Hypertext Transfer Protocol (HTTP): haladó lehetőségek

Jeszenszky Péter
Debreceni Egyetem, Informatikai Kar
jeszenszky.peter@inf.unideb.hu

Utolsó módosítás: 2022. november 15.

Tartalom

- Feltételes kérések
- Sütik
- Felhasználó követés
- Hitelesítés
- Kapcsolatkezelés

Biztonságos metódusok

- **Biztonságos**nak tekintünk egy metódust, ha alkalmazása a cél erőforrásra várhatólag nem eredményez semmiféle állapotváltozást az eredet szerveren.
  - Biztonságos metódusok: `GET`, `HEAD`, `OPTIONS`, `TRACE`
  - Nem biztonságos metódusok: `CONNECT`, `DELETE`, `POST`, `PUT`
- A biztonságos metódusuk információ lekérési célokra szolgálnak és nem kellene, hogy mellékhatást okozzanak a szerveren.
- A gyakorlatban egy biztonságos metódusnak (mint például a `GET`) is lehet mellékhatása a szerveren.
  - Ha van is, nem tehető érte felelőssé a kliens.
  - Lehetnek ártalmatlan mellékhatások, mint például a kérés naplózása.

Idempotens metódusok

- **Idempotens**nek tekintünk egy metódust, ha egy azt tartalmazó kérés többszöri végrehajtása ugyanazt a kívánt hatást eredményezi a szerveren, mint egyetlen végrehajtás.
  - A biztonságos metódusok definíció szerint idempotensek.
  - Idempotensek a `DELETE` és `PUT` metódusok is.
  - A `CONNECT` és a `POST` metódus nem idempotens.
- Egy idempotens kérés megismétlése ugyanazt a kívánt hatást eredményezi a szerveren, bár a válasz eltérő lehet.
- Egy idempotens kérés automatikusan megismételhető, ha kommunikációs hiba történik azt megelőzően, hogy a kliens be tudná olvasni a szerver válaszát.

Feltételes kérések (1)

- Egy vagy több olyan fejlécmezőt tartalmazó kérések, melyek egy olyan előfeltételt jeleznek, melyet ellenőrizni kell a metódus a cél erőforrásra történő alkalmazása előtt.

Feltételes kérések (2)

- Felhasználások:
  - **Gyorsítótárazás**:
    - A feltételes `GET` kérések jelentik a gyorsítótár frissítés leghatékonyabb módját.
  - **Az elveszett módosítás (*lost update*) problémájának megelőzése**:
    - Feltételes mód alkalmazható az erőforrások állapotát megváltoztató metódusokra is, mint például a `PUT` és `DELETE`, annak megakadályozása érdekében, hogy egy kliens véletlenül felülírja egy vele párhuzamosan cselekvő másik kliens munkáját.

Feltételes kérések (3)

- **Érvényesítő** (***validator***): egy erőforrás állapotát tükröző olyan metaadat, mely révén észlelhető az erőforrás állapotának megváltozása.
  - Előfeltételekben használhatók feltételes kérések létrehozásához.
- A HTTP/1.1 kétfajta érvényesítőt definiál:
  - **Módosítási dátum** (lásd a `Last-Modified` fejlécmezőt)
  - **Entitás címke** (***entity tag***) (lásd az `ETag` fejlécmezőt)

Feltételes kérések (4)

- **`Last-Modified`**: egy időbélyeget szolgáltató válasz fejlécmező, mely azt a dátumot és időt jelzi, amikor az eredet szerver szerint utoljára módosult a kiválasztott reprezentáció.
  - Pontosság: másodperc
  - Időzóna: egyezményes koordinált világidő (UTC)
  - Példa:
    - `Last-Modified: Sun, 01 Jul 2007 22:55:35 GMT`

Feltételes kérések (5)

- **`ETag`**: a kiválasztott reprezentáció aktuális entitás címkéjét szolgáltató válasz fejlécmező.
  - Egy entitás címke egy átlátszatlan érvényesítő ugyanazon erőforrás több különböző reprezentációjának megkülönböztetésére.
    - Több reprezentáció létezésének okai: (1) az erőforrás állapota idővel változik, (2) az erőforrás tartalomegyeztetésnek van alávetve.
  - Egy entitás címke formailag egy kettős idézőjelekkel (`'"'`) határolt átlátszatlan karakterlánc, melyet megelőzhet a gyengeséget jelző `W/` előtag.
  - Példa:
    - `ETag: "101b85-67bf-4a50dc474f600"`
    - `ETag: "785b937e834cb8ad8a997c38e9aacbf3"`
    - `ETag: "1423137102365|#public|0|en|||0"`
    - `ETag: W/"884da3e-4b59-50dba044d35c1"`

Feltételes kérések (6)

- Az a javasolt viselkedés egy eredet szerver számára, hogy `GET` és `HEAD` kérésekre adott `200-as` (`OK`) válaszokban `ETag` és `Last-Modified` fejlécmezőt is küldjön.

Feltételes kérések (7)

```
> GET /licenses/gpl-3.0.txt HTTP/1.1
> Host: www.gnu.org
> User-Agent: curl/7.84.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: Tue, 17 Aug 2021 09:40:10 GMT
< Server: Apache/2.4.29
< Last-Modified: Sat, 30 Sep 2017 07:16:26 GMT
< ETag: "894d-55a62eb645dcd"
< Accept-Ranges: bytes
< Content-Length: 35149
< Vary: Accept-Encoding
< Content-Type: text/plain
< Content-Language: non-html
<
<                        GNU GENERAL PUBLIC LICENSE
<                           Version 3, 29 June 2007
< ...
```

Feltételes kérések (8)

- Előfeltétel fejléc mezők:
  - `If-Match`
  - `If-None-Match`
  - `If-Modified-Since`
  - `If-Unmodified-Since`
  - `If-Range`

Entitás címkék előállítása

- **Apache HTTP Server**:
  - *Apache HTTP Server Version 2.4 Documentation – FileETag Directive*
    https://httpd.apache.org/docs/current/mod/core.html#fileetag
- **nginx**:
  - http://lxr.nginx.org/source/xref/nginx/src/http/ngx_http_core_module.c?r=7848%3A1bde031b59ff#1673

Feltételes kérések: `If-None-Match` (1)

- `If-None-Match` fejlécmezőt fogadó eredet szerver a metódus végrehajtása előtt ki kell, hogy értékelje az előfeltételt.
  - Ha a mezőérték `'*'`:
    - A feltétel igaz, ha az eredet szervernek nincs a cél erőforráshoz aktuális reprezentációja, hamis egyébként.
  - Ha a mezőérték entitás címkék egy listája:
    - A feltétel igaz, ha a felsorolt entitás címkék egyike sem egyezik meg a kiválasztott reprezentáció entitás címkéjével, hamis egyébként.

Feltételes kérések: `If-None-Match` (2)

- Az eredet szerver nem hajthatja végre a kért metódust, ha a feltétel hamis.
  - `304` (`Not Modified`) állapotkóddal kell válaszolnia, ha a kérés metódusa `GET` vagy `HEAD`.
  - `412` (`Precondition Failed`) állapotkóddal kell válaszolnia az összes többi metódusra.

