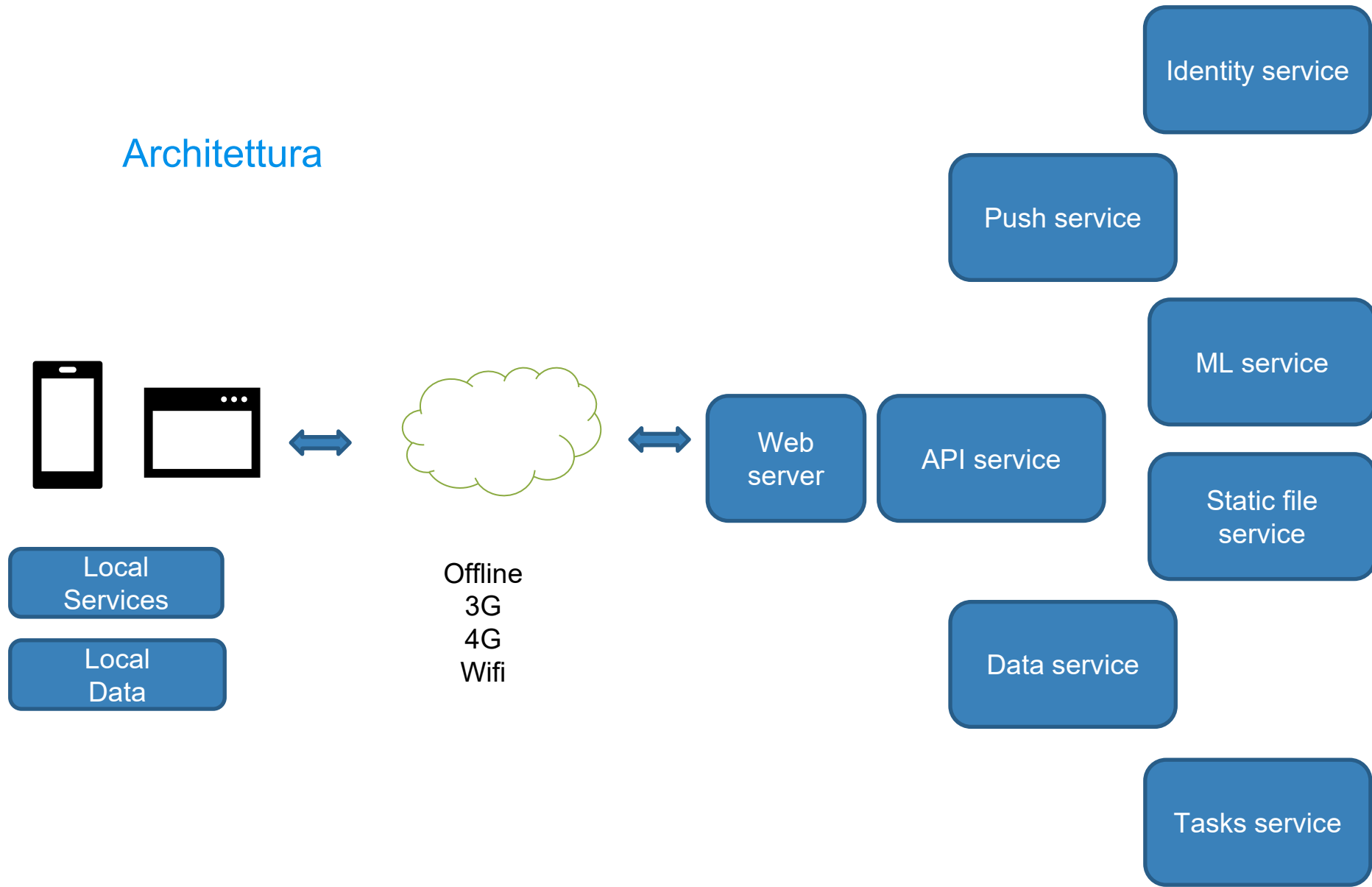


A decorative network diagram in the top-left corner, consisting of various sized nodes (some solid grey, some hollow white) connected by thin grey lines, forming a complex web structure.

