**Certificates and Encryption**

**HTTPS everywhere (Plugin)**

Enables HTTPS encryption automatically on sites that are known to support it

Gives option to block all HTTP requests

* NoScript and uBlock can also do this

SSL Observatory

* Sends copies of HTTPS certificate to observers’ tree to help prevent MITM attacks and build their DB
* Let’s them warn you about insecure connections or attacks on your browser
* Privacy concern, constant communication with SSL Observatory, providing them with certificates of sites you visit
  + Can be used through Tor
  + Not good for privacy unless using another anonymising service

**Firefox config**

* About:config
* Browser.urlbar.trimURLs
* Change to false to show HTTP or HTTPS connection

Certificate Patrol

* Tells you when certificates are changed
* So, you can determine manually whether the change is dodgy or legitimate
* However, sites change their certificates so often, this is sometimes not that useful

Perspectives

* Checks certificates against network notaries to securely identify certificates
* Shows what certificates are being shown to other people
  + If most people are being shown the same certificates, chances are its legit
  + Decentralised
  + Needs more users to be useful
* Difficult again because certificates change all the time
* Potential privacy concern

Calomel SSL Validation

* Score strength of SSL encryption
* Like SSL labs

CipherFox

* Displays current SSL/TLS cipher, protocol and certificate chain in the add-on bar

Toggle Cipher Suites

* Change the cipher suites that your browser supports
* GUI for about:config 🡪 security.ssl3

Test browser with SSL labs or Qualys

* Show which cipher suites your browser supports