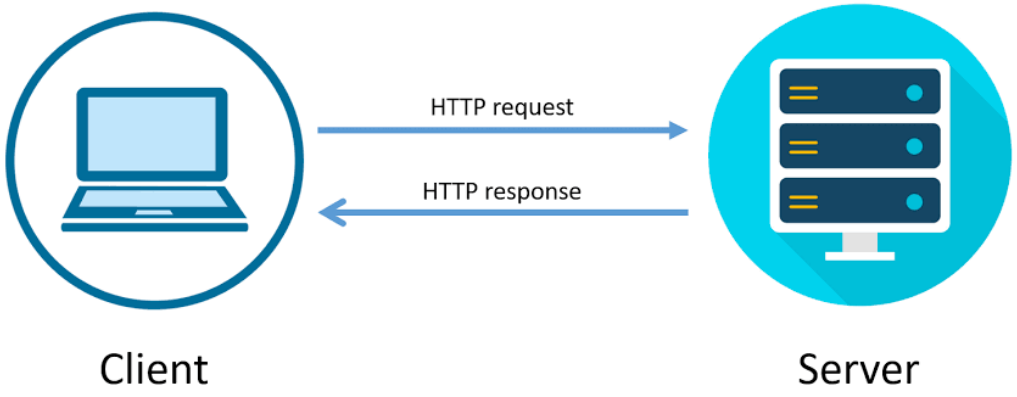
HTTP, HTTPS & TLS

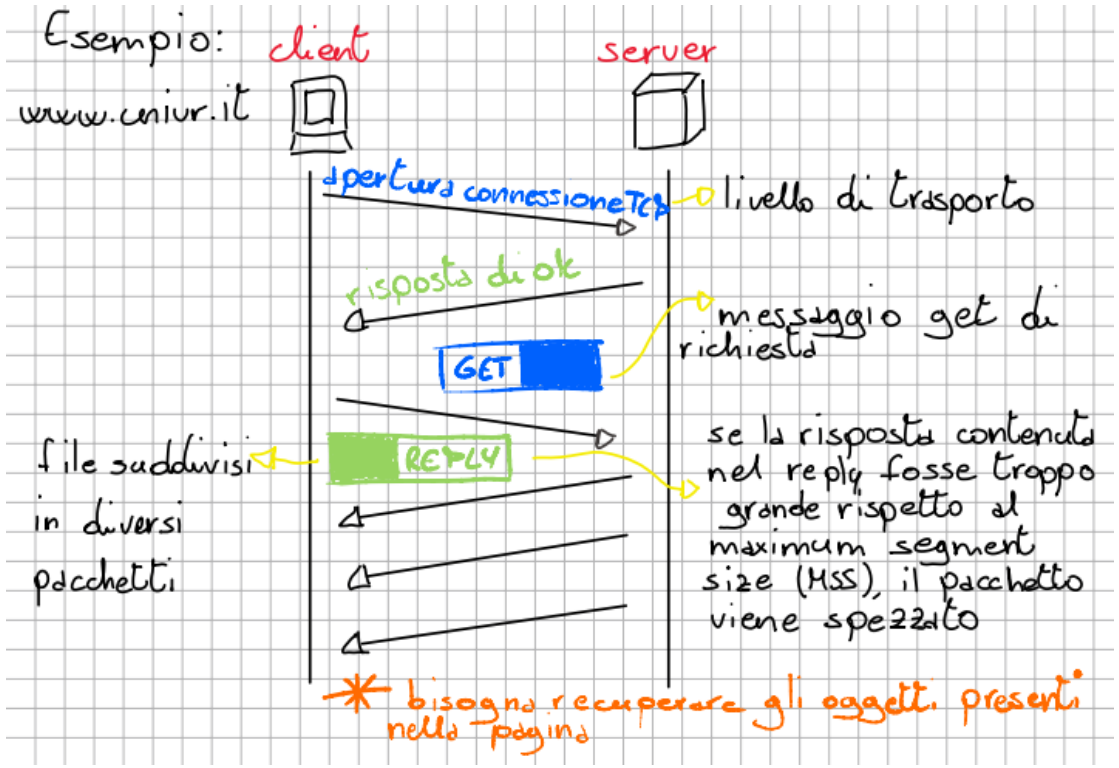
Mattia Pacchin – mattia@v-research.it

V-ReseArch Edu

HTTP

- HTTP = Hyper Text Transfer Protocol
- Viene utilizzato dal web
- Deve garantire una comunicazione affidabile -> TCP
- Porta di default: 80