2. Architettura

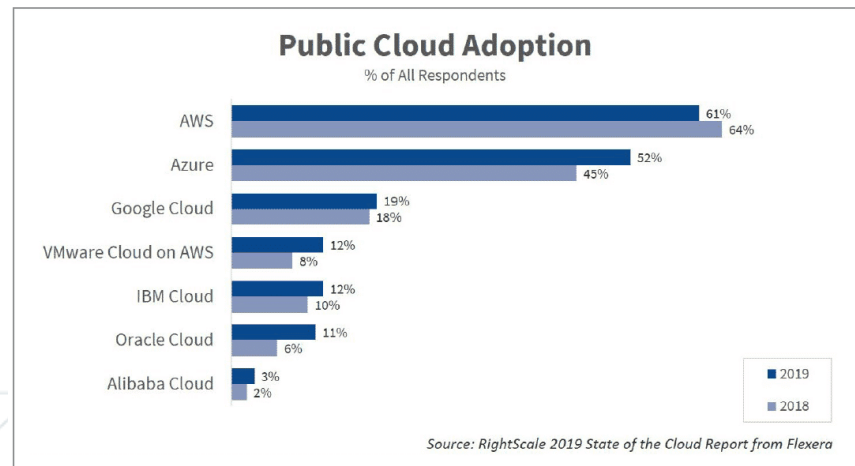
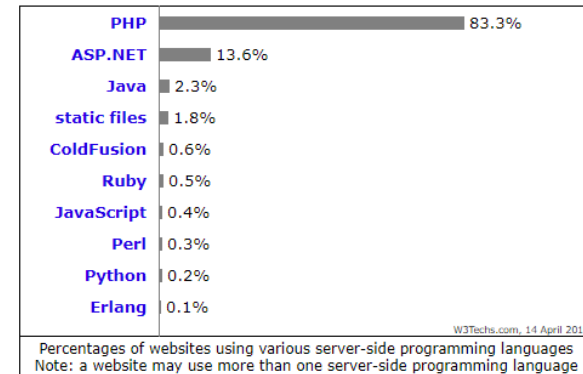
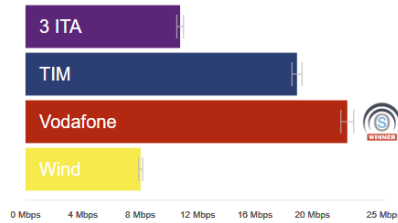
Architettura



