TLSv1.0 and TLSv1.1

Is it time to begin deprecation?

https://tools.ietf.org/html/draft-moriarty-tls-oldversions-diediedie-00

Stephen Farrell & Kathleen Moriarty

Contributions Requested

1. Meaningful statistics across different applications using TLS
    a. HTTP, SMTP, XMPP, etc.
2. Examples of systems or applications for which no upgrade path is available
3. Considerations for networks where upgrades may be difficult
    a. Can systems be isolated to the point that using a deprecated protocol does not matter?
    b. If there are cases on internal networks, is it possible for clients to continue support for deprecated protocols in limited use cases? For example, HTTP to internal or partner networks that is explicitly allowed by subdomain or some other means of identifying applications, systems, or network domains.
4. Additional considerations?

GitHub: https://github.com/sftcd/tls-oldversions-diediedie

Timing

Considering libraries like OpenSSL will continue to support TLSv1.0 and TLSv1.1 in their next release for 5 years, should we begin the formal deprecation process?

- Numbers reported for HTTP are very low for Internet facing usage
- Allows a gradual transition to possibly gain momentum
- Deprecation takes a while even with the formal statement