Preventing TLS Version Downgrade

IETF 84

Eric Rescorla

ekr@rtfm.com

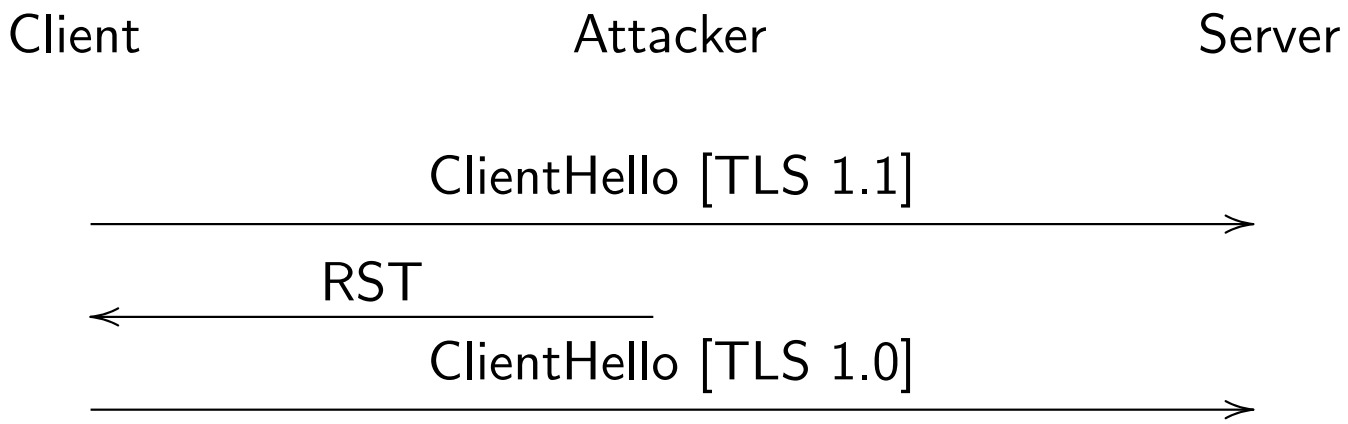
Overview

- TLS 1.n+1 is better than version TLS 1.n
  - Hopefully, at least
- And some extensions make TLS more secure
  - cf. Renegotiation Indication Extension [RFC 5746]

Unfortunately TLS Version/Feature Negotiation isn't perfect

- Some *server* implementations are broken
  - Fail when they receive requests for versions/extensions they don't support
  - *Before the TLS handshake finishes*
- Attackers can simulate these failures
  - In ways indistinguishable from broken implementations

Fallback logic in browsers



Would be nice to do something about this

- Need some way for client/server to detect that they actually do a newer version
  - (Or at least could negotiate correctly)
  - After they have been forced down to an older version
- Only one safe place to signal this
  - In the cipher-suites field
  - Effectively all servers handle unknown cipher-suites correctly
    - That's why we used it for RFC 5746
  - So it's safe for client to advertise capabilities here

Existing Proposals

- Client advertises and server checks
  - Highest supported version (`http://svn.resiprocate.org/rep/ietf-drafts/ekr/draft-rescorla-tls-version-cs.txt`)
  - Indication of TLS support when fallback enabled (`http://www.ietf.org/mail-archive/web/tls/current/msg08861.html`)
- Support of Renegotiation Info as proxy for negotiation compliance (`http://tools.ietf.org/html/draft-pettersen-tls-version-rollback-removal-00`)

Pros/Cons

- New SCSV will be accurate (low false positives)
  - But requires changes on both client and server
  - And nobody has done it yet
  - So will miss a lot of attacks
- Using RI will catch more attacks
  - Already a lot of RI deployment
  - But some false positives ($.1\%$ of RI-patched servers don't negotiate version correctly)

Other challenges

- Some servers choke on big ClientHellos
  - Argument for keeping this list short
- Some intermediaries enforce versions
  - But don't edit cipher-suite list
  - This looks like a downgrade attack
    - Because it is

Questions

- Does the WG want to work on this?
- What approach seems best to start with?