REPUBLIKA E SHQIPËRISË

UNIVERSITETI I TIRANËS

FAKULTETI I EKONOMISË

DEPARTAMENTI "STATISTIKË DHE

INFORMATIKË E ZBATUAR"

Temë Diplome

"Ndjekja e përdoruesve në web"

Diplomë e ciklit të parë të studimit

"BACHELOR"

Punoi:

Anisa Bruçi

Pedagog udhëheqës:

Prof. Dr. Fatmir Memaj

Tiranë, 2018

DEKLARATË

Unë (Ne), i/e nënshkruari/s Anisa Bruçi deklaroj që: **(1)** Kjo mikrotezë përfaqëson punimin tim origjinal, përveç rasteve të citimeve dhe referencave dhe **(2)** Kjo mikrotezë nuk është përdorur më parë si mikrotezë apo projekt kursi në këtë Universitet apo në Universitete të tjera.

_____

FALENDERIME DHE DEDIKIME

Mirënjohje dhe falenderim i veçantë për udhëheqësin tim shkencor, Prof. Dr. Fatmir Memaj, i cili me profesionalizmin e tij ndihmoi gjatë etapave të formulimit dhe realizimit të studimit me këshillat dhe sugjerimet e tij.

Gjithashtu, një falenderim dua t'i bëj familjes time, të cilët që në zanafillë e deri në finalizimin e studimit kanë qenë për mua shtysa dhe mbështetja ime më e fuqishme.

Abstrakti

Ndjekja e përdoruesve në web është shumë e përhapur në ditët e sotme. Të gjitha teknikat e mundshme përdoren për të ndjekur përdoruesit në internet. Jo vetëm cookies, por nga mëenyrat më të ndryshme te ndjekjes dhe gjithashtu metoda e fingerprinting. Disa përdorues mund të fshijnë rregullisht cookies, pëerdorimi I dritareve private të shfletuesit ose të përdorin plugin për të reduktuar shtesat nga të cilat mund të ndiqen.

Të qenurit I ndjekur gjithsesi mund të shmanget asnjëherë plotësisht. Ekzistojnë një numër metodash ndjekëse, të cilat janë shumë të veshtira ose pothuajse të pamundura për tu bllokuar. Shumica e këetyre metodave janë si rezultat I lojës macj me miun midis palëve ndjekëse dhe përdoruesve të përgjegjshem mbi privatësinë e tyre.

Në këtë tezë, do të shohim mënyrën sesi shfletuesit dhe shtesat e privatësisë "luftojnë" ndjekjen si dhe mangësitë që ata kanë. Ne vumë re që shfletuesit përgjithësisht aplikojnë të njëjtat teknika për të bllokuar ndjekësit. E njëjta gjë është dhe për shtesat e shfletuesve, të cilat pothuajse mbështeten tek "lista e zezë" (blacklist) për të bllokuar ndjekësit.. aktualisht vetëm Privacy Badger përdor një mënyrë tjetër, një algoritm I cili identifikon ndjekësit. Për mendimin tim, kjo është një veçori premtuese e cila mund të jetë akoma më e mirë se blacklists.

Përmbajtja e punimit

Listë tabelash dhe figurash

Kapitulli 1

1. Hyrja

Në ditët e sotme, Interneti është bërë pjesë e pandashme e jetës për shumë persona. Së fundi me shpërndrjen aq të madhe të Smartphones, mund të konsiderohet pjesë e jetës së përditshme. Komunikimi modern është i papërfytyrueshëm pa Internetin ku dhe SMS klasike janë zëvendësuar nga aplikacionet siç është WhatsApp[23]. Gjithsesi Interneti po përdoret dhe për më shumë, si: për të bërë blerje, për të kërkuar për gjëra që ju interesojnq,për të lexuar lajme ose thjesht për tu argëtuar. Duke konsideruar të gjithë përdorimët, një çështje harrohet : Sa më shumë Interneti përdorët, aq me shumë informacion personal zbulohet.

Interneti ka ndryshuar shumë që nga koha kur ai ishte thjesht static, ku ndërveprimi me përdoruesin ishte pothuajse joekzistente. Shumë e shumë koncepte u futën në mënyrë që Interneti të bëhej më dinamik. Kjo normalisht solli më shumë kompleksitet dhe rrezik për privatësinë.

Këto shtesa ju dhanë pronarëve të faqeve të Internetit më shumë karakteristika të reja për faqet e tyre, duke përfshirë ndjekjen e përdoruesve. Një ndër teknikat kryesore për këtë janë HTTP cookies, edhe pse jo të gjithë metodat e ndjekjes I përdorin ato. Shumë teknika janë dominuese sepse HTTP cookies mund të çaktivizohen ose të fshihen nga përdoruesi. Alternativat për HTTP cookies janë më së shumti është ruajtja e një identifikuesi në memorien e pajisjes, të vështirë për tu gjetur dhe më e rëndësishmja për tu fshirë nga përdoruesi. Një tjetër mënyrë e njohur është fingerprinting I përdoruesit dhe I pajisjes së tij. Në këtë rast identifikuesit përdorin të dhënat të cilat "rrjedhin" gjatë shfletimit, siç është adresa IP, fontet e instaluara ose zakonet e tyre në të shkruar. Këto teknika do të shpjegohen më tej në Kapitullin 2.

Ndjekja vetëm me HTTP cookies do të ishte mënyra më transparente për të ndjekur përdoruesit, por përdoruesit e gjetën këtë metodë të qëndrueshme mjaftueshëm. Interesat komercialë të palëve ndjekëse i bëjnë ata të duan të ndjekin përdoruesit sa më saktë dhe më këmbëngulës [15]. Kjo po bëhet sa e lehtë dhe e vështirë në të njëjtën kohë: e lehtë meqënëse shumë e shumë teknika janë shpikur, e vështirë sepse përdoruesit përdorin shumë e shumë pajisje të ndryshme për të kërkuar në web dhe sepse ata aplikojne dritaret private të kërkimit dhe rritjen e plugins për privatësine[16]. Në lojën e maces dhe miut që është ndjekja në web, ndjekësit mundohen të jenë gjithmonë një hap përpara konsumatorit.

Kjo ngre pyetjen: Çfarë opsionesh ka për uljen e nivelit të të qenurit I ndjekur dhe cilat metoda të ndjekjes ende nuk mund të shmangen? Me të gjithë shfletuesit e njohur që ofrojnë cilësime të privatësisë dhe veglat për rritjen e privatësisë, të bëjnë të mendosh se ndjekësit në web pothuajse mund të çaktivozohen të gjithë.

Sigurisht, mund të ketë zgjidhje për ndalimin e çdo metode ndjekjeje, por ato janë të pavlefshme nëse jane të veshtira për tu gjetur, të vështira për tu kuptuar ose të limituara në përdorim. Kështu që do ta ndalim kërkimin tonë në kundërmasat ndaj ndjekjes në web që janë lehtësisht të gjetshme dhe kanë një bazë të gjerë përdoruesish. Kjo do të thotë që opsionet të cilat ofrohen nga shfletuesit janë interesante për tu mësuar, siç janë shtesat e privatësisë plugins të cilat janë lehtësisht të instalueshme dhe nuk kanë shumë nevojë te konfigurohen .

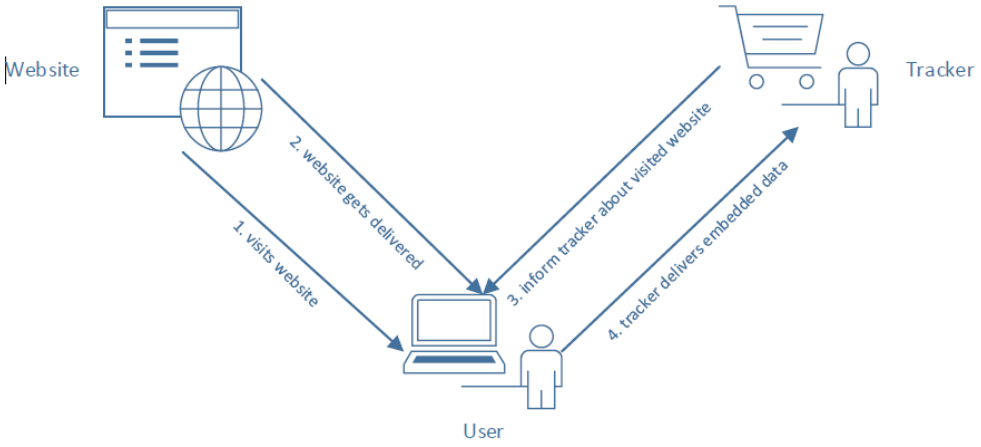

Figura 1.1 Si funksionon ndjekja në web

Ne do të donim të gjenim balancën midis ndjekjes online dhe opsionet për mbrojtjen e privatësisë. Për të parë këtë balance, ne do të bëjmë një rishikim të teknikave të ndjekjes që përdoren dhe sigurisht mënyrat sesi ato mund të kundërshtohen ose pengohen nga metodat e rritjes së privatësisë. Siç u përmend dhe më lart, ne do të fokusohemi në teknikat (të ndjekjes dhe mbrojtjes ndaj ndjekjes) që përdoren nga shumë përdorues.

Pritshmërite janë që sa më "e vjetër" dhe më e njohur metoda e ndjekjes ajo mund te kundërshtohet efektivisht si nga cilësimet e privatësisë së shfletuesit dhe nga shtesat add-ons të jashtme. Teknikat më të panjohura ose fingerprinting me shumë mundësi do të jenë më të vështira për tu kundërshtuar, dhe gjithashtu mund të ketë metoda të cilat mund të jenë të pakundërshtueshme deri tani. Që do të thotë se shfletuesit me shumë mundësi nuk kanë opsione për të bllokuar ndjekjen nga këto metoda.

Baza për këtë hipotezë është hulumtimi I kryer në këtë fushë. Një kërkim kyç në web për ndjekjen dhe fingerprinting ëeshtë dhe kërkimi I panopticlick [17] në të cilin EFF (Electronic Frontier Foundation) tregoi se mbi 90% e shfletuesve mund te jenë unikisht fingerprinted duke parë fontet e instaluara ne shfletues.

Në kapitullin 2, do të bëhet një rishikim I teknikave të ndjekjes që përdoren aktualisht. Këtu do të ndalemi tek metodat që përdorin një formë të të dhënave të ruajtura dhe ndjekjes së përdoruesve si dhe fingerprinting I pajisjeve. Për metodën e që përdor të dhënat në memorie, do të shohim metodat më të njohura. Ndërsa tek fingerprinting do të ndahet në atë active dhe passive.

Kapitulli 3 do të prezantojë kundërmasat ndaj ndjekjes në web që janë të implementuar në shfletues. Këtu përfshihen cilësimet e ofruara në shfletuesit web si dhe dritaret private të shfletimit, por gjithashtu do të përfshihen dhe Do Not Tracj dhe P3P(Platform for Privacy Preferences).

