

Cookie

When you open any website



Marina Ribaud, marina.ribaud@unige.it

HTTP è stateless

2

- Il web server non ha "memoria" delle comunicazioni HTTP successive, anche se arrivano dallo stesso client
- Per questo motivo, per realizzare applicazioni web complesse, sono stati introdotti altri meccanismi
 - **Cookie** e Token
 - Access control
 - Session control

Cookie: definizione

3

“ ... a cookie is a **bit of text**, containing some unique information, that web servers send in the **HTTP header**. The client's browser keeps a list of cookies and web sites. When the user goes back to a web site, the browser will automatically return the cookie, provided it hasn't expired ... ”

Vedi: http://en.wikipedia.org/wiki/HTTP_cookie

Cookie: nascita


4

- **1994**: primo uso dei cookie, usati per controllare se i lettori del sito di **Netscape** lo avessero già visitato in precedenza (“magic cookie”)
- **1995**: i cookie vengono integrati in **Internet Explorer 2** per ricordare le preferenze degli utenti e per tenere traccia del **carrello della spesa** degli utenti nei negozi online
- A quel punto i cookie cominciano a diventare popolari...

Cookie: formato

5

Un cookie è una **stringa di testo** formata da diverse parti (separate da ;) alcune opzionali

- Name = <VALUE>;  **obbligatorio**
- Expires = <DATE>; oppure
Max-age = <DURATION IN SECOND>
- Path = <PATH>;
- Domain = <DOMAIN_NAME>;
- Secure
- HttpOnly
- SameSite

Cookie: formato

6

- **Secure**
 - il cookie può essere trasmesso **solo in connessioni HTTPS**, protegge da accessi non autorizzati perché le connessioni HTTPS sono crittografate. Il valore di default è **no**
- **HttpOnly**
 - Il cookie **non è accessibile tramite JavaScript** e questo aiuta a prevenire attacchi di tipo XSS. Il valore di default è **no**
- **SameSite**
 - il cookie può essere inviato solo tra lo stesso dominio (strict) o tra domini diversi con stessa origine (**lax**, valore di default) o senza restrizioni (none)

Cookie: risposta HTTP

7

Un cookie viene memorizzato nel browser se il server include l'header **Set-Cookie:** come parte di una risposta HTTP

Set - Cookie :

```
customer=56FRP13456UYH;  
domain=.trenitalia.com;  
expires=Wednesday, 20-Nov-24;  
Secure; HttpOnly
```

ATTENZIONE: non si devono mettere dati sensibili nei cookie

Cookie: sicurezza

8

Security

When you store information in cookies, by default all cookie values are visible to, and can be changed by, the end user. You really don't want your cookies to be misused — for example accessed/modified by bad actors, or sent to domains where they shouldn't be sent. The potential consequences can range from annoying — apps not working or exhibiting strange behavior — to catastrophic. A criminal could for example steal a session ID and use it to set a cookie that makes it look like they are logged in as someone else, taking control of their bank or e-commerce account in the process.

