
**VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ**
**BRNO UNIVERSITY OF TECHNOLOGY**

**FAKULTA INFORMAČNÍCH TECHNOLOGIÍ**
**FACULTY OF INFORMATION TECHNOLOGY**

**ÚSTAV INFORMAČNÍCH SYSTÉMŮ**
**DEPARTMENT OF INFORMATION SYSTEMS**


# POROVNÁNÍ WEBOVÝCH ROZŠÍŘENÍ ZAMĚŘENÝCH NA BEZPEČNOST A SOUKROMÍ

**COMPARISON OF SECURITY AND PRIVACY WEB EXTENSIONS**

**BAKALÁŘSKÁ PRÁCE**
**BACHELOR'S THESIS**


**AUTOR PRÁCE** — **JANA PETRÁŇOVÁ**
**AUTHOR**

**VEDOUCÍ PRÁCE** — **Ing. LIBOR POLČÁK, Ph.D.**
**SUPERVISOR**



**BRNO 2020**

**Vysoké učení technické v Brně**
Fakulta informačních technologií

Ústav informačních systémů (UIFS) Akademický rok 2020/2021

# Zadání bakalářské práce


Studentka: **Petráňová Jana**
Program: Informační technologie
Název: **Porovnání webových rozšíření zaměřených na bezpečnost a soukromí**
**Comparison of Security and Privacy Web Extensions**
Kategorie: Web

Zadání:

1. Nastudujte a popište dostupné seznamy sledovacích prvků jako je EasyList a EasyPrivacy.
2. Vyhledejte rozšíření zaměřené na bezpečnost a ochranu soukromí (např. uMatrix, uBlock Origin, PrivacyBadger, JavaScript Restrictor, Web API Manager, NoScript, DuckDuckGo Privacy Essentials, First Party Isolation). Popište rizika, před kterými rozšíření chrání.
3. Navrhněte testovací prostředí demonstrující možnosti jednotlivých rozšíření. Zaměřte se na to, jak se jednotlivá rozšíření doplňují a v čem se překrývají.
4. Testovací prostředí implementujte.
5. Otestujte jednotlivá rozšíření. Ohodnoťte uživatelskou přívětivost v přizpůsobování jednotlivých rozšíření.
6. Vyhodnoťte výsledky práce.

Literatura:

- G. Merzdovnik, aj.. Block Me If You Can: A Large-Scale Study of Tracker-Blocking Tools, 2017 IEEE European Symposium on Security and Privacy (EuroS&P), Paris, 2017, str. 319-333.
- Imane Fouad, aj. Missed by Filter Lists: Detecting Unknown Third-Party Trackers with Invisible Pixels. PETS 2020 - 20th Privacy Enhancing Technologies Symposium, 2020, Montréal, Canada.
- Gunes Acar, aj. No boundaries: data exfiltration by third parties embedded on web pages. PETS2020 - 20th Privacy Enhancing Technologies Symposium, 2020, Montréal, Canada.
- Arunesh Mathur, aj. Characterizing the Use of Browser-Based Blocking Extensions To Prevent Online Tracking. USENIX Symposium on Usable Privacy and Security (SOUPS). 2018, Baltimore, MD, USA.

Pro udělení zápočtu za první semestr je požadováno:

- Body 1 až 3 zadání.

Podrobné závazné pokyny pro vypracování práce viz https://www.fit.vut.cz/study/theses/

Vedoucí práce: **Polčák Libor, Ing., Ph.D.**
Vedoucí ústavu: Kolář Dušan, doc. Dr. Ing.
Datum zadání: 1. listopadu 2020
Datum odevzdání: 12. května 2021
Datum schválení: 26. října 2020

# Abstrakt

Tato práce se zabývá představením a porovnáním dostupných seznamů sledovacích prvků a webových rozšíření zaměřených na bezpečnost. Dále pojednává o nebezpečí, kterému je uživatel každodenním prohlížením internetu vystaven a před kterým jej rozšíření chrání. Součástí práce je návrh a implementace testovacího prostředí zaměřeného na porovnání služeb poskytnutých rozšířením. Cílem práce je porovnat na trhu dostupná rozšíření se zaměřením na bezpečnost a soukromí, nastínit všednímu uživateli rizika související s pohybem po internetu a doporučit mu konkrétní rozšíření v závislosti na jeho potřebách.



# Abstract

This work concerns the introduction and comparison of available filter lists and security and privacy web extensions. Furthermore, it describes the dangers the user is facing while browsing the internet and outlines the risks said web extensions are meant to protect the user from. This work involves the design and implementation of a testing environment created with the purpose of comparing said web extensions. The aim of this work is to compare security and privacy web extensions currently available on the market and to to shed light on the risks of internet browsing to an everyday user with the intend to recommend optimal web extensions based on their needs.



# Klíčová slova

Webová rozšíření, internet, bezpečnost, soukromí, sledující prvky stránek, cookies, osobní údaje

# Keywords

Web extensions, internet, security, privacy, trackers, cookies, personal data



# Citace

PETRÁŇOVÁ, Jana. *Porovnání webových rozšíření zaměřených na bezpečnost a soukromí.* Brno, 2020. Bakalářská práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Ing. Libor Polčák, Ph.D.

# Porovnání webových rozšíření zaměřených na bezpečnost a soukromí

## Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracovala samostatně pod vedením pana Ing. Libora Polčáka, Ph.D. Uvedla jsem všechny literární prameny, publikace a další zdroje, ze kterých jsem čerpala.

.....
Jana Petráňová
8. května 2021


## Poděkování

Ráda bych poděkovala panu Ing. Liboru Polčákovi, Ph.D. za cenné rady, věcné připomínky a vstřícnost při konzultacích a vypracování bakalářské práce.

# Obsah

# Kapitola 1

# Úvod

Internet se stal zásadní součástí lidského života. Každý jeho uživatel se však je jeho používáním vystavuje bezpečnostnímu riziku. Samotným použitím internetu po sobě zanechává elektronickou stopu, která umožňuje obchodníkům s informacemi profilovat uživatele do absurdních detailů. Z nesčetně podobných společností obchodujících s informacemi lze zmínit například americkou firmu *Acxiom* [2], která profiluje a sbírá informace o amerických občanech. Významné množství dat pochází z jejich pohybu po internetu a z interakce s webovými stránkami, které navštěvují. Společnost sbírá, spojuje a analyzuje data získaná monitorováním uživatelovy aktivity a vytváří tak osobní profily obsahující informace jako jejich rasu, pohlaví, telefonní čísla, jaká auta vlastní, stupeň dosaženého vzdělání, velikost jejich domů, věk, váhu politické názory, zdravotní stav, zaměstnání, nebo co si v poslední době na internetu koupili [27].

Cílem je poskytnout potenciálním zákazníkům – marketingovým společnostem – co nejpřesnější uživatelský profil. Ten je využit pro nabízení reklamy cílené na konkrétního uživatele při jeho každodenním prohlížení internetu. Například uživatel, který je ve svém profilu označen jako křesťan, může při prohlížení internetu vídat reklamy vybízející k nákupu Bible. Uživatel, který nedávno zadal do vyhledávače slovní spojení „sportovní boty“ a navštívil internetový obchod nabízející podobný sortiment, pravděpodobně v blízké budoucnosti naráží na reklamy internetových obchodů se sportovními doplňky. Dojde-li k využití profilu uživatele pro zacílení reklamy, jedná se o tzv. *behaviorální reklamu*. Čím přesnější profil je, tím cennějším se stává. Vhodně cílená reklama vytvořená na základě přesného uživatelského profilu přímo vede ke zvýšení výdělku až o 30% [13].

Třetí strany představují složku internetové komunikace, která je uživateli skrytá a jejichž existence je často pro většinového uživatele často neodhalitelná. Jejich motivací bývá potenciální výdělek, jako v případě situace popsané výše. Existují ale případy, ve kterých jsou motivace třetích stran zákeřné a mohou ohrozit bezpečí uživatele. Například senioři používající internet mohou být na základě informací shromažďovaných třetími stranami často obětí virtuálního podvodu a vydírání [23].

V EU jsou z pohledu regulace významné především dvě zákonné normy [12]. (1) Směrnice 2002/58/ES (obvykle označovaná jako *ePrivacy*) reguluje důvěrnost komunikace a v novele z roku 2009 vyžaduje souhlas uživatele s jakýmikoliv zásahy do jeho zařízení, pokud nejsou nezbytně nutné pro poskytnutí vyžádané služby. Tato směrnice je v českém právním řádu implementovaná v zákoně 127/2005 Sb. a zákon v době odevzdání práce nebyl novelizován. I tak však vyžaduje, aby měl uživatel možnost podání námitky proti zásahům do koncového zařízení, které nejsou nezbytné. (2) Nařízení EU 2016/679 (obvykle označovaná jako *GDPR*) pojednává o soukromí uživatelů. Definuje role aktérů nejen v on-line

prostředí, jako je správce a zpracovatel. Dále klade požadavky na zpracování osobních údajů, mj. na provádění testů proporcionality mezi oprávněnými zájmy správce pro marketingové účely a oprávněnými zájmy uživatelů (subjekt údajů) na zachování soukromí.

Cílem této práce je nezkušenému uživateli nastínit rizika, kterým je prohlížením vystaven 3 a nabídnout řešení ve formě instalace rozšíření zaměřených na bezpečnost a soukromí. Možnost výběru rozšíření je široká a mnoho z nich se ve své funkcionalitě překrývá. Teoretická část práce volně řadí testovaná rozšíření do kategorií podle principu, na kterém fungují a funkcionality, kterou nabízí 2. Následně uvádí základní informace o testovaných rozšířeních a navrhuje vhodný způsob, jakým lze testovat jejich individuální efektivitu v závislosti na přiřazené skupině 4. Praktická část implementuje návrh popsaný v teoretické části 5. Mimo jiné jsou pomocí nástroje *OpenWPM* [25] provedeny automatizované průchody internetových stránek. Výsledné databáze jsou podrobeny analýze, jejíž výsledky jsou zpracovány do přehledných grafů a tabulek. Výsledkem práce je doporučení konkrétních rozšíření v závislosti na potřebách uživatele.

# Kapitola 2

# Webová rozšíření zaměřená na bezpečnost a ochranu soukromí

Jako řešení problémů nastíněných v úvodu této práce se nabízí webová rozšíření, která pohyb po webu učiní pohodlnějším a bezpečnějším. Jejich efektivita spočívá v prevenci zneužití informací o uživateli blokováním obsahu třetích stran webu. Bezpečnostní rozšíření dostupná na trhu lze volně kategorizovat v závislosti na ochraně, kterou nabízí.

Většina rozšíření zaměřujících se na blokování reklam funguje na principu využití seznamů blokovacích prvků. Blokováním reklam tato rozšíření prohlížení webu zpříjemní a zpřehlední a často společně s reklamou zabrání i jiným potenciálním hrozbám při prohlížení. Populární rozšíření tohoto typu, jako třeba *AdBlock Plus* nebo *uBlock Origin* se ale nesoustředí na blokování dalšího potenciálně nebezpečného obsahu třetích stran. Profilování uživatele při prohlížení tedy stále v určité míře probíhá, rozšíření pouze zabrání prohlížeči reklamu na straně uživatele zobrazit. Mimo ochranu dat a soukromí často nabízí tato rozšíření i značné vylepšení výkonu na straně uživatele. To vyplývá z podstaty rozšíření, tedy z redukce oboustranného internetového provozu. Zvyšují rychlost načítání webových stránek a snižují využití šířky pásma až o 30% [33].

Existují proto i rozšíření zaměřená na blokování sledovacích prvků využívaných pro profilování uživatele. Sledovací prvky se na internetu vyskytují nejčastěji ve formě nevyžádaných skriptů. Jejich volání může být vedlejším efektem při využití webového API, které navštěvovaná stránka využívá. Z toho vyplývá, že čím populárnější je služba API skrze internet, tím větší potenciál má její provozovatel uživatele sledovat. Příkladem může být společnost *Google*, která provozuje nejen stejnojmenný vyhledávač, ale i jednu z nejnavštěvovanějších stránek internetu, *YouTube*. Rozšíření se zaměřují na rozeznání potenciálních hrozeb analýzou internetového provozu a jejich následné omezení.

Alternativním způsobem zamezení nasazení sledovacích prvků je omezení spustitelného obsahu, který navštívené stránky implementují. Rozšíření mohou zakázat volání všech, nebo některých metod skriptů. Taková ochrana před sledováním je nejefektivnější. Problém nastane v momentě, kdy zákaz potenciálně nebezpečného volání navštívenou stránku „rozbije“ – kriticky omezí její základní funkcionalitu. Uživatel je tedy před profilováním chráněn, návštěva stránky se ale stane nesmyslnou.

V otázce udržení integrity dat zasílaných po internetu a znemožnění jejich odposlechu při pohybu transportní vrstvou lze využít rozšíření pro docílení šifrovaného spojení HTTPS při komunikaci s navštívenou stránkou. Tento typ komunikace však nejde vždy realizovat, uživatel by měl tedy navštěvovat pouze stránky, kterým důvěřuje.

## 2.1 Seznamy sledovacích prvků

Mnoho bezpečnostních internetových rozšíření obsahuje seznam pravidel blokování nevyžádaného obsahu. Takový obsah je automaticky odstraněn. Tyto seznamy jsou vytvořeny a udržovány za účelem ochrany uživatele nejen před reklamami, ale také škodlivým malware softwarem, pop-upy, trackery, nevyžádanými vyskakujícími formuláři a dalším. Jsou tvořeny jednotlivci, nebo malými skupinami. Nejedná se tedy o výsledek automatizovaného procesu. Tvorba a údržba seznamů úzce závisí na spolupráci komunity. Kterýkoli uživatel internetu má možnost vývojáře seznamů kontaktovat a přispět tak k jejich rozvoji. Seznamy jsou využity v bezpečnostních webových rozšířeních, prohlížeče samotné jejich využití bez rozšíření nepodporují.

Bezpečnostní webová rozšíření typu 2.2 pracují jako překladač syntaxe seznamů. Filtrování se projeví v momentě, kdy prohlížeč zašle HTTP požadavek na server. Většina nevyžádaného obsahu se nachází na odlišném serveru, než který uživatel právě navštěvuje. Pokud zašle prohlížeč požadavek na nevyžádanou doménu, je rozšířením prozkoumán a porovnán s dostupnými filtry v seznamech sledovacích prvků. Jedná-li se o nevyžádaný požadavek na získání obsahu nabízeného třetí stranou, pak je odfiltrován. Prohlížeč získává odpověď pouze na vyhovující požadavky. Mimo jiné se blokování požadavku pozitivně projevuje i na rychlosti načítání stránky.

Další případ využití seznamu je filtrování obsahu, který se nachází přímo na navštěvované stránce. Při načtení každé webové stránky vytvoří prohlížeč její *Document Object Model (DOM)*. HTML DOM má stromovou strukturu, jeho větvím odpovídají elementy stránky. Webové rozšíření větve prochází a pomocí CSS filtru maže nevyžádaný obsah. Ve výsledku se ideálně v prohlížeči uživatele zobrazí stránka bez nevyžádaného obsahu.

### Syntaxe filtrovacích pravidel

Syntaxe filtrovacích pravidel záleží na typu obsahu, který má být blokován, a na rozšíření, který tento filtr interpretuje. Při tvorbě filtru lze využít:

- jednoduchých blokovacích pravidel.
- výjimek v blokování.
- filtrů aplikovaných na pravidlo.
- pravidel blokujících elementy stránky.
- CSS selektorů.

Jednoduchá blokovací pravidla se vztahují převážně na filtraci URL adres. Lze blokovat části adres, nebo celé domény. K filtraci se využívají následující znaky [3]:

- ***** značící libovolný počet libovolných znaků.
- ^ značící konec adresy, nebo separátor (např. **?**, **/**).
- || značící doménovou adresu.
- | značící začátek konkrétní adresy, musí být ukončena |.

Blokování obsahu může mít negativní vliv na koncového uživatele. Některá pravidla musí být za účelem efektivity velice robustní, mohou tedy skrýt i uživatelem žádaný obsah. Z tohoto důvodu jsou v seznamech implementovány výjimky v blokování. Začátek výjimky značí klíčové znaky `@@`.

### EasyList a EasyPrivacy

Oba tyto seznamy jsou dílem skupiny jednotlivců a jsou licencované pod *GPLv3*[1]. Původně se jednalo o projekt vytvořený výhradně pro rozšíření AdBlock, nyní se seznamy nachází i v dalších webových rozšířeních, jako třeba AdBlock Plus, nebo uBlock Origin.

Při porovnání obou seznamů je na první pohled znatelný jejich individuální účel. V případě EasyList se ve velké míře objevují klíčová slova jako *ad*, *advertisement*, nebo *banner*. V seznamu EasyPrivacy se zase hojně vyskytují slova jako *track/tracking*, *js*, *script* a *analytics*.

**EasyList** je nejrozšířenější filtrovací seznam vůbec. Vyvíjen je už od roku 2005 a je neustále aktualizován. Celý seznam je dostupný na oficiálních stránkách EasyList[2]. Nejnovější verze je dedikována rozšíření Ad Block Plus 2.0. V současné době je aktualizován každé čtyři dny. Obsahuje tisíce filtrovacích pravidel. EasyList odstraňuje většinu reklam, včetně obrázků a objektů.

Seznam **EasyPrivacy** je zaměřený na kompletní odfiltrování sledovacích prvků z internetu. Filtruje sledovací skripty, webové majáky a sběr informací o návštěvníkovi stránky. Efektivně tím chrání osobní údaje uživatelů internetu. EasyPrivacy je ve vývoji od roku 2006 a je stejně jako EasyList je aktualizován každé čtyři dny. Obsahuje více záznamů, než jeho protějšek.

### Jazykové varianty seznamů

Předchozí zmíněné seznamy jsou sepsány v celosvětovém měřítku. Jelikož je tvorba a údržba seznamu sledovacích prvků neautomatizovatelná, bylo by velice obtížné zahrnout pravidla pro všechny specifické země světa. Dobrovolníci z konkrétních oblastí místo toho vytváří jazykové alternativy seznamů blokovacích prvků. Konkrétně pro Českou a Slovenskou republiku se jedná o seznam *EasyList Czech and Slovak*[3] od tvůrce *Tomáše Tara*, který se podílel na vývoji rozšíření AdBlock. Oproti EasyList je seznam značně kratší. Soustředí se pouze na generická filtrová pravidla a pravidla nad českými a slovenskými doménami jako jsou *super.cz*, nebo *serialzone.cz*.

### Oisd domain blocklist

Skupina seznamů blokovacích prvků vytvořena úpravou a spojením již existujících seznamů[4] obsahující pouze jména blokovaných domén. Autor projektu vystupuje pod přezdívkou *sjhgvr*. Celkem šest různých seznamů obsahuje záznamy z více než 600 různých již existujících zdrojů. Každý je dostupný v *normal* a *light* verzi. Mezi těmito verzemi je enormní rozdíl znatelný již podle velikosti souboru, ve kterém je seznam obsažen. Například *normal* verze seznamu *Adblocker-syntax domains* je o 354041 záznamů delší, než jeho *light* verze. Seznamy jsou aktualizovány každý den. Dá se tedy říci, že se jedná o nejaktuálnější skupinu seznamů vůbec.