Përgjatë kërkimit, u pa se duhej te bëhej e qartë diferenca midis një vëzhguesi local(ose sulmues) nga ai I largët. Kjo është e nevojshme pasi disa masa të privatësisë që do të diskutohen fokusohen më shumë në vëzhguesit local sesa në ndjekësit në web, që tregon se qëllimi I tyre është I ndryshëm nga masat që fokusohen në ndjekësit e largët. Diferenca do të shpjegohet me tej ne seksionin 3.3.1

Kapitulli 2

2. Metodat aktuale të ndjekjes

Në këtë kapitull do të listohen metodat e ndjekjes që përdoren aktualisht në web dhe mënyrën sesi funsionojnë. Teknikat që përdorin ruajtjen e të dhënave do te mbulohen në seksionin 2.1. fingerprinting do të trajtohet në seksionin 2.2. ndërsa përsa u përket masat që merren për ta do të shpjegohen në kapitullin 3.

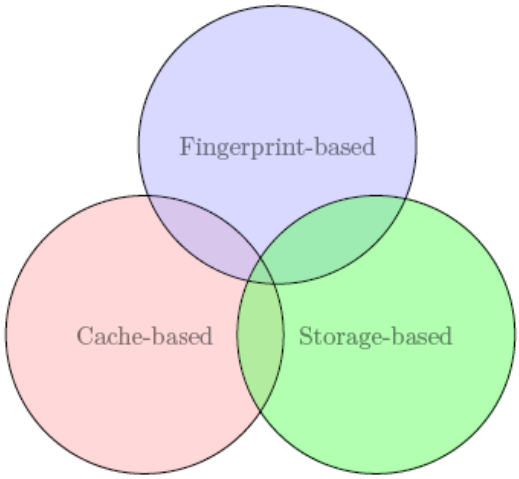

Figura 2.1 Kategoritë e metodave të ndjekjes

2.1 Teknikat e ndjekjes duke përdorur ruajtjen e të dhënave

Mënyra më e zakonshme për të ndjekur përdoruesit nëpër internet është duke ruajtur nje identifikues unik diku në memorien e kompjuterit te tyre. Ky identifikues mund të perdoret nga palët ndjekese, duke ndjekur përdoruesit në internet. Ndryshimi me fingerprinting (që mbulohet në seksionin 2.2) është se fingerprinting nuk ruajnë një identifikues lokalisht në kompjuterin e përdoruesit dhe se mbështetet në atributet e një përdoruesi, siç është adresa e tij IP . Ndjekja duke përdorur ruajtjen e të dhënave funksionon me një identifikues që krijohet nga një palë ndjekëse dhe nuk kanë të bëjnë fare me atributet specifike të përdoruesit.

2.1.1 HTTP cookies

Mënyra më e njohur për të ndjekur përdoruesit është duke përdorur HTTP cookies, shpesh të referuara thjesht si cookies. Shfletuesit e uebit mbështeten në protokollin HTTP (Hyper Text Transfer Protocol) për të transferuar informacionin[9]. HTTP, megjithatë, është një protokoll pa shtetësi, që do të thotë se asnjë informacion nga një sesion nuk mbahet as nga serveri, as klienti. Kjo bëri shfletimin të pamundur në shërbime për të cilat duhet te mbahej gjendja e shfletuesit (si p.sh. përdoruesi i regjistruar). Si zgjidhje, u bë e mundur që të ruhen në skedarë të vegjël (deri në 4KB) në kompjuter , në të cilin ruhet gjendja e shfletuesit[1]. Këto skedarë teksti dërgohen me çdo mesazh kërkese HTTP. Ky koncept u bë më vonë i njohur si cookies.

Cookies HTTP funksionojne duke përdorur nje header Set-Cookie. Ky header është pjesë e një përgjigje HTTP nga një server. Një header Set-Cookie bën që shfletuesi të ruajë një cookie në kompjuterin e përdoruesit e cila do të dërgohet për çdo kërkesë në serverin që krijoi cookie-n. Cookies me një datë skadimi ruhen në kompjuterin e përdoruesit derisa të kalojë data e skadimit ose derisa cookie të fshihet. Kur nuk përcaktohet data e skadimit gjatë formimit të cookies, ai konsiderohet si një cookie sesion. Kjo do të thotë se cookie do të fshihet sapo të përfundojë sesioni i shfletuesit. Fjalë kyçe të tjera për cookies janë Domain, Secure dhe HttpOnly. Këto specifikojnë domenin në të cilin bie cookie (dhe kështu në cilat serverët cookie mund të dërgohet nga klienti), nëse cookie mund të dërgohet vetëm mbi një lidhje të sigurt dhe nëse cookie mund të jetë e aksesueshme nga scripte në anën e klientit.

Përveç HTTP Set-Cookie header, cookies gjithashtu mund të vendosen (dhe lexohen) nga JavaScript, duke bashkëvepruar me Document Object Model (DOM). HTTP mund të jetë ose "palë e parë" ose "palë e tretë". Cookies e palës së parë janë cookies të përcaktuara nga domein që një përdorues po viziton drejtpërdrejt, ndërsa cookies e palës së tretë vendosen nga domeinet që vizitohen në mënyrë indirekte, për shembull kur pala e parë ngarkon një burim nga një palë e tretë. Një shembull do të ishte firstparty.com i cili ka përfshirë një imazh nga thirdparty.com. Kur një përdorues viziton firstparty.com, cookies të përcaktuara nga firstparty.com janë cookies e palës së parë, ndërsa cookies nga thirdparty.com janë cookie të palës së tretë.

Code

```
function getCookie(Diploma)
{
// Si fillim shohim nese ka nje cookie te ruajtur
// Perndryshe gjatesia e document.cookie duhet te jete zero

if (document.cookie.length > 0)
{
// Se dyti shohim nese emri I cookie eshte I ruajtur ne
// objektin "document.cookie" per faqen.
// Meqenese me shume se nje cookie mund te vendoset ne nje faqe,
// mund te jete e mundur qe cookie jone te mos ndodhet
// por "document.cookie" nuk eshte nje tekst bosh
// Nese emri I cookie nuk gjendet atehere vlera -1 ruhet ne
//variablin e quajtur "vazhdo"

vazhdo = document.cookie.indexOf(Diploma+"=");
if (Vazhdo != -1) //
{

// Cookie ishte vendosur
//vlera e ruajtur ne cookie kthehet nga funksioni

vazhdo += Diploma.length+1;
end = document.cookie.indexOf(";", vazhdo);
if (end == -1) end = document.cookie.length;
return unescape(document.cookie.substring(vazhdo, end)); }
}
return null;
// Cookie nuk ishte vendosur
// Nga funksioni kthehet vlera "null"
}

function setCookie(Diploma, value, expiredays)
{
```

```
// Per te vendosur cookie e re perdoren 3 variabla
// Emri I cookie, vlera qe do te ruhet, numri I diteve pas sa diteve skadon
// Rreshtat e pare ne funksion konvertojne numrin e diteve ne nje date te sakte

var ExpireDate = new Date ();
ExpireDate.setTime(ExpireDate.getTime() + (expiredays * 24 * 3600 * 1000));


// Rreshtat e tjere ruajne cookie, thjesht duke I vendosur

// nje vlere ne objektin "document.cookie"
// Data konvertohet duke perdorur funksionin "toGMTstring()"

document.cookie = Diploma + "=" + escape(value) +
((expiredays == null) ? "" : "; expires=" + ExpireDate.toGMTString());
}

function delCookie (Diploma)
{

// Funksioni kontrollon nese cookie eshte vendosur
// Nese po data e skadences 30 Gusht 2019

if (getCookie(Diploma)) {
document.cookie = Diploma + "=" +
"; expires=Wed, 30 Aug 2019 00:00:00 GMT";
}
}
```

Përdorimi në ndjekje

HTTP cookies mund të përdoren si një mjet ndjekes në mënyra të shumta. Ato mund të përdoren më vete, duke vendosur vetëm një cookie me një identifikues në pajisjen e përdoruesit kur ai viziton faqen e internetit, ose ato mund të përdoren në kombinim me teknika të tjera. Këto përfshijnë sinkronizimin e cookie-t, ri-zbulimin e cookie-t (respawning) dhe ndjekja e bashkuar (tracking aggregators)[21]. Syncing Cookie do të thotë që cookies janë kaluar nga një fushë në një tjetër. Respawning cookies i kthejnë cookies të fshira nga një vend tjetër ruajtës, në të cilin është ruajtur identiteti i njëjtë. Kjo do të trajtohet më tej në seksionin 2.1.2. Disa palë ndjekëse shërbejnë si agregues për shërbime të tjera ndjekëse. Pala ndjekëse pastaj dërgon kërkesë në agregues, që përfshin identitetin e ruajtur në cookie të vendosur nga pala ndjekëse. Kjo do të thotë se agreguesi do të mbledhë identifikuesit e vendosur nga shumë palë ndjekëse.
Jo të gjitha HTTP cookies përdoren për qëllime ndjekese, por Li et al. kanë treguar se cookies gjurmuese dhe jo-gjurmuese mund të dallohen me një saktësi shumë të lartë[22].

2.1.2 Flash cookies

Adobe Flash përdor Local Storage Objects (LSOs) për të ruajtur të dhënat. Këto të ashtuquajturat Flash cookies përdoren nga aplikacionet Flash për të ruajtur të dhënat lokale që përdoren prej tyre. Flash Cookies përdoren gjithashtu për të gjurmuar përdoruesit e internetit. Ata kanë disa përparësi mbi HTTP Cookies për ndjekjen e palëve. Paraprakisht, Flash cookies ruhen në 100 KB. Kjo mund të shtrihet në një sasi "të pafundme", kur lejohet nga përdoruesi. Kjo është të paktën 25 herë më e madhe se 4 KB e ruajtjes së HTTP cookie. Ruajtja ekstra mund të jetë e dobishme për ruajtjen e më shumë informacion rreth përdoruesve, por identifikuesit e veçantë ruhen lehtësisht edhe në 4KB. Më e rëndësishmja, Flash cookies janë ruajtur në një vend tjetër të fshehtë dhe më të fshehur sesa HTTP cookies.

Një tjetër dallim midis Flash cookies dhe homologëve të tyre HTTP është se Flash cookies nuk skadojnë sipas një date të paracaktuar. Në fakt, ata nuk kanë fare datë skadimit. Kjo do të thotë se Flash LSOs

qëndrojnë në kompjuterin e përdoruesit derisa ato të fshihen. Së fundi, Adobe Flash nuk ka një hapësirë të veçantë ruajtjeje për secilin shfletues në të cilin është instaluar plugin. Kjo do të thotë që cookies Flash të vendosura në një shfletues ,mund të aksesohen dhe nga platforma te tjera të shfletimit me Flash cookies.

Përdorimi në ndjekje

Cookies Flash përdoren për të gjurmuar përdoruesit në një mënyrë të ngjashme me HTTP cookies. Kjo ndodh sepse një identifukues mund të ruhet si LSO. Ky identifikues mund të aksesohet më vonë nga faqet e internetit që përmbajnë elementë të Adobe Flash. Këto elemente nuk duhet të jenë elementë vizualë, prandaj ky aplikacion i Flash mund të jetë duke funksionuar në sfond, i fshehur nga sytë e përdoruesit.

2.1.3 HTML5 ruajtja lokale dhe IndexedDB

HTML5, i prezantuar në vitin 2014, përpiqet të përmirësojë mbështetjen për aplikacionet në ueb me ndërveprimin me përdoruesit. Ky standard i ri gjithashtu erdhi me disa vende të reja magazinimi dhe kështu vende për të ruajtur identifikuesit e ndjekjes. Dy opsionet kryesore të magazinimit HTML5 janë Local storage dhe IndexedDB.