Diffusione tecnologie



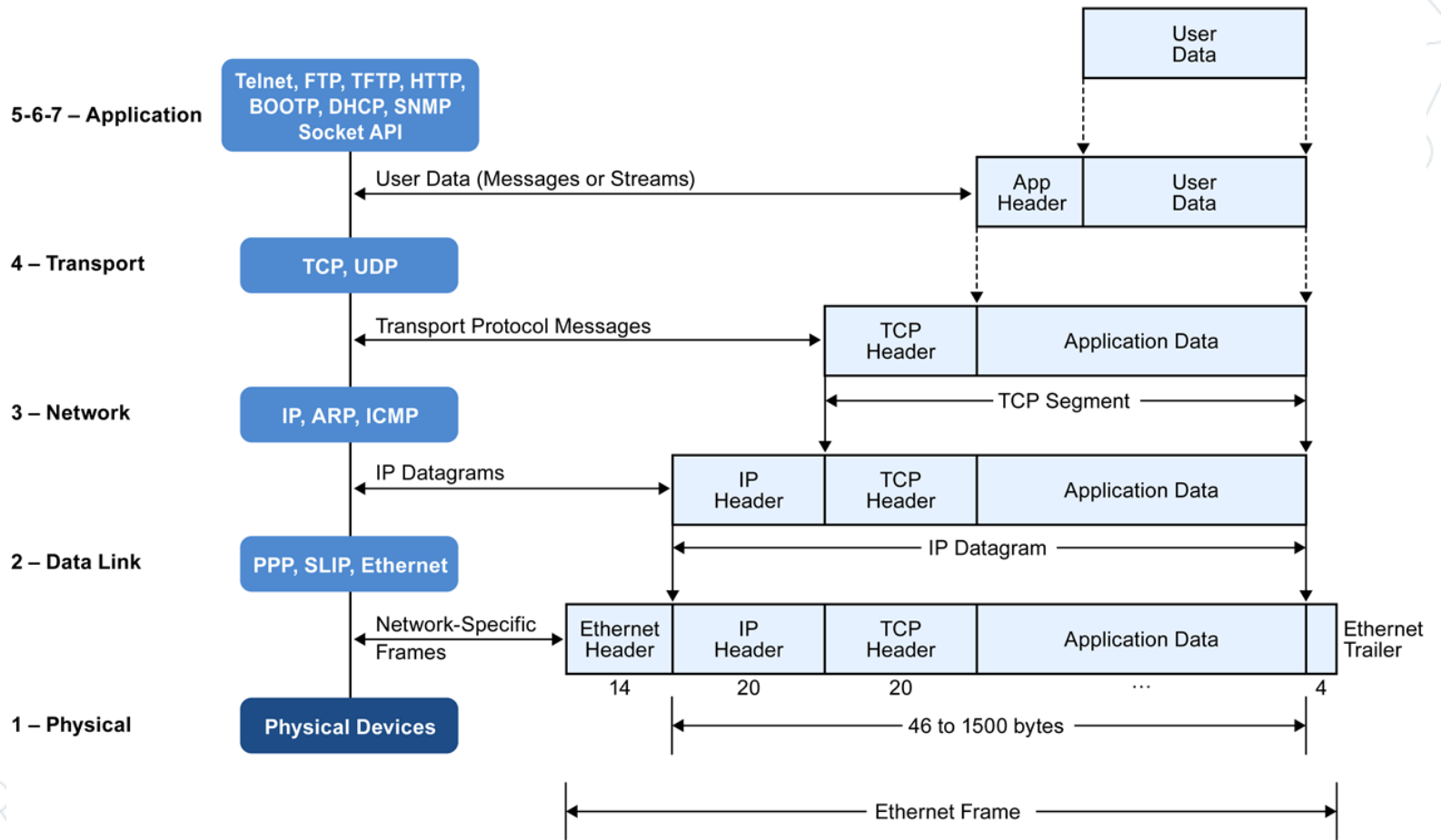
Download Speed: Overall OpenSignal



Protocolli

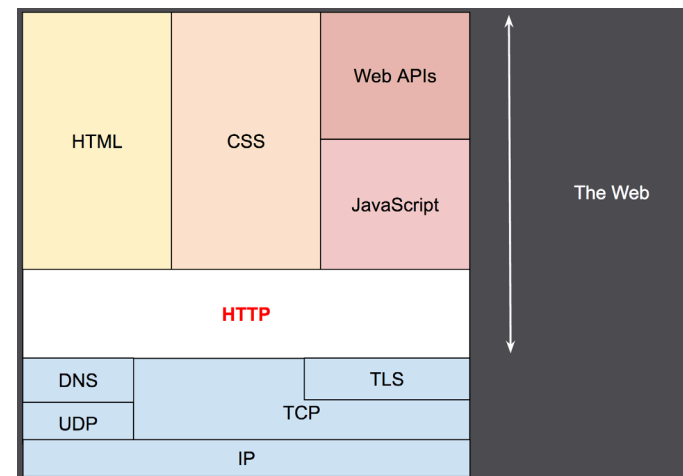


Modello ISO/OSI



HyperText Transfer Protocol (HTTP - rfc2616)

- Protocollo a livello applicativo
- A livello di trasporto si basa sul TCP (o TLS)
- Request/Response (Client / Server)
- Url composta da http://host:port/path/file
- Metodo: GET/POST/PUT/DELETE/OPTIONS..
- Stato nella risposta: 200/300/400/404/500
- Header di request e di response
- Gestione cookie
- Diversi content-type (html/text/image/json/xml)



HyperText Transfer Protocol

(1) User issues URL from a browser
<http://host:port/path/file>



(5) Browser formats the response and displays

Client (Browser)

(2) Browser sends a request message

```
GET URL HTTP/1.1  
Host: host:port  
.....  
.....
```