Feltételes kérések: `If-None-Match` (3)

- Elsősorban feltételes `GET` kérésekben használják gyorsítótárazott információk hatékony frissítéséhez.
- `'*'` értékkel annak megelőzésére használható, hogy egy nem biztonságos metódus (például `PUT`) véletlenül módosítsa a cél erőforrás egy létező reprezentációját.
  - Amikor a kliens azt feltételezi, hogy a cél erőforrásnak nincs aktuális reprezentációja.

Feltételes kérések: `If-None-Match` (4)

- Példa:
  - `curl -v \`
    `-H "If-None-Match: \"894d-55a62eb645dcd\"" \`
    `http://www.gnu.org/licenses/gpl-3.0.txt`

```
> GET /licenses/gpl-3.0.txt HTTP/1.1
> Host: www.gnu.org
> User-Agent: curl/7.84.0
> Accept: */*
> If-None-Match: "894d-55a62eb645dcd"
>
< HTTP/1.1 304 Not Modified
< Date: Sat, 20 Nov 2021 09:58:12 GMT
< Server: Apache/2.4.29
< ETag: "894d-55a62eb645dcd"
<
```

Feltételes kérések: `If-Modified-Since` (1)

- A mezőérték egy időbélyeg.
- Az `If-Modified-Since` fejlécmező attól tesz függővé egy `GET` vagy `HEAD` metódust, hogy a kiválasztott reprezentáció utolsó módosítási ideje későbbi-e, mint az adott dátum.
  - A fogadó figyelmen kívül kell, hogy hagyja az `If-Modified-Since` fejlécmezőt, ha a kérés metódusa nem `GET` vagy `HEAD`.
- Ezáltal elkerülhető a kiválasztott reprezentáció átvitele, ha az nem változott.

Feltételes kérések: `If-Modified-Since` (2)

- `If-Modified-Since` fejlécmezőt fogadó eredet szerver számára ajánlott az előfeltétel kiértékelése a metódus végrehajtása előtt:
  - A feltétel hamis, ha a kiválasztott reprezentáció utolsó módosítási ideje korábbi vagy ugyanaz, mint a mezőértékben adott dátum.
  - Egyébként a feltétel igaz.
- Az szerver számára nem ajánlott a kért metódus végrehajtása, ha a feltétel hamis.
  - Helyette egy `304`-es (`Not Modified`) válasz előállítása ajánlott.

Feltételes kérések: `If-Modified-Since` (3)

- Jellemzően két különböző célra használják:
  - Lehetővé tenni egy olyan gyorsítótárazott reprezentáció hatékony frissítését, melynek nincs entitás címkéje.
  - Olyan erőforrásokra korlátozni az információ lekérdezést, melyek nemrég módosultak.

Feltételes kérések: `If-Modified-Since` (4)

- Példa:
  - `curl -v -z "1 Jan 2018 12:00:00 CET" \ http://www.gnu.org/licenses/gpl-3.0.txt`

```
> GET /licenses/gpl-3.0.txt HTTP/1.1
> Host: www.gnu.org
> User-Agent: curl/7.84.0
> Accept: */*
> If-Modified-Since: Mon, 01 Jul 2019 11:00:00 GMT
>
< HTTP/1.1 304 Not Modified
< Date: Sat, 06 Aug 2022 09:20:17 GMT
< Server: Apache/2.4.29
< ETag: "894d-55a62eb645dcd"
<
```

Sütik (1)

- **Süti** (***cookie***):
  - Egy név-érték pár és kapcsolódó metaadatok (attribútumok), melyeket egy eredet szerver egy válasz `Set-Cookie` fejlécmezőjében küld a felhasználói ágensnek.
    - Az attribútumok segítségével az eredet szerver egy hatáskört határozhat meg a sütihez.
  - A felhasználói ágens a további kérésekben a név-érték párt a `Cookie` fejlécmezőben küldi vissza az eredet szervernek.
- A jelenleg aktuális specifikáció:
  - Adam Barth. *RFC 6265: HTTP State Management Mechanism*. April 2011. https://www.rfc-editor.org/rfc/rfc6265
    - A `Cookie` és a `Set-Cookie` és fejlécmezők definiálása.

Sütik (2)

- Felhasználás:
  - Munkamenet kezelés
  - Testreszabás
  - Felhasználó követés (lásd a `Referer` fejlécmezőt)
- Süti adatbázis: *Cookiedatabase.org* https://cookiedatabase.org/
  - Példa: `VISITOR_INFO1_LIVE` https://cookiedatabase.org/cookie/youtube/visitor_info1_live/

Sütik (3)

- Példa:
  - `curl --http1.1 --head https://stackoverflow.com/`

```
< HTTP/1.1 200 OK
< Connection: keep-alive
< cache-control: private
< content-type: text/html; charset=utf-8
< ...
< Set-Cookie: prov=79b21a73-d2e2-6533-62e4-69144a825187;
  domain=.stackoverflow.com; expires=Fri, 01-Jan-2055 00:00:00 GMT;
  path=/; HttpOnly
<
```

Sütik (4)

- Egy eredet szerver akár több sütit is küldhet egy válaszban:
  - `curl --http1.1 --head https://www.youtube.com/`

```
> HTTP/1.1 200 OK
> Content-Type: text/html; charset=utf-8
> ...
> Set-Cookie: YSC=taP-NIv1YGg; Domain=.youtube.com; Path=/; Secure;
  HttpOnly; SameSite=none
> Set-Cookie: VISITOR_INFO1_LIVE=; Domain=.youtube.com;
  Expires=Wed, 19-Feb-2020 13:50:24 GMT; Path=/; Secure; HttpOnly;
  SameSite=none
> Set-Cookie: __Secure-YEC=CgtEdUJyNS1pOGZZYyigss6bBg%3D%3D;
  Domain=.youtube.com; Expires=Fri, 15-Dec-2023 13:50:23 GMT; Path=/;
  Secure; HttpOnly; SameSite=lax
> Set-Cookie: CONSENT=PENDING+701;
  expires=Thu, 14-Nov-2024 13:50:24 GMT; path=/; domain=.youtube.com;
  Secure
>
```

Sütik (5)

- Amikor a felhasználói ágens egy `Set-Cookie` fejlécmezőt kap, eltárolja az attribútumaival együtt.
- A továbbiakban, amikor a felhasználói ágens egy HTTP kérést hajt végre, a `Cookie` fejlécmezőbe illeszti az alkalmazható, nem lejárt sütiket.
  - Csak a név-érték párokat, az attribútumokat nem!
- Ha a felhasználói ágens egy olyan új sütit kap, melynek neve, valamint `Domain` és `Path` attribútuma megegyezik egy már tárolt sütiével, akkor az új sütire cseréli ki a korábbit.