Ruajtja lokale në HTML5 është pjesë e WebStorage API. Objektet e ruajtjes ruhen si një palë kyçe , e cila është e ngjashme me HTTP cookies. Objektet janë megjithatë janë më të mëdha (të paktën 5 MB) dhe informacioni nuk dërgohet automatikisht në një server, por një faqe interneti duhet ta kërkojë vetë atë. Magazinimi lokal gjithashtu ka një formë më të përkohshme: Ruajtja e Sesionit. Ruajtja e sesionit për një sesion të caktuar hiqet sapo skedari i shfletuesit të mbyllet. Kjo do të thotë që skedat e shumta që tregojnë të njëjtën web faqe, nuk do të jenë në gjendje të hyjnë në ruajtjen e Sesionit të njëri-tjetrit. Kjo është ajo ku ruajtja e sesionit HTML5 vërtet ndryshon nga HTTP cookies, meqë cookies jo të paqendrueshme do të mbahen derisa i tërë shfletuesi i internetit të mbyllet. Meqënëse ruajtja e Sesionit mbahet shumë shpejt, nuk ka vlere të vërtetë ndjekja e përdoruesve me vendodhjen e memories.

HTML5 Ruajtja lokale(Local Storage) mund të jetë "zgjidhje" për këtë. Magazinimi lokal është një metodë e vazhdueshme e ruajtjes. Artikujt e ruajtur në këtë vend, nuk kanë një datë skadimi dhe kështu nuk skadojnë automatikisht. Përveç kësaj, ruajtja lokale mund të arrihet në mes të dritareve të ndryshme të shfletuesit[18].

HTML5 ofron një mënyrë tjetër të ruajtjes, IndexedDB. Në këtë bazë të dhënash ruhen objektet e JSON. Një veçori e IndexedDB është aftësia për të shtuar një indeks për artikujt në bazën e të dhënave. Në këtë mënyrë, disa hyrje mund të gjenden më lehtë. IndexedDB është një metodë e ruajtjes së vazhdueshme, por i nënshtrohet kufizimeve të caktuara. Këto janë të ngjashme me ruajtjen HTML5 lokale, duke qenë e njëjta politikë ne origjinë (e cila do të përpunohet në seksionin 3.1.) dhe duke qenë në gjendje të lexojë shënimet e vendosura nga i njëjti domain dhe protokoll. Për qëllime të ndjekjes, ruajtja lokale HTML5 dhe IndexedDB nuk kanë ndryshime te medha.

Ruajtja lokale HTML5 dhe IndexedDB mund të pastrohen lehtësisht nga brenda një shfletuesi. Regjistrimet individuale mund të fshihen përmes veglave të shfletuesit te internetit, të cilat mund të japin një pasqyrë të memories së përdorur nga faqet e internetit. HTML5 ruajtja lokale është e përfshirë dhe të dhënat mund të fshihen nga përdoruesi. Një tjetër mënyrë shumë më e lehtë për të pastruar magazinimin lokal është duke përdorur " clear all cookies " – në opsionet e shfletuesve të uebit. Kjo jo vetëm që fshin

të gjitha HTTP cookies të ruajtura, por edhe të gjitha të dhënat e HTML5 ruajtja lokale. Megjithatë ky opsion nuk I fshin IndexedDB. Kjo do të përpunohet më tej në seksionin 3.2/

Përdorimi në ndjekje

Karakteristikat e përmendura më lart të lënë të mendosh se ruajtja lokale HTML5 ose IndexedDB mund të bëhen një alternativë ndaj HTTP cookies. Aktualisht, ruajtja lokale përdoret shpesh, por së bashku me HTTP cookies. Kjo do të thotë që ruajtja lokale përdoret për ndjekjen, por nuk ka zëvendësuar plotësisht HTTP cookies. Këto kopje të HTTP cookies të ruajtura në HTML5 ruajtja lokale ofrojnë një mënyrë për të rikthyer HTTP cookies.

Për IndexedDB, e njëjta gjë vlen si për HTML5 ruajtjen lokale. Ata të dy ofrojnë një vend tjetër për ruajtjen e të dhënave në të cilat mund të ruhen identifikuesit, por nuk paraqesin kërcënime shtesë për privatësinë, përveç cookie respawning (që pothuajse paraqitet në çdo hapësirë magazinimi). Për IndexedDB specifikisht ka dëshmi se ajo gjithashtu përdoret për rindërtimin e Flash cookies.

Respawning Flash cookies në vend të cookies HTTP është mjaft e palogjikshme, sepse HTTP cookies janë dërguar automatikisht me kërkesat HTTP[8]. Flash cookies në anën tjetër duhet të merren nëpërmjet JavaScript-it. Respawning Flash cookies në vend të HTTP cookies mund të bëhet për t'i dhënë ndjekësit një alternativë tjetër, nëse përdoruesi fshin të dyja cookies e tij HTTP dhe Flash.

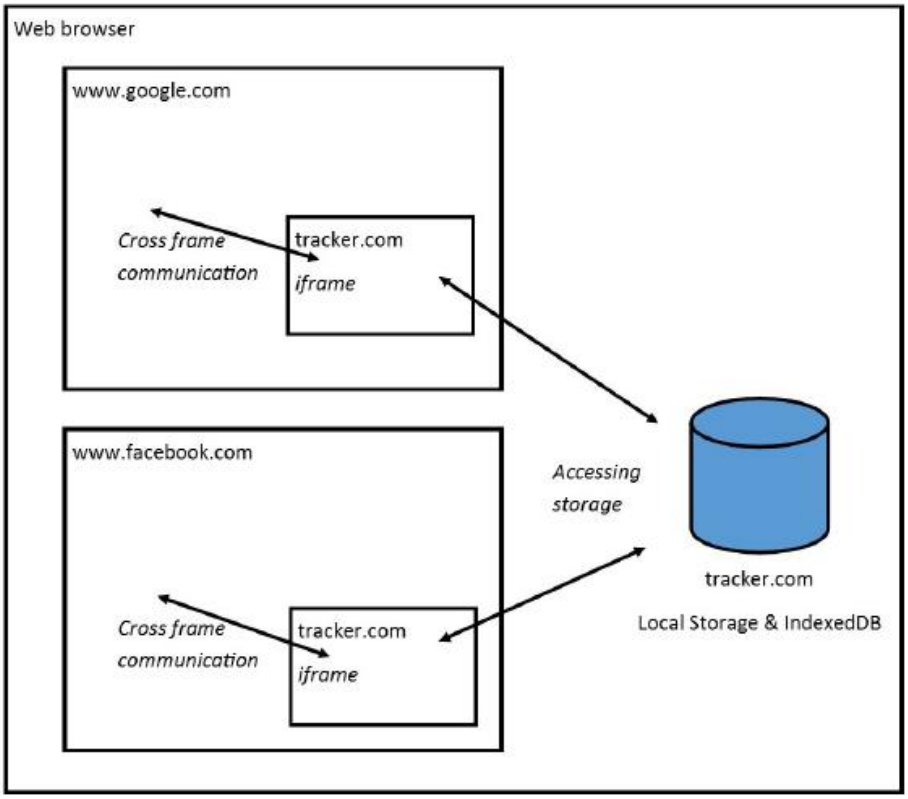

Figura 2.1.3 Prezantimi grafik i ndjekjes së përdoruesit duke përdorur Local Storage ose IndexedDB

2.1.4 ETags

ETags janë pjesë e header-it të përgjigjes HTTP. Një webserver krijon një ETag për faqet e saj dhe e dërgon këtë tag me faqe kur kërkohet fillimisht nga një shfletues. Shfletuesi pastaj do ta dërgojë këtë ETAG përsëri në fushën if-none-match, kur ajo kërkon përsëri të njëjtën faqe. Kur faqja nuk ka ndryshuar, serveri do tëkthejë këtë përgjigje dhe shfletuesi mund ta ngarkojë faqen e internetit vetëm nga cache e saj, në vend që ta marrë atë përsëri nga serveri.

Përdorimi në ndjekje

ETags janë krijuar nga webserver dhe nuk kanë kufizime të tjera , përveç madhësisë maksimale 81864 bit. Për shkak të kësaj mungese kufizimesh, vëzhguesit e internetit mund të dërgojnë etiketa unike për përdoruesit e ndryshëm dhe kështu t'i ndjekin ato, meqë etiketa unike është gjithmonë e kthyer në server kur kërkon përsëri të njëjtën faqe.

Ndjekja me ETags është e vështirë të kundërshtohet, pasi mbështetet në një funksion thelbësor të shfletuesve të uebit. Për të bllokuar ndjekjen me ETags, ju do të duhet të pastroni cache-in e shfletuesit në mes të çdo vizite të një faqe interneti.

2.2 Teknikat që përdorin fingerprinting

Ndjekja gjithashtu mund të bëhet edhe pa ruajtjen e identifikuesve në pajisjen e një përdoruesi. Metoda më e zakonshme për këtë është e ashtuquajtura fingerprinting. Këtu një përdorues, pajisje ose kombinim identifikohet nga informacioni që "rrjedh" dhe "variacione delikate, por të matshme që i lejojnë ato të bëhen pjesë e fingerprinting."[17] Fingerprinting mund të bëhet në dy mënyra: aktiv ose pasiv. Fingerprinting pasiv është bërë duke analizuar informacionin që është dërguar në rrjet në çdo rast, pa kërkuar informacion të caktuar. Për shembull, adresa IP e një pajisjeje është gjithmonë e dukshme nëse kjo pajisje lidhet me një shërbim të internetit. Fingerprinting aktiv në anën tjetër kërkon në mënyrë aktive pajisjen për më shumë informacion. Kjo përfshin sistemin operativ dhe fontet e instaluar të një pajisjeje.

2.2.1 Fingerprinting pasiv

Siç u tha më lart, fingerprinting pasiv nga një shërbim i internetit nënkupton vëzhgimin e trafikut të rrjetit dhe nga kjo, duke krijuar një identitet unik për kombinimin e përdoruesit / pajisjes. Me këtë fingerprinting, palët ndjekëse mund të ndjekin përdoruesit, madje edhe për periudha më të gjata kohore. Vetitë e përdoruesit ose të pajisjes mund të ndryshojnë me kalimin e kohës, por është vërtetuar nga Peter Eckersley se mund të zbulohet kur një fingerprinting është një "pasues" i një fingerprinting tjetër[17] . Kjo mund të bëhet edhe me më shumë se 99% saktësi në rastin e tij.Fingerprinting pasiv nuk mund të vërehet nga përdoruesit, pasi një faqe interneti nuk dërgon ndonjë kërkesë të veçantë ose të ruaje informacion mbi pajisjet. Të gjitha fingerprinting dhe ndjekja ndodhin në anën e serverit. Kjo e bën atë një formë vërtet të vështirë të ndjekjes për tu vënë re ose kundërshtuar dhe për këtë arsye është një formë jashtëzakonisht interesante e ndjekjes.