(4) Server returns a response message

```
HTTP/1.1 200 OK  
.....  
.....
```

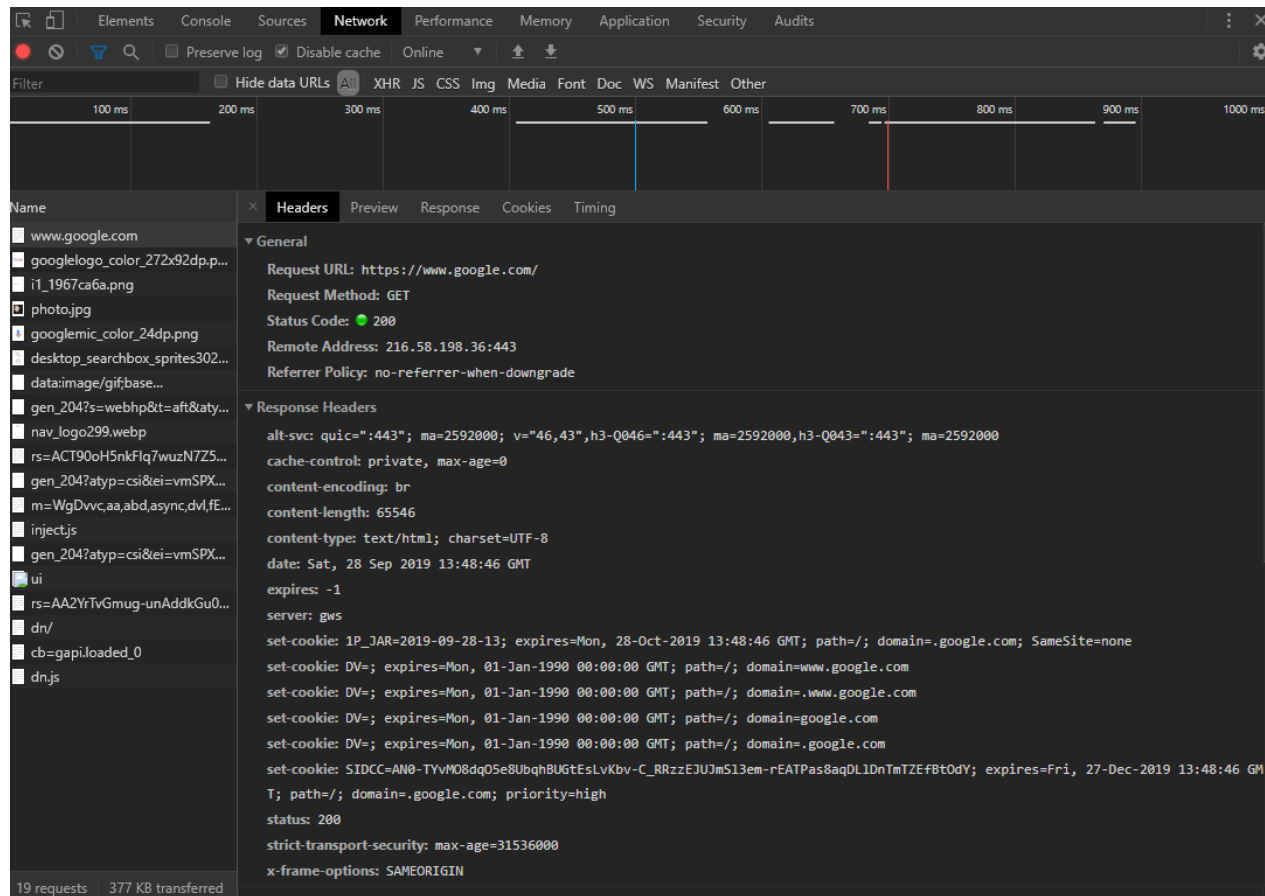
HTTP (Over TCP/IP)

(3) Server maps the *URL* to a file or program under the document directory.

Server (@ *host:port*)

HyperText Transfer Protocol

Studiare:
Headers – Metodi - Cookie – Status Code - Timing



The screenshot displays the Chrome DevTools Network tab. The top panel shows a timeline of network requests. The selected request is a GET request to `www.google.com`. The 'Headers' tab is active, showing the following details:

- General:**
 - Request URL: `https://www.google.com/`
 - Request Method: `GET`
 - Status Code: `200`
 - Remote Address: `216.58.198.36:443`
 - Referrer Policy: `no-referrer-when-downgrade`
- Response Headers:**
 - `alt-svc: quic=":443"; ma=2592000; v="46,43",h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000`
 - `cache-control: private, max-age=0`
 - `content-encoding: br`
 - `content-length: 65546`
 - `content-type: text/html; charset=UTF-8`
 - `date: Sat, 28 Sep 2019 13:48:46 GMT`
 - `expires: -1`
 - `server: gws`
 - `set-cookie: 1P_JAR=2019-09-28-13; expires=Mon, 28-Oct-2019 13:48:46 GMT; path=/; domain=.google.com; SameSite=none`
 - `set-cookie: DV=; expires=Mon, 01-Jan-1990 00:00:00 GMT; path=/; domain=www.google.com`
 - `set-cookie: DV=; expires=Mon, 01-Jan-1990 00:00:00 GMT; path=/; domain=.www.google.com`
 - `set-cookie: DV=; expires=Mon, 01-Jan-1990 00:00:00 GMT; path=/; domain=google.com`
 - `set-cookie: DV=; expires=Mon, 01-Jan-1990 00:00:00 GMT; path=/; domain=.google.com`
 - `set-cookie: SIDCC=AN0-TYVM08dq05e8UubqhBUGtEslvKbv-C_RRzzEJU7mS13em-rEATPas8aqDL1DnTmTZEfBt0dY; expires=Fri, 27-Dec-2019 13:48:46 GMT; path=/; domain=.google.com; priority=high`
 - `status: 200`
 - `strict-transport-security: max-age=31536000`
 - `x-frame-options: SAMEORIGIN`

At the bottom of the network panel, it indicates '19 requests' and '377 KB transferred'.

