HTTPS

Normal HTTP process

- Open connection to server on fixed network port (default 80)
- Transmit HTTP request
- Receive HTTP response

Safety of transmitted data?

- Can be tapped
- Can be altered!

Secure sockets

- Set up an “encrypted” channel between client and server
- How?
  - Need a shared secret - eg. long binary string - this is the “key”
  - XOR all input data with key to generate new binary data
  - Attacker without key cannot derive actual data
- How to set up shared secret?
  - Must assume anything on the wire can be tapped!
  - What about pre-existing key?
  - Secure side channel - send a token by post, SMS

Types of security

- Channel (wire) security
  - Ensure that no one can tap the channel - most basic need for other auth mechanisms etc.
- Server authentication
  - How do we know we are actually connecting to mail.google.com and not some other server?
  - DNS hijacking possible - redirect to another server!
  - Server certificates
  - Common root of trust needed - someone who “vouches for” mail.google.com
- Client certificate
  - Rare but useful - server can require client certificate
  - Used especially in corporate intranets etc.

mail.google.com/n

GTS Root R1

GTS CA 1C3

mail.google.com

mail.google.com

Issued by: GTS CA 1C3

Expires: Monday, 8 November 2021 at 9:27:01 AM India Standard Time

This certificate is valid

Trust

Details

Subject Name	
Common Name	mail.google.com
Issuer Name	
Country or Region	US
Organisation	Google Trust Services LLC
Common Name	GTS CA 1C3
Serial Number	00 B5 B5 F0 63 90 2E B6 D9 0A 00 00 00 00 FA

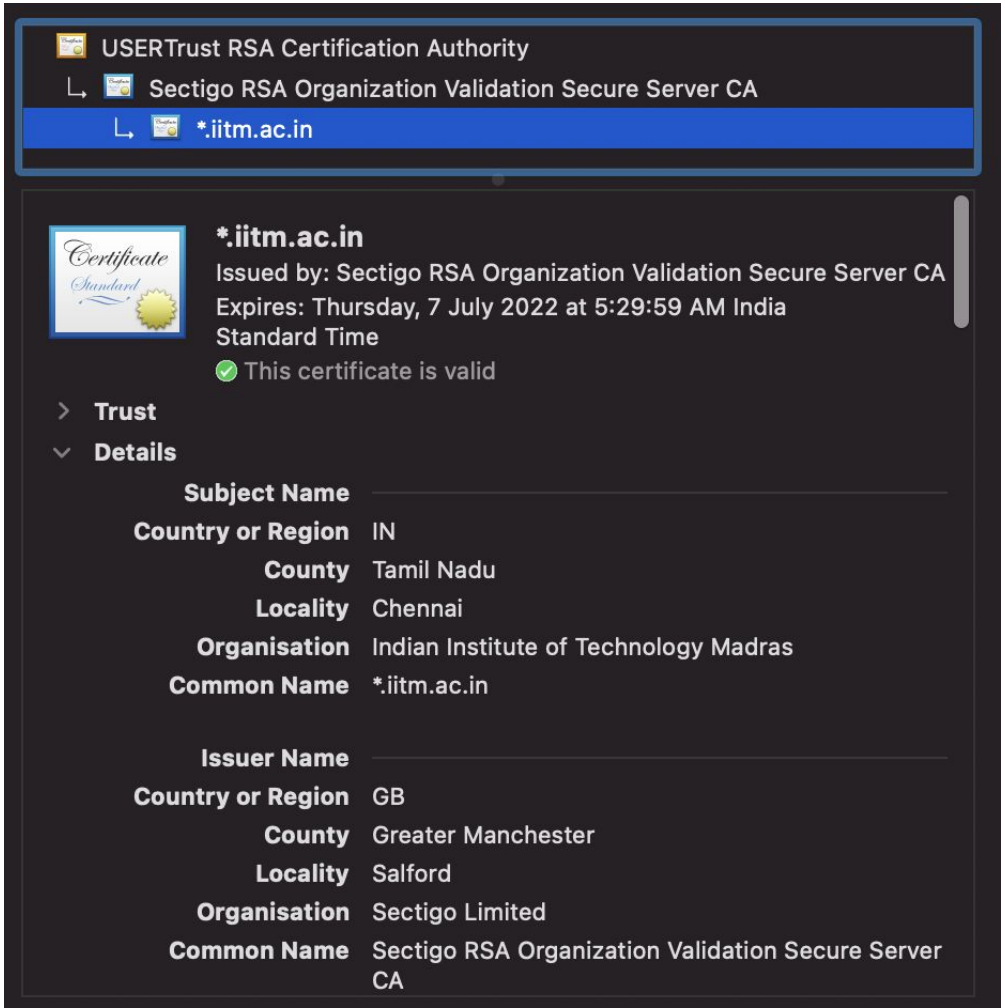
Chain of Trust

- Chain of trust
  - mail.google.com issued certificate by
  - GTS CA1C3 issued certificate by
  - GTS Root R1
- GTS Root R1 certificate stored in Operating System or Browser
  - Do you trust your OS? Do you trust your browser?
- From there on a secure (crypto) chain

Potential problems

- Old browsers
  - Not updated with new chains of trust
- Stolen certificates at root of trust
  - Certificate revocation, invalidation possible
  - Need to ensure OS, browser can update their trust stores
- DNS hijacking
  - Give false IPs for server as well as entries along chain of trust
  - But certificate in OS will fail against eventual root of trust

Wildcard certificates



Impact of HTTPS

- Security against wiretapping
- Better in public WiFi networks

Negative:

- Affects caching of resources (proxies cannot see content)
- Performance impact due to run-time encryption