

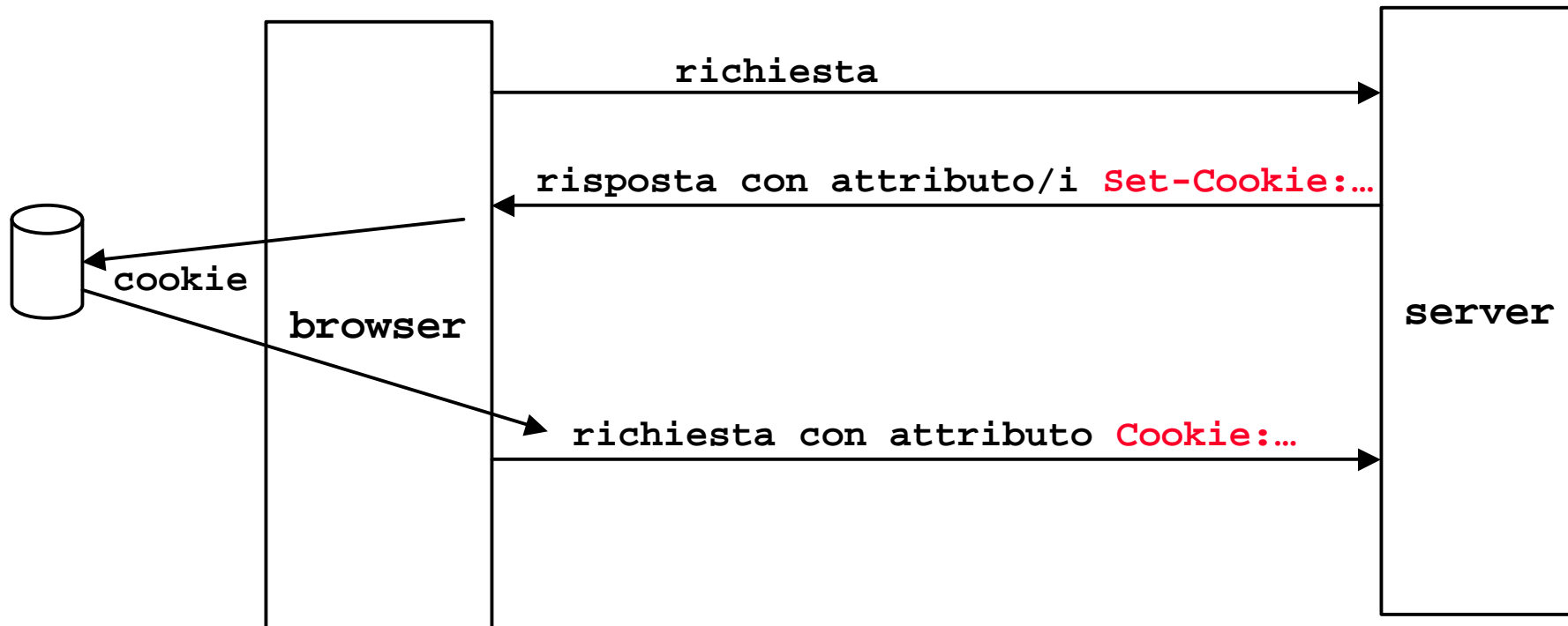
I Cookie

- Sono piccoli pacchetti di dati testuali che
 - vengono memorizzati in modo persistente da un browser web
 - vengono scambiati tramite (un'estensione del) protocollo HTTP
- Si prestano per diversi tipi di uso:
 - identificazione di un utente, memorizzazione di dati utente (p. es. preferenze) senza necessità di gestione lato server
- Riferimenti:
 - Proposta Iniziale (Netscape)
 - Rfc 2965: HTTP State Management Mechanism
 - Rfc 2964: Use of HTTP State Management

Relazione tra i due Standard

- Il meccanismo definito in Rfc 2965
 - può essere considerato una nuova versione di quello specificato originariamente da Netscape
 - ne condivide l'impostazione
 - è stato definito in modo da consentire la convivenza dei due meccanismi
- In questa presentazione ci riferiremo al meccanismo Netscape