[1] Dostupné z: https://www.gnu.org/licenses/gpl-3.0.html
[2] https://easylist.to/
[3] https://github.com/tomasko126/easylistczechandslovak
[4] https://oisd.nl/

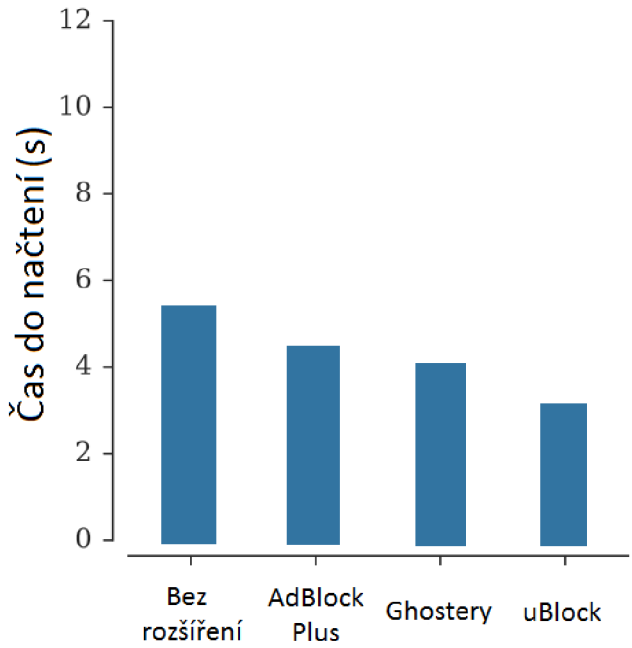
## 2.2 Existující webová rozšíření

Uživatelé mají na výběr z mnoha webových rozšíření pro jejich zvolený prohlížeč. Tato práce se zaměřuje na rozšíření dostupná pro prohlížeč *Mozilla Firefox*, která jsou ke stažení ze stránky *Firefox Browser Add-ons* v kategorii *Privacy and security* [8]. Výběr rozšíření z uvedeného zdroje byl zvolen po konzultaci s vedoucím práce. Prohlížeč *Mozilla Firefox* je jedním z nejpopulárnějších dostupných prohlížečů a na rozdíl od dalšího populárního prohlížeče *Google Chrome* obsahuje na stránkách nabízející rozšíření vhodnou kategorii k testování. Rozšíření byla vybrána v závislosti na počtu jejich stažení. Mnoho oblíbených rozšíření se často ve své funkcionalitě překrývá. Pro účel této práce byla rozšíření začleněna do čtyř různých skupin podle jejich funkčnosti nabízené uživateli bez jakéhokoliv dalšího nastavení.

### Rozšíření na bázi seznamu sledovacích prvků

V kapitole 2.1 již byl popsán princip seznamu sledovacích prvků jako takových. Tato kategorie webových rozšíření ve své základní formě pracuje téměř výhradně na bázi filtrace pomocí přednastavených seznamů. Uživateli je většinou umožněno množství seznamů rozšířit, nebo naopak zúžit.

Hlavními body, ve kterých se rozšíření této skupiny liší, jsou využité seznamy blokovacích prvků a algoritmy, které tyto seznamy implementují. Právě u použitých algoritmů lze nejlépe porovnat jejich zátěž na CPU a to, v jaké míře jejich implementace zpomaluje, nebo naopak zrychluje načítání stránek.

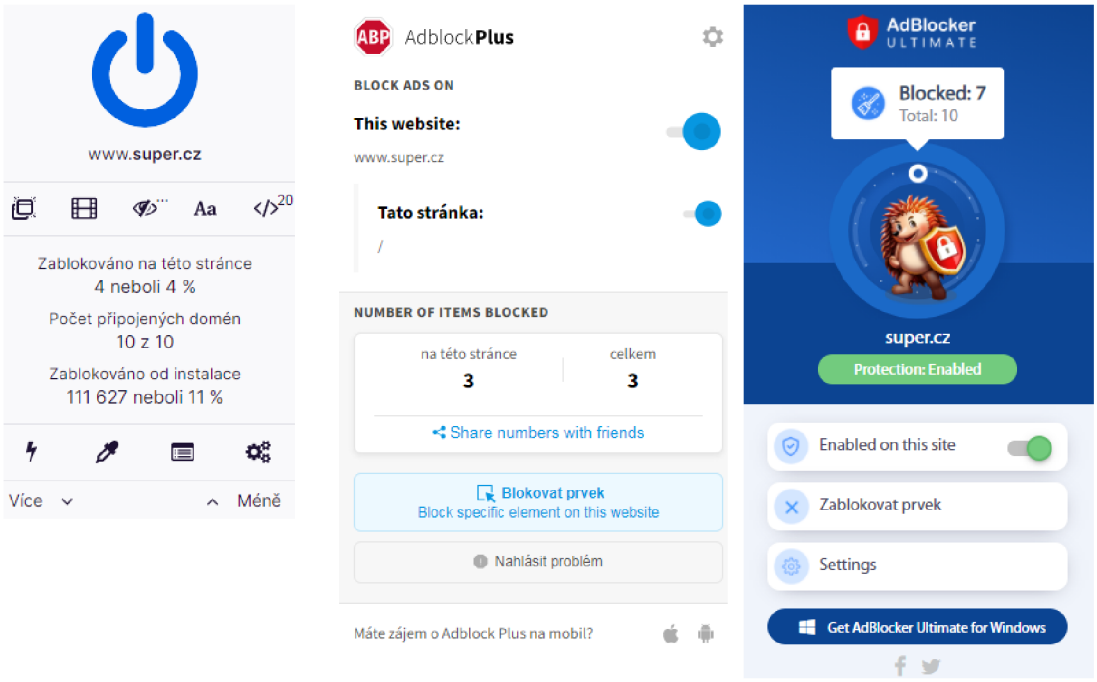



Obrázek 2.1: Graf znázorňující dopad použití rozšíření na čas potřebný k načtení internetové stránky. Převzato a upraveno z [33].

Z obrázku 2.1 lze soudit, že využití zobrazených rozšíření uživateli zpříjemní pohyb po internetu. Díky snížení počtu HTTP požadavků a odpovědí, kterým musí prohlížeč vyhovět, se stává prohlížení rychlejší. Míra zrychlení závisí na konkrétním nainstalovaném rozšíření.

Využití dvou takových rozšíření najednou ale může vést k opačného účinku. Čas potřebný k běhu filtračního algoritmu se totiž zdvojnásobí a negativně ovlivní dopad na CPU. Dále je pravdou, že mnoho rozšíření této kategorie využívá v základu stejné seznamy blokovacích prvků, při načtení stránky jsou tedy ta samá pravidla zbytečně procházena vícekrát.

Rozšíření v této kategorii se překrývají nejen ve funkcionalitě, ale také v celkovém vzhledu jejich GUI. Uživateli často podávají informace o počtu zablokovaných domén, které se vyskytují na navštívené stránce a celkovém počtu zablokovaných domén od instalace rozšíření (viz. obrázek 2.2). Všechna rozšíření této kategorie jsou velmi jednoduše konfigurovatelná a obsahují přehledné, dobře barevně rozlišené menu.




Obrázek 2.2: Obrázek znázorňující GUI rozšíření *uBlock Origin*, *Adblock Plus* a *Adblocker Ultimate* na stránce `https://www.super.cz/`.

Prvním a tedy nejstahovanějším rozšířením této kategorie je **Adblock Plus**[5]. Je open source, multiplatformní a pochází z rukou vývojářů *Henrika Aasteda Sorensena*, *Michaela McDonalda* a *Wladimira Palanta*. Zároveň se jedná o nejkontroverznější rozšíření této kategorie. Od roku 2011 totiž implementuje seznamy tzv. *Acceptable Ads*, což jsou seznamy rozšířením povolených reklam. Rozšíření, jehož principem je reklamy blokovat, v důsledku reklamy prodává. *Adblock Plus* obdrží *6%* z celkového výdělku z neblokovaných reklam [4]. List *Acceptable Ads* je možné v nastavení kdykoliv vypnout, je však součástí výchozí verze rozšíření [1]. Pravděpodobně z tohoto důvodu není *Adblock Plus* označen jako *doporučené* rozšíření v kategorii *Privacy and security* [8].

Druhým nejpopulárnějším rozšířením je **uBlock Origin**[6]. Jedná se o open source projekt vývojáře *Raymonda Hilla* ve vývoji od roku 2007. Je dostupné pro velké množství prohlížečů a blokuje nejen reklamy, ale i trackery a malware.

[5] `https://adblockplus.org/`
[6] `https://ublockorigin.com/`

**AdBlocker Ultimate**[7] je open source rozšíření vyvíjené společností *AdAvoid Ltd*, jeho první verze byla přidána na stránky *Firefox Browser Add-ons* v roce 2016. Rozšíření je multiplatformní a dostupné pro širokou řadu internetových prohlížečů. Za měsíční poplatek je možné stáhnout také aplikaci pro desktop. Jako jeho předchůdci je open source a uživatelům dává možnost přispět jeho vývoji. Využívá vlastní implementované seznamy blokovacích prvků.

**Ghostery**[8] bylo založeno roku 2009 *Davidem Cancelem* a dnes se na jeho vývoji aktivně podílí již dvaceti sedmi členný tým. Samotné rozšíření je open source a zdarma, uživatelé si ale mohou dokoupit měsíčně placenou aplikaci pro desktop včetně balíčku obsahujícího vlastí VPN.

Posledním rozšířením je další open source projekt – **AdGuard AdBlocker**[9]. Je vyvíjeno od roku 2009 společností *AdGuard Software Ltd.*. V základní verzi zdarma nabízí blokování reklam v prohlížeči, uživatel má možnost si za měsíční poplatek přikoupit multiplatformní verzi na desktop a mobil, nebo vlastní VPN. Od podobných rozšíření v této kategorii jej liší funkcionalita, která neblokuje reklamy propagující stránku samotnou a výsledky hledání zboží z vyhledávačů, jako je například *Google*, nebo *Yahoo* [16].

Zmíněná rozšíření se překrývají v mnohých funkcionalitách a využívají stejné seznamy sledovacích prvků. V tabulce níže jsou znázorněny relevantní faktory pro jejich porovnání.

| | Seznamy | Blokuje | Počet stažení | Hodnocení |
|---|---|---|---|---|
| Adblock Plus | ABP filters<br>EasyList<br>Nonintrusive advertising | reklamy | 6 637 945 | 4.5 |
| uBlock Origin | uBlock filters<br>EasyList<br>EasyPrivacy | reklamy<br>trackery<br>malware | 5 138 805 | 4.8 |
| AdBlocker Ultimate | Ultimate Ad Filter<br>Ultimate Privacy Filter<br>Ultimate Security Filter | reklamy<br>trackery<br>malware | 1 407 697 | 4.8 |
| Ghostery | Ghostery Advertising<br>Ghostery Tracking | reklamy<br>trackery<br>malware | 1 227 702 | 4.3 |
| AdGuard Adblocker | AdGuard base filter<br>Search ads, self promotion | reklamy | 511 606 | 4.7 |

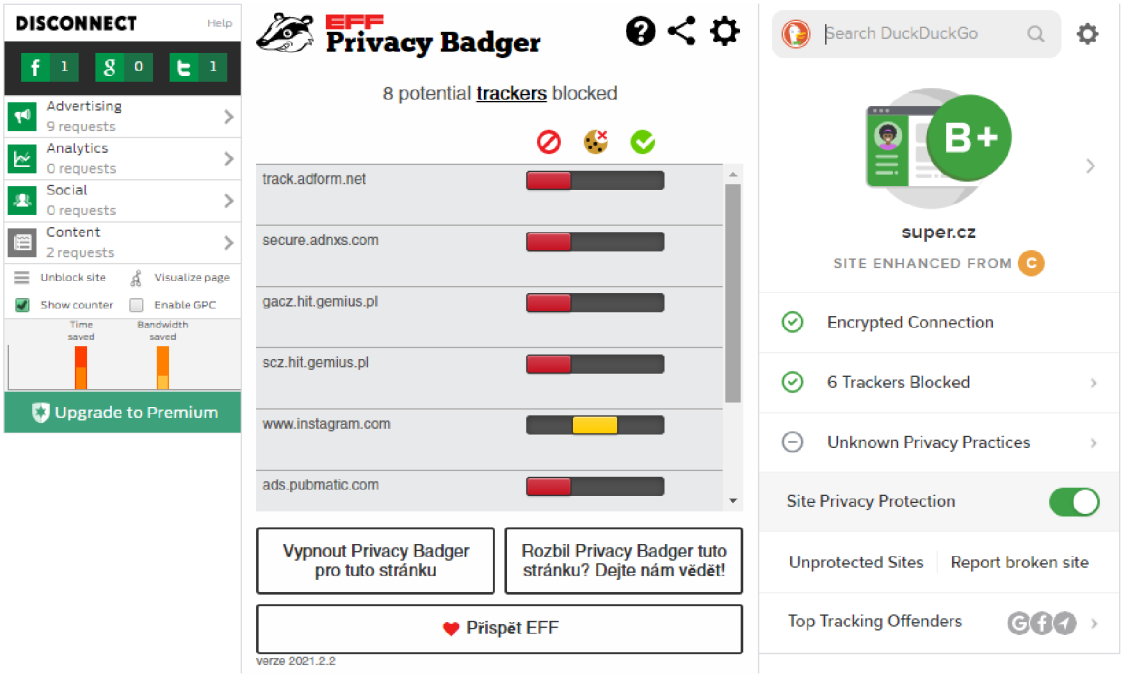
Tabulka 2.1: Tabulka shrnující relevantní vlastnosti porovnávaných rozšíření na bázi seznamu sledovacích prvků, počet jejich stažení a jejich hodnocení na stránce https://addons.mozilla.org/en-US/firefox/extensions/category/privacy-security/

Tabulka 2.1 zahrnuje verzi rozšíření ihned po jeho instalaci bez dalšího zásahu uživatele. Zobrazuje seznamy blokovacích prvků aktivované ihned po instalaci. Už ze jmen seznamů můžeme vidět, jakou funkcionalitu rozšíření nabízí.

[7] https://adblockultimate.net/
[8] https://www.ghostery.com/
[9] https://adguard.com/cs/welcome.html

### Rozšíření blokující sledovací prvky

Na rozdíl od předchozí skupiny implementují tato rozšíření opatření bez využití seznamů sledovacích prvků, zároveň se soustředí výhradně na blokování, nebo zmatení trackerů po internetu. Některá rozšíření této kategorie nabízí i další výhodné funkce. Obrázek 2.3 znázorňuje příklad vzhledu GUI rozšíření této kategorie. Uživatelské rozhraní těchto rozšíření je barevně rozlišeno a lehce čitelné. Zároveň nabízí ve vlastním menu možnost jednoduché konfigurace. V porovnání s rozšířeními předchozí kategorie podporuje ale méně možností nastavení v menu.




Obrázek 2.3: Obrázek znázorňující GUI rozšíření *Disconnect*, *Privacy Badger* a *DuckDuckGo Privacy Essencials* na stránce https://www.super.cz/.

Rozšíření **DuckDuckGo Privacy Essentials**[10] od vývojářů *DuckDuckGo* je ve vývoji od roku 2008 a přímo navazuje na jejich původní projekt, internetový vyhledávač *DuckDuckGo Search Engine*. Kromě již zmíněného vyhledávače rozšíření nutí stránku komunikovat šifrovaným spojením HTTPS (více v kategorii Docílení šifrovaného spojení). Dále rozpoznává *privacy practices* [11] stránek, čímž uživateli usnadní rozlišit stránky, které mohou potenciálně omezit jeho soukromí. Největší přínos rozšíření však spočívá v implementaci *Global Privacy Control* [9]. *DuckDuckGo Privacy Essentials* automaticky zasílá *Global Privacy Control* signál navštěvovaným stránkám, čímž oznamuje uživatelovi preference neprodávat jeho osobní data a omezit sdílení jeho osobních dat s jinými společnostmi [7].

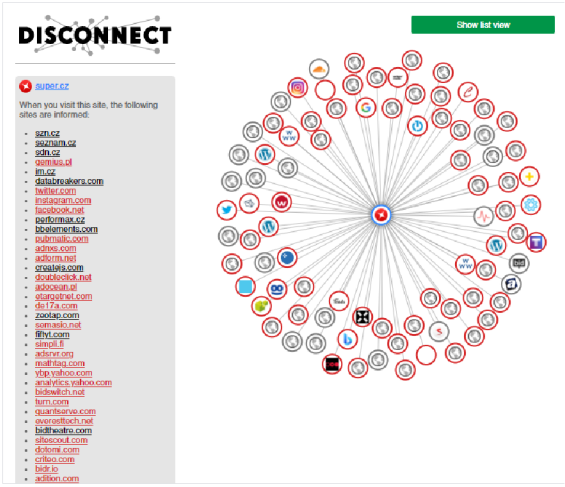
**Privacy Badger**[11] je webové rozšíření ve vývoji od roku 2014 neziskovou organizací *Electronic Frontier Foundation* zaměřující se na internetovou ochranu soukromí a legislativu. Fungoval na principu odhalení neviditelných trackerů třetích stran. Pokud objevil existenci nežádoucího sledování uživatele, vyslal původcům trackeru *Do Not Track* signál. Nepřestali-li uživatele sledovat, zablokoval je *Privacy Badger* úplně. Pracoval tedy zcela

[10] https://duckduckgo.com/app
[11] https://privacybadger.org/

autonomně bez závislosti na správcích seznamů filtrovacích prvků a nad svými konkurenty měl v tomto ohledu velkou výhodu. Využíval pouze jeden typ seznamu, a to tzv. "žlutý seznam"domén jako třeba *Instagram*, nebo *Twitter*, které uživatele sledují, ale jsou nezbytné pro správné fungování webové stránky [10].

Detekce sledování závisela například na detekci unikátních *cookies*, *supercookies*, *canvas fingerprinting* a sdílení *cookies* třetím stranám pomocí neviditelných pixelů. Blokování proběhlo tehdy, kdy *Privacy Badger* odhalil sledování stejnou třetí stanou na třech různých webových stránkách. Na podzim roku 2020 byla však schopnost rozšíření rozeznat sledovací prvek bez závislosti na seznamech pozastavena [21]. Důvodem bylo možné zneužití samoučícího algoritmu třetími stranami. V současné době pracuje rozšíření podobným způsobem, jako rozšíření z kategorie první 2.2.