HyperText Transfer Protocol

GET www.google.it

Untitled Request

GET www.google.it

Params Authorization Headers (9) Body Pre-request Script Tests Settings

Query Params

KEY	VALUE	DESCRIPTION
Key	Value	Description

Body Cookies (2) Headers (12) Test Results

Status: 200 OK Time: 69ms Size: 5.57 KB Save Response

KEY	VALUE
Date	Sat, 28 Sep 2019 14:00:55 GMT
Expires	-1
Cache-Control	private, max-age=0
Content-Type	text/html; charset=ISO-8859-1
P3P	CP="This is not a P3P policy! See g.co/p3phelp for more info."
Content-Encoding	gzip
Server	gws
Content-Length	4996
X-XSS-Protection	0
X-Frame-Options	SAMEORIGIN
Set-Cookie	1P_JAR=2019-09-28-14; expires=Mon, 28-Oct-2019 14:00:55 GMT; path=/; domain=.google.it; SameSite=none
Set-Cookie	NID=188=bYVhzxIbugZ36jBJEs90gZwulQ8oVHVIVPWDzr4d-JQkMWk-hFF75qXqnZWQjmq-mLeIKe3NoLb9_UN4oNnZMCm6fWl3jbTmNbM7...

HyperText Transfer Protocol

Limiti del protocollo:

- Una connessione per request/response
- Mancanza di gestione delle priorità su connessioni multiple
- Bassa compressione (no header compression)

Es: Apache Web Server Settings

Concurrent Connections

By default apache2 is configured to support 150 concurrent connections. This forces all parallel requests beyond that limit to wait. Especially if, for example, active sync clients maintain a permanent connection for push events to arrive.

This is an example configuration to provide 8000 concurrent connections.

```
<IfModule mpm_worker_module>
  ServerLimit          250
  StartServers         10
  MinSpareThreads     75
  MaxSpareThreads     250
  ThreadLimit         64
  ThreadsPerChild     32
  MaxRequestWorkers   8000
  MaxConnectionsPerChild 10000
</IfModule>
```

Browsers:

Version	Maximum connections
Internet Explorer® 7.0	2
Internet Explorer 8.0 and 9.0	6
Internet Explorer 10.0	8
Internet Explorer 11.0	13
Firefox®	6
Chrome™	6
Safari®	6
Opera®	6
iOS®	6
Android™	6