V-ResearchEdu

Richiesta HTTP

- Ci sono due modi per recuperare gli oggetti presenti nella pagina:
  1. Connessioni persistenti (stateful)
  2. Connessioni non persistenti (stateless) -> per ogni oggetto richiesto apro e chiudo la connessione
- Come sono fatti i messaggi di richiesta e di risposta?
- Il protocollo HTTP è un protocollo testuale il cui messaggio è formato da due parti:
- Riga di richiesta: GET /pagina.html HTTP/1.1
  - Sul browser: www.univr.it/pagina.html -> server/file che voglio ottenere
- Righe di intestazione:
  - HOST: www.univr.it -> sola riga obbligatoria per sicurezza
  - User-agent: Mozilla/4.0 -> permette al server di dare una risposta su misura (es. mobile)
  - Accept language: en
- Sul browser avrò, per esempio, www.univr.it/index.html

Risposta HTTP

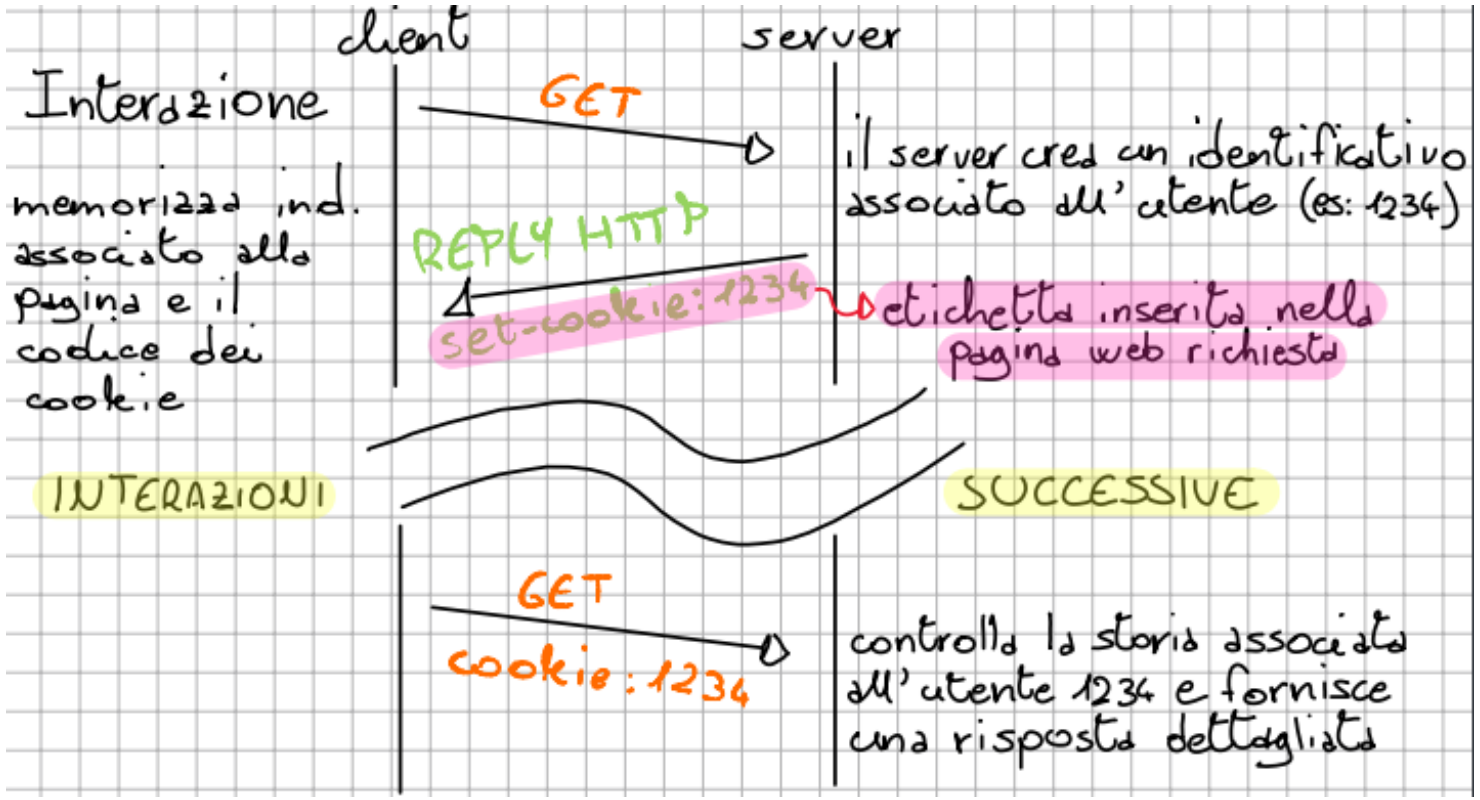
- Messaggio di risposta HTTP -> c'è sempre, per ogni richiesta
- È formato da:
- Riga di stato: HTTP/1.1 «codice di risposta» «descrizione della risposta»
  - Esempi di codici di risposta:
    - 200 -> oggetto richiesta presente sul server
    - 404 -> not found
    - 400 -> richiesta non compresa (non seguiva il protocollo)
- Righe di intestazione:
  - Etichetta: valore
- Riga vuota: [ ]
- Dati: _____dati _____