**Disconnect**[12] vyvíjen stejnojmennou společností od roku 2011 nabízí efektivní ochranu před sledováním uživatele skrze web. V základním balíčku zdarma nabízí ochranu před trackery, zároveň zvýrazňuje technické výhody jeho využití, jako ušetřený čas pro načtení stránek, nebo šířku pásma. Uživateli také nabízí grafickou vizualizaci přítomného obsahu vhodnou pro jednodušší pochopení (viz. 2.4). Za měsíční poplatek nabízí *Disconnect* vlastní VPN.




Obrázek 2.4: Obrázek znázorňující GUI rozšíření *Disconnect*, konkrétně grafické zobrazení obsahu na stránce `https://www.super.cz/`.

Rozšíření **Privacy Possum**[13] chrání uživatele před sledováním po internetu alternativním způsobem. Mimo blokování trackerů funguje tak, aby stál společnosti sledující uživatele co nejvíce peněz. Vývojář tohoto projektu je bývalým členem týmu vyvíjející rozšíření **Privacy Badger**, *cowlicks*. V mnoha směrech se snaží navázat na nedokonalosti jmenovaného rozšíření. Například v metodě bránění fingerprintingu místo blokování spustitelného obsahu stránky podvrhuje data, která může skript získat. Díky tomu je získaný fingerprint prohlížeče vždy nepřesný [14]. Dále blokuje všechny cookies třetích stran, `refer` hlavičky HTTP požadavků, čímž znemožňuje třetím stranám sledování pohybu uživatele po internetu, a `etag` sledování.

[12] `https://disconnect.me/`
[13] `https://github.com/cowlicks/privacypossum`

**First Party Isolation**[14] implementuje koncept převzatý z *Tor* prohlížeče s názvem *Cross-Origin Identifier Unlinkability* [6]. Jeho principem je ověřování zdrojů podle *URL* navštěvované domény – první strany.

| | Počet stažení | Hodnocení |
|---|---|---|
| DuckDuckGo Privacy Essentials | 1 459 942 | 4.6 |
| Privacy Badger | 889 728 | 4.8 |
| Disconnect | 113 734 | 4.2 |
| Privacy Possum | 95 113 | 4.5 |
| First Party Isolation | 3 789 | 4.2 |

Tabulka 2.2: Tabulka shrnující rozšíření blokující sledovací prvky, počet jejich stažení a jejich hodnocení na stránce https://addons.mozilla.org/en-US/firefox/extensions/category/privacy-security/

Z tabulky 2.2 lze pozorovat, že popularita webových rozšíření, která nejsou zaměřená na blokování reklam, je značně nižší.

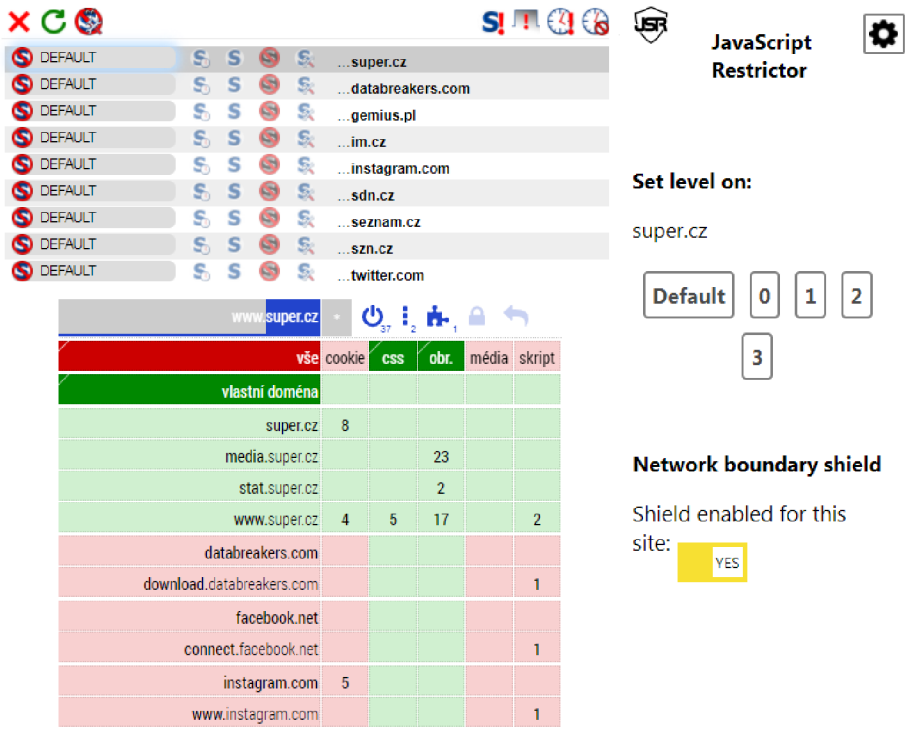
### Rozšíření blokující spustitelný webový obsah

Převážná většina webových stránek dnes využívá nějakou formu spustitelného obsahu. V drtivé většině se jedná o *JavaScript* – jazyk umožňující webové stránce chovat se dynamicky. Bez *JavaScriptu* by uživatel stránky přišel o zásadní poskytnuté funkce a výhody. Nebylo by možné například online nakupování, nebo čtení komentářů v reálném čase na sociálních médiích. Na druhou stranu je jeho použití jednoduše zneužitelné třetími stranami (více v kapitole 3). Řešení se naskýtá ve formě webových rozšíření blokující spustitelný obsah stránek.

Nejstahovanějším rozšířením této kategorie je rozšíření **NoScript**[15]. Je *open-source* a ve vývoji od roku 2005. Jeho autorem je *Giorgio Maone*. Rozšíření zabraňuje spuštění jakéhokoli spustitelného obsahu stránky, kterému uživatel neposkytne důvěru. Ihned po nainstalování obsahuje rozšíření seznam domén, které jsou na internetu často používané a zakázání jejich spustitelného obsahu by uživateli značně znepříjemnilo prohlížení internetu (jako například `youtube.com`, nebo `google.com`). Uživatel může na seznam důvěryhodných domén kdykoli přidat domény vlastní, nebo může doménám přidělit dočasná práva pro spouštění obsahu. Práva jsou takovým doménám odebrána po uzavření prohlížeče.

Druhým populárním rozšířením je **uMatrix**[16]. Jedná se o projekt vývojáře *Raymonda Hilla* – stejně jako výše zmíněné rozšíření *uBlock Origin*. Ve vývoji bylo od roku 2014, v roce 2020 byl však jeho vývoj autorem zastaven [22]. Rozšíření je však stále dostupné pro prohlížeče *Mozilla Firefox* a *Google Chrome*. V nenakonfigurované verzi využívá rozšíření *host lists* pro blokování domén v globálním měřítku. Uživateli umožňuje přidávat a odebírat vlastní pravidla. Dále nabízí uživateli například možnost podvrhovat *HTTP refer* hlavičky, čímž zabraňuje třetím stranám zjistit informace o pohybu uživatele. Pro každou navštívenou stránku nabízí volbu blokování konkrétního spustitelného obsahu připojených domén.

[14] https://github.com/mozfreddyb/webext-firstpartyisolation
[15] https://noscript.net/
[16] https://github.com/gorhill/uMatrix




Obrázek 2.5: Obrázek znázorňující GUI rozšíření *NoScript*, *JavaScript restrictor* a *uMatrix* na stránce `https://www.super.cz/`.

**JavaScript Restrictor**[17] je rozšíření vyvíjené vedoucím této práce, *Liborem Polčákem*. Uživatel má na výběr ze 4 úrovní funkčnosti:

- 0 – žádná ochrana, rozšíření neblokuje žádný spustitelný obsah
- 1 – minimální ochrana, rozšíření blokuje nějaký spustitelný obsah, funkcionalita navštívených stránek zůstává stejná. Manipuluje s přesností údajů `date` a `performance`, podvrhuje informace o uživatelově *hardware*, limituje možnost geolokace uživatele na přesnost v rámci metrů a zamezuje API číst údaj o stavu baterie zařízení.
- 2 – doporučená ochrana, rozšíření blokuje nevyžádaný spustitelný obsah, funkcionalita navštívených stránek zůstává stejná. Nabízí stejnou ochranu jako předchozí vrstva, navíc chrání uživatele před `canvas fingerprinting`, zamezuje čtení periferií, která zařízení využívá, a limit přesného určení polohy uživatele omezuje na kilometry.
- 3 – vysoká úroveň ochrany, funkčnost navštěvovaných stránek může být omezena. Mimo ochrany předchozích vrstev nabízí například filtrování `XMLHttpRequest` požadavků a ochranu proti zneužití objektu `ArrayBuffer` k indentifikaci uživatele. Znemožňuje lokalizovat uživatele pomocí cizích API.

Ihned po instalaci pracuje rozšíření na úrovni číslo 2. Lze nastavit libovolnou úroveň ochrany na kteroukoli stránku, buďto pomocí tlačítek v GUI rozšíření, nebo přidáním jména domény a zvolené úrovně ochrany do seznamu pomocí nastavení.

[17] `https://polcak.github.io/jsrestrictor/`

| | Počet stažení | Hodnocení |
|---|---|---|
| NoScript | 385 945 | 4.4 |
| uMatrix | 32 055 | 4.8 |
| JavaScript Restrictor | 30 | - |

Tabulka 2.3: Tabulka shrnující rozšíření blokující spustitelný obsah, počet jejich stažení a jejich hodnocení na stránce https://addons.mozilla.org/en-US/firefox/extensions/category/privacy-security/

Tabulka 2.3 zobrazuje počet stažení a uživatelská hodnocení zmíněných rozšíření blokující spustitelný obsah. Rozšíření této kategorie jsou výrazně méně populární, než rozšíření kategorií předchozích. Kvůli jejich povaze mohou být nevhodná pro nezkušeného uživatele, který se v technologii nevyzná a není schopen po instalaci rozšíření vhodně nakonfigurovat.

### Rozšíření pro docílení šifrovaného spojení

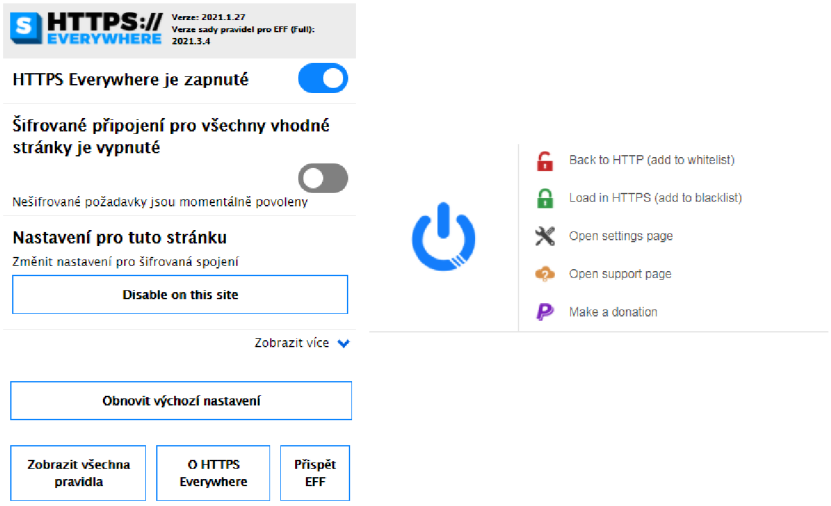
Od doby vzniku internetu uplynulo více než šedesát let a v zárodku jeho vývoje nebylo možné předpovědět rozměr, do kterého v současnosti internet dospěl. Pro internetovou komunikaci mezi zařízeními je stále využíváno protokolu *HTTP – Hypertext Transfer Protocol*, který nebyl navržen pro síť v tak velkém měřítku, kterou se internet stal. Protokol *HTTP* není dostatečně bezpečný pro přenášení dat bez rizika narušení jejich integrity, nebo jejich odposlechu. Při pohybu po transportní vrstvě totiž nepodporuje šifrování přenášených dat. Zároveň není možné verifikovat identitu stránky, která protokolem *HTTP* s klientem komunikuje, takové stránce není možné vystavit bezpečnostní certifikát. Řešením se stal protokol *HTTPS – Hypertext Transfer Protocol Secure*, který v sobě zahrnuje i využití protokolů *SSL – Secure Sockets Layer* a *TLS – Transport Layer Security*. Pomocí protokolů *SSL*, nebo *TLS* jsou data v transportní vrstvě komunikace mezi zařízeními šifrována díky jejich existenci lze ověřit identitu navštívené stránky.

Přes výhody protokolu *HTTPS* nad protokolem *HTTP* narazí uživatel při prohlížení internetu na mnoho stránek, které sice protokol *HTTPS* ke komunikaci s klientem podporují, ale v první řadě upřednostňují využití komunikace pomocí protokolu *HTTP*. Důvodem může být například zastaralá architektura stránky. Rozšíření této kategorie umožňují klientské straně automaticky upravit obsah internetových dotazů a tím vynutit použití protokolu *HTTPS* místo protokolu *HTTP*. Stránky, které využití protokolu *HTTPS* nepodporují vůbec, by měl uživatel navštěvovat pouze pokud jim důvěřuje.

Rozšíření **HTTPS Everywhere**[18] je nejpopulárnějším rozšířením tohoto typu. Na internetu se poprvé objevilo v roce 2014. Je dílem vývojářů skupiny *Electronic Frontier Foundation*, kteří se podílejí i na vývoji již zmíněného rozšíření *Privacy Badger*. Rozšíření automaticky přepisuje všechny *HTTP* požadavky zaslané klientem po dobu komunikace s navštívenou stránkou na požadavky *HTTPS*.

Druhé nejpopulárnější rozšíření této kategorie je **Smart HTTPS**[19]. Jeho autorem je vývojář s přezdívkou *ilGur* od roku 2018. Steně jako předchozí rozšíření nutí stránky komunikovat skrze protokol *HTTPS*, pokud jej podporují. V případě, že při *HTTPS* komunikaci narazí na chybu, přidá navštívenou stránku do své databáze výjimek.

[18] https://www.eff.org/https-everywhere
[19] https://mybrowseraddon.com/smart-https.html




Obrázek 2.6: Obrázek znázorňující GUI rozšíření *HTTPS Everywhere* a *Smart HTTPS* na stránce https://www.super.cz/.

| | Počet stažení | Hodnocení |
|---|---|---|
| HTTPS Everywhere | 744 535 | 4.7 |
| Smart HTTPS | 18 807 | 4.3 |

Tabulka 2.4: Tabulka shrnující rozšíření pro vynucení šifrovaného sopojení, počet jejich stažení a jejich hodnocení na stránce https://addons.mozilla.org/en-US/firefox/extensions/category/privacy-security/

### Negativa webových rozšíření zaměřených na bezpečnost a soukromí

Rozšíření zaměřená na bezpečnost a soukromí nemusí přinášet pouze výhody. Rozšířením, která uživatel využívá, může být zastaven vývoj (jako v případě již zmíněného rozšíření uMatrix). Kvůli rychlému vývoji využívané technologie na straně prohlížečů mohou být rozšíření zablokována, nebo mohou po aktualizaci prohlížeče ztratit podporu [30]. V nejhorším případě mohou být bezpečnostní rozšíření zneužita ke krádeži a dat [26].

Kromě těchto negativ musí uživatel vzít v potaz existenci rizik, proti kterým jej pomocí bezpečnostního rozšíření nelze ochránit. Například v případě rozšíření využívajících seznamy blokovacích prvků – pokud se na internetu objeví nová sledovací doména, je nutno ji začlenit do seznamů, která rozšíření používá k filtraci. V období od vzniku a nasazení sledovacího prvku a jeho začlenění do filtrovacího seznamu je uživatel před touto konkrétní hrozbou nechráněn. V případě sledovacího skriptu uvnitř uzavřeného systému (jako třeba specifický informační systém) nemusí být do seznamu zařazen nikdy. Kontrola všech individuálních skriptů v podobném prostředí je jednoduše nad rámec možností návštěvníků stránek. Z tohoto důvodu by měl uživatel vždy navštěvovat pouze stránky, kterým důvěřuje.

# Kapitola 3

# Bezpečnostní rizika

Rozšíření momentálně dostupná na trhu se z velké části zaměřují na blokování reklam. U reklam však rizika prohlížení nekončí. Většina uživatelů si buďto žádná rizika neuvědomuje, nebo je neshledávají jako dostatečně významná. Podle studie [34] *58%* dotazovaných Američanů v otázce internetového soukromí na toto své právo resignovalo kvůli pocitu bezmoci a matoucím internetovým opatřením.

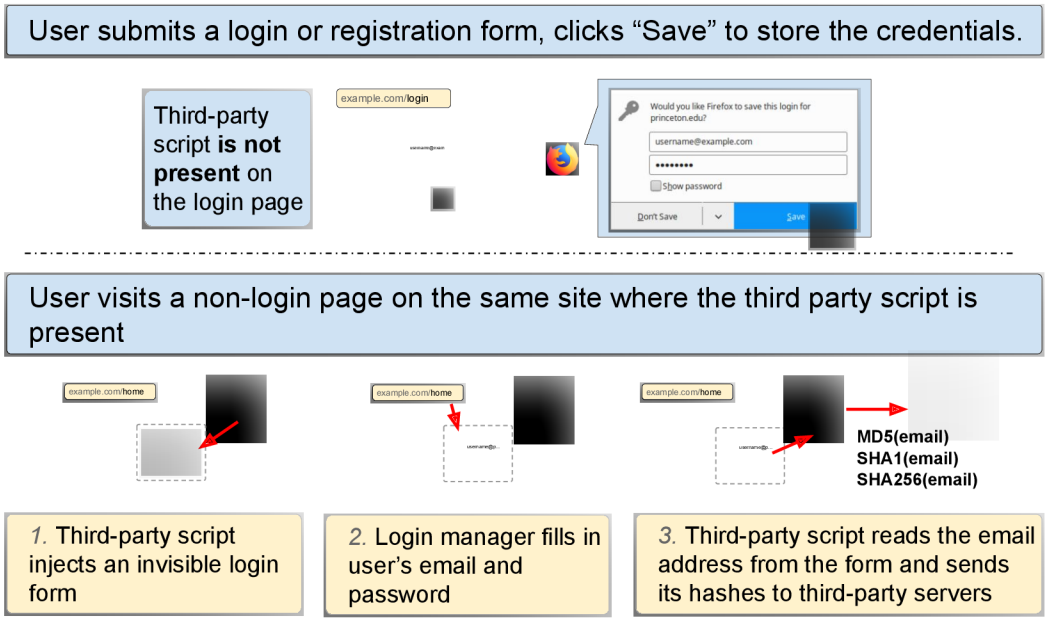
## 3.1 Získání a zneužití osobních údajů

Naprostá většina webových stránek obsahuje skripty třetích stran [20]. Ty dovolují netransparentním způsobem získávat a dále zpracovávat data netušících uživatelů stránky. Může se jednat o reálné osobní údaje jako třeba přihlašovací jména a hesla, bankovní údaje, či zdravotní záznamy.