HTTP2 - rfc7540

Multiplexing

Upwork

HTTP 1.1

3 TCP CONNECTIONS



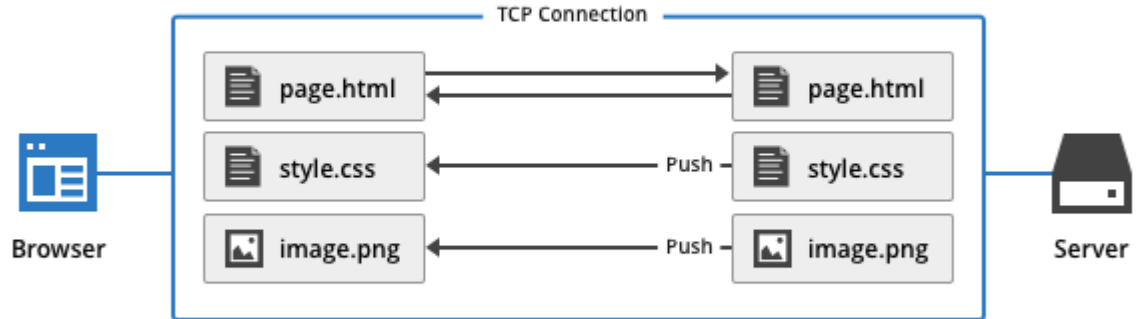
HTTP/2

1 TCP CONNECTION

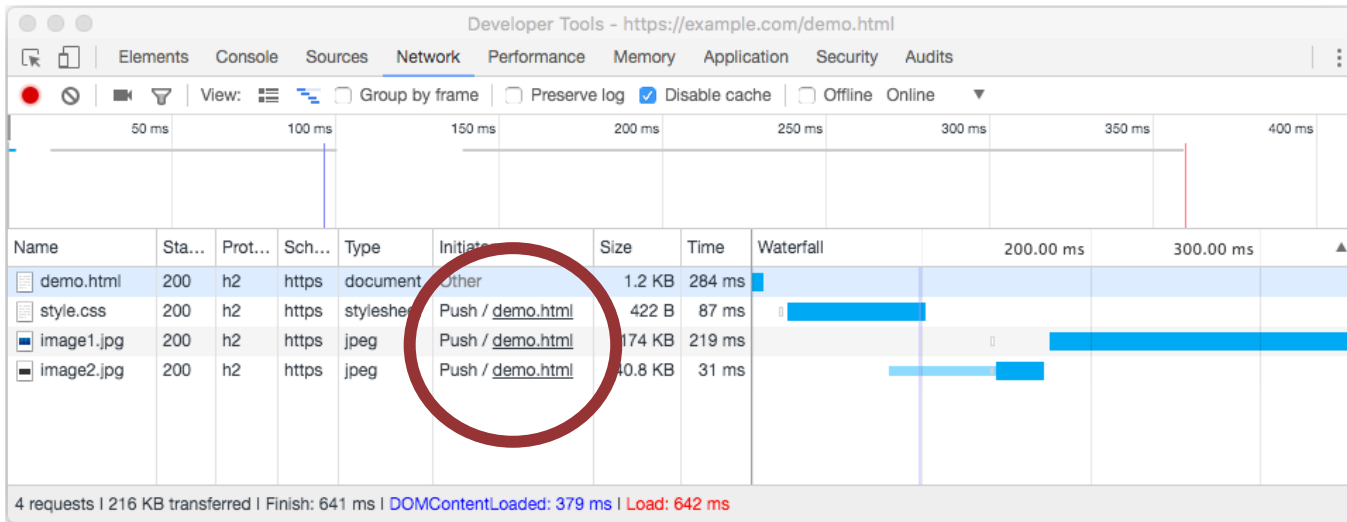


HTTP2

HTTP/2 (With Server Push)



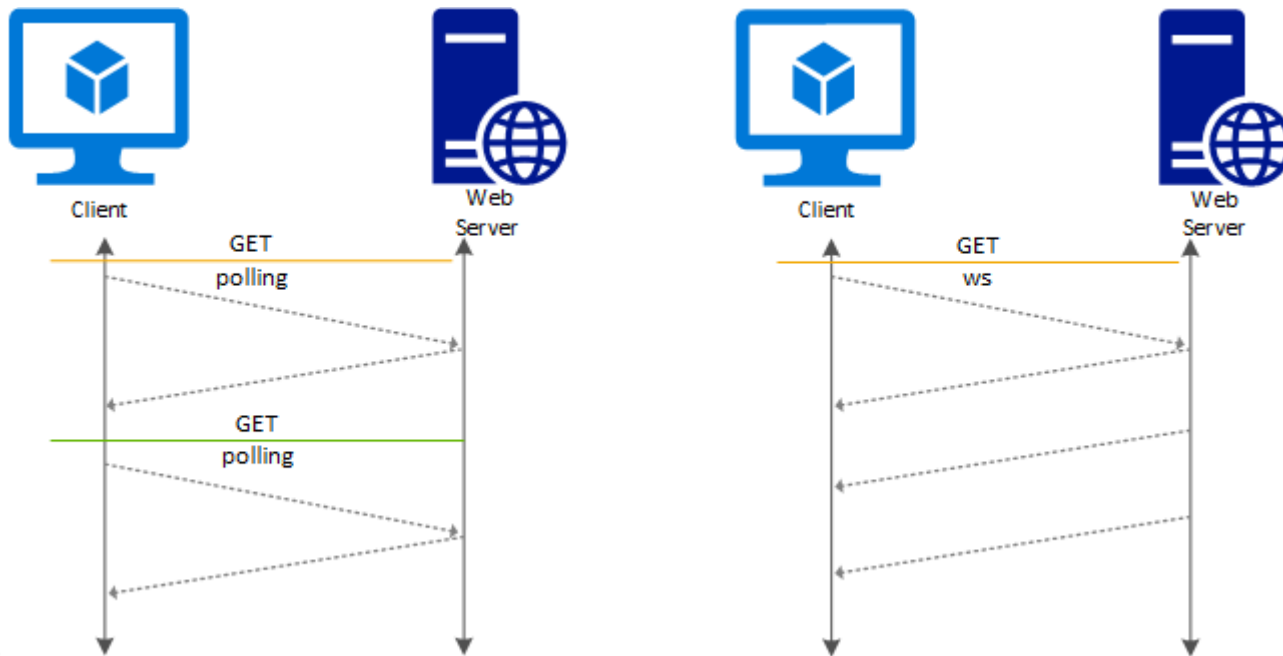
Single TCP Connection, Single HTTP Request



WebSocket - rfc6455

Limiti del protocollo:

- Primo handshake su http
- Se tutto va bene il protocollo della connessione passa da http a websocket (usando la connessione Tcp precedentemente aperta dalla prima connessione http)
- A questo punto rimane solo il protocollo websocket
- Scambio messaggi bidirezionale



OT: Come gestire le password



Sicurezza

No matter how secure you think you might be, something malicious can always happen. Because, "***With the right tools and Talent, a Computer is an open book.***"

Joanna Rutkowska

Sicurezza

Sono riuscito a violare un Sistema. Cosa faccio?