2.2.2 Fingerprinting aktiv

Fingerprinting aktiv është pak a shumë një tregti me fingerprinting pasiv, midis të qenurit në gjendje të aksesojnë më shumë informacion dhe në këtë mënyrë të jenë në gjendje të krijojnë një fingerprinting më të veçantë dhe përdoruesit të jenë në gjendje të dallojne dhe ndoshta të kundërshtojnë këtë fingerprinting. Sidoqoftë, disa kundërshtime mund ta bëjnë më të lehtë fingerprinting. Konsideroni shembullin ku Adobe Flash mund të japë detaje të caktuara rreth pajisjes suaj. Kjo e bën më të lehtë për të krijuar një

fingerprinting të saktë. Por kur të çaktivizoni Flash Player, kjo mund të bëjë që ju të jeni pjesë e një grupi edhe më të vogël të përdoruesve, gjë që e bën edhe më të lehtë fingerprinting e pajisjes tuaj.

Fingerprinting aktiv mund të shihet si një shtesë e fingerprinting pasiv. Shumica e teknikave aktive gjithashtu përdorin informacionin që mblidhet me fingerprinting pasiv. Mënyrat më të përdorshme për fingerprinting aktiv janë duke përdorur listën e fonteve të instaluar[17] ose duke përdorur canvas fingerprinting[13]. Në këtë teknikë, mënyra se si një pajisje merret me nxjerrjen e një imazhi në një faqe interneti, përdoret si një fingerprinting unik.

Çdo teknikë e fingerprinting që kërkon një kërkesë aktive në një pajisje, shihet si fingerprinting aktiv.

Kapitulli 3

3. Masat e privatësisë në shfletuesit e web

Në këtë kapitull renditen masat më të njohura kundër ndjekjes në ueb, të cilat janë të implementuara në shfletuesit web.

3.1 Rregullorja dhe politikat

Që prej vitit 2002, Bashkimi Evropian është përpiqur të rregullojë vendosjen dhe rikthimin e informacionit mbi pajisjet e përdoruesve nga faqet e internetit. Kjo është bërë përmes direktivës së ePrivacy , e cila urdhëroi vendet anëtare të BE-së që të detyrojnë pronarët e faqeve të internetit të lejojnë përdoruesit të bëjnë zgjedhjen e tyre përsa iu përket cookies (dhe ruajtjen e të dhënave të tjera). Vetëm cookies e nevojshme ishin të përjashtuara.

Në vitin 2009, përjashtimi nga direktiva u ndryshua në një liste zgjedhjesh me e qartë [4]. Në Holandë ky ndryshim u miratua në të ashtuquajturën "telecommunicatiewet" (neni 11.7a 1), zakonisht i quajtur ligji i cookies. Ky ligj kërkonte pëlqimin e shprehur nga përdoruesit dhe i bëri faqet e internetit përgjegjëse për të provuar që një cookie e caktuar nuk përdoret për qëllime ndjekëse. Ndryshimi në legjislacion bëri që faqet e internetit të implementonin mënyra të ndryshme për të marrë pëlqimin nga përdoruesi. Ndër zgjidhjet ishin të ashtuquajturat cookiewalls, të cilat bllokojnë përmbajtjen e faqes, përveç nëse një vizitor pranon të gjitha cookies dhe marrëveshje të nënkuptuar kur viziton një faqe interneti.

Vende të tjera të BE-së zgjodhën rrugë të ndryshme. Britania e Madhe dhe Spanja, për shembull, zgjodhën të kërkonin pëlqimin e tyre vetëm nga përdoruesit, por në Spanjë vendosja e cookie-t është vetëm legjitime nëse një përdorues është aktiv në një faqe interneti[1].

3.2 Cilësimet e shfletuesit

Shfletuesit më popullor Google Chrome, Mozilla Firefox, Microsoft Internet Explorer / Edge dhe Safari të gjithe ofrojnë cilësimet e konfigurimit të përdoruesit nga të cilat ata mund të përfitojnë privatësi. Cilësimet që rezultojnë nga shfletuesit e internetit janë:

- Cilësimet në cookie-t e palës së parë dhe të palës së tretë
- Opsioni për të mundësuar Do Not Track
- Opsioni për të mundësuar mbrojtjen ndaj ndjekjes
- Cilësimet në shërbimet parashikuese
- Cilësimet në shërbimet e vendndodhjes

[1] https://cookiepedia.co.uk/cookie-laws-across-europe

3.2.1 Cilësimet në cookie-t e palës së parë dhe të palës së tretë

Qëllimi

Qëllimi i cilësimeve të cookies është që të lejojë përdoruesit të përcaktojnë nga cilat fusha ata duan të pranojnë cookies dhe nga të cilat jo. Shumë cookies përdoren për të ruajtur identifikuesit e përdoruesve, me të cilët faqet e internetit mund të gjurmojnë vizitorët e tyre, sidomos cookies e palës së tretë. Sidoqoftë, cookies përdoren gjithashtu për të mbajtur gjendje të dobishme të faqeve të internetit, të tilla si një shportë në një dyqan online. Prandaj, nevojitet një ekuilibër i mirë midis këtyre dy llojeve.

Implementimi

Cilësimet mbi cookies zbatohen në mënyrë të ngjashme në shumicën e shfletuesve të njohura. Chrome, Firefox dhe Edge i lejojnë përdoruesit të zgjedhë ndërmjet lejimit të të gjithë cookies, duke mos lejuar asnjë cookie dhe vetëm duke lejuar cookies e palës së parë. Google Chrome dhe Mozilla Firefox lejojnë përdoruesin gjithashtu të zgjedhë të ruajë të gjitha cookies derisa sesioni i shfletimit të jetë i mbyllur. Kjo do të thotë që të gjitha cookies (edhe cookies sesionit) fshihen pas mbylljes së sesionit të shfletimit. Egde, Safari dhe Internet Explorer nuk e bëjnë këtë opsion.

Safari, sipas parazgjedhjes, bllokon cookies e palës së tretë, por kishte një të metë që bëri të mundur që një palë e tretë të vendoste akoma cookies, edhe pse është I zgjedhur opsioni i bllokimit të tyre. Ai funksionoi duke dorëzuar të dhëna përmes një formulari HTML. [10]. Ky bug më vonë u rregullua në WebKit, motorin e shfletuesit që përdoret nga Safari dhe u miratua edhe në Safari4. Internet Explorer i trajton cilësimet rreth cookies pak më ndryshe. Preferenca të ndryshme mund të vendosen për zonën e rrjetit: internet, intranet, faqet e internetit të besuara dhe faqet e internetit të kufizuara. Opsionet janë te vendosura në një slider, që shkon nga lejimi i të gjitha cookies, përmes bllokimit të cookie-ve që personalisht mund të identifikojnë një përdorues ose bllokimin e cookie-ve pa një "politikë kompakte të privatësisë" (të lexueshme kompjuterisht), për të bllokuar të gjitha cookies. Internet Explorer përdor standardin P3P dhe e përdor këtë për të përcaktuar se cilat cookies konsiderohen identifikuese personale dhe cilat nuk janë.

Niveli më i lartë i privatësisë në Internet Explorer pohon gjithashtu se cookies të cilat tashmë janë në kompjuter nuk mund të lexohen nga faqet e internetit. Ne provuam se kjo ishte e vërtetë. Duke vizituar një faqe interneti që përdor cookies për të mbajtur përdorues të regjistruar, duke u futur në atë faqe dhe pastaj duke ndryshuar sliderin e privatësisë në cilësimet më të larta dhe freskimin e faqes së internetit, përdoruesi nuk ishte më I logguar.

Limitime

Kufizimi kryesor i çaktivizimit të cookie-ve të HTPP-së, sidomos i cookies të palës së parë, është se shumë faqe interneti thjesht ndalojnë së punuari, pasi ato mbështeten në cookies për funksionalitetin e tyre. Një tjetër kufizim i bllokimit të paautorizuar (të palëve të treta) HTTP është se ka shumë alternativa në dispozicion për gjurmuesit që ende ju gjurmojnë. Edhe me të gjitha cookies bllokuar, përdoruesit ende mund të gjurmohen me lehtësi. Sipas mendimit tim, bllokimi i cookies palës së parë nuk është opsion i mundshëm, për shkak të humbjes së funksionalitetit të përmendur. Bllokimi i cookies të palës së tretë ende është një opsion i mundshëm. Nëse faqet e internetit nuk funksionojnë si duhet me cookies e palës së

tretë të çaktivizuara dhe nëse përdoruesit i besojnë faqes që po vizitojnë, këto vende mund të shtohen në një listë të veçantë. Kjo siguron që cookies e palëve të treta lejohen vetëm në domein-et e besuara.

3.2.2 Do Not Track dhe P3P (Platform for Privacy Preferences)

Qëllimi

Opsionet e tjera të rritjes së privatësisë janë headear i HTTP Do Not Track (DNT) dhe standardi P3P . DNT u propozua në 2009 [3] dhe u standardizua në vitin 2015 [20], ndërsa P3P filloi në 2002 dhe u pezullua në 2007. DNT punon duke shtuar një fushë në header-in e kërkesës HTTP. Vlera e DNT header mund të jetë ose 0, 1 ose null. Këto vlera tregojne se përdoruesi pranon të gjurmohet, nuk dëshiron të gjurmohet ose nuk ka preferencë. Një fushë DNT e 1 duhet të ndalojë faqet e internetit nga vendosja e cookies ose mënyra të tjera të ndjekjes. Politika P3P specifikon se cilat informacione rreth përdoruesve janë të ruajtura, se si përdoren dhe për sa kohë. Përdoruesit mund të vendosin gjithashtu një politikë për veten e tyre, e cila krahasohet me politikën e serverit. Nëse serveri dëshiron të ruajë më shumë informacione sesa përdoruesit dëshiron, kjo nuk lejohet dhe serveri nuk do të caktojë cookies me këtë informacion të padëshiruar.

Implementimi

Do Not Track zbatohet në të njëjtën mënyrë në të gjithë shfletuesit web. Ky është një opsion që përdoruesit mund ta ndryshojnë. Nëse Do Not Track është aktivizuar, shfletuesi do të shtojë një fushë DNT = 1 për kërkesat që HTTP bën. Firefox-i dhe Chrome-i i tregojnë përdoruesit se çfarë Do Not Track është dhe si funksionon. Shfletuesit e tjerë nuk e bëjnë këtë. Politikat P3P mund të merren si një skedar XML. Politikat kompakte P3P gjithashtu mund të përfshihen në header-in e përgjigjeve HTTP nga serverat. P3P ka qenë aktiv vetëm në shfletuesit e internetit të Microsoft-it Internet Explorer dhe Edge. Ata ofrojnë nivele të caktuara të cilësimeve të privatësisë (të përmendura në seksionin 3.2.1), gjë që ndryshon parametrat e P3P në përputhje me rrethanat. Në Edge dhe Internet Explorer 11 për Windows 10, pajtueshmëria P3P u hoq[2], sepse funksionaliteti shihet si i vjetëruar dhe sepse standardi nuk u pranua shumë.