Příkladem získání osobních informací je zneužití možnosti tvorby nového uživatelského účtu na stránkách skrze *Facebook* účet. Mnoho stránek, včetně například sociální sítě *Instagram*, nabízí uživatelům možnost takového přihlášení za účelem snížení režie plynoucí z tvorby nového uživatelského účtu. Pokud uživatel důvěřuje podobné stránce, nesdílí svá osobní data pouze s danou stránkou, ale i s třetími stranami s ní spojenými. Tím umožňuje třetím stranám zasílat autorizované požadavky na *Facebook* API, což může mít za následek získání globálního ID uživatele, jeho profilového obrázku, nebo dalších veřejně přístupných dat [20].

Prohlížeče jako *Mozilla Firefox*, nebo *Google Chrome* umožňují ukládání hesel a uživatelských jmen nebo e-mailů pro zjednodušení procesu přihlašování se na navštívené webové stránky. Skripty třetích stran mohou ukládání zneužít a do HTML kódu vložit neviditelný přihlašovací formulář. Nemusí se nutně vyskytovat konkrétně na přihlašovací stránce, může být vložen na jakoukoli jinou stránku tohoto webu [20]. Formulář je prohlížečem automaticky vyplněn a data jako hash e-mailové adresy jsou zaslána třetím stranám.

Webové stránky často implementují tzv. *session replay* skripty, které zaznamenávají aktivitu uživatele po dobu jeho prohlížení. Tyto skripty jsou schopné zaznamenat nejen kliknutí, ale i pohyb kurzoru po obrazovce a stisknutí kláves. Původním záměrem jejich existence je sbírat užitečná data pro analýzu prohlížení potenciálních zákazníků stránek, bohužel může ale dojít i k jejich zneužití třetími stranami [28]. Skript zaznamenává veškerý HTML obsah stránek, včetně DOM struktury. V mnoha případech může DOM obsahovat citlivé informace zobrazené uživateli, které skript serializuje a zasílá třetím stranám.




Obrázek 3.1: Schéma naznačující princip zneužití vyplnění údajů. Dostupné z https://webtransparency.cs.princeton.edu/no_boundaries/

## 3.2 Sledování uživatele za účelem jeho profilování

Pojem sledování se v tomto kontextu vztahuje na zaznamenávání uživatelovi aktivity při pohybu internetem, často za účelem analýzy a prodeje těchto informací třetím stranám, jako jsou zprostředkovatelé internetových reklam. Probíhá nejčastěji ve formě *cookies* nebo *supercookies*, vložených skriptů a *fingerprintingu*.

*HTTP cookies* jsou malá data ukládaná v prohlížeči uživatele navštěvovanou stránkou [32]. Zaznamenávají navštívené stránky, historii hledání, přihlašovací údaje a další. Lze rozlišit dva druhy *HTTP cookies* [17]:

1. ***first-party cookies***, vytvořené stránkou samotnou, využívané převážně k vylepšení nabízených služeb nebo autentizaci uživatele. K tomuto typu *cookies* má přístup pouze navštívená stránka. Nelze však vyloučit, že jejich obsah stránka prodá, nebo poskytne třetí straně (tuto skutečnost musí podle směrnice *ePrivacy* uživateli oznámit).

2. ***third-party cookies***, vytvořené třetími stranami, které se na stránce vyskytují. Často vzniknou voláním skriptů třetích stran, jako třeba při sdílení obsahu stránky na sociálních médiích. Využívají se typicky pro utvoření osobního profilu uživatele za účelem tvorby personalizovaných reklam cílených na konkrétní osobu.

*Third-party cookies* často existují výhradně za účelem sledování uživatele napříč všemi navštívenými stránkami. Protože doména `a.com` nemá přístup ke *cookies* domény `b.com`, často mezi sebou se soubory *cookies* obchodují za účelem zlepšení cílené reklamy a zvýšení zisku. Této transakci se říká *cookie syncing*, nebo také *cookie matching* [5].

*Fingerprinting* v kontextu webové bezpečnosti je sbírání informací o konkrétním uživateli na základě jeho hardwarových specifikací, nainstalovaných aplikací, rozlišení obrazovky, dostupných fontů a dalších [24]. Tyto informace lze použít k jeho efektivní identifikaci skrze internet.

Takové sledování probíhá naprosto bez souhlasu a vědomí uživatele. Často se vyskytuje v těchto formách:

1. *passive fingerprinting* zahrnuje shromažďování dat bez aktivního zásahu třetí strany, například vyčtení informací z HTTP dotazu zaslaného uživatelem. V dotazu se objevuje IP adresa klienta, používaný prohlížeč, jeho verze, i verze operačního systému.

2. *active fingerprinting* spočívá v implementaci aktivních prvků jako například volání *JavaScriptových* metod k získání dalších informací o uživateli. Techniky zahrnují zjištění rozlišení obrazovky uživatele, dostupné fonty, nainstalovaná webová rozšíření, u mobilních zařízení i data poskytována senzory a další. Konkrétním příkladem je metoda *canvas fingerprinting* využívající elementu `<canvas>`, který je součástí HTML5, k vykreslení obrazců. Tím podává uživatel stránce informace o své grafické kartě. Díky své podstatě je možné tyto na straně uživatele techniky identifikovat a zakázat.

Schopnost třetích stran vytvářet uživatelův *fingerprint* závisí například na použitých protokolech, nainstalovaných rozšířeních, používaných fontech, rozšíření obrazovky, využívaných jazycích, poloze uživatele, jeho periferních zařízení (reproduktory, mikrofony), grafické kartě, počtu CPU a velikosti RAM. Kromě unikátních informací shromažďují *fingerprintující* skripty též další genetická data o uživateli. Pomocí tzv. *grafů identit* lze i z informací, které jsou na první pohled generické, vytvořit „nepřesný“ odhad identity uživatele, který stránku právě navštívil. Využívá se vhodného zpracování velkého množství dat o uživateli a jeho porovnání s daty shromážděnými o dalších návštěvnících stránky. Vznikne tak *pravděpodobnostní* profil identity uživatele [19]. Ve skutečnosti je tento odhad celkem přesný. Touto metodou lze například identifikovat různá zařízení, která konkrétní uživatel vlastní (jako stolní počítač a mobilní telefon) [29].

## 3.3 Škodlivý software

Jako škodlivý software označujeme skupinu programů vytvořených s cílem poškodit uživatelův systém. Jako zastřešující termín je využit pojem „malware“, kombinace anglických slov „malicious“ (zákeřný) a „software“. Uživatel je prohlížením internetu a využitím internetové pošty vystavován riziku stáhnutí podobného softwaru do svého zařízení. Malware rozlišujeme na několik podtypů v závislosti na motivaci útočníka:

- **Virus** je malware schopný napadení více souborů počítače, napojuje se na programy spuštěné uživatelem a replikuje sama sebe napříč celým systémem skrze další modifikace napadených souborů.

- **Červ** je jako virus schopný replikovat sám sebe, na rozdíl od viru ale nepotřebuje k rozšíření přímou interakci uživatele, rozšiřuje se pomocí identifikace a využití bezpečnostních slabin jiného softwaru, kterých útočník využije k tvorbě vlastního kódu.

- **Trojský kůň** se vydává za legitimní program, například antivirový software. V pozadí po spuštění negativně ovlivňuje uživatelova data.

- **Adware** zobrazuje uživateli nežádanou reklamu, často v prohlížeči přesměrovává při vyhledávání na identicky vypadající stránky plné obsahu třetích stran. Bývá součástí jiných programů dostupných na internetu.

- **Spyware** sleduje uživatelovu aktivitu v rámci celého jeho zařízení, včetně stisknutých kláves, nebo zadaných hesel. Podmnožinou spyware jsou internetové **trackery** (také **sledovací prvky**). V této práci často zmiňovaný pojem označuje prostředky vytvořené za účelem sledování uživatele po internetu – nejčastěji se jedná o sledovací skript napsaný v jazyce *JavaScript*.

- **Ransomware** je v posledních letech díky potenciálně rychlému zisku v prudkém vzrůstu. Jeho cílem je zašifrovat data přítomná v uživatelově zařízení a za jejich zpřístupnění vyžadovat výkupné (*slovo ransom, česky výkupné*). Ve své podstatě se jedná o trojské koně s konkrétním účelem. Útočník vyzve oběť k zaplacení částky do jeho *Bitcoinové* peněženky. Dodatečně může program vyčkat a uživatele sledovat, dokud podle jeho aktivity neodhadne částku, kterou by byl uživatel reálně ochoten zaplatit. Útoky jsou často cíleny na větší organizace, spíše než na jednotlivce.


Obrázek 3.2: Zpráva od útočníka uživateli, **WannaCry ransome** útok 2017. Dostupné z https://securelist.com/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/78351/

Webová rozšíření nemohou zabránit šíření škodlivého softwaru v zařízení, ani jej ze zařízení odstranit. Místo toho implementují překlad blokovacích seznamů známých domén, která tento software šíří. Rozšíření zabraňuje vzniku jakéhokoli spojení s nežádanou malware doménou. Rozšíření *uBlock Origin* obsahuje blokovací seznam *Badware risks*, fungující jako prevence před vpuštěním nežádaného softwaru do zařízení uživatele.

Webová rozšíření usnadňují koncovému uživateli navigaci internetem bezpečným způsobem, zároveň chrání jeho nárok na soukromí a znesnadňují třetím stranám zneužít jeho citlivá data, sledovat jeho pohyb, nebo napadení zařízení uživatele nežádaným softwarem. Jejich využitím však vznikají další otázky: *Mohu jako uživatel věřit mnou nainstalovaným rozšířením? Mohu se na rozšíření spolehnout?*. Odpověď není vůbec jednoduchá. Z výsledků dostupných zkoumání vyplývá, že nejpopulárnější webová rozšíření zaměřená na bezpečnost mají dost odlišnou efektivitu. To platí zejména v závislosti na konkrétním nebezpečí, před kterým vyžaduje uživatel ochranu. Podle výzkumu je k blokování trackerů nejefektivnější vhodně nakonfigurované rozšíření *Ghostery* [33].

# Kapitola 4

# Návrh testovacího prostředí webových rozšíření

Tato kapitola se věnuje způsobu návrhu testovacího prostředí pro porovnání výše zmíněných webových rozšíření se zaměřením na bezpečnost v rámci přiřazených skupin. Testovací prostředí se soustředí na vlastnosti webových rozšíření. Pozornost bude věnována zejména oblastem, ve kterých se rozšíření ve funkčnosti překrývají.

Teoretická část této práce nastínila hlavní funkce daných webových rozšíření, podle nich byla vybrána testovací kritéria jako schopnost skupiny rozšíření:

- **rozšíření na bázi seznamu sledovacích prvků** – rozeznat nevyžádaná HTTP přesměrování a zamezit tím sledování uživatele po internetu. Rozeznat nevyžádané HTTP požadavky zasílané klientskou stranou a zablokovat je. Odhalit škodlivá volání *JavaScriptových* metod využívaných ke sledování a profilování uživatele a zakázat je. Rozlišit mezi *cookies* prvních a třetích stran a zamezit ukládání nebezpečných *cookies* do uživatelova zařízení.
- **rozšíření blokující sledovací prvky** – stejná kritéria, jako první skupina rozšíření.
- **rozšíření blokující spustitelný webový obsah** – rozeznat *fingerprintující* a škodlivé skripty obsažené na internetových stránkách a zakázat jejich provedení.

## 4.1 Využité nástroje

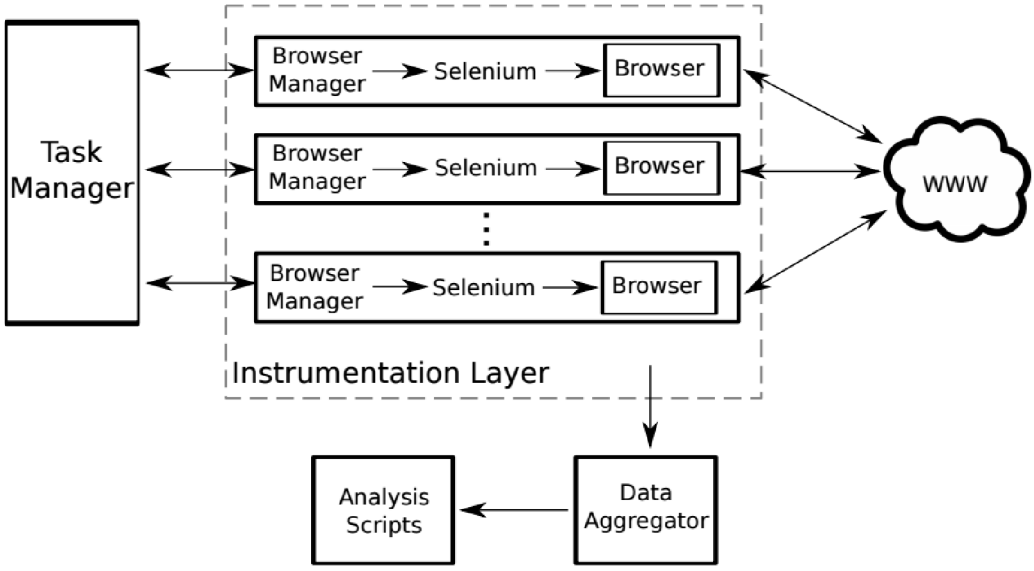
Pro účely práce nebyly vytvořeny žádné speciální nástroje. Výsledků bylo dosaženo využitím již existujících technologií. Všechny zahrnuté technologie jsou volně dostupné a zdarma. Testy byly prováděny na operačním systému **Linux Mint** v domácím prostředí.

### OpenWPM

*OpenWPM* je nezávislý framework pro kolekci dat z internetových stránek [25]. Funguje na bázi *Selenia*[1], tudíž vytváří instance webových prohlížečů. *OpenWPM* automatizuje procházení webových stránek pomocí tzv. *crawls* v závislosti na nastavení *TaskManager* (viz. obrázek níže). Je jednoduše rozšiřitelné pro potřeby konkrétního výzkumu a implementuje možnost vytvářet profil prohlížeče, včetně jeho nainstalovaných rozšíření. Této vlastnosti

[1] https://www.selenium.dev/

bude využito pro získání relevantních dat prohlížení v závislosti na právě testovaném rozšíření. Platforma je implementována v jazyce *Python*. V dočasné verzi podporuje nástroj pouze prohlížeč *Mozilla Firefox*.




Obrázek 4.1: Schéma naznačující princip fungování *OpenWPM*. Dostupné z https://www.semanticscholar.org/paper/OpenWPM-%3A-An-automated-platform-for-web-privacy-Englehardt-Eubank/2ccde1be1ff725aa8740868929cd1a6f5072ab3a

Výhodnou částí nástroje je možnost nastavit parametry prohlížeče při průchodech. Parametry se vztahují na průchod všemi stránkami a v průběhu průchodu není možné je změnit. Nastavitelnými parametry, které je vhodné zmínit v rámci této práce, jsou:

- `bot_mitigation` – upraví styl průchodu s cílem zabránit odhalení jeho automatizace navštívenými stránkami.
- `display_mode` – upřesňuje zobrazení prohlížeče při průchodu, v režimu `native` zobrazí prohlížeč včetně jeho GUI, v režimu `headless` pouze obsah procházené stránky. Projeví se zejména v případě, že uživatel zvolí možnost ukládání snímků obrazovky, také ovlivňuje výpočetní náročnost.
- `tp_cookies` – specifikuje způsob nakládání s cookies třetích stran, možnost `always` ukládá veškeré cookies, `never` žádné a `fromvisited` pouze ze stránek, které byly navštíveny jako první strana.
- `donottrack` – automaticky vysílá navštíveným stránkám signál *Do Not Track*
- `tracking_protection` – zapíná ochranu proti sledování implementovanou v prohlížeči *Mozilla Firefox*, v současné době není tato možnost nástrojem podporována.

*OpenWPM* nabízí průchody s využitím uživatelských profilů – profil lze načíst před průchodem z disku ve formátu `.tar` i ukládat jej v průběhu nebo na konci průchodů pro další využití, případně analýzu. Nástroj nabízí provádění průchodů dvěma způsoby:

- **stateful** – při průchodu stránkami si nástroj uchovává buďto uživatelem nastavený profil, nebo na začátku vytvoří profil nový, v obou případech jej aktualizuje postupně skrz průchod – jedná se o automatizaci prohlížení odpovídající uživatelovu pohybu po internetu.
- **stateless** – nástroj po projití každé stránky terminuje dočasný profil a novou stránku navštěvuje bez existujícího profilu, nebo načítá původní uživatelem poskytnutý profil, aniž by jej v průběhu průchodů měnil – procházení neodpovídá reálnému pohybu uživatele po internetu, ale téměř nezkresluje. výsledná data

Nejdůležitější části nástroje pro tuto práci je možnost jeho instrumentace. *OpenWPM* shromažďuje data při každé návštěvě uživatelem poskytnuté stránky. Výsledkem každého průchodu je rozsáhlá databáze zahrnující tabulky v závislosti na zvolené instrumentaci průchodu. Detailní schéma vytvořené databáze je dostupné na stránce [15]. V tabulce 4.1 níže se nachází přehled základních tabulek databáze s jejich krátkým popisem.

| **Název tabulky** | **Popis funkce** |
|---|---|
| `callstacks` | obsahuje zásobník volání funkcí |
| `crawl` | informace o provedeném průchodu |
| `crawl_history` | informace o průchodu konkrétní stránkou |
| `dns_responses` | DNS resoluce obdržené klientem |
| `http_redirects` | přesměrování provedená návštěvou stránky |
| `http_requests` | HTTP požadavky zaslané klientem |
| `http_responses` | HTTP odpovědi obdržené klientem |
| `incomplete_visits` | v případě přerušení návštěvy stránky uchovává `visit_id` |
| `javascript` | instance volání *JavaScriptových* funkcí |
| `javascript_cookies` | informace o vzniklých *cookies* |
| `navigations` | informace o pohybu v rámci instance prohlížeče |
| `site_visits` | informace o navštívených stránkách |
| `task` | příkazy prováděné skrze průchody |

Tabulka 4.1: Tabulka shrnující data shromažďovaná do tabulek nástrojem *OpenWPM* a jejich obsah.

Instrumentaci lze modifikovat nejen pro každý průchod, ale dokonce i pro každý automatizovaný prohlížeč. Nástroj totiž umožňuje uživateli provádět průchody ve více instancích *Mozilla Firefox* zároveň. Maximální počet instancí je omezen jejich výpočetní náročností. Vývojáři *OpenWPM* vybízí uživatele přispět k vývoji projektu, v této fázi mají uživatelé na výběr ze šesti různých nástrojů pro sběr dat:

- `http_instrument` – sběr HTTP požadavků, odpovědí a přesměrování do patřičných tabulek databáze.
- `js_instrument` – zaznamenává volání *JavaScriptových* metod (včetně argumentů). Navíc zahrnuje sbírání dat webových API, která by mohla potenciálně vést k *fingerprintingu* uživatele.
- `navigation_instrument` – zaznamenává pohyb v rámci instance prohlížeče.

