Université de Montréal

HTTP-Cookies

Guy Lapalme

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

rali

But

- Identification d'un usager qui se reconnecte
- HTTP est un protocole sans état
- Information envoyée par le serveur
  - conservée sur le client
  - retournée telle qu'elle au même serveur à chaque connexion

Cookie

- réutilisation du concept de *magic cookie*
- inventé en 1994 par Netscape
- ne contient pas de code ou de virus
- mais peut être utilisé pour suivre un client

Structure

1. Paire *nom=valeur*
2. Date d'expiration
3. Path de validité
4. Domaine de validité
5. Besoin de connexion sécurisée
6. Est-ce qu'il peut être accédé autrement que par HTTP (e.g. Javascript)

- Seulement 1 est obligatoire
- Browser doit gérer
  - cookies d'au plus 4K
  - 50 cookies de chaque domaine
  - au minimum 3000 cookies

rali

Implantation

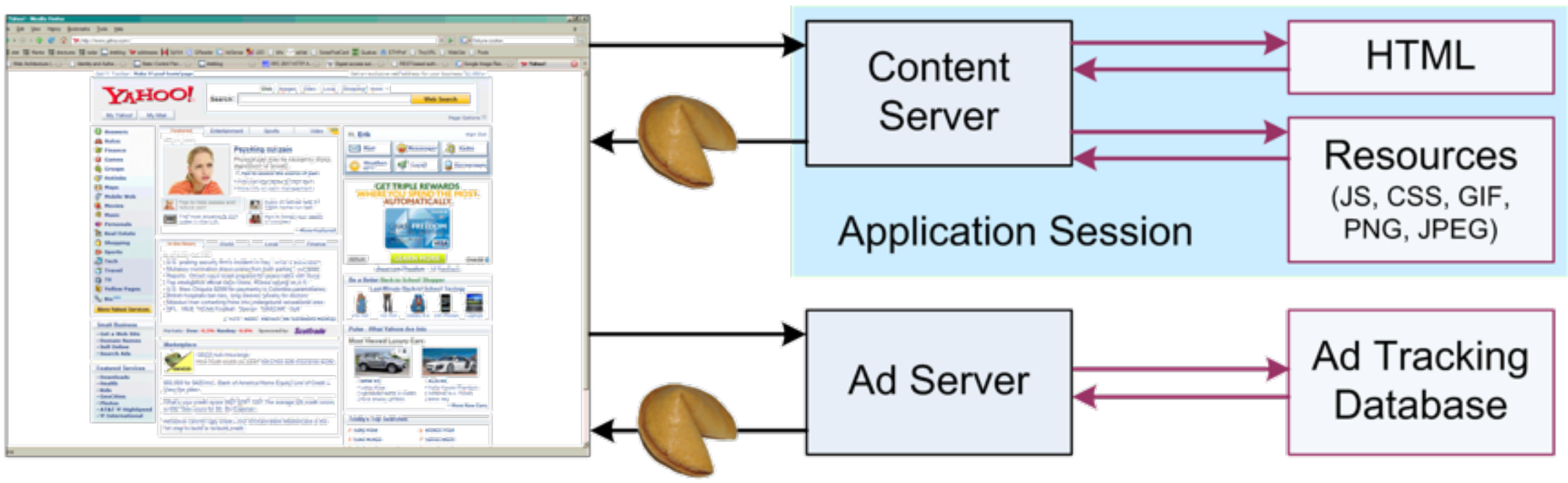
Sortes de cookies

- Session
- Persistent
- Secure
- HTTPonly
- Third-party
- Supercookie
  - origine Top-Level domain
  - tracking sans cookies
- Zombie

rali

Third Party Cookie

- Cookie qui ne vient pas du site qui est indiqué dans la barre d'adresse du navigateur
- Souvent des sites de gestion d'annonces



http://courses.ischool.berkeley.edu/i153/su11/cookies#(17)

Désavantages de cookies

- Identification inexacte
- État inconsistant entre le client et le serveur (e.g. lors d'un *Back*)
- Support inégal des browsers

Alternatives aux cookies

- Adresse IP
- Query string
- Champs cachés
- window.name
- Authentification HTTP
- Web storage
- Browser fingerprint

rali

Browser fingerprint

Variable	**Source**	**Remarks**
User Agent	Transmitted by HTTP, logged by server	Contains Browser micro-version, OS version, language, toolbars and sometimes other info.
HTTP ACCEPT headers	Transmitted by HTTP, logged by server	
Cookies enabled?	Inferred in HTTP, logged by server	
Screen resolution	JavaScript AJAX post	
Timezone	JavaScript AJAX post	
Browser plugins, plugin versions and MIME types	JavaScript AJAX post	Sorted before collection. Microsoft Internet Explorer offers no way to enumerate plugins; we used the PluginDetect JavaScript library to check for 8 common plugins on that platform, plus extra code to estimate the Adobe Acrobat Reader version.
System fonts	Flash applet or Java applet, collected by JavaScript/AJAX	Not sorted; see Section 6.4.
Partial supercookie test	JavaScript AJAX post	We did not implement tests for Flash LSO cookies, Silverlight cookies, HTML 5 databases, or DOM globalStorage.