1. Apertura file wp-config.php (wordpress) o configuration.php (joomla)
2. Individuazione delle informazioni in chiaro della connessione al mysql
3. Esecuzione di uno script per il dump del DB
4. Download del dump in locale

Password in chiaro:

id	username	password	passwordHint
1	admin	1337	k3w1 dud
2	pumpkin22	halloween	my favorite holiday
3	johndoe	queen	Freddie Mercury's band
4	alexa45	password	password
5	guy	123456	<i>NULL</i>
6	maryjane	queen	I'm one!
7	dudson123	halloween	scary movie!

Sicurezza

MD5 : funzione di hash non reversibile

Password = MD5>PasswordInseritaDallUtente);

Password crittografate:

id	username	password	passwordHint
1	admin	7E7274BAC45E467C5AB832170F12E418	k3wl dud
2	pumpkin22	5377DBF76D995CC213ED76924A31CB13	my favorite holiday
3	johndoe	512239D9AE0C3B5567DE188739F689F2	Freddie Mercury's band
4	alexa45	2FE5421E49061F8225C2FB7CB81980FD	password
5	guy	ABE35E2827DDA834C9612FE9E9C92CE0	NULL
6	maryjane	198670893B2781C83F3DA5D45150123D	I'm one!
7	dudson123	59E2113217E65B9885F9DA73FDC5697B	scary movie!

Potrei avere un db ti migliaia di hash generati da password conosciuti e scoprire le password.

Sicurezza

Secret: Bdy~)]/S%@QgSHYH^MdO3&>c9q*2#i

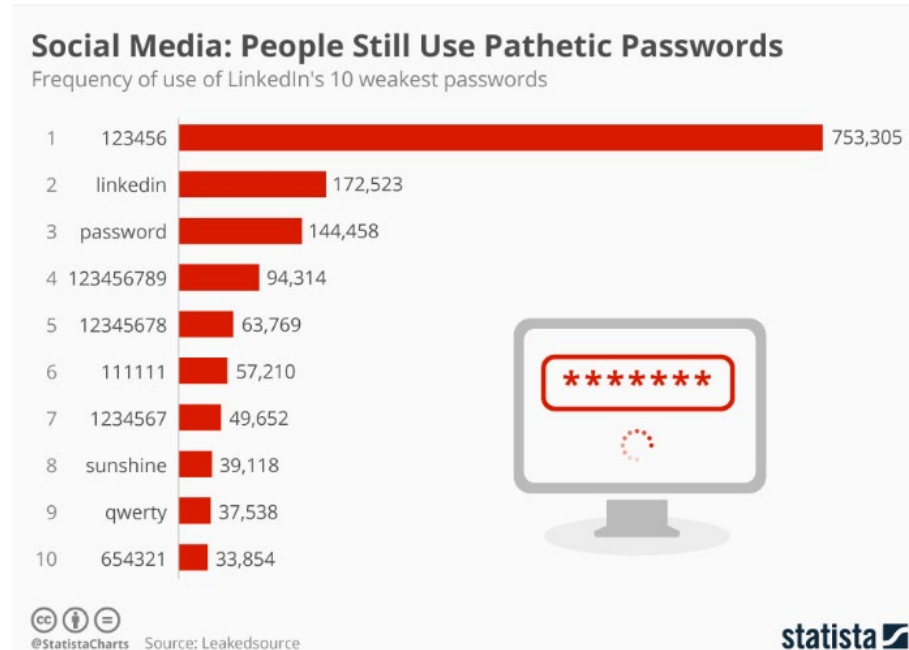
Password = MD5(PasswordInseritaDallUtente + **Secret**);

Password crittografate:

id	username	password	passwordHint
1	admin	7E7274BAC45E467C5AB832170F12E418	k3wl dud
2	pumpkin22	5377DBF76D995CC213ED76924A31CB13	my favorite holiday
3	johndoe	512239D9AE0C3B5567DE188739F689F2	Freddie Mercury's band
4	alexa45	2FE5421E49061F8225C2FB7CB81980FD	password
5	guy	ABE35E2827DDA834C9612FE9E9C92CE0	NULL
6	maryjane	198670893B2781C83F3DA5D45150123D	I'm one!
7	dudson123	59E2113217E65B9885F9DA73FDC5697B	scary movie!

Non posso più utilizzare tabelle di password conosciute perché la Secret è differente dalla mia. Dovrei rigenerarmi tutta la mia tabella di password conosciute con la Secret.