- `callstack_instrument` – zaznamenává volání funkcí ze zásobníku.
- `dns_instrument` – obsahuje informace o DNS resolucích.
- `cookie_instrument` – zaznamenává *cookies* vytvořené *JavaScriptem* i skrze HTTP odpovědi

Dále nabízí *OpenWPM* možnost analýzy dat pomocí jednoduše modifikovatelných skriptů. Výstupem průchodu pomocí nástroje je databáze ve formátu *SQLite*, je tedy snadné ji podrobit analýze pomocí jazyka *SQL*.

## 4.2 Vstupní data

Jako vstupní data poslouží výsledky průchodů získané pomocí platformy *OpenWPM*. Průchody budou prováděny na nejnavštěvovanějších internetových stránkách podle statistik dostupných z *Tranco Top sites*[2].

Nastavení a instrumentace nástroje pro průchod bude záležet na konkrétní testované kategorii (více v kapitole 5). Všechna zkoumaná data budou ve formátu *SQLite* databáze.

## 4.3 Návrh způsobu testování jednotlivých kategorií

Teoretická část práce rozčlenila rozšíření do čtyř skupin podle jejich funkcionality. Tyto skupiny jsou:

| | |
|---|---|
| **Rozšíření na bázi seznamu sledovacích prvků** | AdBlock Plus<br>uBlock Origin<br>AdBlocker Ultimate<br>Ghostery<br>AdGuard AdBlocker |
| **Rozšíření blokující sledovací prvky** | DuckDuckGo Privacy Essentials<br>Privacy Badger<br>Disconnect<br>Privacy Possum<br>First Party Isolation |
| **Rozšíření blokující spustitelný webový obsah** | NoScript<br>uMatrix<br>JavaScript Restrictor |
| **Rozšíření pro docílení šifrovaného spojení** | HTTPS Everywhere<br>Smart HTTPS |

Tabulka 4.2: Tabulka shrnující testovaná rozšíření a jejich příslušné kategorie.

Z principu fungování rozšíření popsaném v kapitole 2 je vhodné zaměřit se na různé vlastnosti testovaných rozšíření podle jejich přiřazené kategorie. Je opět nutno zmínit, že mnoho rozšíření se ve své funkčnosti překrývá – rozčlenění do kategorií je tedy spíše orientační za účelem celkově zpřehlednit tuto práci a její výsledky. Chování nástroje *OpenWPM* při průchodu individuální stránkou je následující:

[2] https://tranco-list.eu/

1. pokus se navštívit stránku.
2. pokud je návštěva úspěšná, počkej 30 vteřin.
3. zaznamenej internetový provoz do databáze.
4. ukonči návštěvu stránky.
5. přejdi na další stránku v řadě.

Při průchodu stránkou pomocí nástroje *OpenWPM* nejde zaručit jeho celistvost. Na navštívené stránce může dojít k přerušení spojení, nebo vypršení limitu pro provedení příkazu. Nástroj je, i v případě přerušení spojení, schopen zaznamenat dosavadní internetový provoz, který na stránce proběhl. Vzhledem k identickému vzorku procházených internetových stránek lze očekávat porovnatelnou chybovost při průchodech s instalací libovolného testovaného rozšíření.

### Rozšíření na bázi seznamu sledovacích prvků

Pro porovnání rozšíření této kategorie bude využito databáze vytvořené průchody pomocí nástroje *OpenWPM*. Data budou shromažďována ze žebříčku *Tranco Top sites* navštívením prvních 2000 stánek. Počet stránek je omezen výpočetní silou stroje, na kterém budou průchody realizovány.

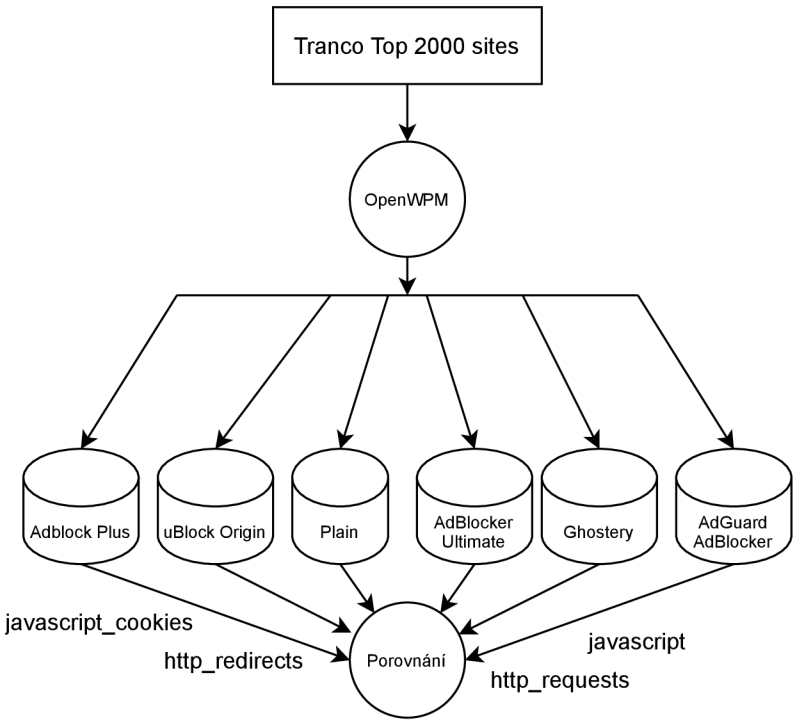
Při porovnání bude využito instrumentace nástroje `http_instrument`. Důvodem je princip algoritmizace rozšíření této kategorie. Cílem testů je zjistit, v jaké míře jsou rozšíření schopna zabránit nevyžádanému internetovému provozu pomocí filtrace na bázi seznamů sledovacích prvků. Porovnání se soustředí na kvantitativní stránku ochrany, kterou rozšíření nabízí.

Konkrétně se testy soustředí na výsledky průchodů v rámci zaznamenaných HTTP přesměrování a dotazů. V reálné databázi vytvořené nástrojem *OpenWPM* se jedná konkrétně o tabulky `http_redirects` a `http_requests`.

Dále využije test možnosti instrumentace `js_instrument` a `cookie_instrument`. Při průchodu internetem je uživatel profilován pomocí *fingerprintovacích JavaScriptů*. *OpenWPM* rozezná a zaznamená každé *JavaScriptové* volání na právě procházené stránce. Navíc nabízí nástroj možnost vytvářet „zkratky“ pro jednodušší rozeznání potenciálně *fingerprintujících* webových API, které klient při průchodu využije. Jejich definice se nachází v souboru `fingerprinting.py`. Dále nástroj zaznamená všechna *cookies* uložená dotazovanými servery na straně uživatele. Test bude porovnávat konkrétně obsahy tabulek `javascript` a `javascript_cookies`. Motivace zvolení těchto metrik je následovná:

- `http_redirects` – jak schopné je rozšíření rozeznat škodlivá HTTP přesměrování a zakázat je. HTTP přesměrování lze snadno využít k sledování uživatele po internetu.
- `http_requests` – jak schopné je rozšíření rozeznat a zablokovat nevyžádané HTTP požadavky zasílané klientskou stranou komunikace. Navštívením internetových stránek může zaslat prohlížeč značné množství nevyžádaných požadavků bez uživatelova vědomí.
- `javascript` – kolik volání *JavaScriptových* metod rozšíření blokuje. Jaké množství potenciálně *fingerprintujících* metod rozšíření zakáže.

- `javascript_cookies` – jak velké množství *cookies* dovolí rozšíření uložit na uživatelově straně komunikace.




Obrázek 4.2: Schéma zobrazující proces testování rozšíření na bázi seznamu sledovacích prvků

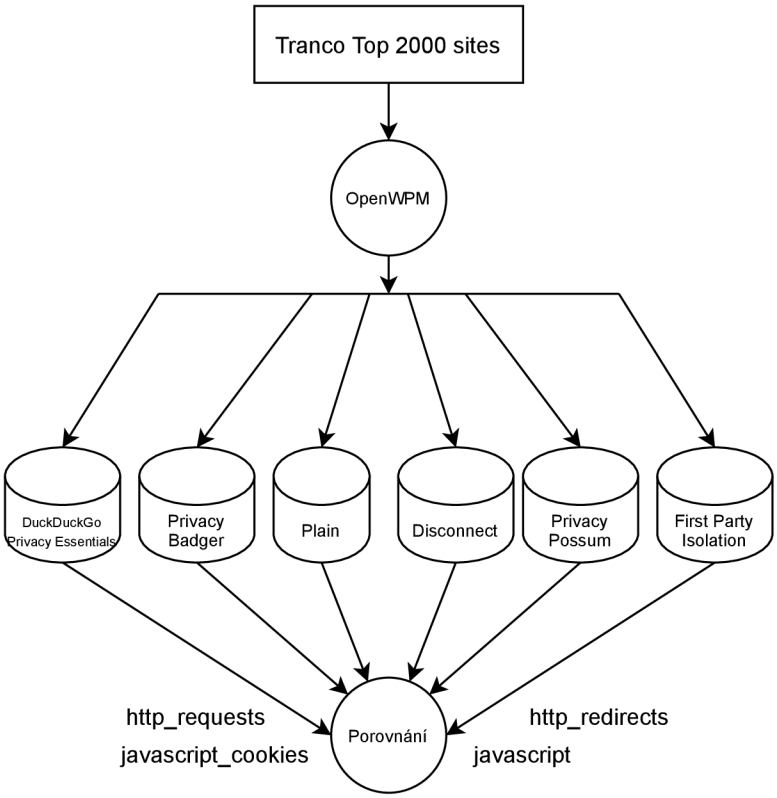
Na obrázku 4.4 je znázorněno schéma procesu porovnání webových rozšíření. Porovnání bude probíhat nejen mezi rozšířeními, ale i vůči průchodu bez jakéhokoli nainstalovaného rozšíření.

Výsledky v databázi budou porovnány na základě již zmíněných kritérií. Cílem tohoto testu je zjistit, které rozšíření implementuje nejefektivnější seznamy filtrovacích prvků a algoritmy pro jejich průchod.

### Rozšíření blokující sledovací prvky

Testování druhé kategorie rozšíření se zaměří na jejich schopnost zamezit sledování uživatele po internetu. Teoretická část práce 3.2 nastínila nejběžnější způsoby, kterými mohou třetí strany uživatele sledovat. Jedná se o využití *cookies* a *fingerprint* skriptů. Při porovnání této a předchozí kategorie rozšíření je důležité zmínit, že účelem v této části práce testovaných rozšíření není blokovat reklamy – to ovlivní intenzitu omezeného internetového provozu. Test se ale zaměří i na dopad na počty provedených HTTP přesměrování a zaslaných HTTP požadavků jako v předchozí kategorii rozšíření. Metriky prvních dvou testovaných kategorií jsou tedy totožné. Test rovněž využije možnosti instrumentace `http_instrument`, `js_instrument` a `cookie_instrument`.

K testování rozšíření této kategorie bude opět využit nástroj *OpenWPM*. Vzorek průchodů bude rovněž stejný, jako při předchozím testu – prvních 2000 stránek v žebříčku *Tranco Top sites*.




Obrázek 4.3: Schéma zobrazující proces testování rozšíření blokující sledovací prvky

Porovnání počtu zmíněných záznamů pro všechna testovaná rozšíření nastíní efektivitu rozšíření v oblasti zabránění sledování a profilování uživatele po internetu.

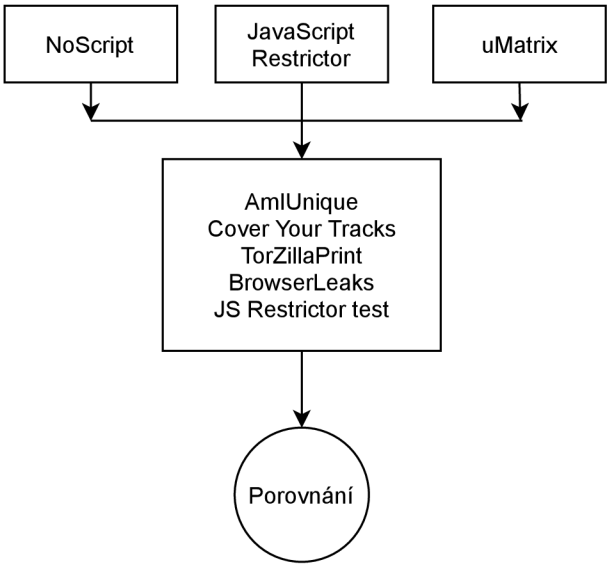
### Rozšíření blokující spustitelný webový obsah

Z důvodu povahy a odlišného přístupu rozšíření nelze tuto skupinu testovat a porovnat stejným způsobem, jako skupiny předchozí. Mimo rozšíření *Privacy Possum* v předchozích testech praktikovala rozšíření podobný přístup k docílení bezpečného prohlížení, jako všechna rozšíření testované skupiny. V případě rozšíření blokujících spustitelný webový obsah by výsledky automatizovaného průchodu stránek nepřinesly žádná relevantně porovnatelná data. Navíc rozšíření *NoScript* zakazuje volání *JavaScriptových* metod nástroje *OpenWPM*. Z tohoto důvodu je třeba v případě kategorie rozšíření blokujících spustitelný obsah upravit metriku a porušit dosavadní konzistenci testu rozšíření v původním stavu ihned po instalaci do prohlížeče bez další konfigurace ze strany uživatele. Cílem tohoto testu je zjistit, jak efektivně je rozšíření schopné zabránit *fingerprintingu* uživatele.

Test spočívá v instalaci rozšíření a navštívení veřejně dostupných stránek generujících *fingerprint* návštěvníka. Tyto stránky byly vytvořeny konkrétně za účelem testu unikátnosti *fingerprintu* uživatele při jejich návštěvě. Stránky využité k testu jsou:

1. AmIUnique – `https://amiunique.org/`,
2. Cover Your Tracks – `https://coveryourtracks.eff.org/learn`,
3. TorZillaPrint – `https://arkenfox.github.io/TZP/`,

4. JavaScript Browser Information – https://browserleaks.com/javascript,
5. Simple examples for implemented browser extension – https://polcak.github.io/jsrestrictor/test/test.html.




Obrázek 4.4: Schéma zobrazující proces testování rozšíření blokující spustitelný webový obsah

Test byl proveden opět pomocí prohlížeče **Mozilla Firefox**. Výběr prohlížeče je pro test důležitý, protože prohlížeč může sám v základu implementovat metody za účelem ochrany uživatele při prohlížení. Při testu záleží na schopnosti rozšíření zabránit *fingerprintingu* uživatele a složitosti konfigurace potřebné pro nejefektivnější výsledek.

### Rozšíření pro docílení šifrovaného spojení

Z principu funkce této kategorie rozšíření nelze provádět kvantitativní porovnávací testy. Při jejich nainstalování lze předpokládat navázání šifrovaného spojení HTTPS, pokud jej navštívená stránka podporuje. Efektivita je tedy závislá především na typu navštívené stránky. Z tohoto důvodu nebudou rozšíření *HTTPS Everywhere* a *Smart HTTPS* porovnávána. Přesto je tento typ rozšíření důležitou součástí pochopení principu dosažení co nejbezpečnější internetové komunikace.

# Kapitola 5

# Implementace a výsledky

Tato kapitola se věnuje implementaci testovacího prostředí pro porovnání rozšíření zaměřených na bezpečnost a soukromí v rámci jednotlivých skupin zmíněných v kapitole 2. Zároveň zahrnuje výsledky testování rozšíření.

Všechny testy byly prováděny v období **1. března 2021** až **20. dubna 2021**. V tomto krátkém časovém rozmezí bylo internetové prostředí navštěvovaných stránek porovnatelné. Implementací testovacího prostředí bylo možné rozšíření testovat v přednastavených šablonách a vytvořit tím porovnatelný vzorek získaných dat.

Je třeba zdůraznit, že při analýze databází vzniklých průchodem stránek byly zahrnuty i **podpůrné metody nástroje *OpenWPM*** (volání vlastních *JavaScriptových* metod, podpůrné funkce spojené s implementací nástroje). Nicméně vzorek testovaných stránek se pro každou kategorii testu shodoval – z toho důvodu lze zanedbat položky databáze získané výhradně využitím jmenovaného nástroje.

### Nastavení nástroje *OpenWPM*

Použitý nástroj byl lehce modifikován, aby odpovídal účelům této práce. Konkrétně se jedná o instalaci testovaného webového rozšíření před každým průchodem. Modifikaci zdrojového kódu souboru `deploy_firefox.py` nástroje znázorňuje algoritmus 1.

```
#Install custom extension

ext_loc = os.path.join(root_dir, "../extension_path/custom_extension.xpi")
ext_loc = os.path.normpath(ext_loc)
driver.install_addon(ext_loc, temporary=True)

logger.debug(
    "BROWSER %i: Custom extension loaded" % browser_params.browser_id
        )
```

**Algoritmus 1:** Úprava zdrojového kódu nástroje *OpenWPM* pro instalaci vlastních rozšíření.

Průchody byly prováděny na **pěti** instancích prohlížeče *Mozilla Firefox* zároveň, v režimu `stateless` bez využití předchozího existujícího uživatelského profilu. Režim prohlížeče byl nastaven na `headless`. Algoritmus 2 níže zobrazuje příkazy provedené na každé stránce.

```
command_sequence = CommandSequence(
            site,
            site_rank=index,
            callback=callback,
        )

command_sequence.append_command(GetCommand(url=site, sleep=30), timeout=90)

manager.execute_command_sequence(command_sequence)
```

**Algoritmus 2:** Algoritmus znázorňující postup při tvorbě a vykonání příkazů na zadané stránce.

### Analýza databáze vzorků

Všechny individuální databáze vzniklé použitím nástroje *OpenWPM* byly analyzovány pomocí jednoduchého skriptu `analysis.py` obsahujícího *SQL* dotazy. *SQL* dotazy provedené na databáze se zaměřily na konkrétní položky databáze v závislosti na testované skupině. Pro skupinu rozšíření na bázi seznamů sledovacích prvků a skupinu rozšíření blokující sledovací prvky byly vytvořeny dotazy na počet provedených HTTP přesměrování, zaslaných HTTP požadavků, počty volání *JavaScriptových* metod a *cookies* ukládaných na straně uživatele. Skripty nezohlednily nedokonalost nástroje *OpenWPM*, která spočívá v opětovné reinstalaci testovaného rozšíření při obnovení instance prohlížeče. Pro každou stránku podrobenou průchodu vytvoří nástroj individuální instanci prohlížeče *Mozilla Firefox*, do které ihned po vzniku nainstaluje soubor právě testovaného rozšíření ve formátu `.xpi` podle kritérií v souboru `deploy_firefox.py`. V případě testovaných rozšíření AdBlock Plus, AdBlock Ultimate, Ghostery a AdGuard AdBlocker se bezprostředně po instalaci zobrazí uživateli uvítací stránka rozšíření. Výsledkem je vyšší četnost HTTP dotazů (pouze v rámci pár tisíců) na doménu rozšíření ve vytvořené databázi.