Schema di Funzionamento



Sintassi di Set-Cookie

attributi opzionali

Set-Cookie: *NAME=VALUE*; expires=*DATE*; path=*PATH*; domain=*DOMAIN*; secure

- NAME,VALUE: sono il nome e i dati del cookie
- DATE: è la data di scadenza. Se non specificata, il cookie viene eliminato alla chiusura del browser
- DOMAIN, PATH: specificano i domini e i path ai quali il cookie dovrà essere inviato (se non specificati, sono quelli della richiesta attuale)
- secure: se presente, richiede che l'invio del cookie avvenga solo su canali sicuri (HTTPS)

Determinazione dei Cookie da inviare

- Ad ogni richiesta, il browser determina quali cookie inviare usando i loro attributi DOMAIN e PATH:
 - Il cookie può essere inviato solo se il suo attributo DOMAIN coincide con la parte *finale* dell'hostname di destinazione
Esempio: se DOMAIN="polito.it", il cookie può essere inviato agli host www.polito.it, www.webservices.polito.it, ecc.
 - Il cookie può essere inviato solo se il suo attributo PATH coincide con la parte *iniziale* del path di destinazione
Esempio: se PATH="/foo", il cookie può essere inviato quando i path di destinazione sono /food/, /foo/bar.html, ecc.

Invio dei Cookie

- I cookie vengono inviati tutti tramite un'unica riga con sintassi:

Cookie: NOME1=VALORE1; NOME2=VALORE2; . . .

Capacità Minime di Memorizzazione

- Ogni implementazione di user agent dovrebbe garantire certe capacità minime di memorizzazione (le uniche su cui il programmatore può fare affidamento):
 - User agent “normali”
 - Almeno 300 cookie
 - Almeno 4096 byte per cookie (come compagno nell’header)
 - Almeno 20 cookie per ogni host o dominio
 - User agent particolari (p. es. su dispositivi di piccole dimensioni)
 - Almeno 20 cookie di 4096 byte ciascuno

Problemi di Security/Privacy

- Nel caso in cui i cookie viaggino su canali non protetti, sono possibili diversi attacchi:
 - intercettazione/alterazione dei cookie (sniffing, spoofing)
- I cookie potrebbero essere usati a insaputa dell'utente per tracciare i siti da esso visitati
 - l'unica difesa possibile è disabilitare o cancellare i cookie
- Per evitare l'invio indiscriminato dei cookie, gli standard restringono i valori leciti per gli attributi PATH e DOMAIN

Programmazione

- Il trattamento dei cookie (invio e ricezione) avviene
 - sul browser, in modo automatico
 - sul server, sotto il controllo di programmi (applicazioni CGI o altro)
- Esempio: usando CGI, i cookie inviati con la richiesta (nell'header HTTP Cookie) si recuperano nella variabile d'ambiente HTTP_COOKIE

Gestione delle Sessioni

- Per **sessione** si intende un'interazione tra un server ed un client composta da una serie di richieste-risposte tra loro correlate. Esempio: sessione di acquisto on-line
- Poiché il protocollo HTTP è stateless, occorrono tecniche ausiliarie per:
 - identificare richieste successive come appartenenti alla stessa sessione (tipicamente usando un identificatore univoco)
 - memorizzare e modificare lo stato della sessione su server (e/o client)

Tipico Esempio di Soluzione basata interamente su HTTP

- Il server crea la sessione e ne gestisce lo stato (su un file, un database, un'applicazione esterna, ecc.)
- Il server crea anche un identificatore (univoco) di sessione, che viene comunicato al client e incluso in ogni richiesta e/o risposta successiva
- L'identificatore può essere:
 - memorizzato sul client tramite cookie
 - inviato ogni volta dal server nel documento HTML (form)

Tipico Esempio di Soluzione Mista

- L'interazione HTTP serve solo per instaurare il primo contatto: creare la sessione ed avviare una coppia di processi client(applet)-server
- Client e server si connettono su un altro canale (p. es. RMI) e conducono la sessione