Metodi HTTP

- I metodi HTTP più utilizzati sono:
  1. GET -> ottenere una risposta
  2. POST -> inviare informazioni al server (es. risposta di un forum)
  3. DELETE -> eliminare un file sul server

Altri elementi di HTTP - Cookie

- Cookie -> permettono al server di sapere se ha già interagito con un determinato client

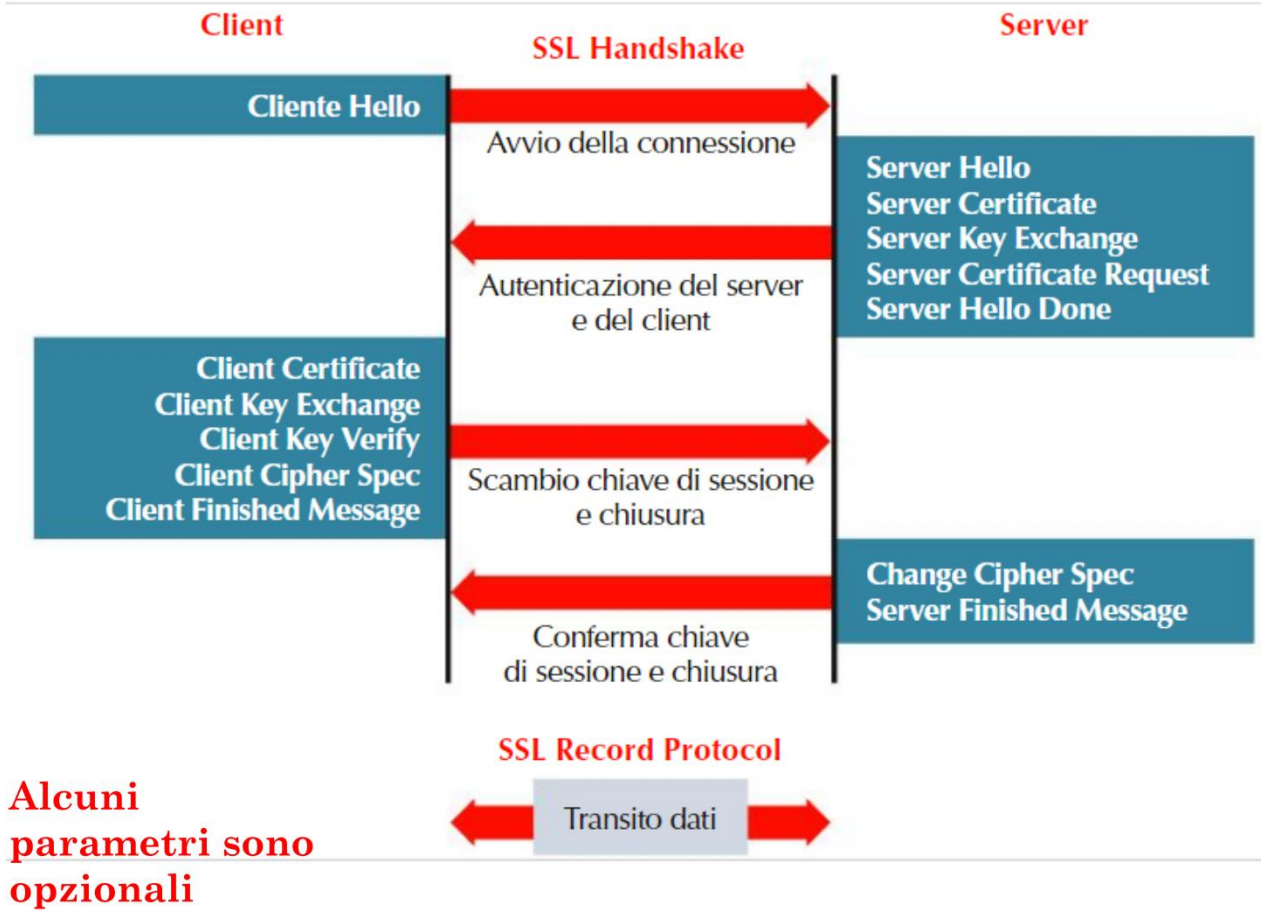


V-ResearchEdu

SSL/TLS

- Obiettivi del TLS per una comunicazione sicura:
  1. Autenticazione delle parti (server sempre autenticato; client facoltativo)
  2. Confidenzialità dei dati
  3. Integrità dei dati
- Insieme di protocolli crittografici che aggiungono funzionalità di autenticazione e cifratura
- Si colloca tra il livello di trasporto (TCP) e il livello applicativo, garantendo così una comunicazione sicura a tutte le applicazioni che si appoggiano ad esso