Limitimet

Deri tani, Do Not Track është vetëm një politikë pa efekte, pasi teknika kërkon pajtueshmëri nga ndjekja e palëve, të cilat sigurisht nuk do të jenë lehtësisht në përputhje me një standard që do të kufizojë biznesin e tyre [5]. Nëse zbatohet plotësisht dhe do të respektohet nga gjurmuesit, kjo mund të jetë një teknologji shumë premtuese. Mendimi i përgjithshëm megjithatë është se DNT nuk do të punojë në formën aktuale [8, 17, 21, 5, 6]. P3P ka të njëjtat kufizime si DNT, pasi P3P gjithashtu nuk zbatohet aspak. Kjo do të thotë që faqet e internetit nuk kanë nevojë për një politikë P3P dhe nëse ata kanë një politikë të tillë, ata nuk kanë nevojë t'i përmbahen asaj. Për më tepër, P3P nuk u miratua më 2002 [2], dhe gjithashtu jo në 2007 [6], kur puna për P3P u pezullua. Gjithashtu, faqet që zbatuan P3P jo gjithmonë e zbatonin atë saktësisht [19] ose nuk i përmbaheshin politikës fare [14].

[2] https://msdn.microsoft.com/en-us/library/mt146424(v=vs.85).aspx

3.2.3 Mbrojtja ndaj ndjekjes

Qëllimi

Disa shfletues zbatojnë një funksion që quhet Mbrojtja ndaj Ndjekjes, e cila është një teknikë që miratohet nga zgjerimet e privatësisë. Ky cilësim, nëse aktivizohet, përdor një listë për të bllokuar gjurmuesit e njohur. Me këtë opsion, shfletuesit po përpiqen të arrijnë një sesion më privat për përdoruesit e tyre pa pasur nevojë të instalojnë zgjatime të ndara.

Implementimi

Mozilla Firefox dhe Microsoft Internet Explorer të dyja ofrojne Mbrojtjen ndaj Ndjekësve. Në Firefox kjo funksion vetëm në dritare private. Ky cilësim, nëse aktivizohet, nuk ngarkon përmbajtje nga ndjekësit e palëve të treta bazuar në një listë të gjurmuesve të njohur. Firefox përdor një listë nga Disconnect[3] dhe i ofron përdoruesit mundësinë për ta ndryshuar këtë listë.

Limitimet

Mbrojtjen ndaj Ndjekësve që zbatohet në Firefox dhe Internet Explorer ka disa kufizime. Në Firefox, Mbrojtjen ndaj Ndjekësve mund të aktivizohet vetëm në dritaret private të shfletimit. Gjithashtu, përdoruesit mund të zgjedhin vetëm midis listës normale dhe të rreptë të bllokimit të ofruar nga Disconnect, pa mundësi për të shtuar ose fshirë domein-et. Internet Explorer lejon përdoruesit të zgjedhin çdo listë bllokimi në dispozicion, por kjo e bën përdoruesin përgjegjës për zgjedhjen e një liste të mirë bllokimi. Internet Explorer gjithashtu nuk ka opsionin për të shtuar përjashtime në listën e bllokimit.

3.2.4 Cilësimet në shërbimet parashikuese

Qëllimi

Google Chrome ofron opsione për të zgjedhur ose jo që shfletuesi të kontaktojë një shërbim në internet që mund të parashikojë pyetjet e kërkimit të shtypur në shiritin e URL-së të shfletuesit ose mund të paraqesin alternativa nëse nuk ekziston faqja web që një përdorues po përpiqet të arrijë (gabimet e navigimit). Është e rëndësishme të theksohet se ky funksionalitet ekziston vetëm në Google Chrome, pasi është shfletuesi i vetëm i internetit që përdor shërbimet parashikuese. Çaktivizimi i shërbimeve parashikuese të internetit do të thotë që Google nuk merr URL-në një përdorues që po përpiqet të arrijë, me të cilin Google mund të bëjë një parashikim.

Implementimi

Google Chrome i ofron përdoruesit të tyre tre zgjedhje. Ato mund të aktivizojnë ose çaktivizojnë një shërbim të uebit për gabimet e navigimit, për plotësimin e URL-ve dhe pyetjeve të kërkimit dhe një shërbimi parashikimi për të ngarkuar më shpejt faqet. Opsioni i fundit përdor DNS për të marrë adresat IP të të gjitha lidhjeve që janë të treguar në një faqe aktualisht. Kjo I kursen DNS kerkimin nëse një përdorues lundron në një link që është ngulitur në faqen aktuale, por nuk ka ndonjë rrezik të madh privat. I vetmI informacion i ruajtur është regjistrimi DNS i lidhjeve në një faqe që përdoruesi ka vizituar. Ky informacion gjithashtu ruhet derisa sesioni i shfletimit të mbyllet.

[3] https://disconnect.me

Limitimet

Çaktivizimi i shërbimeve parashikuese të Google Chrome nuk ka pothuajse asnjë të metë për përdoruesit. Ata mund të kenë nevojë të shkruajnë më shumë, meqë kërkimet e tyre nuk përfundojnë automatikisht ose a mund të pengohen në një faqe 404: Nuk gjendet, por kompromisi është se Google nuk merr çdo hyrje në shiritin e URL-ve që një përdorues kërkon.

3.2.5 Cilësimet në shërbimet e vendndodhjes

Qëllimi

Safari, Chrome, Firefox, Edge dhe Internet Explorer ofrojne opsione për të mos lejuar që faqet e internetit të aksesojnë vendndodhjen tuaj fizike. Qëllimi i këtij cilësimi është që të pengojë reklamuesit në shërbimin e reklamave specifike të vendndodhjes së përdoruesit dhe të kufizojë fingerprinting bazuar në vendndodhjen e pajisjeve dhe përdoruesve të tyre. Geolokimi i një pajisje gjenerohet nga një sërë burimesh të dhënash, duke përfshirë adresën IP dhe informacionin për rrjetet WiFi me një pajisje të lidhur[11].

Implementimi

Mënyra se si ky cilësim ofrohet në shfletuesit, është i njëjtë për Safari, Internet Explorer, Edge dhe Chrome. Përdoruesit i ofrohet opsioni të mos lejojë aksesimin në vendndodhjen fizike të pajisjes, e cila mund të aktivizohet ose çaktivizohet. Në Edge, nëse lejohen shërbimet e vendndodhjes, përdoruesi kërkohet ende për leje kur viziton një faqe interneti që dëshiron të hyjë në detaje të vendndodhjes për herë të parë. Firefox-i e ka zbatuar këtë mundësi ndryshe. Çdo herë që një faqe interneti dëshiron të hyjë në vendndodhjen e përdoruesit, ai ka mundësinë për ta lejuar këtë apo jo. Nëse përdoruesit duan të çaktivizojnë plotësisht shërbimet e vendndodhjes, do të thotë që aksesi në detajet e vendndodhjes gjithmonë do të mohohet, ata duhet ta bëjnë këtë nëpërmjet skedarit about:config të Firefox-it.

Limitimet

Heqja e aksesit në shërbimet e vendndodhjes ka një kufizim të madh për përdoruesit, gjë që është përcaktimi i vendndodhjes (i përafërt) i një pajisjeje ende të mundshme, për shembull me adresën e IP, e cila gjithmonë do të "dalë në shesh". Mund të mos jetë aq e saktë sa me të gjitha shërbimet e gjeolokimit të aktivizuara, por çaktivizimi i këtyre opsioneve nuk e bën të pamundur gjetjen e vendndodhjes së pajisjes suaj. Prandaj opsioni , për mendimin tim, është paksa mashtrues.

3.2.6 Përmbledhja e opsioneve të shfletuesve

Duke parë shfletues të ndryshëm që kemi analizuar në këtë kapitull, mund t'i krahasojmë ato në lidhje me opsionet e tyre të privatësisë. Mozilla Firefox dhe Google Chrome paraqesin një sërë parametrash të ngjashme, me dallimin mes tyre duke qenë se Firefox është duke ndjekur Mbrojtjen ndaj Ndjekjes në dritaren private të shfletimit, ndërsa Chrome ka opsione për vendndodhjen dhe shërbimet parashikuese web. Firefox nuk ofron cilësime në shërbimet e internetit parashikuese, sepse nuk ka implementuar shërbime të tilla. Shumica e cilësimeve të privatësisë që Internet Explorer ofron,mbështeten në P3P për të punuar, që do të thotë se ndërsa cilësimet duket premtuese, ato nuk do të jenë të efektshme për të bllokuar ndjekësit në web. Prandaj nuk është e çuditshme që Edge ka lënë shumë nga cilësimet që janë në dispozicion në Internet Explorer. Safari është shfletuesi i vetëm nga ato që ne pamë në të cilën bllokohen cookies te palës së tretë me parazgjedhje default.

Shfletuesit	Firefox	Chrome	Edge	Internet Explorer	Safari
Cilësimet default të cookies	Pranohen të gjitha	Pranohen të gjitha	Pranohen të gjitha	Pranohen të gjitha	Bllokon palët e treta
A mund të bllokojë palët e treat?	Po	Po	Po	Po	Po, por jo të gjitha
A mund të vendosen përjashtime në politikat e cookies?	Po	Po	Jo	Po, por e pamundur nëse të gjitha cookies janë bllokuar	Jo
Ofron Do Not Track	Po	Po	Po	Po	Po
Ofron mbrojtjen ndaj ndjekjes	Vetëm ne dritaret private	Jo	Jo	Po	Jo
Përdor shërbimet e parashikimit	Po, nga bookmarks dhe historia	Po	Jo	Jo	Jo
A mund të çaktivizohen shërbimet parashikuese?	Po	Po	Nuk aplikohet	Nuk aplikohet	Nuk aplikohet
Përdor shërbimet e vendodhjes	Po	Po	Po	Po	Po
A mund të çaktivizohen shërbimet e vendodhjes?	Po, lejimi për faqe	Po	Po	Po	Po

Tabela 3.2 Cilësimet e shfletuesve më të njohur

Duke parë cilësimet e këtyre shfletuesve persa i përket privatësisë, mund të shohim se Firefox dhe Chrome janë më të besueshme. Si parazgjedhje, Safari performon mirë sepse bllokon cookies te palës së tretë me cilësimet e paracaktuara të aktivizuara. Një tjetër gjë që vjen përpara është se Edge nuk ka aq shumë parametra të privatësisë sa Internet Explorer. Kjo mund të jetë për shkak se përdoruesit nuk i përdorin cilësimet në Internet Explorer shumë dhe Microsoft donte të përqëndrohej në një pasqyrë të thjeshtë të cilësimeve, pa shumë konfigueshmëri.

3.3 Dritaret e shfletimit privat

Dritaret e shfletimit privat (ndonjëherë të quajtura incognito ose InPrivate) është një opsion për rritjen e privatësisë që fokusohet në mbajtjen e një sesioni të veçantë nga shfletimi "normal". Seksioni në vijim do të shqyrtojë funksionalitetin e dritareve të shfletimit privat dhe rritjen e privatesise së tij.

3.3.1 Modele të ndryshme të sulmuesve

Dritaret e shfletimit privat mundësojne mbrojtjen kundër dy llojeve të ndryshme të sulmuesish ose vëzhguesish. I pari është një sulmues i ashtuquajtur lokal, i dyti është një sulmues i largët. Një sulmues lokal është një sulmues që ka akses fizik në pajisjen e një përdoruesi dhe përpiqet të mbledhë informacion nëpërmjet kësaj. Për shembull, një bashkëpunëtor ose një anëtar i familjes që sheh historinë tuaj të shfletimit dhe nga kjo, duke parë se cilat faqe interneti keni vizituar mund të shihen si një sulm lokal. Një sulmues / vëzhgues i largët nga ana tjetër nuk ka akses ndaj pajisjes fizike të objektivit të tyre dhe përpiqet të marrë informacion nga distanca. Vlen të përmendet se shfletimi privat përdoret kryesisht për të parë faqe me përmbajtje për të rritur [7].

