HTTP and TLS
HTTP and TLS in One Slide

• Separate port (default: 443) and separate URI scheme (https://)
  • Optional and at the pleasure of the server
• Server authentication is mandatory
• Client authentication is optional and rare
Opportunistic Encryption

- TLS for http:// URIs
  - Protects against passive (not active) attackers
  - Come to HTTPbis on Tuesday AM for more
The Proxy Problem

- Proxies are interposed by networks to do many things
  - Content filtering, access control, virus scanning, etc.
- More encryption disadvantages networks
  - Response is to block encrypted connections to unknown servers
- Discussion of making the proxy role more explicit/refined is starting
TLS Issues from a HTTP Perspective

• CAs have become a significant attack vector / escape valve
  • Current model or trust is simplistic
• Emerging tendency to put more information in ClientHello
  • Interop issues?
• HTTP over TLS only allows one origin per connection
  • Limits benefits of using HTTP/2.0
• TLS is still very difficult to deploy for many