- Viene utilizzata una chiave asimmetrica per autenticare client e server e per lo scambio della chiave di sessione
- Per garantire la riservatezza dei dati viene utilizzata la crittografia simmetrica la cui chiave di sessione viene scambiata con crittografia asimmetrica
- Introduce controlli sull'integrità del messaggio tramite hash (es. SHA)

TLS handshake protocol

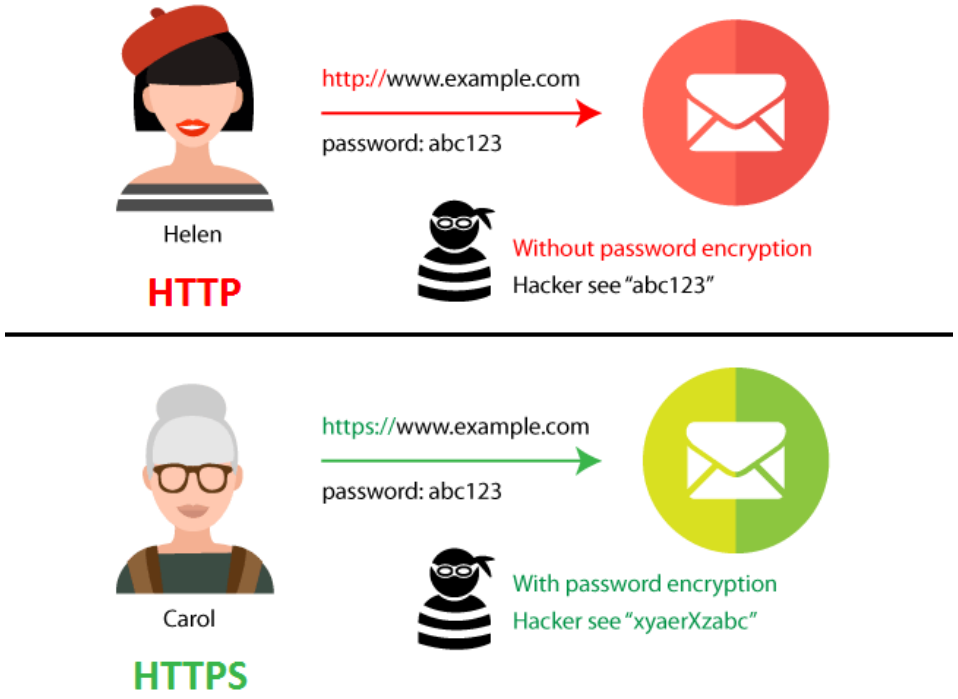


Alcuni parametri sono opzionali

V-ResearchEdu

HTTPS (HTTP over SSL)

- HTTPS è la versione sicura di HTTP, ovvero implementa – a contrario di quanto indicato dall'acronimo – il TLS
- Implementa tutte le funzionalità di sicurezza previste da TLS
- Porta di default: 443



V-ReseArch Edu