Një sulmues i largët është më i rëndësishëm në sferën e ndjekjes së uebit, pasi një ndjekës i uebit në thelb është një vëzhgues i largët.

Qëllimi

Qëllimi i dritares të shfletimit privat është të sigurojë një sesion më privat për përdoruesit, kundër një vëzhgues lokal dhe një të largët. Ky është një ndryshim me Mbrojtjen ndaj Ndjekjes (siç mbulohet në çështjen 3.2.3) ose Do Not Track, të cilat përqendrohen vetëm në një ndjekës të largët. Siç mund të shihet në seksionin e Implementimit , të gjithë shfletuesit e internetit të internetit aktualisht kanë të njëjtin fokus, i cili është më i përqendruar tek një vëzhgues lokal se sa ai i largët.

Implementimi

Dritaret e shfletimit privat aktualisht ofrohet në të gjitha shfletuesit e njohur. Dritaret e shfletimit privat nuk ruhen në historikun e shfletimit, cookies ose historikun e kërkimit. Kjo do të thotë që këto tre lloje të të dhënave fshihen pas mbylljes së sesionit, në vend që të mos mbahen fare, gjë që do t'i bënte faqet e internetit të humbnin pothuajse të gjithë funksionalitetin e tyre. Shfletimi privat krijon një sesion të izoluar, i cili jo vetëm që pretendon të jetë më privat, por gjithashtu mund të përdoret për të hyrë në dy llogari në të njëjtën kohë.

Në Safari të Apple, historia e shfletimit, cookies dhe ruajtja lokale HTML5 të vendosura në një sesion "publik" ishin të aksesueshme në një sesion privat në 2010 [7]. Në anën tjetër: shikimi i vlerave të vendosura në një sesion privat gjatë një sesioni publik, nuk ishte e mundur. Sidoqoftë, mënyra se si historia dhe vlerat e cookie / HTML5 të vendosura në një sesion publik mund të shihen në një sesion privat, ishte abuzues nga gjurmuesit e uebit. Për shembull, një përdorues mund të ketë vizituar një faqe interneti që përdor një cookie për të mbajtur gjurmët e këtij përdoruesi. Nëse përdoruesi atëherë dëshiron të ketë një sesion të veçantë nga vizita e parë, kjo nuk do të ishte e mundur dhe një ndjekës do ta lidhte lehtë përdoruesin në sesionin e tij privat me të njëjtin përdorues në sesionin e mëparshëm publik.

Kjo tregon se dritaret e shfletimit privat në Safari fillimisht u përqendruan kryesisht në mbrojtjen kundër vëzhguesve lokalë dhe jo aq shumë në mbrojtjen e një ndjekësi të largët. Kjo diferencë në modelin e sulmit është diçka që duhet të mbahet në mend kur shikoni në mënyrën private të shfletimit. Aktualisht, siç testohet në versionin Safari në MacOS , zbatimi i modalitetit privat është i njëjtë me atë në shfletuesit e tjerë të internetit. Kur hapëm një faqe interneti që i jep një vizitori të ri një identifikues unik në një cookie dhe përdoret për të mbajtur përdorues të regjistruar, vlerat e cookie-t në një dritare të re private janë të ndryshme nga cookie-et e paracaktuar në një sesion publik dhe përdoruesi nuk ishte më të lidhur. Kjo do të thotë që cookies nuk shpërndahen më në mes sesioneve publike dhe private.

Limitimet

Dritaret e shfletimit privat nuk janë pa rreziqe të privatësisë. Ai ruan cookies dhe historinë e shfletimit në një vend të veçantë dhe i largon ato pas shfletimit, por një sulmues lokal ende mund të shohë se çfarë po ndodh në sesionin privat, pasi informacioni ende ruhet në kompjuterin e përdoruesve. Rjedhimisht, teknika të tjera të ndjekjes janë ende të përdorshme, siç janë fingerprinting i shfletuesit të uebit. Shtesat dhe shtojcat e shfletuesit mund të rrjedhin gjithashtu nga një sesion privat, i cili nuk ka për qëllim të ruhet ose të jetë i arritshëm. Për shembull, Adobe Flash Player përdorte ruajtjen në kompjuterin e përdoruesit i cili nuk u fshi pas mbylljes së një sesioni privat të shfletimit. Që nga Flash Player 10.1, kjo çështje është fikse dhe Flash Player aktualisht mbështet shfletimin privat [12]. Për Microsoft Silverlight nuk ka dëshmi se ai cenon ose ka shkelur regjimin privat të shfletimit.

3.4 Rekomandim për përdoruesit

Pra, pasi analizuam në cilësimet e shfletuesve më të njohur dhe funksionalitetet e tyre përsa I përket mbrojtjes ndaj ndjekjes , çfarë do të ishte një rekomandim i mirë për përdoruesit për të minimizuar ndjekjen ne ueb, por pa humbur përdorshmërinë?

Zgjedhja e rekomanduar për një shfletues web është Mozilla Firefox. Arsyeja për këtë zgjedhje është se është një shfletues me burim të hapur, i cili nuk është në pronësi të një pale thjesht komerciale. Google dhe Microsoft nuk janë vetëm kompani komerciale, por gjithashtu kanë dhe rrjetet e tyre të reklamimit. Cilësimet e privatësisë te Internet Explorers dukeshin premtues kur P3P ishte i ri, por shumica e cilësimeve janë të vjetruara që tani. Kjo do të thotë që cilësimi i vetem ekzistues në Internet Explorer është për të bllokuar të gjitha cookies ose për të mos bllokuar asnjë cookie. Safari është një zgjedhje e besueshme vetëmpër sistemet Mac, sepse zhvillimi i sistemeve të tjera operative është ndalur. Për Mac OS, Firefox është gjithashtu në dispozicion, që ne e rekomandojmë.

Përparësitë kryesore të Firefox-it në krye të disponueshmërisë për shumë platforma janë sasia e madhe e shtesave në dispozicion dhe konfigurabiliteti i shfletuesit.

Listimi i cilësimeve të shfletuesit është hapi tjetër. Që Mozilla Firefox të jetë sa më private, duhet të aktivizohen cilësime të caktuara.

1. Bllokimi I dritareve pop-up, për të ndaluar vendosjen e cookies të palëve të para
2. Përdorimi I mbrojtjes ndaj ndjekejes në dritare private
3. Ndryshimi nga block list në Disconnect strict list
4. Aktivizimi I Do Not Track (DNT)
5. Përdorimi I cilësimeve të personalizuara për historinë
    - 5.1 Ruaj cookies deri kur sesioni mbaron
    - 5.2 Mos prano asnjëherë cookies nga palët e treta

Organizata holandeze e të drejtave digjitale Bits Of Freedom (BOF) gjithashtu paraqet një rekomandim përdoruesit në faqen e tyre[4]. Ky rekomandim mbulon se cili shfletues web rekomandohet dhe paraqet një pasqyrë të mjeteve të mundshme të privatësisë për t'u përdorur. Megjithatë ajo nuk analizon teknikat që përdoren nga shfletuesit dhe zgjerimet e tyre.

BOF rekomandon Mozilla Firefox-in si një shfletues interneti, për shkak të përshtatshmërisë së tij dhe sepse Chrome ka disa mangësi sipas mendimit të tyre, siç është se Google nuk është i qartë në atë që përdor të dhëna të sinkronizuara nga Chrome. BOF nuk mbulon Microsoft Internet Explorer / Edge ose Safari në faqen e tyre të internetit. Nga hulumtimi ynë, mund të konkludojmë se këto shfletues web nuk funksionojnë më mirë për privatësinë kur konfigurohen saktë. Megjithatë, Safari funksionon më mirë, por që bllokon biskotat e palës së tretë në këtë parazgjedhje

[4] https://toolbox.bof.nl/playlist/prive-online/

Kapitulli 4

Konkluzione

Konkluzione në ndjekjen në web

Nga rishikimi I metodave të ndjekjes si dhe masave më të përdorshme mund tëdalim në disa konkluzione. Rizbulimi I cookies mund të arrihet nëpërmjet çdo metode ruajtje që shfletuesit dhe plugins ofrojnë. Opsionet e Do Not Track dhe P3P nuk do të funksionojnë si pasojë e e pëlqimit të kërkuar nga palët ndjekëse. Nuk ka kundërmasa ndaj fingerprinting pasiv, meqënëse ai mbështetet në informacionin që dërgohet nga një pajisje që po shfleton në web. Teknikat e ndjekjes në web dhe fingerprinting po zhvillohen shumë e më shumë dhe po arrijnë ti ndjekin përdoruesit në mënyrë më preçize. Në anën tjetër , kundërmasat janë duke u zhvilluar gjithashtu për të mbuluar të gjitha metodat e ndjekjes. Si duket loja macja me miun po vazhdon ende.

Konkluzione për shfletuesit

Kur analizon ndryshimet ndërmjet shfletuesit më të përdorshëm, bëhet më e qartë fakti se të gjithë ofrojnë cilësime të ngjashme privatësie. Nga shfletuesit e analizuar, Mozilla Firefox ofrron konfigurimin më të mire. Cilësimet e parazgjedhura gjithashtu nuk kanë ndonjë ndyshim të madh, me përjshtim të Safari, I cili bllokon cookies të pales së tretë. Kjo për mendimin tim është një parazgjedhje shumë e mirë, sepse I bllokon disa ndjekës paraprakisht. Dritaret e shfletimit privat kanë një focus tjetër krahasuar me teknikat që kanë si qëllim të përmirësojnë privatësinë. Ajo fokusohet më shumë në sulmuesit locale sesa tek ata të largët. Është e rëndësishme të kujtohet diferenca midis një sulmuesi lokal dhe një sulmuesi të largët ose vëzhguesi. Implementimi I shfletimit privat është I ngjashëm për të gjithë shfletuesit. Më pare Safari kishte një mënyrë tjetër por që shfaqi disa problem, ndaj u ndryshua në atë që është dhe tani.

Për aq sa konfigurimi I shfletuesve shkon, Mozilla Firefox dhe Google Chrome ofrojnë më shumë cilësime për privatësinë përdoruesit. Internet Explorer ka shumë nivele të privatësisë që përdoruesi mund të zgjedhë, por për sa kohë ato mbështeten vetëm në P3P për të funksionuar, atëherë nuk kanë vlerë. Një tjetër avantazh I Firefox dhe Chrome është numri I madh I shtesave që janë të disponueshme.

Reflektim

Duke u kthyer pas në proçesin e ndërtimit të kësaj teme, dal në përfundimin se fusha e ndjekjes në web është shumë e gjerë dhe e ndryshueshme gjatë gjithë kohës. Si rezultat, pothuajse çdo aspect I ndjekjes në web dhe I privatësisë mund të ishte një temë më vete. Pjesa më e vështirë e kërkimeve për mua, ishte të limitoje sferën e trajtimit për diçka interesante, por në të njëjtën kohë e përdorshme për temën.

