TLS_FALLBACK_SCSV

draft-ietf-tls-downgrade-scsv-00:

“TLS Fallback Signaling Cipher Suite Value (SCSV) for Preventing Protocol Downgrade Attacks”

Bodo Möller
Adam Langley

IETF TLS Interim, October 2014

The problem

- Version negotiation can fail in practice
  - Version-intolerant servers look fine until it's too late
- Many clients (notably, browsers) use fallback retries to work around such server bugs
  - Documented in RFC 5246, App. E.1:
    "Interoperability with such buggy servers is a complex topic beyond the scope of this document, and may require multiple connection attempts by the client."
- Attackers can trigger downgrade

Avoiding downgrade attacks

- Ideally, stop doing fallback retries
- If that's not practical, clients should add `TLS_FALLBACK_SCSV` to `ClientHello.cipher_suites` in fallback retries
- Servers that detect `TLS_FALLBACK_SCSV` will reject the connection if `ClientHello.client_version` is a downgrade

Practical experience

- Supported in suitable versions of Chrome, Firefox
- Supported on Google servers
- Deployed for more than half a year
- Win: protection against POODLE attack

Design rationale

- Why a SCSV?
  - Originally, required for SSL 3.0 (w/o extensions)
  - Don’t require TLS servers to parse extensions
  - SCSV is sufficient (very simple mechanism)
  - Side benefit: more efficient wire format
- Why client-side “SHOULD [send]”, server-side “MUST [reject]”?
  - Client drives fallback strategy
  - Don’t allow server heuristics to interfere

Expected changes

- No change to mechanism, but clarify:
  - Qualify RFC 5246 App. E.1's "SHOULD initiate the connection in [the server's] native protocol"
    - don't stick to version indefinitely
  - If client sees `inappropriate_fallback`, forget server's highest protocol version
  - Be fully clear that TLS_FALLBACK_SCSV is *only* for downgraded handshakes (say when *not* to send it)

Expected changes (cont'd)

- Update False Start I-D:
  - Shouldn't do False Start if server picks old protocol
    - might be attacker selecting the protocol
  - TLS_FALLBACK_SCSV Security Considerations to point out that the SCSV can't prevent this