Table 1. Browser measurements included in Panopticlick Fingerprints

https://panopticlick.eff.org/browser-uniqueness.pdf

Variable	Value
User Agent	Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.1.7) Gecko/20100106 Ubuntu/9.10 (karmic) Firefox/3.5.7
HTTP ACCEPT headers	text/html, */* ISO-8859-1,utf-8;q=0.7,*;q=0.7 gzip,deflate en-us,en;q=0.5
Cookies enabled?	Yes
Screen resolution	1280x800x24
Timezone	300
Browser plugins	Plugin 0: DivX Web Player; DivX Web Player version 1.4.0.233; libtotem-mully-plugin.so; (AVI video; video/divx; divx). Plugin 1: QuickTime Plug-in 7.2.0; The ＜a href=”http://www.gnome.org/projects/totem/”＞Totem＜/a＞ 2.28.2 plugin handles video and audio streams.; libtotem-narrowspace-plugin.so; (QuickTime video; video/quicktime; mov) (MPEG-4 video; video/mp4; mp4) (MacPaint Bitmap image; image/x-macpaint; pntg) (Macintosh Quickdraw/PICT drawing; image/x-quicktime; pict, pict1, pict2) (MPEG-4 video; video/x-m4v; m4v). Plugin 2: Shockwave Flash; Shockwave Flash 10.0 r42; libflashplayer.so; (Shockwave Flash; application/x-shockwave-flash; swf) (FutureSplash Player; application/futuresplash; spl). Plugin 3: VLC Multimedia Plugin (compatible Totem 2.28.2); The ＜a href=”http://www.gnome.org/projects/totem/”＞Totem＜/a＞ 2.28.2 plugin handles video and audio streams.; libtotem-cone-plugin.so; (VLC Multimedia Plugin; application/x-vlc-plugin;) (VLC Multimedia Plugin; application/vlc;) (VLC Multimedia Plugin; video/x-google-vlc-plugin;) (Ogg multimedia file; application/x-ogg; ogg) (Ogg multimedia file; application/ogg; ogg) (Ogg Audio; audio/ogg; oga) (Ogg Audio; audio/x-ogg; ogg) (Ogg Video; video/ogg; ogv) (Ogg Video; video/x-ogg; ogg) (Annodex exchange format; application/annodex; anx) (Annodex Audio; audio/annodex; axa) (Annodex Video; video/annodex; axv) (MPEG video; video/mpeg; mpg, mpeg, mpe) (WAV audio; audio/wav; wav) (WAV audio; audio/x-wav; wav) (MP3 audio; audio/mpeg; mp3) (NullSoft video; application/x-nsv-vp3-mp3; nsv) (Flash video; video/flv; flv) (Totem Multimedia plugin; application/x-totem-plugin;). Plugin 4: Windows Media Player Plug-in 10 (compatible; Totem); The ＜a href=”http://www.gnome.org/projects/totem/”＞Totem＜/a＞ 2.28.2 plugin handles video and audio streams.; libtotem-gmp-plugin.so; (AVI video; application/x-mplayer2; avi, wma, wmv) (ASF video; video/x-ms-asf-plugin; asf, wmv) (AVI video; video/x-msvideo; asf, wmv) (ASF video; video/x-ms-asf; asf) (Windows Media video; video/x-ms-wmv; wmv) (Windows Media video; video/x-wmv; wmv) (Windows Media video; video/x-ms-wvx; wmv) (Windows Media video; video/x-ms-wm; wmv) (Windows Media video; video/x-ms-wmp; wmv) (Windows Media video; application/x-ms-wms; wms) (Windows Media video; application/x-ms-wmp; wmp) (Microsoft ASX playlist; application/asx; asx) (Windows Media audio; audio/x-ms-wma; wma).
System fonts	wasy10, UnDotum, Century Schoolbook L, OpenSymbol, msam10, Mukti Narrow, Vemana2000, KacstQurn, Umpush, DejaVu Sans Mono, Purisa, msbm10, KacstBook, KacstLetter, cmr10, Norasi, Loma, KacstDigital, KacstTitleL, mry_KacstQurn, URW Palladio L, Phetsarath OT, Sawasdee, Tlwg Typist, URW Gothic L, Dingbats, URW Chancery L, FreeSerif, ori1Uni, KacstOffice, DejaVu Sans, VL Gothic, Kinnari, KacstArt, TlwgMono, Lohit Punjabi, Symbol, Bitstream Charter, KacstOne, Courier 10 Pitch, cmmi10, WenQuanYi Zen Hei Mono, Nimbus Sans L, TlwgTypewriter, VL PGothic, Rachana, Standard Symbols L, Lohit Gujarati, kacstPen, KacstDecorative, Nimbus Mono L, Mallige, Nimbus Roman No9 L, KacstPoster, Mukti Narrow, WenQuanYi Zen Hei, FreeSans, cmex10, KacstNaskh, Lohit Tamil, Tlwg Typo, UnBatang, KacstFarsi, Waree, KacstTitle, Lohit Hindi, DejaVu Serif, Garuda, KacstScreen, FreeMono, URW Bookman L, cmsy10 (via Flash)
(Partial) supercookie tests	DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No

Table 3. A typical Panopticlick fingerprint

Résultats

470 161 participants à https://panopticlick.eff.org

- 86 % des browsers avec signature unique
- 5% des browsers vus 2 fois
- si Flash ou Java activés
  - 94% uniques
  - 5% vus 2 fois
- entropie de 18.1 bits
  - un browser unique parmi 286 777

rali

Cookies vs
données dans les pages

- cookie retourné automatiquement
- cookie ne dépend pas du fait que l'usager reste sur le site
- cookie lisible par tous
- cookie non portable entre ordinateurs
- cookie peuvent être désactivés
- cookie peuvent être persistants

rali

Scripting client vs serveur

- validation locale

- programmation Javascript
- interaction locale efficace

- minimise les transferts!
- logique de l'application visible de l'utilisateur
- client doit pouvoir exécuter le script

- validation distante en fonction des données partagées
- n'importe quel language
- interaction lointaine sujette aux variations de charge

- minimise les transferts!
- peut cacher la logique du traitement
- charge le serveur

Choix d'architecture à évaluer
en fonction de chaque situation

rali