Fillimisht u fokusova ne analizën e reklamimit online dhe rikthimit të cookies. Por nuk I vazhdova pasi më dukej sikur isha shumë e limituar në atë që doja të trajtoja. Pas disa hulumtimesh, vendosa që të fokusohesha në teknikat e ndjekjes dhe cilësimet e shfletuesve. Shumë nga studimet e tjera të bëra në këtë fushë fokusoheshin vetëm në një prej këtyre çështjeve. Prej kësaj ndonjëherë është e paqartë cilat kundërmasa ndaj ndjekjes janë implementuar dhe në përdorim në shfletuesit e web-it.

Bibliografia

[1] A. Barth. RFC 6265: Http state management mechanism. https://tools.ietf.org/html/rfc6265.

[2] A. I Ant_on, J. Brande Earp, and A. Reese. Analyzing website privacy requirements using a privacy goal taxonomy. In Requirements Engineering, 2002. Proceedings. IEEE Joint International Conference on, FAQET 23-31. IEEE, 2002.

[3] C. Soghoian. The history of the do not track header. http://paranoia.dubfire.net/2011/01/history-of-do-not-track-header.html.

[4] European Commission. Directive 2009/136/ec of the European parliament and of the council of 25 november 2009,2009. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32009L0136&from=EN.

[5] F. Roesner, T. Kohno, and D. Wetherall. Detecting and defending against third-party tracking on the web. In Proceedings of the 9th USENIX conference on Networked Systems Design and Implementation, faqja 12. USENIX Association, 2012.

[6] G. Kontaxis and M. Chew. Tracking protection in _refox for privacy and performance. arXiv preprint arXiv:1506.04104, 2015.

[7] G. A. Elie Bursztein, C. Jackson, and D. Boneh. An analysis of private browsing modes in modern browsers. In Proceedings of the 19th USENIX Security Symposium, 2010.

[8] G. Acar, C. Eubank, S. Englehardt, M. Juarez,A. Narayanan, and C. Diaz. The web never forgets: Persistent tracking mechanisms in the wild. In Proceedings of the 2014
ACM SIGSAC Conference on Computer and Communications Security, faqet 674-689. ACM, 2014.

[9] J. Reschke,R. Fielding. RFC 7230: Hypertext transfer protocol (http/1.1): Message syntax and routing. https://tools.ietf.org/html/rfc7230.

[10] J. Mayer. Web policy. safari trackers.[online] web policy blog, february 17, 2012. Available on http://webpolicy.org/2012/02/17/safari-trackers/.

[11] Ji_r__ Kysela. Comparison of web applications geolocation services. In Computational Intelligence and Informatics (CINTI), 2014 IEEE 15th International Symposium on, faqet 449-453. IEEE, 2014.

[12] J. Xu & T. Nguyen. Private browsing in ash player 10.1, Qershir 2010. http://www.adobe.com/devnet/flashplayer/articles/privacy_mode_fp10_1.html.

[13] K. Mowery and H. Shacham. Pixel perfect: Fingerprinting canvas in html5. Proceedings of W2SP, 2012.

[14] L. Faith Cranor. Internet explorer privacy protections also being circumvented by google, facebook, and many more. Techpolicy. com , 2012. Available on http://www.techpolicy.com/Cranor_InternetExplorerPrivacyProtectionsBeingCircumvented-by-Google.aspx.

[15] M. Abraham, C. Meierhoefer, and A. Lipsman. The impact of cookie deletion on the accuracy of site-server and ad-server metrics: An empirical comscore study. Retrieved October, 14:2009, 2007.

[16] PageFair. The 2015 ad blocking report. https://blog.pagefair.com/2015/ad-blocking-report/.

[17] P. Eckersley. How unique is your web browser? In International Symposium on Privacy Enhancing Technologies Symposium, faqet 1-18. Springer, 2010.

[18] P. Verleg. Cache Cookies: searching for hidden browser storage,2014. Bachelor Thesis. Radboud University Nijmegen.

[19] P. G. Leon, L. F. Cranor, A. M McDonald, and R. McGuire. Token attempt: the misrepresentation of website privacy policies through the misuse of p3p compact policy tokens. In Proceedings of the 9th annual ACM workshop on Privacy in the electronic society, faqet 93-104. ACM, 2010

[20] R. T. Fiedling and D. Singer. Tracking preference expression (DNT). https://www.w3.org/TR/tracking-dnt/.

[21] T. Bujlow, V. Carela-Espa~nol, J. Sol_e-Pareta, and P. Barlet-Ros. Web tracking: Mechanisms, implications, and defenses.arXiv preprint arXiv:1507.07872, 2015.

[22] Tai-Ching Li, Huy Hang, M. Faloutsos, and P. Efstathopoulos. Trackadvisor: Taking back browsing privacy from third-party trackers. In International Conference on Passive and Active Network Measurement, Faqet 277-289. Springer, 2015.

[23] Whatsapp sails past sms, but where does messaging go next?, 1 2015. URL http://benevans.com/benedictevans/2015/1/11/whatsapp-sails-past-sms-but-wheredoes-messaging-go-next.