## 5.1 Testování rozšíření na bázi seznamů sledovacích prvků

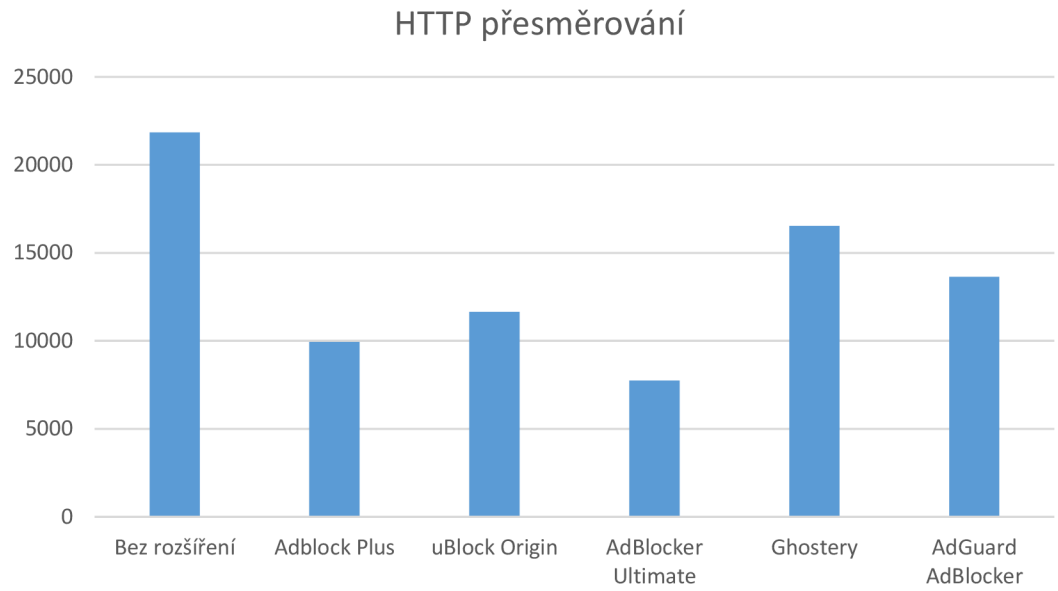
Testování bylo provedeno podle návrhu v části 4.3. Byly využity nástroje *OpenWPM* pro vytvoření informací o průchodech stránkami. Při testu každého rozšíření bylo využito instrumentací `http_instrument` pro sběr dat o HTTP přesměrováních, požadavcích a odpovědích, `javascript_instrument` pro sběr dat o volání *JavaScriptových* metod a `cookie_instrument` pro zaznamenání *cookies* ukládaných na straně uživatele. Výsledná databáze byla podrobena analýze pomocí *SQL* dotazů. Analýza databáze byla zpracována a promítnuta do shrnujících tabulek a grafů.

### HTTP přesměrování

Stránky, na které je uživatel automaticky přesměrován, jsou schopny analyzovat jeho pohyb díky `referer` hlavičce, nebo parametrům vyskytujícím se v URL [18]. Při návštěvě stránky `a.com` může být uživatel bez jeho souhlasu automaticky přesměrován na stránku `track1.com`. Ta přesměrováním získává informace o pohybu uživatele. Dále může být uživatel ze stránky `track1.com` přesměrován na stránku `track2.com`, ze stránky `track2.com` na stránku `track3.com`. Tento řetězec pokračuje a každá ze stránek, na kterou byl uživatel přesměrován, získává informace o jeho pohybu po internetu. Nelze generalizovat a usoudit,

že každé HTTP přesměrování je pro uživatele škodlivé. Při sledování uživatele a narušení jeho soukromí má ale zneužití HTTP přesměrování pro sledovací prvky vysoký potenciál.

Průchody s využitím testovacích rozšíření prokazovaly výrazně rozdílné množství HTTP přesměrování. Procentuální pokles u individuálních rozšíření vypovídá o jejich schopnosti rozeznat a zablokovat nevyžádaná přesměrování, kterým je uživatel na stránkách vystaven. Nejnižší počet zaznamenaných HTTP přesměrování se vyskytl v průchodu při testování rozšíření AdBlocker Ultimate, a to o 64.79% méně než v porovnání s průchodem bez rozšíření. Množství přesměrování tak bylo sníženo o více než polovinu. Nejmenší pokles byl zaznamenán při využití rozšíření Ghostery, a to o 24.60% přesměrování méně. Nejméně efektivní rozšíření tak zablokovalo cca. čtvrtinu provedených přesměrování. Mimo tato rozšíření můžeme pozorovat výrazný rozdíl i mezi testovanými rozšířeními navzájem. Například rozšíření Adblock Plus a uBlock Origin podle testu vykazují podobné poklesy počtu přesměrování, a to o 54.73% a 46.70%. Rozšíření AdGuard AdBlocker se se svým výsledkem snížení požadavků o 44.71% pohybuje mezi rozšířeními uBlock Origin a Ghostery. Graf níže znázorňuje poměr počtu HTTP přesměrování provedených při použití jednotlivých rozšíření.




Obrázek 5.1: Graf znázorňující rozdíl počtu HTTP přesměrování při prohlížení stránky podle použitého rozšíření na bázi sledovacích prvků.

V průběhu návštěvy stránky v domácím prostředí a stejně tak pomocí průchodů nástroje *OpenWPM* se uživateli může pokaždé objevit jiná internetová reklama. Například při průchodu za využití rozšíření Ghostery byl nabízený reklamní obsah na právě navštívené stránce jiný, než při průchodu téže stránky s rozšířením uBlock Origin, přesto že byly průchody prováděny v úzkém časovém rozmezí. Jiný reklamní obsah může přímo vést k rozdílným přesměrováním, kterým je uživatel vystaven. To znamená, že v případě počtu provedených HTTP přesměrování není možné porovnávat konkrétní přesměrování.

Vyjádřením množství přesměrování v procentuálních poměrech mezi sebou vznikla tabulka 5.1. Z podstaty testu, který spočívá v pouhém navštívení stránky, lze usoudit, že nejefektivnější rozšíření musí být takové, které je schopné zabránit největšímu počtu přesměrování. I přes výrazný rozdíl v počtu zablokovaných přesměrování mezi rozšířeními Ad-

Blocker Ultimate a Ghostery byl internetový provoz v porovnání s průchodem bez rozšíření značně omezen. Z nasbíraných dat lze usoudit, že rozšíření AdBlocker Ultimate prokazuje nejlepší výsledky, avšak rozšíření AdBlock Plus a uBlock Origin zabránila porovnatelnému počtu HTTP přesměrování. Na druhou stranu rozšíření Ghostery se od ostatních vzorků výrazně liší. Rozšíření AdGuard Adblocker nevykazuje v tomto ohledu výraznou výhodu před ostatními testovanými rozšířeními.

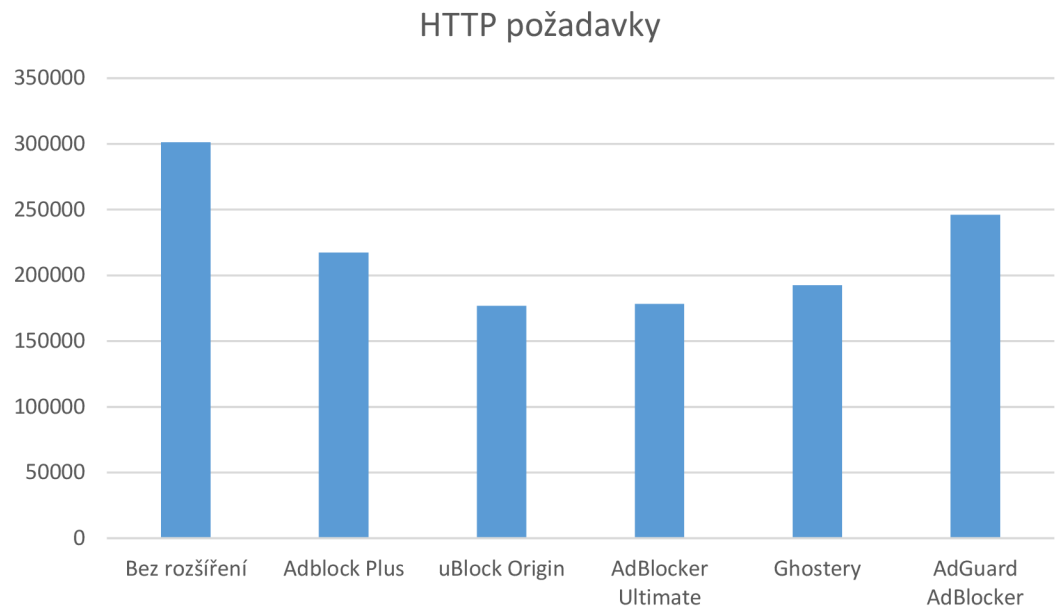
| | Bez rozšíření | AdBlock Plus | uBlock Origin | AdBlock Ultimate | Ghostery | AdGuard AdBlocker |
|---|---|---|---|---|---|---|
| Bez rozšíření | 0% | +120.90% | +87.61% | +184.04% | +32.63% | +80.87% |
| AdBlock Plus | -54.73% | 0% | -15.07% | +28.58% | -39.96% | -18.13% |
| uBlock Origin | -46.70% | +17.75% | 0% | +51.40% | -29.31% | -3.60% |
| AdBlock Ultimate | -64.79% | -22.22% | -33.95% | 0% | -53.31% | -36.32% |
| Ghostery | -24.60% | +66.56% | +41.46% | +114.17% | 0% | +36.37% |
| AdGuard AdBlocker | -44.71% | +22.14% | +3.73% | +57.05% | -26.67% | 0% |

Tabulka 5.1: Tabulka zobrazující procentuální změnu počtu HTTP přesměrování při použití testovaných rozšíření na bázi sledovacích prvků.

### HTTP požadavky

V případě HTTP požadavků se porovnávaná čísla výrazně odlišují. Zároveň se liší celkové výsledky provedených testů rozšíření. V tomto testu je počet zaslaných HTTP požadavků při nainstalování rozšíření uBlock Origin výrazně nižší, než v případě dalších testovaných rozšíření. Počet zaslaných HTTP požadavků je v porovnání s během bez rozšíření o 41.23% nižší. Rozšíření tak zablokovalo výrazné množství internetového provozu. Rozšíření AdBlocker Ultimate zabránilo porovnatelnému množství požadavků, jejich počet se snížil o 40.77%. Nejmenší procentuální rozdíl lze vidět při použití rozšíření AdGuard AdBlocker, a to o pouhých 26.89% méně. V porovnání s předchozím testem rozšíření Ghostery podalo výrazně lepší výsledek – počet HTTP požadavků při průchodu snížilo o 36.17%. Výsledek testu rozšíření AdBlock Plus předvídatelně vypovídá o méně výrazném zmenšení počtu HTTP požadavků, a to o 27.88%.

Na základě testu počtu provedených HTTP požadavků lze předpokládat, že všechny zablokované požadavky byly nevyžádané (viz. princip fungování seznamů blokovacích prvků 2.1). Nejefektivnějším rozšířením je tedy rozšíření, které zablokovalo nejvíce požadavků. Na rozdíl od prvního testu podle výsledků v této kategorii vítězí rozšíření uBlock Origin. V porovnání s předchozím výsledkem je zároveň výsledný procentuální rozdíl mnohem více znatelný. Rozšíření AdGuard AdBlocker vykazuje podobnou efektivitu při blokování nevyžádaných požadavků (rozdíl pouze 0.77% viz. 5.2). Efektivita rozšíření Ghostery oproti prvnímu testu značně stoupla. AdBlock Plus v druhém testu prokázal výrazně nižší efektivitu v porovnání s předchozím testem. Jedním z důvodů je program *Acceptable Ads* implementovaný rozšířením. V případě rozšíření AdGuard AdBlocker lze pozorovat stálý trend




Obrázek 5.2: Graf znázorňující rozdíl počtu provedených HTTP dotazů při prohlížení stránky podle použitého rozšíření na bázi sledovacích prvků.

v podobě nejmenší odchylky od průchodu bez nainstalovaných rozšíření, v tomto testu je však jeho výsledek porovnatelný s rozšířením AdBlock Plus. Tabulka 5.2 obsahuje porovnání procentuální změny počtu HTTP požadavků při použití testovaných rozšíření.

| | Bez rozšíření | AdBlock Plus | uBlock Origin | AdBlock Ultimate | Ghostery | AdGuard AdBlocker |
|---|---|---|---|---|---|---|
| Bez rozšíření | 0% | +38.66% | +70.12% | +68.82% | +56.67% | +36.78% |
| AdBlock Plus | -27.88% | 0% | +22.68% | +21.75% | +12.99% | -1.33% |
| uBlock Origin | -41.22% | -18.50% | 0% | -0.76% | -7.90% | -19.59% |
| AdBlock Ultimate | -40.77% | -17.86% | +0.77% | 0% | -7.20% | -18.98% |
| Ghostery | -36.17% | -11.50% | +8.58% | +7.75% | 0% | -12.70% |
| AdGuard AdBlocker | -26.89% | +1.37% | +24.37% | +23.42% | +14.54% | 0% |

Tabulka 5.2: Tabulka zobrazující procentuální změnu počtu HTTP požadavků při použití testovaných rozšíření na bázi sledovacích prvků.

Tabulka 5.3 zobrazuje průměrný počet zaslaných HTTP požadavků při využití testovaných rozšíření. Při průchodu po instalaci rozšíření uBlock Origin je průměrný počet zaslaných požadavků nejnižší. Stejně jako v případě počtu provedených HTTP přesměrování lze předpokládat, že čas pro načtení stránek a využití šířky pásma bude v tomto případě nejnižší. Na druhém místě se zanedbatelným rozdílem se umístilo rozšíření AdBlock Ultimate.

Naopak při použití rozšíření AdGuard AdBlocker je odchylka od průchodu bez nainstalovaného rozšíření výrazně méně znatelná. Průchody pro testování počtu provedených HTTP přesměrování a zaslaných HTTP požadavků byly prováděny na stejném vzorku vstupních dat. Vzhledem k poměru počtu přesměrování a požadavků lze odhadovat výraznější rozdíl při použití rozšíření v případě zasílání požadavků – efektivita jejich blokování má výraznější dopad na uživatelův požitek z prohlížení internetu, než v případě přesměrování. To se týká doby potřebné pro načtení stránky a využití šířky pásma při prohlížení.

| | **Celkový počet požadavků** | **Průměrný počet požadavků** |
|---|---|---|
| Bez rozšíření | 301 251 | 150.06 |
| AdBlock Plus | 217 407 | 109.67 |
| uBlock Origin | 176 864 | 89.40 |
| AdBlock Ultimate | 178 307 | 90.07 |
| Ghostery | 192 415 | 97.06 |
| AdGuard AdBlocker | 245 910 | 111.17 |

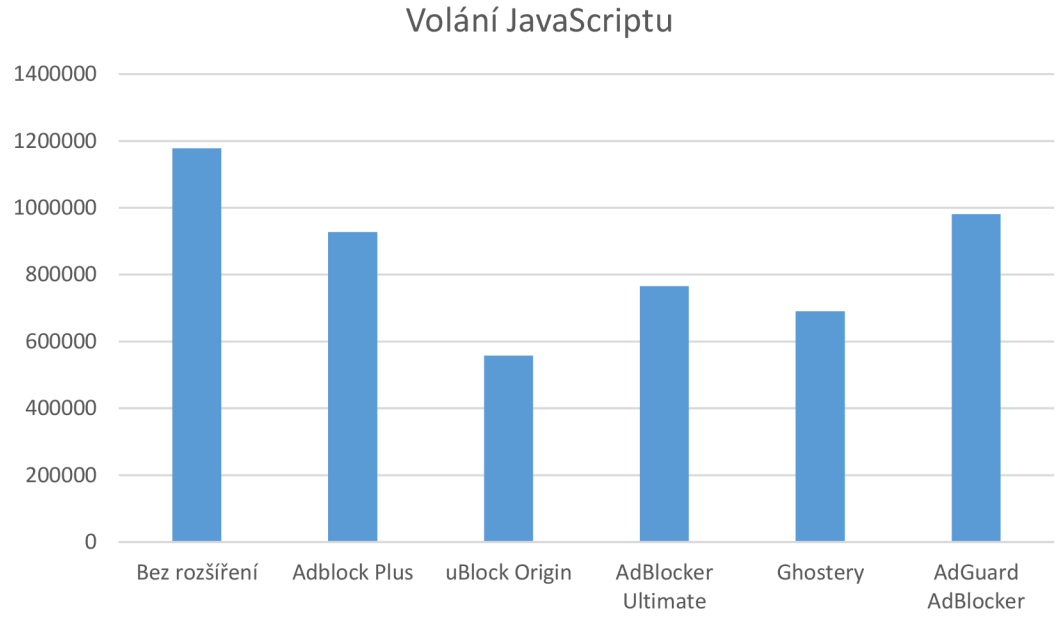
Tabulka 5.3: Tabulka zobrazující průměrný počet zaslaných HTTP požadavků při použití testovaných rozšíření na bázi sledovacích prvků.

### Volání JavaScriptových metod

Počet volání *JavaScriptových* metod je výrazně vyšší, než v případě počtu HTTP přesměrování a odpovědí. Největšímu počtu volání zabránilo rozšíření uBlock Origin. Při průchodu s využitím tohoto rozšíření se počet volání oproti průchodu bez rozšíření snížil o 52.64%. Druhé místo patří rozšíření Ghostery. Počet volání snížilo o 41.39%. Efektivnost rozšíření AdBlock Ultimate byla v tomto testu nižší, než v případě testů předchozích – rozšíření snížilo počet volání o 35.02%. Poslední dvě testovaná rozšíření AdBlock Plus a AdGuard AdBlocker snížila počet volání o 21.29% a 16.66%.

Tabulka 5.4 zobrazuje procentuální rozdíl změny počtu *JavaScriptových* volání při použití testovaných rozšíření. Efektivita rozšíření uBlock Origin je v tomto ohledu velice vysoká. Při použití rozšíření Ghostery, které se v testu umístilo na druhém místě, bylo voláno v porovnání s rozšířením uBlock Origin o 23.74% více *JavaScriptových* metod. Rozdíl mezi prvním a druhým místem je tedy v tomto testu více výrazný. Dále při testování klesla efektivita rozšíření AdBlock Ultimate – počet *JavaScriptových* volání byl při jeho použití navýšen o 37.19% oproti průchodu s rozšířením uBlock Origin. Poslední dvě rozšíření podala porovnatelný výsledek. Rozdíl v počtu volání při použití rozšíření AdBlock Plus a AdGuard AdBlocker je pouze 5.87%.