Sütik (6)

- A curl utasítása arra, hogy a kapott sütiket írja egy állományba:
  - `curl --http1.1 https://www.youtube.com/ -c cookies.txt -v -o /dev/null`
  - Lásd: https://curl.se/docs/http-cookies.html

Sütik (7)

- Sütik visszaküldése a curl-lel:
  - `curl --http1.1 https://www.youtube.com/ **-b cookies.txt** -v -o /dev/null`

```
> GET / HTTP/1.1
> Host: www.youtube.com
> User-Agent: curl/7.84.0
> Accept: */*
> Cookie: __Secure-YEC=Cgs3MU9wT0lIeVJGZyjJt86bBg%3D%3D;
  CONSENT=PENDING+134; YSC=x6N1KP7zVtI
>
```

Süti attribútumok (1)

- A specifikáció az alábbi attribútumokat definiálja:
  - `Expires`
  - `Max-Age`
  - `Domain`
  - `Path`
  - `Secure`
  - `HttpOnly`

Süti attribútumok (2)

- A süti maximális élettartamát jelző attribútumok:
  - **`Expires`**: a süti lejáratának dátumát és idejét adja meg.
  - **`Max-Age`**: azt adja meg, hogy hány másodperc múlva jár le a süti.
- **Perzisztens sütik**nek nevezzük az `Expires` vagy `Max-Age` attribútummal rendelkező sütiket, mert ezeket a felhasználói ágens több munkameneten keresztül megtarthatja.
  - Ha egy sütinek `Max-Age` és `Expires` attribútuma is van, akkor a `Max-Age` élvez elsőbbséget az `Expires` attribútummal szemben.
- Ha egy sütinek nincs `Expires` és `Max-Age` attribútuma sem, akkor a felhasználói ágens az aktuális munkamenet végéig tartja meg.
- A szerverek sütiket törölhetnek a felhasználói ágensnek egy olyan új sütit küldve, melynek `Expires` attribútumának értéke egy múltbeli időpont.

Süti attribútumok (3)

- **`Domain`**:
  - Meghatározza, hogy a süti mely szervereknek lesz elküldve.
    - Ha például `example.com` az attribútum értéke, akkor a felhasználói ágens a sütit a `Cookie` fejlécmezőbe illeszti, amikor HTTP kéréseket intéz az `example.com` vagy `www.example.com` szerverekhez..
  - Ha a szerver kihagyja az attribútumot, akkor a felhasználói ágens csak az eredet szervernek küldi vissza a sütit.
  - A felhasználói ágens elutasít minden olyan sütit, melynél az attribútum által meghatározott hatáskör nem tartalmazza az eredet szervert.
  - Biztonsági okokból sok felhasználói ágens úgy van beállítva, hogy elutasítson minden olyan sütit, melynek `Domain` attribútuma egy nyilvános regisztrátor ellenőrzése alatt álló nyilvános utótag, mint például `com`, `co.uk`, …
- **`Path`**:
  - A süti hatáskörét adott útvonalakra korlátozza.
  - Ha a szerver kihagyja az attribútumot, a felhasználói ágens a kért URI útvonal komponensének „könyvtárát” használja alapértelmezett értékként.

Süti attribútumok (4)

- **`Secure`**:
  - A süti hatáskörének biztonságos csatornákra korlátozása.
  - Egy `Secure` attribútummal rendelkező sütit a felhasználói ágens csak akkor akkor tesz bele egy kérésbe, ha annak átvitele biztonságos csatornán keresztül történik.
    - Mivel a süti érzékeny információt tartalmazhat, melynek sima szövegként történő átvitele kockázatot jelent.
- **`HttpOnly`**:
  - HTTP kérésekre korlátozza a süti hatáskörét.
  - Arra utasítja a felhasználói ágenst, hogy ne tegye a sütit elérhetővé kliens oldali API-k (például JavaScript) számára.

Sütik kezelése (1)

- A felhasználói ágenseknek:
  - Törölniük kell a lejárt sütiket.
  - Az aktuális munkamenet végén törölniük kell az összes nem perzisztens sütit.
  - Ajánlott a felhasználók számára lehetővé tenni a tárolt sütik kezelését.
    - Például egy adott időszakban fogadott vagy egy adott tartományhoz kapcsolódó összes süti törlését.
  - Ajánlott a felhasználók számára lehetővé tenni a sütik letiltását.

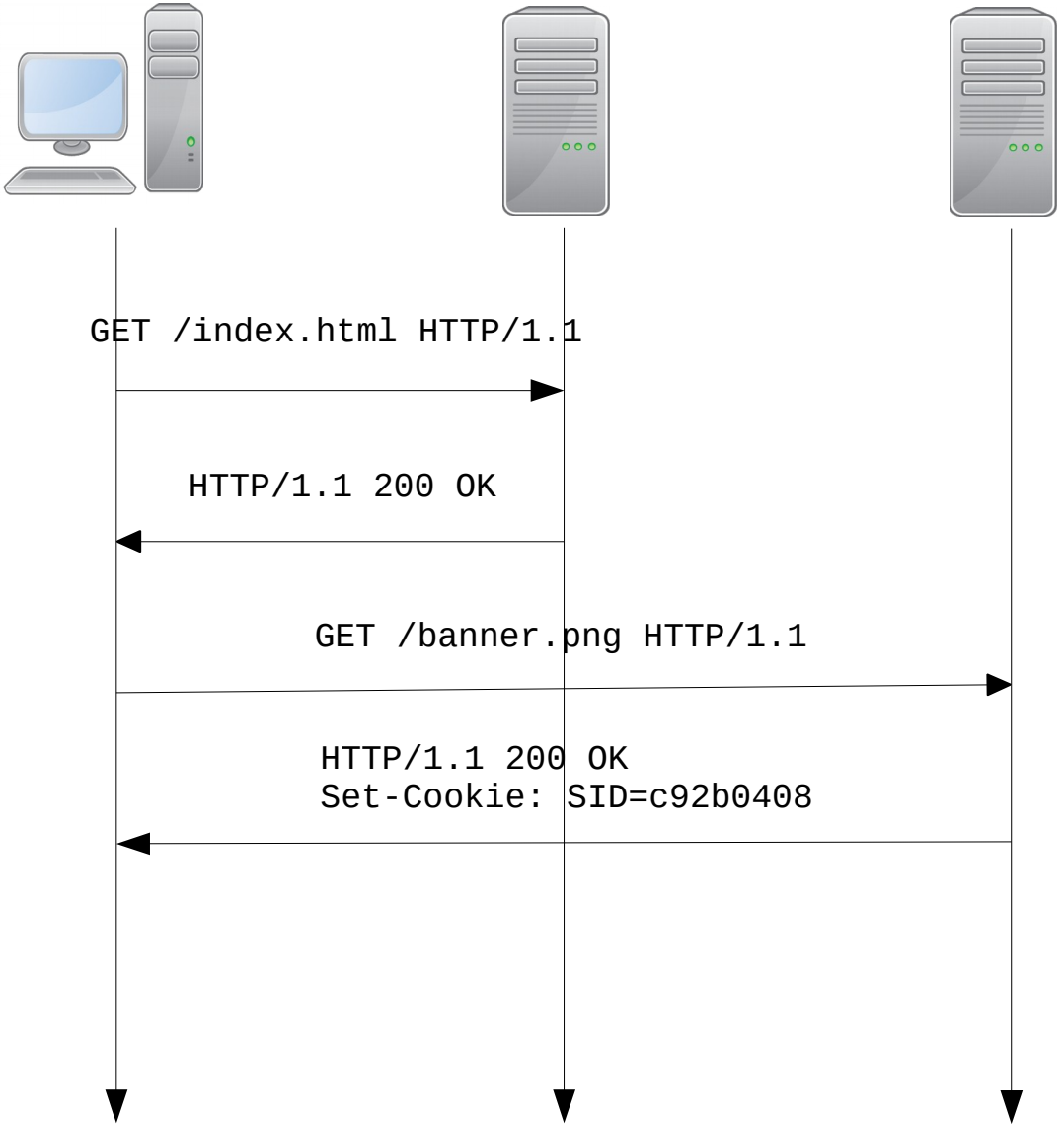
Sütik kezelése (2)