Sicurezza



Individuo nei file php la Secret usata da wordpress/joomla.
Utilizzare un dizionario di password più utilizzate per essere più veloce
e generare una lista di password da confrontare con quella del db

Sicurezza

Secret: Bdy~)]/S%@QgSHYH^MdO3&>c9q*2#i

Salt: differente per ogni utente

Password = MD5>PasswordInseritaDallUtente + **Secret** + **Salt**);

```
SELECT Username, PasswordHash, Salt FROM dbo.[User]
```

Username	PasswordHash	Salt
User1	104f4807e28e401c1b9e1c43ac80bdde	nkV38+/eHsI=
User2	827e877ba7a4676ee4903f2b60de13a	NwHowZ63RVw=
User3	e901b26b3ec928db2753150d04736c44	Z8uDOFE90gE=
User4	72997d54dbe748964c64656cba01e1c8	SKXPm84F2bU=
User5	9207f5635d2622e94e2a67b0190c89a8	ppjsgG33ni=
User6	07168a06f3102a6ee3df50f3355d49c	vINyQVbtPU=
User7	d78c6606bed3d2e4262df59b29e0bfc2	pQQdD514I/E=
User8	c71dcf5a4be211294014537c255ac48a	v-x3ypPTCg=
User9	2ad3269ee1f97858f7f236a02b3a32e	SOwixgcWgvA=
User10	bb0ae47e5b95b896568bc014ac63b9c1	+Bz6pl/G6DQ=
User11	b72c7ec38b64ca39fee15a931f3f5260	UDfOAdDyQQQ=
User12	2e658552d8f83cd7820bff7b2cee7	fvhDCo17aAk=
User13	c5cef9d547088594e022a6581bc44ea6	YaDJlRHZMnk=
User14	ab9a873186c52d0daf11c8a193dc6f9c	8cLo46CTPUE=
User15	30027afd712c3cc235459a0f1a45bea5	bLSAogm+RT4=
User16	50e195fd70d53dc0072e56e54f17f50	7yBcpKnRkpc=
User17	096946878b485dc156d6e0f9e1e10160	i9C8NzVdtDo=
User18	10227757e7d185f0c3578c9fa2a4502	w85scq8DIwo=
User19	cdc3e906dd07fad0f8e4969bc5f46e8c	tu6FYS8silk=
User20	9b153dde1510c64fce08a6f28b940b55	8teTAorVIE=
User21	fa67c40b1d4317078218614154d3f2e7	HV8DjZ9Uz8=
User22	7e533c1aee2145aa25108c3f3beb5bb	R3+QkFNyAFg=
User23	45b4d6d24fd79ed62752db188d2c5803	OprSkliq1DN4=
User24	d7755518f9b08f784c179a456764d5	r68o84BpQCg=
User25	4dc0eef0baf49af20ba51eb0d7d4155b	faSa7MGRwis=

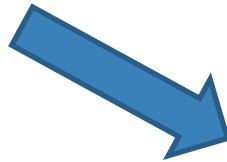
- Individuo il Salt per ogni utente e devo rieseguire l'hash del mio dizionario Per ogni combinazione di salt. Poi confronto il risultato con il db

Sicurezza

MD5 è sicuro?



E' irreversibile



E' efficiente

MD5 for passwords

93

Using salted md5 for passwords is a bad idea. Not because of MD5's cryptographic weaknesses, but because it's fast. This means that an attacker can try **billions** of candidate passwords per second on a single GPU.

What you should use are deliberately slow hash constructions, such as `scrypt`, `bcrypt` and `PBKDF2`. Simple salted SHA-2 is not good enough because, like most general purpose hashes, it's fast. Check out [How to securely hash passwords?](#) for details on what you should use.

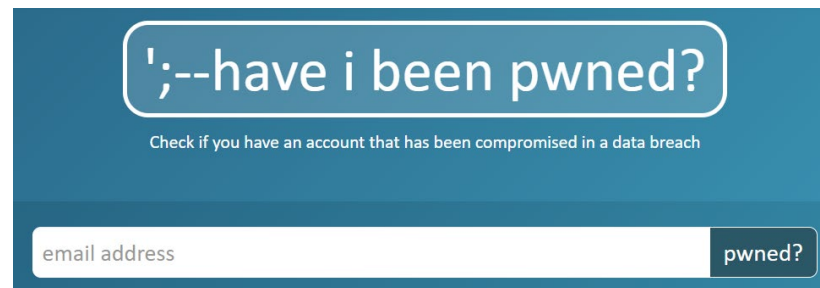
Sicurezza

Scoprite se siete stati **pwned**

A corruption of the word "Owned." This originated in an online game called [Warcraft](#), where a map designer misspelled "owned." When the computer beat a player, it was supposed to say, [so-and-so](#) "has been owned."

Instead, it said, so-and-so "has been pwned."

<https://haveibeenpwned.com/>



;-) have i been pwned?

Check if you have an account that has been compromised in a data breach

email address

pwned?