Tabulka 5.5 zobrazuje průměrný počet volání *JavaScriptových* metod na stránku při průchodech s nainstalovaným rozšířením. Metody *JavaScriptu* mohou být neškodné, jako dynamická aktualizace stránky (například přidání předmětu do košíku uživatele v internetovém obchodě), lze je ale využít i pro uživateli potenciálně nebezpečné účely (*fingerprinting*, pro-




Obrázek 5.3: Graf znázorňující rozdíl počtu volání *JavaScriptových* metod při prohlížení stránky podle použitého rozšíření na bázi sledovacích prvků.

| | Bez rozšíření | AdBlock Plus | uBlock Origin | AdBlock Ultimate | Ghostery | AdGuard AdBlocker |
|---|---|---|---|---|---|---|
| Bez rozšíření | 0% | +27.05% | +111.15% | +53.90% | +70.63% | +20.00% |
| AdBlock Plus | -21.29% | 0% | +66.19% | +21.14% | +34.30% | -5.55% |
| uBlock Origin | -52.64% | -39.83% | 0% | -27.11% | -19.19% | -43.17% |
| AdBlock Ultimate | -35.02% | -17.45% | +37.19% | 0% | +10.87% | -22.03% |
| Ghostery | -41.39% | -25.54% | +23.74% | -9.80% | 0% | -29.67% |
| AdGuard AdBlocker | -16.67% | +5.87% | +75.95% | +28.25% | +42.19% | 0% |

Tabulka 5.4: Tabulka zobrazující procentuální změnu počtu instancí volání *JavaScriptových* metod při použití testovaných rozšíření na bázi sledovacích prvků.

filování). V obou případech zabírá jejich volání výpočetní čas a zpomaluje tak uživatelovo zařízení. Žádná z testovaných rozšíření této kategorie by neměla zásadně negativně omezit funkcionalitu navštěvovaných stránek.

| | Celkový počet volání | Průměrný počet volání |
|---|---|---|
| Bez rozšíření | 1 178 025 | 589.01 |
| AdBlock Plus | 927 210 | 463.61 |
| uBlock Origin | 557 917 | 278.96 |
| AdBlock Ultimate | 765 433 | 382.72 |
| Ghostery | 690 389 | 345.19 |
| AdGuard AdBlocker | 981 677 | 490.84 |

Tabulka 5.5: Tabulka zobrazující průměrný počet provedených *JavaScriptových* volání při použití testovaných rozšíření na bázi sledovacích prvků.

### Ukládání dat cookies

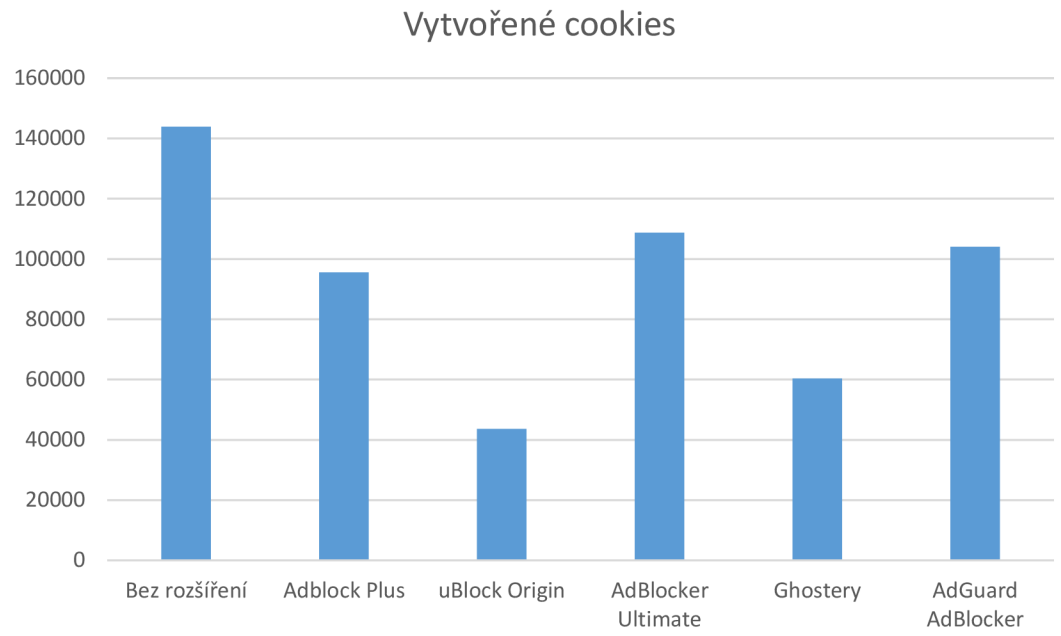
Nejmenší počet souborů *cookies* byl na straně uživatele uložen při použití rozšíření uBlock Origin, a to o 69.65% méně než v porovnání s průchodem bez nainstalovaných rozšíření. Rozšíření Ghostery zmenšilo počet uložených *cookies* o 58.03%. Ostatní testovaná rozšíření v porovnání neprojevila podobně vysokou efektivitu. Při průchodu s rozšířením AdBlock Plus se počet *cookies* zmenšil o 33.59%. V případě rozšíření AdGuard AdBlocker se číslo zmenšuje na 27.66%. Překvapivý výsledek podalo rozšíření AdBlocker Ultimate – počet uložených *cookies* se jeho použitím snížil o pouhých 24.37%.

Tabulka 5.6 znázorňuje porovnání testovaných rozšíření s ohledem na uložené *cookies* na straně uživatele. V tomto testu lze pozorovat zatím nejvýraznější procentuální rozdíl mezi rozšířením na prvním místě a rozšířením na místě posledním. Při použití rozšíření AdBlock Ultimate vzroste počet vytvořených *cookies* o 149.23% v porovnání s rozšířením uBlock Origin. Zároveň se jedná o první test této kategorie rozšíření, ve kterém podal AdBlock Ultimate tak slabý výsledek. V případě Ghostery se počet uložených *cookies* v porovnání s vítězem testu zvýší o 38.29%. Rozšíření AdBlock Plus a AdBlocker Ultimate neprokázala výraznou efektivitu v blokování ukládání *cookies* v porovnání s ostatními rozšířeními.

Počet uložených *cookies* a jejich průměrný počet na stránku je zobrazen v tabulce 5.7. V případě reálného prohlížení internetu by byl počet *cookies* nejspíše výrazně menší. Při testu se totiž při každé návštěvě jednalo o návštěvu první, počet *cookies* byl tedy vyšší, než při opětovném navštěvování stránky v domácím prostředí.

### Závěr testu rozšíření na bázi seznamu sledovacích prvků

V testované kategorii rozšíření se podle výsledků dá usoudit, že v případě blokování nevyžádaných HTTP přesměrování je nejefektivnějším rozšířením AdBlocker Ultimate. V porovnání s rozšířením na druhém místě tohoto testu, AdBlock Plus, proběhlo při průchodu o 22.14% přesměrování méně. Rozdíl mezi prvním a druhým místem v testu je tedy velice výrazný. Na druhou stranu rozšíření Ghostery v prvním testu zablokovalo nejmenší




Obrázek 5.4: Graf znázorňující rozdíl počtu uložených dat *cookies* při prohlížení stránky podle použitého rozšíření na bázi sledovacích prvků.

| | Bez rozšíření | AdBlock Plus | uBlock Origin | AdBlock Ultimate | Ghostery | AdGuard AdBlocker |
|---|---|---|---|---|---|---|
| Bez rozšíření | 0% | +50.57% | +229.52% | +32.22% | +70.63% | +20.00% |
| AdBlock Plus | -33.59% | 0% | +118.84% | -12.19% | +34.30% | -5.55% |
| uBlock Origin | -69.65% | -54.31% | 0% | -59.88% | -19.19% | -43.17% |
| AdBlock Ultimate | -24.37% | +13.88% | +149.23% | 0% | +10.87% | -22.03% |
| Ghostery | -58.03% | -36.81% | +38.29% | -44.51% | 0% | -29.67% |
| AdGuard AdBlocker | -27.66% | +8.93% | +75.95% | -4.35% | +42.19% | 0% |

Tabulka 5.6: Tabulka zobrazující procentuální změnu počtu vytvořených *cookies* při použití testovaných rozšíření na bázi sledovacích prvků.

počet přesměrování – v porovnání s rozšířením na prvním místě zabránilo o 53.20% méně přesměrováním.

Rozšířením, které nejspolehlivěji rozeznává nevyžádané HTTP požadavky, je uBlock Origin. Rozdíl mezi rozšířeními na prvním a druhém místě tohoto testu je však výrazně menší, než v případě testu prvního. AdBlocker Ultimate zabránil provedení pouze o 0.81% méně HTTP požadavků, než uBlock Origin. Díky nestálé povaze internetového provozu je takový rozdíl statisticky nevýznamný. Nejslabší výkon lze pozorovat u rozšíření AdGuard AdBlocker. Počty zaslaných HTTP dotazů jsou výrazně vyšší, než pro jakékoli jiné rozšíření.

| | **Celkový cookies volání** | **Průměrný počet cookies** |
|---|---|---|
| Bez rozšíření | 143 824 | 71.91 |
| AdBlock Plus | 95 519 | 47.76 |
| uBlock Origin | 43 647 | 21.82 |
| AdBlock Ultimate | 108 780 | 54.39 |
| Ghostery | 60 358 | 30.18 |
| AdGuard AdBlocker | 104 047 | 52.02 |

Tabulka 5.7: Tabulka zobrazující průměrný počet uložených *cookies* při použití testovaných rozšíření na bázi sledovacích prvků.

Z tabulek i grafů lze na první pohled vidět jeho nízkou efektivitu v porovnání s ostatními testovanými rozšířeními.

Nejvíce volání *JavaScriptových* metod zablokovalo rozšíření uBlock Origin. Rozšíření Ghostery se v tomto ohledu umístilo na druhém místě, ale v předchozích testech nepodalo uspokojivý výsledek. AdBlock Plus podle očekávání zabránilo malému počtu *JavaScriptových* volání, stejně jako rozšíření AdGuard AdBlocker.

Počet uložených *cookies* na straně uživatele v porovnání s průchodem bez rozšíření kupodivu nejméně ovlivnilo rozšíření AdBlocker Ultimate, které v předchozích testech vykazovalo vysokou efektivitu. Onen výsledek je nejhorší z testovaných rozšíření této kategorie. Rozšíření tak při jeho využití umožňuje *cookies* zabírat nejvíce diskového místa ze všech. Výsledkem porovnání kategorie **rozšíření na bázi seznamu sledovacích prvků** je shrnutí pro uživatele:

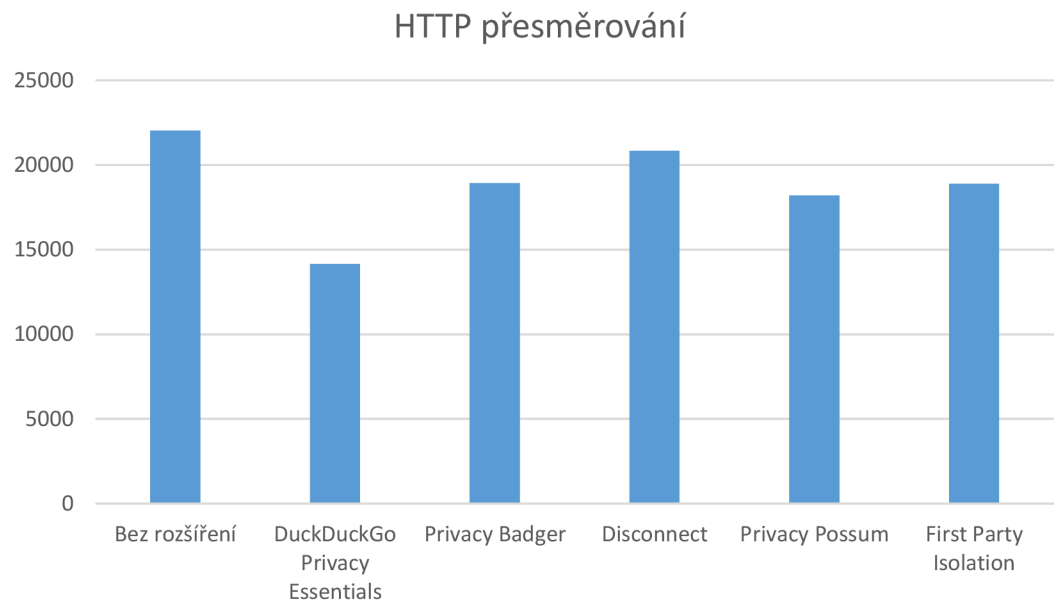
- všechna rozšíření byla testována ve stavu ihned po instalaci bez další konfigurace.
- nejefektivnějším rozšířením pro omezení nevyžádaného internetového provozu je **AdBlocker Ultimate**.
- rozšíření **uBlock Origin** prokazuje lepší efektivitu v blokování nevyžádaných HTTP dotazů, ale **AdBlocker Ultimate** rozezná více nevyžádaných HTTP přesměrování.
- **uBlock Origin** prokázal nejvyšší efektivitu v rozeznání a zablokování nevyžádaných volání *JavaScriptových* metod.
- stejně tak **uBlock Origin** rozeznal nejvíce škodlivých souborů *cookies* a zabránil jejich uložení v zařízení uživatele.
- rozříření **AdBlocker Ultimate** vykazuje **velice nízkou** efektivitu v zabránění uložení *cookies* v zařízení uživatele.
- ostatní testovaná rozšíření nevykazují podobnou efektivitu a jsou ve výsledku **méně efektivní**, než rozšíření předchozí.

## 5.2 Testování rozšíření blokujících sledovací prvky

Při testování kategorie rozšíření blokující sledovací prvky bylo postupováno podle návrhu v části 4.3 práce. Při sběru dat bylo využito instrumentace `http_instrument` pro zaznamenání HTTP přesměrování a požadavků, `js_instrument` pro sběr dat o provedených voláních *JavaScriptových* metod a instrumentace `cookie_instrument` pro zaznamenání ukládání dat *cookies* do zařízení uživatele. Data vytvořená nástrojem *OpenWPM* byla zpracována pomocí jednoduchého *SQL* skriptu. Výsledné hodnoty byly promítnuty do grafů a zpracovány do přehledných tabulek.

### HTTP přesměrování

Účelem rozšíření této skupiny není blokovat reklamní obsah nabízený na navštívených stránkách. Celkové množství provedených HTTP přesměrování pro všechna testovaná rozšíření je tedy vyšší, než v případě předchozí skupiny. Nicméně je pro lepší porovnání vhodné využití stejné metriky. Nejvýraznějšímu počtu HTTP přesměrování v testu zabránilo rozšíření DuckDuckGo Privacy Essentials. Při jeho použití se počet přesměrování snížil o 35.73%. V ostatních případech nebyly počty přesměrování tak výrazně odlišné od průchodu bez rozšíření. Druhé nejefektivnější rozšíření je Privacy Possum, které snížilo počet přesměrování o 17.37%. Rozšíření First Party Isolation, Privacy Badger a Disconnect redukovala počet HTTP přesměrování o 14.23%, 14.10% a 5.42%.




Obrázek 5.5: Graf znázorňující rozdíl počtu HTTP přesměrování při prohlížení stránky podle použitého rozšíření pro blokování sledovacích prvků.

Pomocí tabulky 5.8 lze mezi sebou porovnat efektivitu rozšíření blokovat HTTP přesměrování. Oproti rozšíření DuckDuckGo Privacy Essentials zabránila rozšíření velmi malému počtu přesměrování. Mezi rozšířením na prvním místě a Privacy Badger na místě druhém je výrazný rozdíl 33.67%. Průchody s ostatními testovanými rozšířeními se výrazně neliší od sebe a od průchodu bez nainstalovaného rozšíření.

| | Bez rozšíření | DDGo PE | Privacy Badger | Disconnect | Privacy Possum | FP Isolation |
|---|---|---|---|---|---|---|
| Bez rozšíření | 0% | +55.61% | +16.41% | +5.73% | +21.02% | +16.60% |
| DDGo PE | -35.74% | 0% | -25.19% | -32.10% | -22.23% | -25.07% |
| Privacy Badger | -14.10% | +33.67% | 0% | -9.18% | +3.96% | +0.16% |
| Disconnect | -5.42% | +47.18% | +10.10% | 0% | +14.46% | +10.27% |
| Privacy Possum | -17.37% | +28.58% | +3.81% | -12.64% | 0% | -3.66% |
| FP Isolation | -14.23% | +33.46% | -0.16% | -9.32% | +3.80% | 0% |

Tabulka 5.8: Tabulka zobrazující procentuální změnu počtu provedených HTTP přesměrování při použití testovaných rozšíření pro blokování sledovacích prvků.

### HTTP požadavky

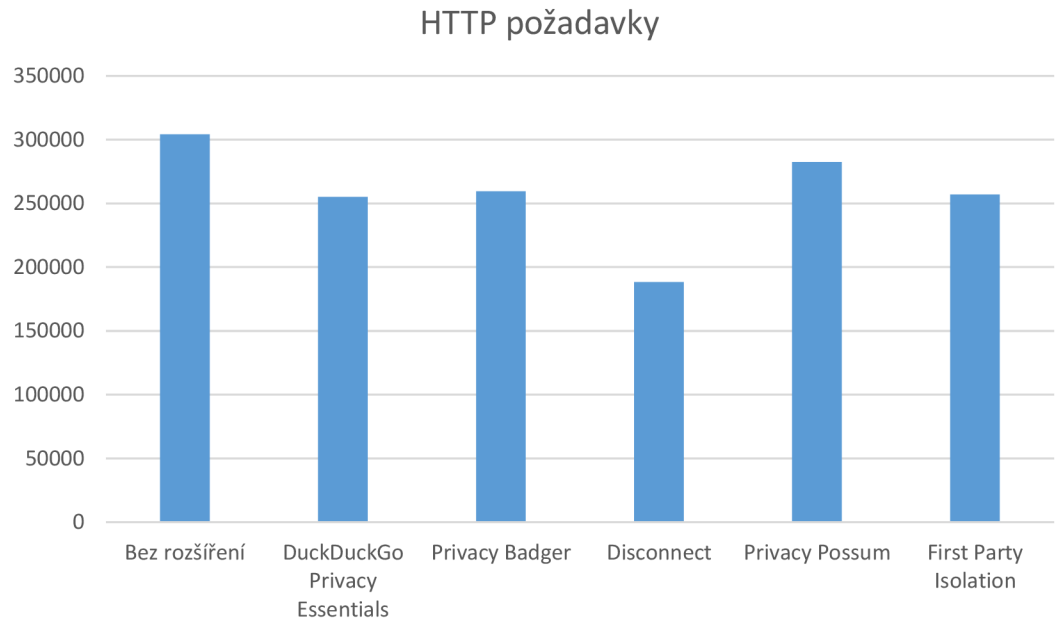
Stejně jako v případě HTTP přesměrování je počet zaslaných HTTP požadavků vyšší, než v případě první kategorie rozšíření. Důvodem je opět fakt, že primárním účelem rozšíření této kategorie není blokovat reklamní obsah. Největší množství zaslaných HTTP požadavků zablokovalo rozšíření Disconnect, a to o 38.06% méně v porovnání s průchodem bez využití rozšíření. Snížení za použití ostatních testovaných rozšíření je výrazně nižší, než v případě první kategorie rozšíření. Na druhém místě je rozšíření DuckDuckGo Privacy Essentials, které počet odpovědí redukovalo o 16.14%. Ostatní testovaná rozšíření ale zabránila podobnému počtu HTTP požadavků – Privacy Badger, First Party Isolation a Privacy Possum snížily počet požadavků o 15.51%, 14.67% a 7.11%.