- A felhasználói ágensek korlátokat szabnak a tárolható sütik számára és méretére.
- A specifikáció az alábbi minimális képességeket ajánlja:
  - Sütinként legalább 4096 bájt.
  - Tartományonként legalább 50 süti.
  - Összesen legalább 3000 süti.

Sütik: adatvédelmi és biztonsági kérdések (1)

- A sütiket gyakran bírálják azért, mert lehetővé teszik a szerverek számára a felhasználók követését.
- Az úgynevezett **harmadik féltől származó sütik** (***third-party cookies***) különösen problémásak.
  - Egy HTML oldal megjelenítése során egy felhasználói ágens gyakran kér le erőforrásokat más szerverekről.
  - Ezek a harmadik félnek számító szerverek sütiket használhatnak a felhasználó követésére még akkor is, ha a felhasználó közvetlenül soha nem látogatja meg őket.

Sütik: adatvédelmi és biztonsági kérdések (2)



Sütik: adatvédelmi és biztonsági kérdések (3)

- Hacsak nem biztonságos csatornán (például TLS) keresztül kerülnek küldésre, a `Cookie` és a `Set-Cookie` fejlécekben nyílt szövegként adódnak át az információk.
  - Az ezekben a fejlécekben továbbított érzékeny információk lehallgatható és egy rosszindulatú közvetítő akár módosíthatja is.
- Ajánlott a szerverek számára a sütik tartalmának titkosítása és aláírása a felhasználói ágensnek történő továbbítás során (biztonságos csatorna esetén is).
- Biztonságos csatorna használata esetén a szerverek számára ajánlott a `Secure` attribútum beállítása minden sütihez.

Sütik: adatvédelmi és biztonsági kérdések (4)

- A jelenleg érvényes EU-s szabályozás:
  - **2002/58/EK**: *Elektronikus hírközlési adatvédelmi irányelv* (2002. július 12.) („ePrivacy irányelv”) https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32002L0058
  - **2009/136/EK**: *Az Európai Parlament és a Tanács 2009/136/EK irányelve* (2009. november 25.) https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32009L0136
    - Lásd az 2002/58/EK irányelv 5. cikkének (3) bekezdésének módosítását.
    - Kimondja, hogy süti csak akkor helyezhető el a felhasználó számítógépén, ha ehhez a felhasználó tájékoztatás alapján előzetes hozzájárulását adja!
  - A 29. cikk szerinti adatvédelmi munkacsoport: *2012/4. számú vélemény a sütikhez való hozzájárulás alóli mentességről* (2012. június 7.) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_hu.pdf

Sütik: adatvédelmi és biztonsági kérdések (5)

- Lásd még:
  - *Cookies, the GDPR, and the ePrivacy Directive* https://gdpr.eu/cookies/

Felhasználó követés (1)

- Egy lehetséges definíció:
  - Egy adott felhasználó több különböző kontextuson keresztüli tevékenységével kapcsolatos adatgyűjtés és az ebből a tevékenységből származtatott adatok megőrzése, felhasználása vagy megosztása azon kontextuson kívül, melyben a tevékenység történt.
  - Egy kontextus olyan erőforrások egy összessége, melyek ugyanazon fél ellenőrzése vagy több fél közös ellenőrzése alatt állnak.
- Forrás: https://www.w3.org/TR/tracking-dnt/#dfn-tracking

Felhasználó követés (2)

- Az alábbiakon alapulhat:
  - IP-cím
  - Sütik
  - Az ETag fejlécmező
  - Eszköz ujjlenyomat (operációs rendszer, képernyőfelbontás, telepített betűkészletek, …)
    - Lásd:
      - *Am I Unique*? https://amiunique.org/
      - *Cover Your Tracks* https://coveryourtracks.eff.org/
  - …

Felhasználó követés (3)

- Statisztikák a követőkről:
  - *WhoTracks.me* https://whotracks.me/
- További információk:
  - *BrowserLeaks.com* https://www.browserleaks.com/

A Referer fejlécmező (1)

- Lehetővé teszi a felhasználói ágens számára, hogy megadja azt az erőforrást azonosító URI-hivatkozást, melyből a cél URI származik.
  - Lásd: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referer
- Példa a használatra:
  - `Referer: https://www.w3.org/`
- Potenciálisan információkat nyújthat a felhasználó böngészési előzményeiről, mely egy biztonsági kockázat.

A Referer fejlécmező (2)

- Nem ajánlott a `Referer` fejlécmező küldése akkor, ha a hivatkozó erőforrás elérése biztonságos protokollon keresztül történt és a kérés céljának eredete eltér a hivatkozó erőforrásétól, hacsak nem engedi meg kifejezetten a `Referer` mező küldését a hivatkozó erőforrás.
- Tilos a `Referer` fejlécmező küldése nem biztonságos HTTP kérésben, ha a mezőértékben jelzett oldal biztonságos protokollon keresztül érkezett.

A Referer fejlécmező használatának szabályozása (1)

- A HTML által biztosított mechanizmus:
  - *HTML Living Standard – Link type `"noreferrer"`*

    https://html.spec.whatwg.org/multipage/semantics.html#link-type-noreferrer
    - Az a elem `rel="noreferrer"` attribútuma.
    - Példa:
      - `<a href="https://example.com/" rel="noreferrer">Click here</a>`
    - Böngésző támogatás: https://caniuse.com/rel-noreferrer

A Referer fejlécmező használatának szabályozása (2)

- *Referrer Policy* (előzetes W3C javaslatterv, 2017. január 26.) https://www.w3.org/TR/referrer-policy/
  - Mechanizmus biztosítása, mely révén a dokumentum szerzők szabályozást határozhatnak meg a kliensek számára a `Referer` fejlécmező küldésére vonatkozólag.
  - Példa:
    - `Referrer-Policy: no-referrer`
    - `<meta name="referrer" content="no-referrer"/>`
    - ```
      <a href="https://example.com/"
         referrerpolicy="no-referrer">Click here</a>
      ```
  - Böngésző támogatottság: https://caniuse.com/referrer-policy
      ```

Védekezés a követés ellen (1)