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies>

Cookie: richiesta HTTP

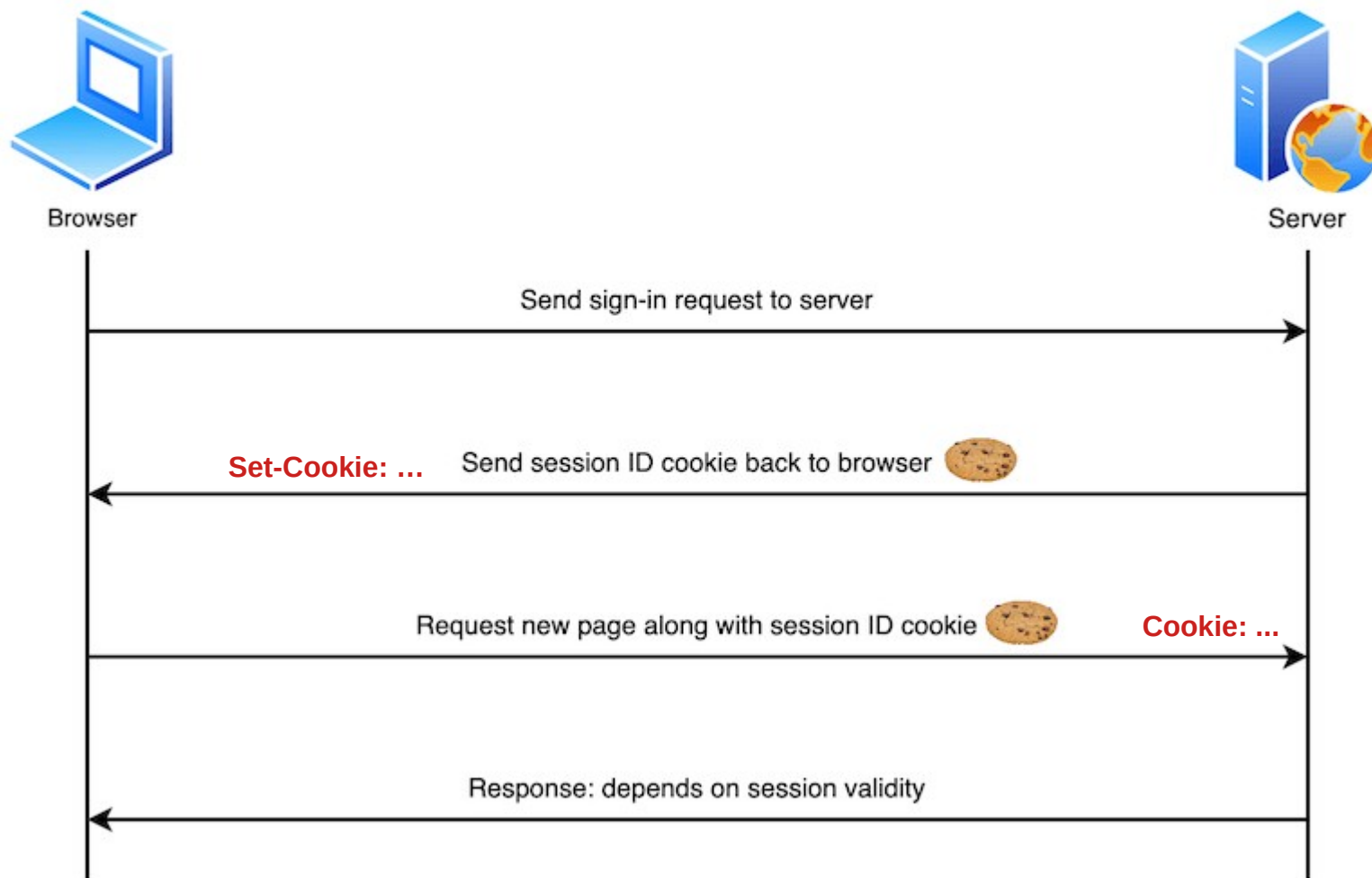
9

Quando un utente torna su un sito che ha già visitato e che gli ha “lasciato” un cookie, il suo browser invia automaticamente il cookie (la coppia name = <VALUE>) come parte della sua richiesta HTTP

Cookie: customer=56FRP13456UYH;

Cookie: interazione

10



<https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies>

Cookie: limitazioni

11

Un browser dovrebbe essere in grado di memorizzare

6. Implementation Considerations

6.1. Limits

Practical user agent implementations have limits on the number and size of cookies that they can store. General-use user agents SHOULD provide each of the following minimum capabilities:

- o At least 4096 bytes per cookie (as measured by the sum of the length of the cookie's name, value, and attributes).
- o At least 50 cookies per domain.
- o At least 3000 cookies total.

Servers SHOULD use as few and as small cookies as possible to avoid reaching these implementation limits and to minimize network bandwidth due to the Cookie header being included in every request.

Servers SHOULD gracefully degrade if the user agent fails to return one or more cookies in the Cookie header because the user agent might evict any cookie at any time on orders from the user.