ANEKSE

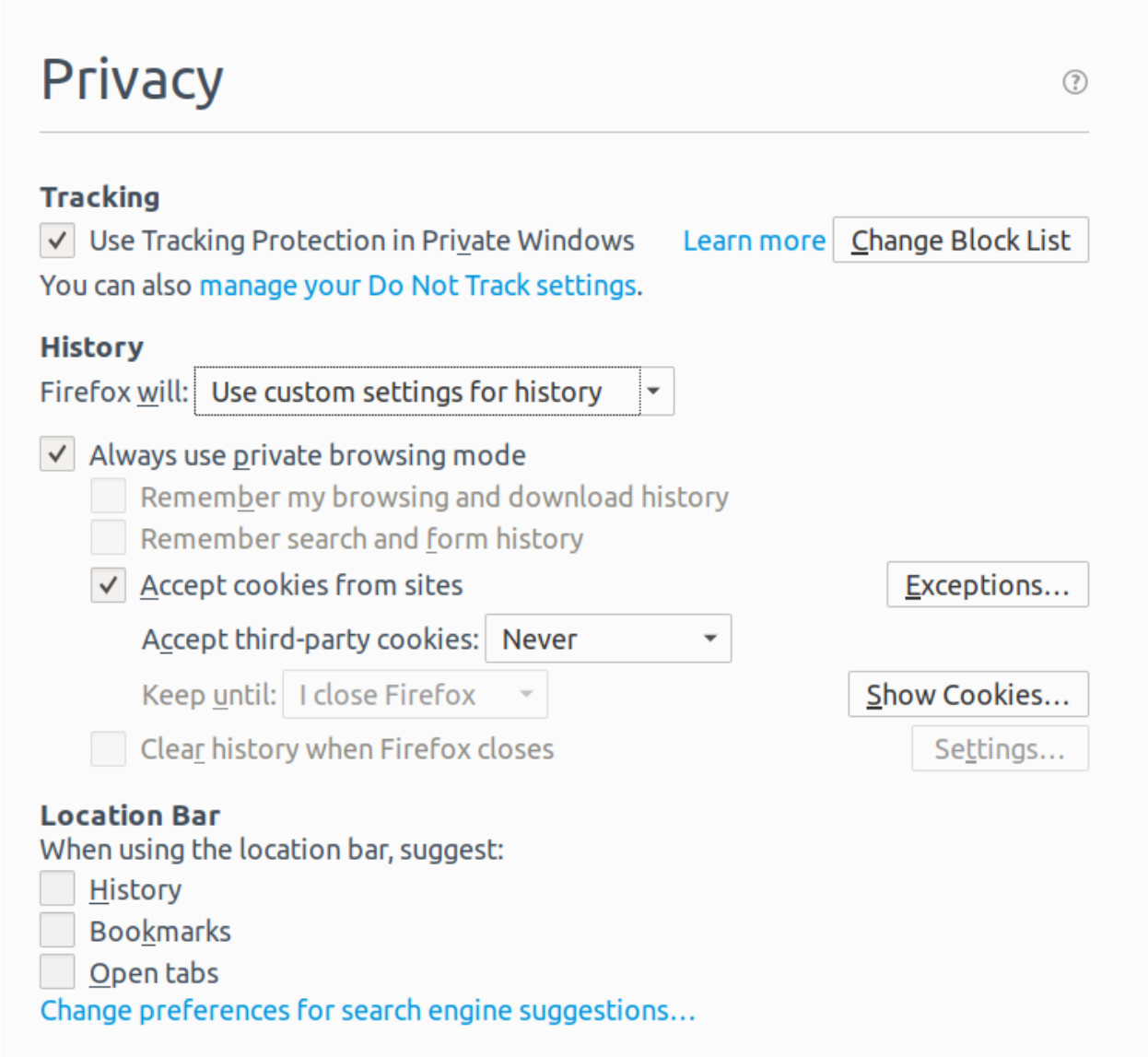

Figura 3 Cilësimet e privatësisë në Firefox

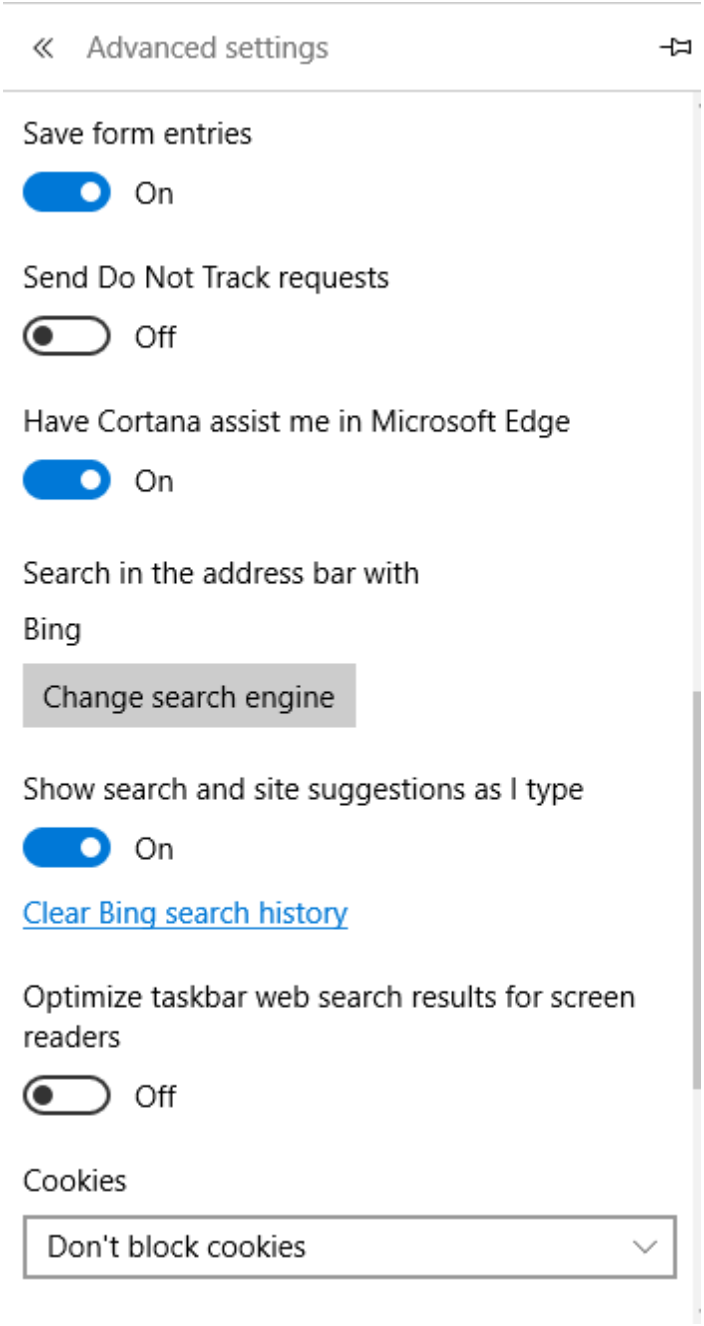

Figura 4 Cilësimet e privatësisë në Microsoft Edge

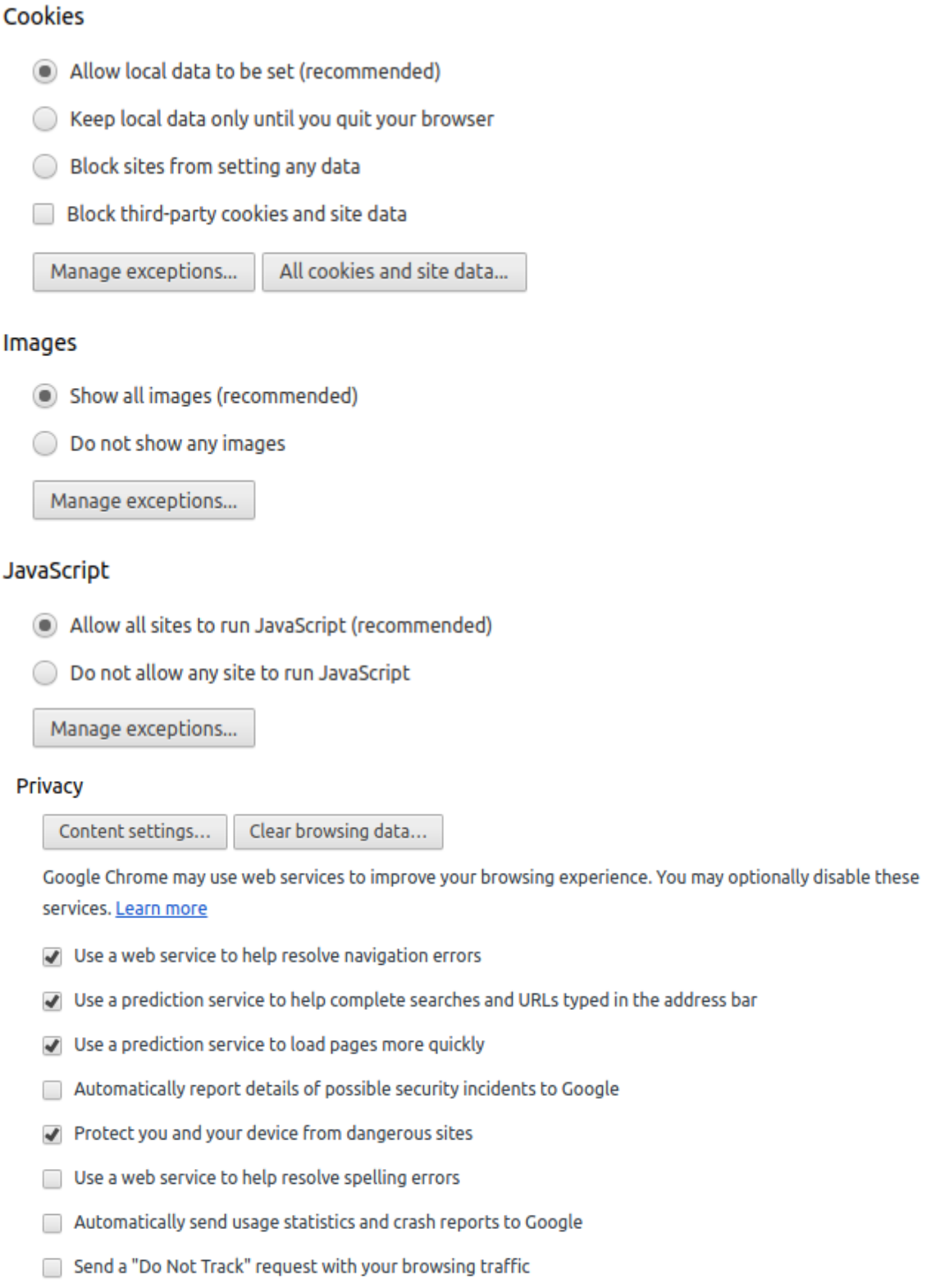

Figura 5 Cilësimet e privatësisë në Google Chrome

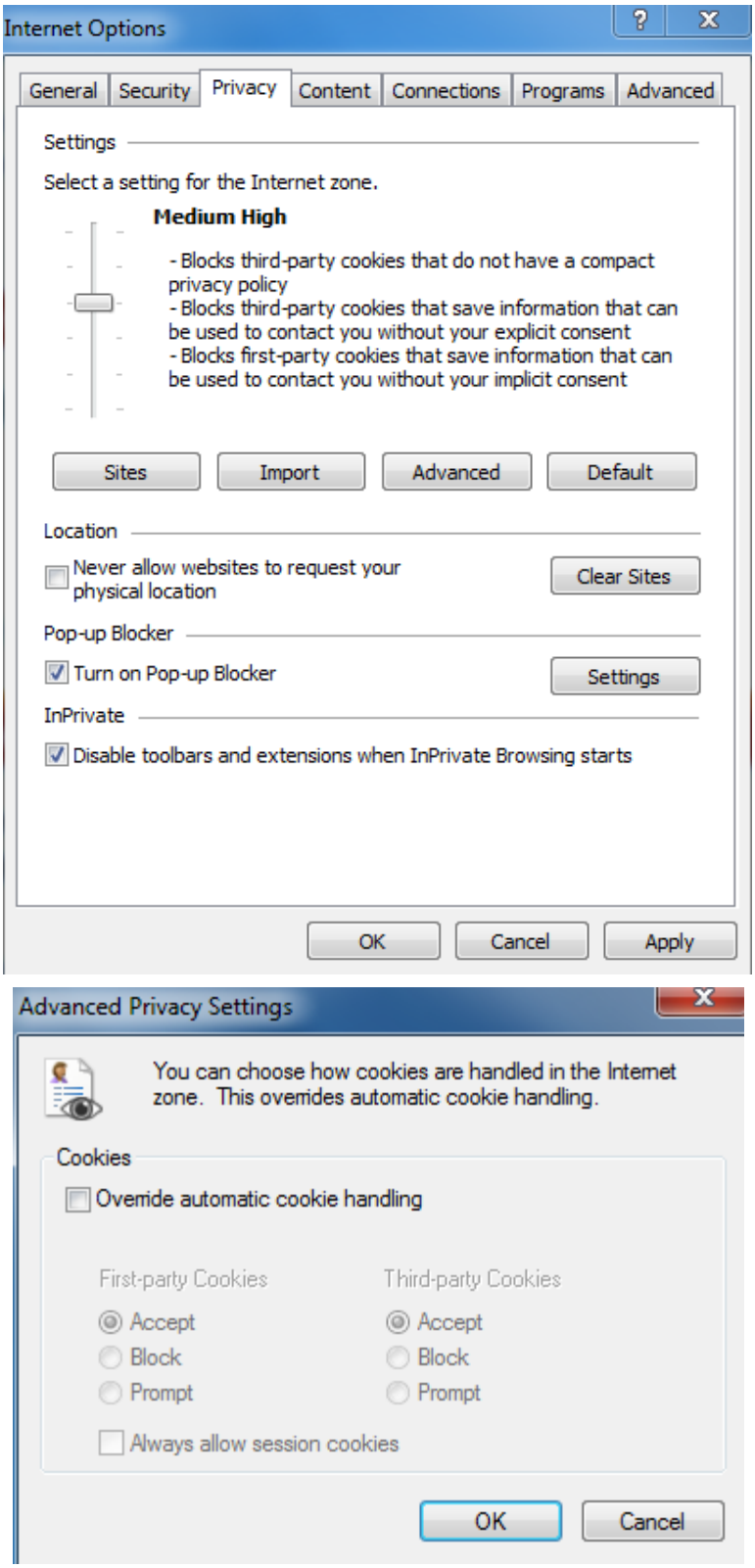

Figura 6 Cilësimet e privatësisë në Microsoft Internet Explorer

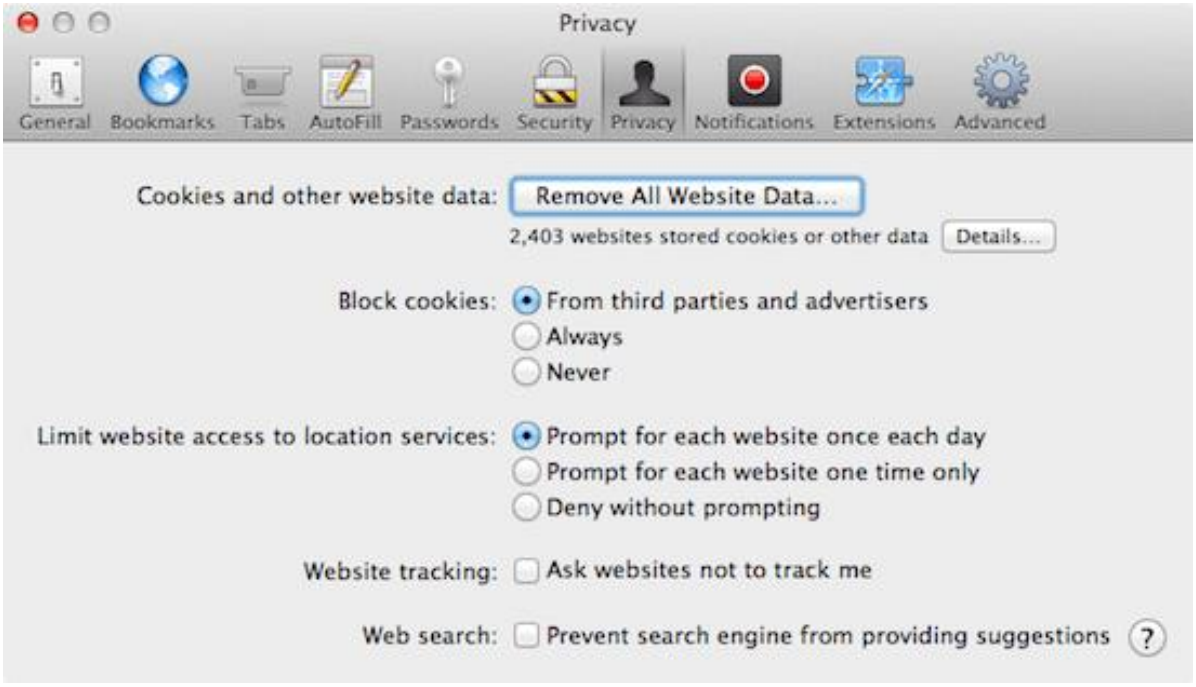

Figura 7 Cilësimet e privatësisë në Safari