TLS Fallback Dance

What is the fallback dance?

- After a failed TLS connection attempt:
    - Client retries with different versions and parameters.

Who does it?

- web browsers
- others ???

Why the fallback dance?

- Buggy servers
  - extension incompatibility
  - version incompatibility
- Clients lose userbase without it

Why not?

- network glitches
- MITM-induced downgrade attack

Can we recommend against it while documenting it?

Different versions?

- Different contexts?
  - Web browsers
  - MTAs (?)
  - ???
- What kind of things should be tried at each step?
- stored state vs amnesiac

Stored State?

What should a TLS client that does the fallback-dance store?

- last known good version
- per server? per domain? per port?
- what kind of timeouts?

UTA's role?

- TLS WG is already working on standardizing a tool for use with fallback (`draft-ietf-tls-downgrade-scsv`)
- No documentation of the right way to do this
- identification of other mechanisms needed?
- plans to kill off fallback?

Risks

- encouraging bad practice

- keeping broken servers on life support