<https://datatracker.ietf.org/doc/html/rfc6265>

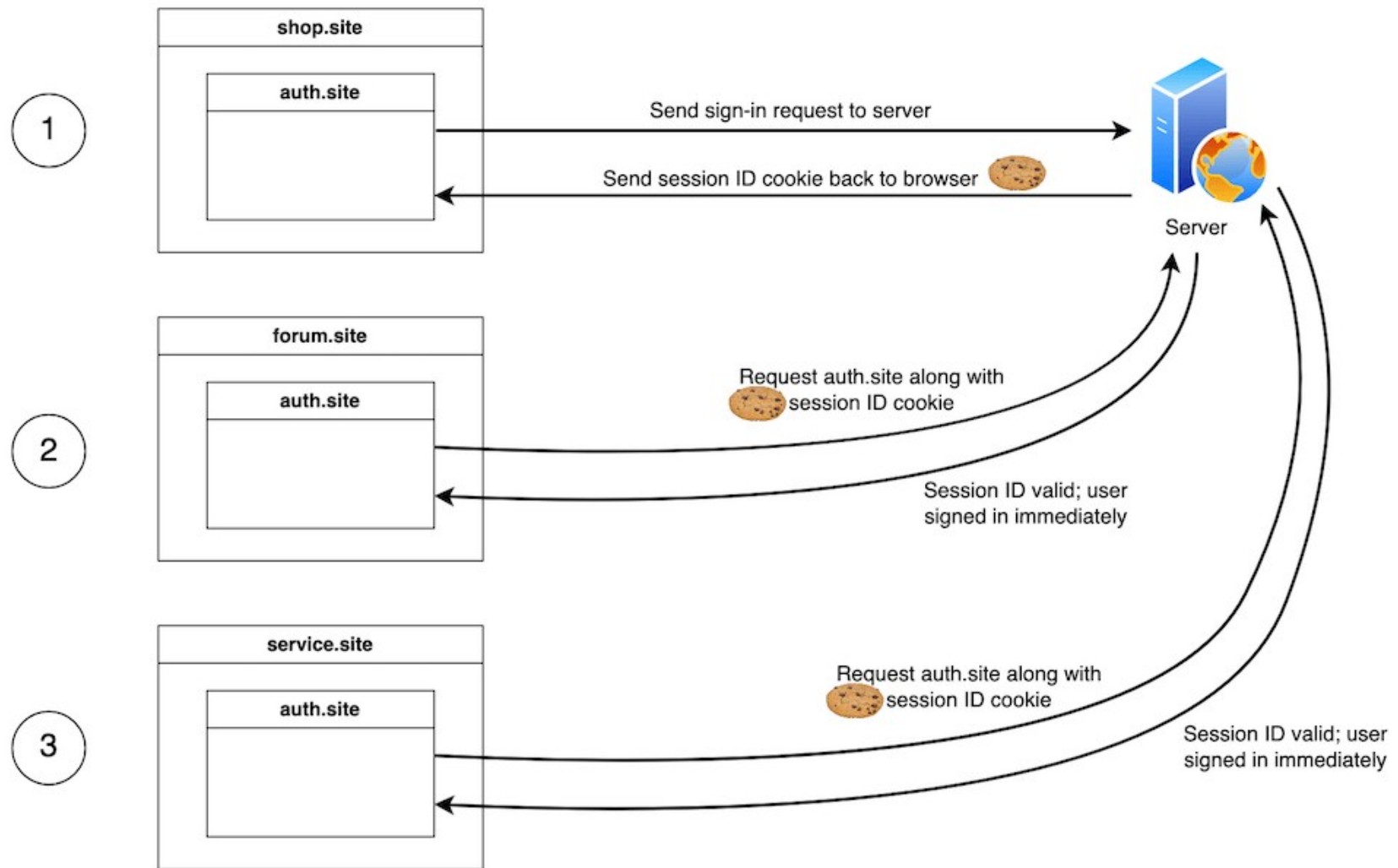
Cookie: diversi tipi

12

- **Cookie di sessione:** sono validi solo per la durata della sessione di navigazione; vengono eliminati alla chiusura del browser (li vediamo più avanti)
- **Cookie permanenti:** rimangono sul browser per un periodo definito, anche dopo la chiusura del browser.
- **Cookie di prima parte:** sono impostati dal sito che si sta visitando
- **Cookie di terze parti:** provengono da domini diversi rispetto a quello visitato, sono spesso usati per il tracciamento e l'invio di pubblicità mirate