- A `Referer` fejlécmező küldésének tiltása:
  - **Firefox**: lásd a `network.http.sendRefererHeader` opciót (`about:config`)
    https://wiki.mozilla.org/Security/Referrer
  - **Chromium, Google Chrome**: Referer Control
    https://chrome.google.com/webstore/detail/referer-control/hnkcfpcejkafcihlgbojoidoihckciin
  - **Opera**: NoRef
    https://addons.opera.com/en/extensions/details/noref/

Védekezés a követés ellen (2)

- Harmadik féltől származó sütik elfogadásának letiltása:
  - **Firefox**: lásd a `network.cookie.cookieBehavior` opciót (`about:config`)
    - Lásd még: *Third-party cookies and Firefox tracking protection – Disable third-party cookies* https://support.mozilla.org/en-US/kb/third-party-cookies-firefox-tracking-protection#w_disable-third-party-cookies
  - **Chromium**, **Google Chrome**: lásd a *Harmadik féltől származó cookie-k letiltása* opciót (`chrome://settings/content/cookies`)
  - **Opera**: lásd a *Harmadik féltől származó cookie-k letiltása* opciót (`opera://settings/content/cookies`)
  - **Chromium-alapú Microsoft Edge**: *Microsoft Edge, browsing data, and privacy* https://support.microsoft.com/en-us/windows/microsoft-edge-browsing-data-and-privacy-bb8174ba-9d73-dcf2-9b4a-c582b4e640dd

Védekezés a követés ellen (3)

- Privát böngészés/inkognitómód:
  - Számos modern böngésző rendelkezik a felhasználó magánszférájának védelmét szolgáló privát böngészési lehetőséggel.
  - Privát böngészési módban a munkamenet végén automatikusan törlésre kerülnek a böngészési információk, úgymint a
    - böngészési előzmények,
    - sütik,
    - gyorsítótárazott tartalmak.

Védekezés a követés ellen (4)

- Privát böngészés/inkognitómód: (folytatás)
  - **Firefox:**
    - *Privát böngészés – internetezés a meglátogatott weboldallal kapcsolatos adatok mentése nélkül* https://support.mozilla.org/hu/kb/privat-bongeszes-internetezes-meglatogatott-webold
  - **Chromium**, **Google Chrome**:
    - *How private browsing works* https://support.google.com/chrome/?p=incognito
  - **Opera**:
    - *Opera Help – Security and privacy – Private window* https://help.opera.com/en/latest/security-and-privacy/#privateWindow
  - **Chromium-alapú Microsoft Edge**:
    - *InPrivate-böngészés a Microsoft Edge-ben* https://support.microsoft.com/hu-hu/microsoft-edge/inprivate-b%C3%B6ng%C3%A9sz%C3%A9s-a-microsoft-edge-ben-cd2c9a48-0bc4-b98e-5e46-ac40c84e27e2

Védekezés a követés ellen (5)

- Beépített követés elleni védelem:
  - **Firefox**:
    - *Továbbfejlesztett követés elleni védelem az asztali Firefoxban*
      https://support.mozilla.org/hu/kb/tovabbfejlesztett-kovetes-elleni-vedelem-az-asztal
      - Lásd: `about:protections`
  - **Chromium-alapú Microsoft Edge**:
    - *Tracking Prevention in Microsoft Edge*
      https://learn.microsoft.com/en-us/microsoft-edge/web-platform/tracking-prevention

Védekezés a követés ellen (6)

- Komplex megoldások:
  - *Adblock Plus* (licenc: GPLv3) https://adblockplus.org/ https://gitlab.com/eyeo/adblockplus
    - Támogatott böngészők: Chrome, Firefox, Opera, Safari, …
    - Lásd az *EasyPrivacy* szűrőt https://easylist.to/
  - *Ghostery Browser Extension* (licenc: nem szabad/Mozilla Public License 2.0) https://www.ghostery.com/ghostery-browser-extension https://github.com/ghostery/ghostery-extension
    - Támogatott böngészők: Chrome, Firefox, Microsoft Edge, Opera, …
  - *Privacy Badger* (licenc: GPLv3) https://privacybadger.org/ https://github.com/EFForg/privacybadger
    - Támogatott böngészők: Chrome, Firefox, Microsoft Edge, Opera
  - *uBlock Origin* (licenc: GPLv3) https://github.com/gorhill/uBlock
    - Támogatott böngészők: Chromium, Firefox, Safari

Védekezés a követés ellen (7)

- További információk:
  - *PrivacyTools* https://www.privacytools.io/

Hitelesítés (1)

- A HTTP **hitelesítési sémák** (***authentication schemes***) egy általános keretrendszert biztosítanak a hozzáférés-vezérléshez és hitelesítéshez.
  - Roy T. Fielding (ed.), Mark Nottingham (ed.), Julian Reschke (ed.). *RFC 9110: HTTP Semantics*. June 2022. https://www.rfc-editor.org/rfc/rfc9110
    - Lásd a HTTP Authentication című 10. fejezetet: https://www.rfc-editor.org/rfc/rfc9110#name-http-authentication
- Az alkalmazások további mechanizmusokat is használhatnak a hitelesítéshez.
  - Például átviteli szintű hitelesítés, hitelesítési információkat megadó további fejlécmezők használata.

Hitelesítés (2)

- **Felszólítás-válasz** (***challenge-response***) hitelesítés:
  - A hitelesítési sémák segítségével egy szerver felszólíthat egy klienst, egy kliens pedig hitelesítési információkat szolgáltathat.

Hitelesítés (3)

- Szintaxis a felszólítás és a hitelesítési információk ábrázolására:
  - A hitelesítési sémát egy kisbetű-nagybetű érzéketlen token azonosítja, melyet a sémán keresztül történő hitelesítéshez szükséges további információk követnek.
    - Az utóbbi paraméterek egy vesszővel elválasztott listája vagy pedig egyetlen olyan karakterlánc, mely alkalmas base64 kódolású információk tárolására.
    - A paraméterek *név=érték* párok, ahol a név kisbetű-nagybetű érzéketlen és minden egyes név csak egyszer fordulhat elő felszólításonként.
  - Példa:
    - `Basic realm="Authentication Required"`
    - `Basic YWxhZGRpbjpvcGVuIHNlc2FtZQ==`

Hitelesítés (4)

- Egy eredet szerver egy 401-es (`Unauthorized`) válaszban szólítja fel hitelesítésre a felhasználói ágenst.
  - A válasznak tartalmaznia kell egy `WWW-Authenticate` fejlécmezőt, mely legalább egy, a kért erőforrásra vonatkozó felszólítást tartalmaz.
    - A fejlécmező értéke felszólítások egy vesszővel elválasztott egy listája.

Hitelesítés (5)

- Ha egy felhasználói ágens egy eredet szerverrel kívánja hitelesíteni magát, a kérésbe egy `Authorization` fejlécmezőt beillesztve teheti ezt meg.
  - Ez általában, de nem szükségszerűen egy 401-es (`Unauthorized`) válasz fogadása után történik.
  - A mezőérték a kliens hitelesítő adatait tartalmazza a kért erőforrás tartományához (egy múltbeli időpontban) egy válaszban kapott felszólítás alapján.

