*:96 Overheads

Part 7b: Cookies

More about this course about Internet application protocols can be found at URL:

`http://www.dsv.su.se/~jpalme/internet-course/Int-app-prot-kurs.html`

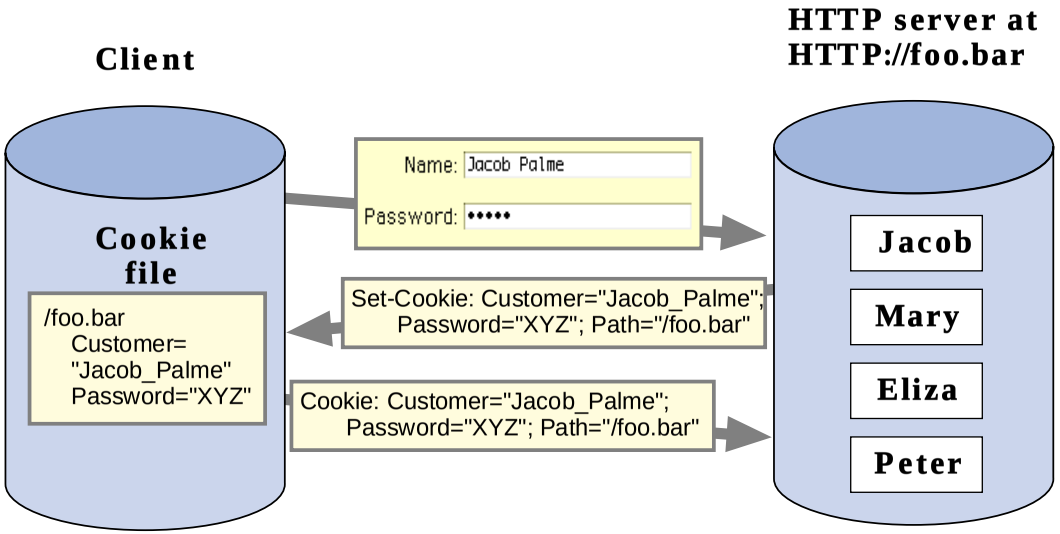
One cookie standard (not entirely accepted by the market):

RFC 2109: HTTP State Management Mechanism

This description follows RFC 2109, even though that may not agree entirely with what is used on the market today.

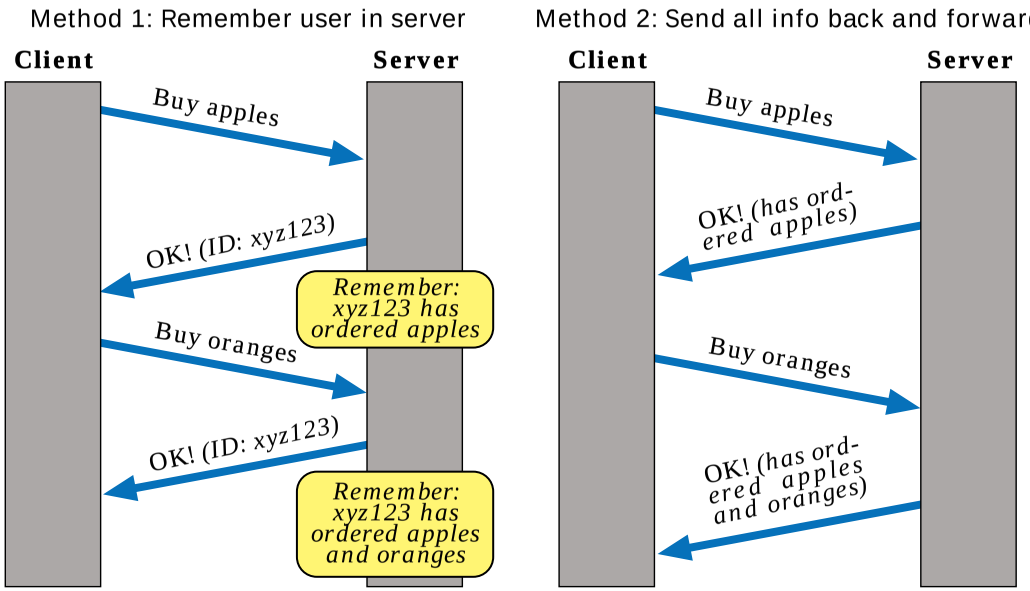
Last update: 98-04-23 12.13

What is a cookie



A cookie is a small piece of data, which the server can store in the client, and which the client sends the next time it connects to the same server to identify itself.

Two ways of remembering what a user did earlier



Example of use of cookies in HTTP transactions

User Server	HTTP command (abbreviated)
→	POST /foo.bar/login HTTP/1.1 [form data with user identification]
←	HTTP/1.1 200 OK Set-Cookie: Customer="JACOB_PALME"; Version="1"; Path="/foo.bar"
→	POST /foo.bar/pickitem HTTP/1.1 Cookie: $Version="1"; Customer="JACOB_PALME"; $Path="/foo.bar" [form data with selection of an item from a shopping basket]
←	HTTP/1.1 200 OK Set-Cookie: Part_Number="Apples-0154"; Version="1"; Path="/foo.bar"
→	POST /foo.bar/shipping HTTP/1.1 Cookie: $Version="1"; Customer="JACOB_PALME"; $Path="/foo.bar"; Part_Number="Rocket_Launcher_0001"; $Path="/foo.bar" [form data]

Cookie management

Creation of cookies

- By client to reside in the client
- By server to reside in the client using the Set-Cookie command
- By server to reside in the server

Usage of cookies

Client sends the cookie when accessing the same server or domain again, using the Cookie header field in the HTTP request.

Set-Cookie header from server to client

Atribute	Description
Name of the cookie, may not start with $	The value of the cookie.
Comment	Explanation for the user, so that the user can decide whether to accept the cookie.
Domain	The domain for which the cookie is valid. Default: the server used. Makes a cookie accessible to several servers in the same domain.
Max-Age	Life time in seconds. Default: When the browser exits. Value 0 can be used to delete an existing cookie.
Path	To which URLs this cookie applies. Restricts which servers can retrieve the cookie.
Secure	Send cookie only using security features.
Version	Version of the standard used.

Privacy issues with cookies

Server can keep track of how often a user accesses the server and what the user does. Can for example be used to select banner advertisment according to the interest of the user. Or can be used to guess at the political opinion of the user, and then used to target political advertising or harassment.

These profiles might be exchanged between servers or sold for profit.

Possible security holes might let the server fetch and modify information it should not have?

Users can set their browsers to reject cookies, or to ask the user before accepting them. But if you reject cookies, you lose a lot of functionality.

There are programs available to help users control and manage their cookies.