Cookie: widget per login

13



https://developer.mozilla.org/en-US/docs/Web/Privacy/Third-party_cookies

Cookie: GDPR

14

- Secondo quanto previsto dal Regolamento generale sulla protezione dei dati personali (GDPR) dell'UE, ogni sito web deve permettere agli utenti europei di **controllare l'attivazione dei cookie** e dei tracker che raccolgono i loro dati personali
- Poiché possono essere utilizzati per tracciare gli utenti su diversi siti web, i cookie di terze parti possono essere utilizzati per creare un profilo dettagliato delle abitudini di navigazione di un utente



Cookie: GDPR

15

- Il GDPR richiede che i siti web
 - ottengano il **consenso esplicito** degli utenti prima di utilizzare cookie non essenziali al funzionamento del sito
 - **forniscano informazioni chiare e comprensibili** sui cookie utilizzati, compresi scopo e durata
 - consentano agli utenti di **gestire le preferenze sui cookie**, permettendo loro di accettare o rifiutare specifiche categorie
- Esistono siti web che aiutano a creare cookie banner conformi alla normativa (vedrete questo argomento nel corso ECA)

Disabilitare i cookie


16

- Si possono bloccare i cookie di terze parti
 - nelle impostazioni del browser
 - con la navigazione in incognito
 - con un browser incentrato sulla privacy, come Brave o DuckDuckGo
 - con una VPN per nascondere l'indirizzo IP
 - con un AdBlock




- Però...


Ultimi articoli pubblicati



Come usare menù



Come creare un disco di
reimpostazione password



Migliori giochi PS4



Come impostare bicicletta su
Google Maps

Informativa

Noi e alcuni partner selezionati utilizziamo cookie o tecnologie simili come specificato nella [cookie policy](#). Per quanto riguarda la pubblicità, noi e alcuni [partner selezionati](#), potremmo utilizzare dati di geolocalizzazione precisi e fare una scansione attiva delle caratteristiche del dispositivo ai fini dell'identificazione, al fine di archiviare e/o accedere a informazioni su un dispositivo e trattare dati personali (es. dati di navigazione, indirizzi IP, dati di utilizzo o identificativi univoci) per le seguenti finalità: *annunci e contenuti personalizzati, valutazione dell'annuncio e del contenuto, osservazioni del pubblico; sviluppare e perfezionare i prodotti.*

Puoi liberamente prestare, rifiutare o revocare il tuo consenso, in qualsiasi momento, accedendo al [pannello delle preferenze pubblicitarie](#).


Puoi acconsentire all'utilizzo di tali tecnologie chiudendo questa informativa.

Accetta

Scopri di più e personalizza



ore Aranzulla



Aranzulla è il blogger e divulgatore più letto in Italia. Noto per aver
elle vulnerabilità nei siti di Google e

con riviste di informatica e cura la
nologica del quotidiano Il Messaggero.
tato per Mondadori e Mondadori
a.

ore di Aranzulla.it, uno dei trenta siti più
alia, nel quale risponde con semplicità a
dubbi di tipo informatico.



Salvatore Aranzulla

Disabilita il blocco della pubblicità per proseguire.

Ho disattivato il blocco della pubblicità

Istruzioni per proseguire

Scegli il filtro della pubblicità che utilizzi:



[Adblock](#)



[Adblock Plus](#)



[uBlock Origin](#)



[Adblock Pro](#)



[Ghostery](#)



[Adguard AdBlocker](#)



[Fair AdBlocker](#)



[Disconnect](#)



[Avira Free Antivirus](#)



[avast! Free Antivirus](#)



[Kaspersky Internet Security](#)

Adblock

Sviluppi futuri?

19

- Sono diverse le critiche contro i cookie di terze parti
- Questo accade perché molto spesso non si sa come vengono utilizzati i dati forniti ai siti web e persino gli sviluppatori a volte non comprendono l'intera catena di fornitura di terze parti
- Molti browser hanno avviato un processo volto alla loro rimozione in tempi brevi sostituendoli con tecnologie alternative

⚠ Chrome is moving towards a new experience that allows users to choose to browse without third-party cookies.