Hitelesítés (6)

- Kényelmi okokból a kliensek és felhasználói ágensek jellemzően megjegyzik és korlátlan ideig tartják meg a hitelesítési információkat.

Hitelesítés (7)

- **Védelmi terület** (**tartomány**):
  - A tartományok lehetővé teszik egy szerver védett erőforrásainak védelmi területekre való felosztását, melyek mindegyikéhez saját hitelesítési séma és/vagy hozzáférési adatbázis tartozhat.
  - A `realm` hitelesítési paraméter van fenntartva a hitelesítési sémák számára a védelmi terület jelzésére.
    - Az értéke egy karakterlánc.
  - Ha egy korábbi kérés engedélyezésre került, akkor a felhasználói ágens a hitelesítési séma, a paraméterek és/vagy a felhasználói beállítások által meghatározott időtartamon belül újra felhasználhatja ugyanazokat a hitelesítő adatokat a védelmi területen belüli összes többi kérésekhez.

Hitelesítés (8)

- Példa:
  - `curl --http1.1 -v \ https://www.w3.org/Style/Group/`

```
> GET /Style/Group/ HTTP/1.1
> Host: www.w3.org
> User-Agent: curl/7.84.0
> Accept: */*
>
< HTTP/1.1 401 Unauthorized
< date: Tue, 15 Nov 2022 15:20:31 GMT
< www-authenticate: Basic realm="W3CACL"
< ...
```

Hitelesítés (9)

- Példa:
  - `curl --http1.1 -v \ https://mail.google.com/mail/feed/atom`

```
> GET /mail/feed/atom HTTP/1.1
> Host: mail.google.com
> User-Agent: curl/7.84.0
> Accept: */*
>
```

Hitelesítés (10)

- Példa (folytatás):

```
< HTTP/1.1 401 Unauthorized
< Content-Type: text/html; charset=UTF-8
< WWW-Authenticate: BASIC realm="mail.google.com"
< Date: Tue, 15 Nov 2022 15:17:07 GMT
< Expires: Tue, 15 Nov 2022 15:17:07 GMT
< Cache-Control: private, max-age=0
< X-Content-Type-Options: nosniff
< X-Frame-Options: SAMEORIGIN
< Content-Security-Policy: frame-ancestors 'self'
< X-XSS-Protection: 1; mode=block
< Server: GSE
< Alt-Svc: clear
< Accept-Ranges: none
< Vary: Accept-Encoding
< Transfer-Encoding: chunked
<
< <HTML>
< <HEAD>
< <TITLE>Unauthorized</TITLE>
...
```

Hitelesítés (11)

- A hitelesítési sémákat az IANA regisztrálja.
  - Lásd: *Hypertext Transfer Protocol (HTTP) Authentication Scheme Registry*
    https://www.iana.org/assignments/http-authschemes/http-authschemes.xhtml

Basic Authentication (1)

- Specifikáció:
  - Julian F. Reschke. *RFC 7617: The 'Basic' HTTP Authentication Scheme*. September 2015. https://www.rfc-editor.org/rfc/rfc7617
- Base64-kódolt felhasználóazonosító/jelszó párokat továbbít hitelesítő adatokként.

Basic Authentication (2)

- Példa:
  - A szerver hitelesítésre buzdítja a klienst `"Private Area"` tartományban:
    - `WWW-Authenticate: Basic realm="Private Area"`

Basic Authentication (3)

- A kliens egy Base64-kódolt felhasználóazonosítót és jelszót küld az `Authorization` fejlécmezőben.
  - Ténylegesen a *felhasználóazonosító*`:`*jelszó* karakterlánc kerül kódolásra.
  - Példa (felhasználói név: `aladdin`, jelszó: `open sesame`):
    - `Authorization: Basic YwxhZGRpbjpvcGVuIHNlYXNtZQ==`
  - Minden egyes kérésben meg kell adni a hitelesítő adatokat, mely hitelesítést igényel.
    - Kényelmi okokból automatikusan beillesztik a hitelesítő adatokat (azaz a felhasználóazonosítót és a jelszót) a további kérésekbe azok a felhasználói ágensek, melyek egy hitelesítést igénylő erőforráshoz sikeresen intéztek kéréseket.

Basic Authentication (4)

- Ez a séma nem tekinthető a felhasználó hitelesítés biztonságos módjának, mivel a felhasználóazonosító és a jelszó nyílt szövegként kerül továbbításra a hálózaton.
  - A lehallgatás a TLS (azaz a HTTPS) használatával előzhető meg.

Basic Authentication (5)

- Példa:
  - `curl -v http://localhost/protected/`

```
> GET /protected/ HTTP/1.1
> Host: localhost
> User-Agent: curl/7.84.0
> Accept: */*
>
< HTTP/1.1 401 Unauthorized
< Date: Tue, 15 Nov 2022 16:01:10 GMT
< Server: Apache/2.4.29 (Ubuntu)
< WWW-Authenticate: Basic realm="Password Required"
< Content-Length: 455
< Content-Type: text/html; charset=iso-8859-1
<
< <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
< <html><head>
< <title>401 Unauthorized</title>
< </head><body>
< ...
```

Basic Authentication (6)

- Példa:
  - `curl -v http://localhost/protected/ -u jeszy:secret`

```
> GET /protected/ HTTP/1.1
> Host: localhost
> Authorization: Basic amVzenk6c2VjcmV0
> User-Agent: curl/7.84.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: Tue, 15 Nov 2022 16:02:21 GMT
< Server: Apache/2.4.29 (Ubuntu)
< Last-Modified: Sat, 16 Nov 2019 14:29:47 GMT
< ETag: "4880-524a93db68cc0"
< Accept-Ranges: bytes
< Content-Length: 18560
< Vary: Accept-Encoding
< Content-Type: text/html
< ...
```

Basic Authentication (7)

