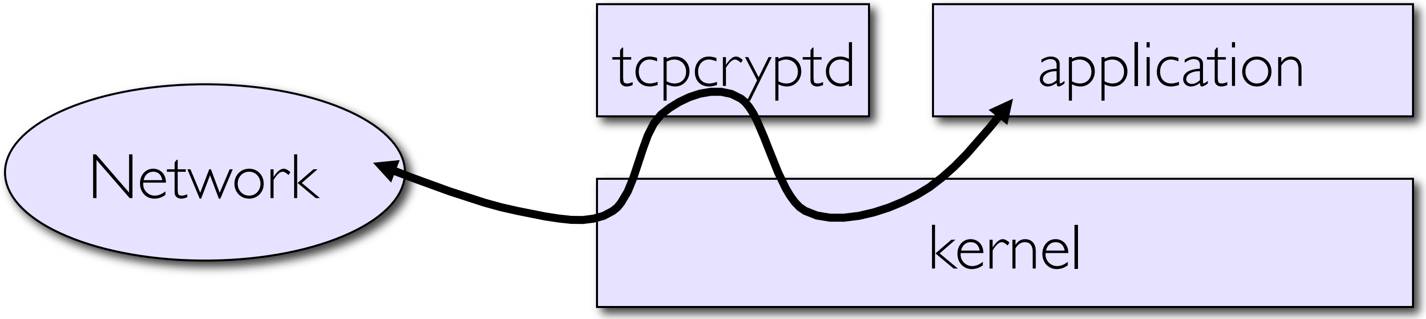
session ID

session ID

tcpcrypt

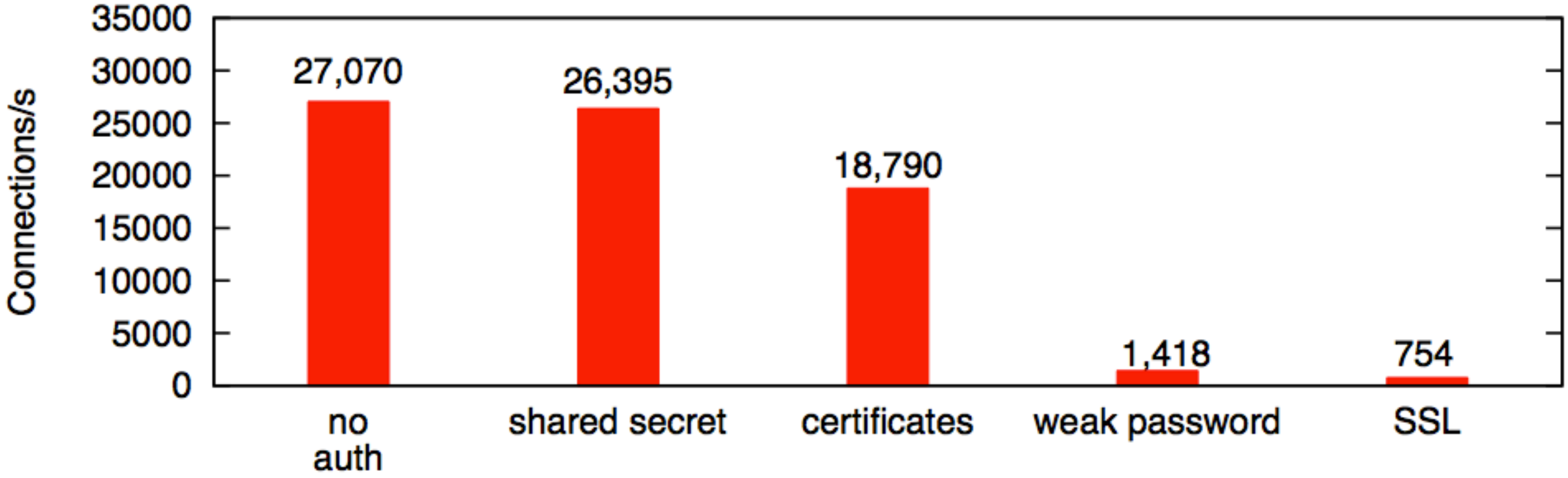
Tcpcrypt implementations

- Linux kernel implementation: 4,500 lines of code
- Portable divert-socket implementation: 7000 LoC
  - Tested on Windows, MacOS, Linux, FreeBSD



- Binary compatible OpenSSL library that attempts tcpcrypt with batch-signing or falls back to SSL.

Authentication over Tcpcrypt is fast.



Summary: the case for ubiquitous transport level encryption

- High server performance makes encryption a realistic default.
- Applications can leverage Tcpcrypt to maximize communication security in every setting.
- Incrementally deployable, compatible with legacy apps, TCP and NATs.

http://tcpcrypt.org

draft-bittau-tcp-crypt-00.txt