TLS Next Protocol Negotiation Extension

Wan-Teh Chang
IETF 82, 2011-11-17
Introduction

Recap of next protocol negotiation (NPN)

Status

Issues
NPN in three steps

Client sends empty NPN extension in ClientHello

Server responds with a list of protocol strings in NPN extension in ServerHello, for example,

```
"\x06spdy/2\x08http/1.1\x08http/1.0"
```

Client informs server of selected protocol in encrypted NextProtocol handshake message (between ChangeCipherSpec and Finished)
Status

draft-agl-tls-nextprotoneg-02 expired in October

Current NPN spec is at
http://technotes.googlecode.com/git/nextprotoneg.html

Implemented in Chrome and Firefox
(upcoming) to piggyback HTTP/SPDY
negotiation on TLS handshake
Issues raised in reviews of draft

Protocol strings vs. port numbers:
● We have come up with more uses for the protocol strings (such as signalling WebSockets over SPDY support)

Encrypted handshake messages between ChangeCipherSpec and Finished:
● The encrypted client certificates extension also needs this