- Példa:
  - `curl https://api.github.com/user -v`

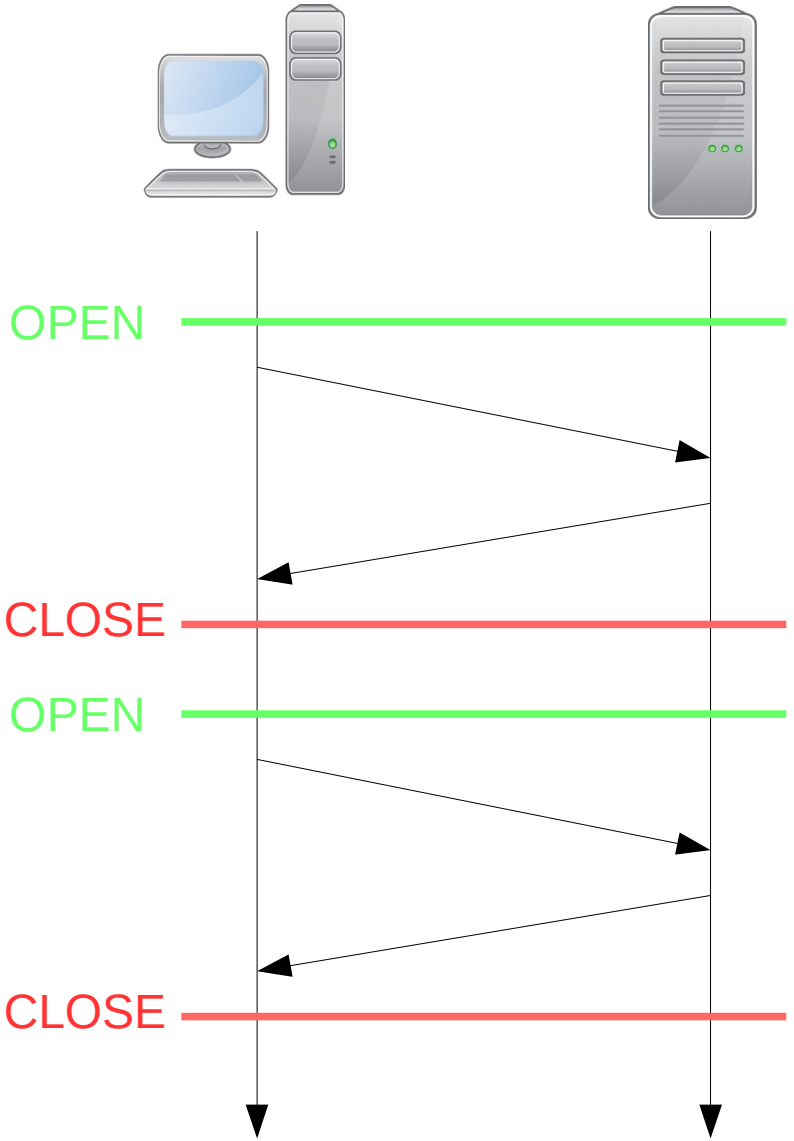
```
> GET /user HTTP/2
> Host: api.github.com
> user-agent: curl/7.84.0
> accept: */*
>
< HTTP/2 401
< server: GitHub.com
< date: Tue, 15 Nov 2022 15:56:50 GMT
< content-type: application/json; charset=utf-8
< content-length: 141
< ...
<
< {
<    "message": "Requires authentication",
< ...
```

Basic Authentication (8)

- Példa:
  - `curl https://api.github.com/user -v -u jeszy75`

```
> GET /user HTTP/2
> Host: api.github.com
> authorization: Basic amVzenk3NTpmYWtlcGFzc3dvcmQK
> user-agent: curl/7.84.0
> accept: */*
>
< HTTP/2 200
< server: GitHub.com
< date: Tue, 15 Nov 2022 15:52:03 GMT
< content-type: application/json; charset=utf-8
<...
< {
<   "login": "jeszy75",
< ...
```

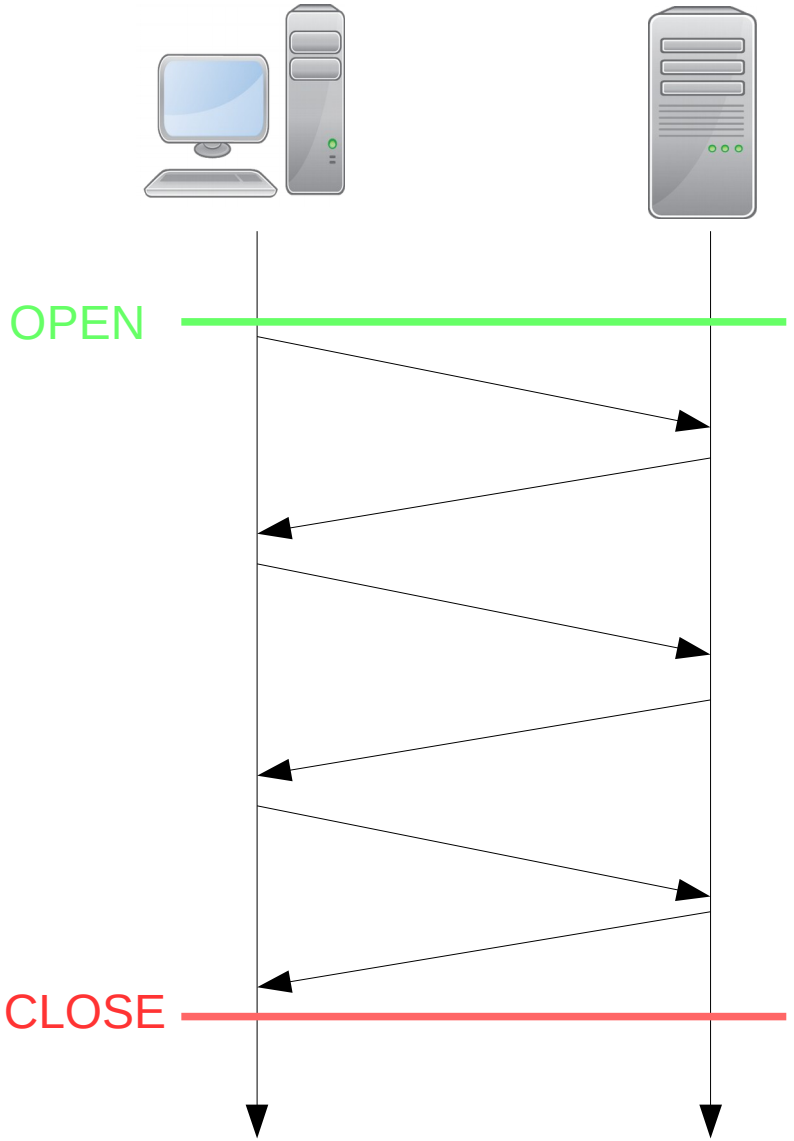
HTTP/1.0 kapcsolatkezelés



Perzisztens kapcsolatok (1)

- A HTTP/1.1 vezette be.
- Lehetővé teszik több kérés és válasz átvitelét egyetlen TCP kapcsolaton át.
- A HTTP/1.1 alapértelmezetten perzisztens kapcsolatokat használ.

Perzisztens kapcsolatok (2)



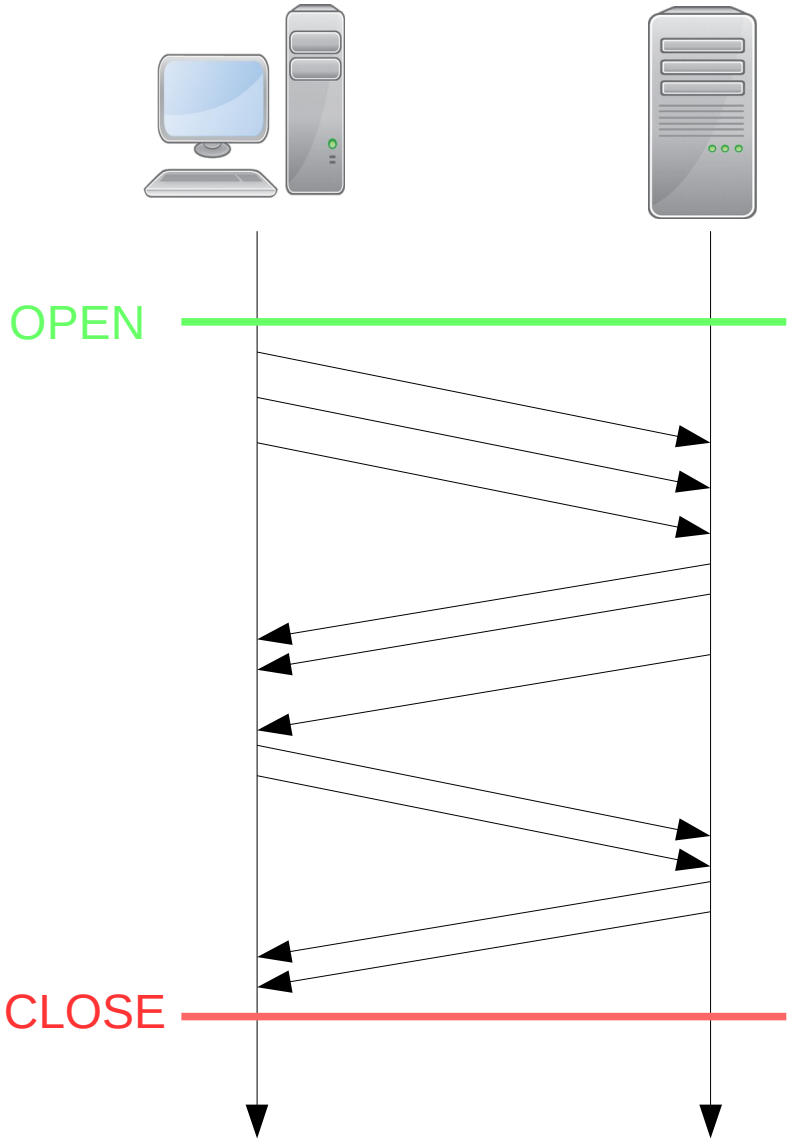
Kapcsolatkezelés: kapcsolati beállítások

- A `Connection` fejlécmező lehetővé teszi a küldő számára az aktuális kapcsolatra vonatkozó vezérlő beállítások megadását.
  - A mezőérték kisbetű-nagybetű érzéketlen opciók listája.

Kapcsolatkezelés: csővezetékezés (1)

- Egy perzisztens kapcsolatokat támogató kliens „csővezetékezheti” a kérései, azaz egymás után több kérést is küldhet anélkül, hogy megvárná a válaszokat.
- Egy szerver csővezetékezett kérések egy sorozatát párhuzamosan is feldolgozhatja, ha minden kérés metódusa biztonságos, de a megfelelő válaszokat ugyanabban a sorrendben kell, hogy elküldje, melyben a kéréseket fogadta.

Kapcsolatkezelés: csővezetékezés (2)



Kapcsolatkezelés: csővezetékezés (3)

- Ha a kapcsolat még azelőtt lezárul, hogy egy kéréseket csővezetékező kliens az összes választ megkapná, akkor megpróbálhatja ismét a megválaszolatlan kéréseket.
- Idempotens kérések próbálhatók újra automatikusan kapcsolati hiba után.

Kapcsolatkezelés: csővezetékezés (4)

- Böngésző támogatás:
  - **Firefox**: támogatott, de alapértelmezésben ki van kapcsolva.
    - Lásd a `network.http.pipelining` opciót (`about:config`).
  - **Chromium**, **Google Chrome**: eltávolították az engedélyezésre szolgáló opciót.
    - Lásd: https://www.chromium.org/developers/design-documents/network-stack/http-pipelining
  - **Opera**: nem támogatott
  - **Chromium-based Microsoft Edge**: nem támogatott

Kapcsolatkezelés: csővezetékezés (5)

- Elméletileg a teljesítmény javítható több HTTP kérés ugyanabba a TCP üzenetbe történő csomagolásával is.
- Feleslegessé teszi egy jobb mechanizmus, a HTTP/2 által használt multiplexelés.
- Lásd: *Connection management in HTTP/1.x – HTTP pipelining*
  https://developer.mozilla.org/en-US/docs/Web/HTTP/Connection_management_in_HTTP_1.x#http_pipelining

Kapcsolatkezelés: kapcsolat lezárása

- Kapcsolat explicit lezárása:
  - A `Connection` fejlécmező biztosít egy `close` opciót, mellyel a küldő jelezheti, hogy az aktuális kérés/válasz befejezése után lezárásra kerül a kapcsolat.
    - Kérésekben és válaszokban is használható.
  - Példa:
    - `Connection: close`
- Időtúllépés:
  - A szerverek általában van valamiféle várakozási ideje, melyen túl nem tartanak fenn tovább egy inaktív kapcsolatot.

Kapcsolatkezelés: egyidejű kapcsolatok (1)

- A legtöbb szervert úgy tervezték, hogy képes legyen sok ezer egyidejű kapcsolatot fenntartani.
- A legtöbb kliens több kapcsolatot tart fenn párhuzamosan, egy szerverhez akár többet is.
  - Jellemzően a **sor eleji blokkolás** (***head-of-line blocking***) problémájának elkerüléséhez használnak több kapcsolatot.

Kapcsolatkezelés: egyidejű kapcsolatok (2)

- A HTTP korábbi kiadásai egy korlátot határoztak meg az egy kliens által egy adott szerverhez egyidejűleg fenntartható kapcsolatok számára.
  - RFC 2616: a kapcsolatok maximális száma 2.
- Ez sok alkalmazáshoz célszerűtlennek bizonyult, ezért a HTTP/1.1 nem ír elő konkrét korlátot, hanem helyette azt javasolja a klienseknek, hogy legyenek óvatosak, amikor több kapcsolat nyitnak.
  - Minden egyes kapcsolat a szerver erőforrásait fogyasztja és a szerver megtagadhatja a kéréseket, ha egy kliens túl sok kapcsolatot nyit meg.

Kapcsolatkezelés: egyidejű kapcsolatok (3)

- Korlátok a kapcsolatok számára:
  - **Firefox**: lásd az alábbi opciókat (`about:config`):
    - `network.http.max-connections` (alapértelmezett érték: 900)
    - `network.http.max-persistent-connections-per-proxy` (alapértelmezett érték: 32)
    - `network.http.max-persistent-connections-per-server` (alapértelmezett érték: 6)
  - **Chromium**, **Google Chrome**: a Firefox fenti opcióinál adott alapértelmezett értékek használata rögzített módon
    - Lásd: https://www.chromium.org/developers/design-documents/network-stack/#connection-management
  - **Chromium-alapú Microsoft Edge**: https://docs.microsoft.com/en-us/microsoft-edge/devtools-guide-chromium/network/issues#queued-or-stalled-requests

További ajánlott irodalom

- *MDN Web Docs – HTTP* https://developer.mozilla.org/docs/Web/HTTP
- *Apache HTTP Server Documentation* https://httpd.apache.org/docs/
- Ilya Grigorik, *High Performance Browser Networking*. O'Reilly, 2013. https://hpbn.co/