Tabulka 5.9 porovnává efektivitu rozšíření v blokování HTTP požadavků. Pouze v případě rozšíření Disconnect je rozdíl od ostatních testovaných rozšíření výrazný. Při použití DuckDuckGo Privacy Essentials, které skončilo v tomto testu na druhém místě, se počet zaslaných HTTP požadavků zvýší o 31.77%. V případě rozšíření na místě třetím, First Party Isolation, vzroste počet o pouhých 0.74%. Podobný výsledek podala i ostatní testovaná rozšíření.

Tabulka 5.10 znázorňující průměrný počet zaslaných HTTP požadavků na stránku ukazuje, že mimo rozšíření Disconnect neredukují rozšíření této kategorie šířku pásma využitého pro nevyžádaný obsah tak výrazně, jako rozšíření kategorie předchozí. Dá se tedy usoudit, že v otázce zmenšení nevyžádaného internetového provozu je pro uživatele lepší využít rozšíření předchozí testované kategorie.

### Volání JavaScriptových metod

Počty volání *JavaScriptových* metod v průběhu průchodů jsou výrazně vyšší, než počty provedených HTTP přesměrování a zaslaných HTTP požadavků. Při průchodu stránek po nainstalování rozšíření Disconnect lze pozorovat nejvýraznější snížení počtu instancí volání *JavaScriptových* metod, a to o 39.62% méně, než při průchodu bez nainstalovaných rozšíření. Na druhém místě v testu počtu zablokovaných volání metod se umístilo rozšíření




Obrázek 5.6: Graf znázorňující rozdíl počtu zaslaných HTTP požadavků při prohlížení stránky podle použitého rozšíření pro blokování sledovacích prvků.

| | Bez rozšíření | DDGo PE | Privacy Badger | Disconnect | Privacy Possum | FP Isolation |
|---|---|---|---|---|---|---|
| Bez rozšíření | 0% | +19.25% | +17.19% | +61.45% | +7.65% | +18.37% |
| DDGo PE | -16.14% | 0% | -1.73% | +35.39% | -9.72% | -0.74% |
| Privacy Badger | -14.67% | +1.76% | 0% | +37.77% | +3.96% | +1.00% |
| Disconnect | -38.06% | -26.13% | -27.42% | 0% | +14.46% | -26.67% |
| Privacy Possum | -7.11% | +10.77% | +8.86% | +49.97% | 0% | +9.95% |
| FP Isolation | -15.52% | +0.74% | -1.00% | +36.40% | -9.05% | 0% |

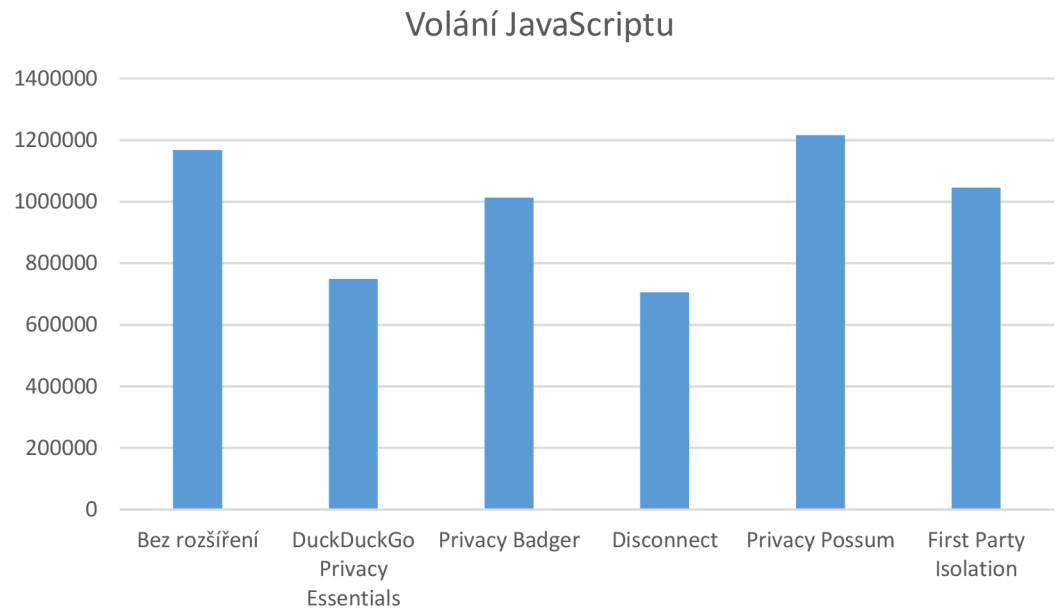
Tabulka 5.9: Tabulka zobrazující procentuální změnu počtu zaslaných HTTP požadavků při použití testovaných rozšíření pro blokování sledovacích prvků.

DuckDuckGo Privacy Essentials, při jeho použití se počet volání snížil o 35.89%. Rozšíření Privacy Badger a First Party Isolation podala v tomto testu podobné výsledky – při průchodu se počet volání *JavaScriptových* metod na stránkách snížil o 13.25% a 10.46%. Oproti předchozím rozšířením lze pozorovat výrazný procentuální rozdíl. Zajímavý výsledek podalo rozšíření Privacy Possum, počet volání metod se zvýšil o 4.13%. Důvodem je princip boje proti sledování uživatele, které rozšíření implementuje. Privacy Possum podvrhuje data, která je možné získat a využít pro tvorbu *fingerprintu* prohlížeče uživatele. Při volání po-

| | Celkový počet požadavků | Průměrný počet požadavků |
|---|---|---|
| Bez rozšíření | 304 132 | 152.07 |
| DDGo PE | 255 044 | 127.52 |
| Privacy Badger | 259 528 | 129.76 |
| Disconnect | 188 376 | 94.12 |
| Privacy Possum | 282 511 | 141.26 |
| FP Isolation | 256 941 | 128.47 |

Tabulka 5.10: Tabulka zobrazující průměrný počet zaslaných HTTP požadavků při použití testovaných rozšíření pro blokování sledovacích prvků.

tenciálně *fingerprintujícího* skriptu přidává vlastní volání za účelem zmatení trackerů (viz. 2.2, rozšíření Privacy Possum).




Obrázek 5.7: Graf znázorňující rozdíl počtu volání *JavaScriptových* metod při prohlížení stránky podle použitého rozšíření pro blokování sledovacích prvků.

Při procentuálním porovnání efektivnosti rozšíření blokovat volání *JavaScriptových* metod vznikla tabulka 5.11. Rozšíření Disconnect zabránilo nejvyššímu počtu volání metod. Při průchodu s rozšířením DuckDuckGo Privacy Essentials bylo provedeno o 6.18% volání více, efektivita těchto dvou rozšíření je tedy srovnatelná. Rozdíl v počtu volání metod při použití rozšíření Privacy Badger a First Party Isolation jsou pouhá 3.21%, výrazně

se ale odlišují od předchozích rozšíření. Rozšíření Privacy Possum dokonce navýšilo počet provedených *JavaScriptových* metod vůči stavu bez rozšíření.

| | Bez rozšíření | DDGo PE | Privacy Badger | Disconnect | Privacy Possum | FP Isolation |
|---|---|---|---|---|---|---|
| Bez rozšíření | 0% | +55.97% | +15.27% | +65.61% | -3.96% | +11.69% |
| DDGo PE | -35.89% | 0% | -26.09% | +6.18% | -38.43% | -28.39% |
| Privacy Badger | -13.25% | +35.30% | 0% | +43.67% | -16.69% | -3.11% |
| Disconnect | -40.81% | -5.82% | -30.39% | 0% | -42.01% | -32.56% |
| Privacy Possum | +4.13% | +62.42% | +20.04% | +72.45% | 0% | +16.30% |
| FP Isolation | -10.46% | +39.65% | +3.21% | +48.28% | -14.02% | 0% |

Tabulka 5.11: Tabulka zobrazující procentuální změnu počtu volání *JavaScriptových* metod při použití testovaných rozšíření pro blokování sledovacích prvků.

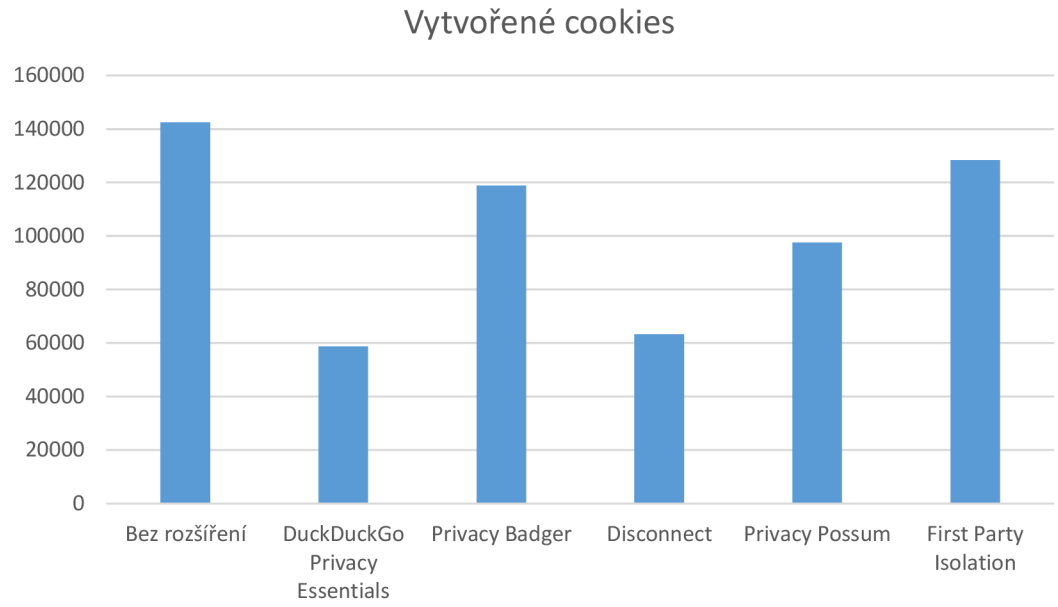
Tabulka 5.12 zobrazuje průměrný počet volání *JavaScriptových* metod na stránku při průchodu s nainstalovaným testovaným rozšířením. Volání metod se projeví při zatížení CPU při jejich vykonání. Menší počet volání tedy pozitivně ovlivní výpočetní čas potřebný pro načtení každé stránky. Rozšíření Disconnect vyžadovalo v testu nejmenší množství výpočetního času, zatímco rozšíření Privacy Possum oproti průchodu bez nainstalovaného rozšíření přidalo marginální výpočetní čas potřebný k prohlížení. Při pohybu po internetu by nebyl rozdíl na individuální stránce pro uživatele znatelný, pro značný vzorek průchodů ale bude mít rozšíření negativní dopad na využití CPU.

| | **Celkový počet volání** | **Průměrný počet volání** |
|---|---|---|
| Bez rozšíření | 1 167 738 | 583.87 |
| DDGo PE | 748 674 | 374.34 |
| Privacy Badger | 1 013 007 | 506.50 |
| Disconnect | 705 102 | 352.56 |
| Privacy Possum | 1 215 975 | 607.99 |
| FP Isolation | 1 045 543 | 522.77 |

Tabulka 5.12: Tabulka zobrazující průměrný počet provedených *JavaScriptových* volání při použití testovaných rozšíření pro blokování sledovacích prvků.

### Ukládání dat cookies

Počet *cookies* omezených rozšířením vyjadřuje schopnost rozšíření rozeznávat a blokovat nevyžádané soubory *cookies*. V tomto testu se nejvýrazněji projevilo rozšíření DuckDuckGo Privacy Essentials, počet uložených *cookies* snížilo o 58.77%. Porovnatelné množství *cookies* zablokovalo rozšíření Disconnect – při jeho použití byl počet vytvořených *cookies* o 55.58% nižší v porovnání s průchodem bez nainstalovaných rozšíření. Ostatní testovaná rozšíření nezabránila stejně výraznému počtu uložených *cookies*. Použitím Privacy Possum vzniklo v zařízení uživatele o 31.56% méně *cookies*, v případě Privacy Badger se procento snižuje na 16.58%. Nejmenší počet *cookies* zablokovalo rozšíření First Party Isolation, a to o pouhých 9.99% méně v porovnání s průchodem bez rozšíření.




Obrázek 5.8: Graf znázorňující rozdíl počtu uložených dat *cookies* při prohlížení stránky podle použitého rozšíření pro blokování sledovacích prvků.

Porovnáním efektivity rozšíření blokovat nevyžádané *cookies* v procentech vznikla tabulka 5.13. Můžeme pozorovat podobnou efektivitu rozšíření DuckDuckGo Privacy Essentials a Disconnect, množství uložených *cookies* při použití Disconnect je o pouhých 7.74% vyšší. Ostatní rozšíření prokazují efektivitu výrazně nižší. Mezi třetím a čtvrtým rozšířením – Privacy Possum a Privacy Badger – je znatelný rozdíl zvýšení počtu *cookies* o 21.88%. Rozšíření First Party Isolation nevykazuje výraznou efektivitu v blokování nevyžádaných *cookies*. Důvodem může být pouze občasná aktualizace ze strany autora.

Tabulka 5.14 zobrazuje průměrný počet uložení *cookies* na stránku v závislosti na testovaném rozšíření. *Cookies* umožňují trackerům například vytvořit unikátní identifikátor uživatele a spojovat tak informace o jeho pohybu po internetu. Tyto informace mohou být následně využité pro retargeting[1] a tvorbu behaviorálních profilů [31]. Zabírají diskový prostor v zařízení uživatele a negativně jej tak ovlivňují.

[1]Strategie provozovatelů e-shopů cílená na uživatele, kteří e-shop navštívili, ale neuskutečnili nákup. Samotná návštěva dává reklamním společnostem možnost tvorby profilu k vytvoření behaviorální reklamy za účelem uživatele přimět k nákupu [31].

| | Bez rozšíření | DDGo PE | Privacy Badger | Disconnect | Privacy Possum | FP Isolation |
|---|---|---|---|---|---|---|
| Bez rozšíření | 0% | +142.57% | +19.88% | +125.14% | +46.12% | +11.09% |
| DDGo PE | -58.77% | 0% | -50.58% | -7.18% | -39.76% | -54.20% |
| Privacy Badger | -16.58% | +102.35% | 0% | +87.81% | +21.88% | -7.33% |
| Disconnect | -55.58% | +7.74% | -46.75% | 0% | -35.10% | -50.66% |
| Privacy Possum | -31.56% | +66.00% | -17.95% | +54.08% | 0% | -23.97% |
| FP Isolation | -9.99% | +118.35% | +7.91% | +102.66% | +31.53% | 0% |

Tabulka 5.13: Tabulka zobrazující procentuální změnu počtu vytvořených *cookies* při použití testovaných rozšíření pro blokování sledovacích prvků.

| | **Celkový počet uložených cookies** | **Průměrný počet cookies** |
|---|---|---|
| Bez rozšíření | 142 543 | 71.27 |
| DDGo PE | 58 764 | 29.38 |
| Privacy Badger | 118 906 | 59.45 |
| Disconnect | 63 313 | 31.66 |
| Privacy Possum | 97 552 | 48.78 |
| FP Isolation | 128 309 | 64.15 |

Tabulka 5.14: Tabulka zobrazující průměrný počet uložených *cookies* při použití testovaných rozšíření pro blokování sledovacích prvků.

### Závěr testu rozšíření blokujících sledovací prvky

V ohledu počtu blokování HTTP přesměrování a dotazů neprokázala rozšíření této kategorie v testu vyšší efektivitu, než rozšíření kategorie první. Tento výsledek je očekávaný, testovaná rozšíření blokující sledovací prvky se nesoustředí na blokování reklam, které tvoří výraznou část internetového provozu.

Při testu počtu instancí volání *JavaScriptových* metod můžeme pozorovat nejlepší výsledky u rozšíření Disconnect. Při využití rozšíření DuckDuckGo Privacy Essentials, které v testu skončilo na druhém místě, se počet volání metod zvýšil o pouhých 6.18%. Rozšíření tedy v tomto ohledu podala srovnatelně kvalitní výsledek. Na druhou stranu použitím rozšíření Privacy Possum se počet volání zvýšil o 4.18% oproti průchodu bez nainstalovaných rozšíření. Tento způsob boje proti profilování je z principu velice účinný, ale oproti

jednoduché blokaci metod výpočetně náročnější. Rozšíření Privacy Badger a First Party Isolation v testu neprokázala výraznou efektivitu v blokování potenciálně nebezpečných *JavaScriptových* metod.

Výsledky v případě počtu uložených *cookies* při prohlížení jsou velice podobné. Největší rozdíl v porovnání s průchodem bez nainstalovaných rozšíření nastal při využití rozšíření DuckDuckGo Privacy Essentials. V porovnání s předchozím testem byl procentuální rozdíl v hodnotách velmi výrazný – při průchodu bez rozšíření na prvním místě se počet uložených *cookies* zvýšil o 142.57%. Rozšíření Disconnect podalo v tomto testu obdobný výsledek. Při jeho využití se oproti rozšíření na prvním místě zvýšil počet uložených *cookies* o pouhých 7.74%. Ostatní testovaná rozšíření počet *cookies* oproti průchodu bez nich neredukovala tak výrazně. Nejméně markantní rozdíl lze opět pozorovat při využití rozšíření First Party Isolation. Závěrem tohoto testu je následující shrnutí pro uživatele:

- všechna rozšíření byla testována ve stavu ihned po instalaci bez další konfigurace.
- rozšíření této kategorie byla výrazně méně efektivní v otázce blokování HTTP přesměrování a požadavků. Pokud má uživatel zájem snížit využití šířky pásma, které reklamní obsah zabírá nebo celkového zpřehlednění a zpříjemnění prohlížení internetu, měl by využít některého rozšíření první testované kategorie.
- v případě rozeznání a blokování potenciálně nebezpečných volání *JavaScriptových* metod projevilo nejvyšší efektivitu rozšíření **Disconnect**, efektivita rozšíření **DuckDuckGo Privacy Essentials** je v tomto ohledu srovnatelná.
- v počtu zablokovaných nevyžádaných *cookies* podalo nejlepší výsledky rozšíření **DuckDuckGo Privacy Essentials**, efektivita rozšíření **Disconnect** je v tomto ohledu obdobná.
- efektivita ostatních rozšíření byla v obou ohledech nižší.
- za zmínku stojí přístup k boji proti profilování uživatele, který implementuje rozšíření **Privacy Possum**. Uživateli může výše zmíněný mechanismus vyhovovat více, než pouhé blokování nevyžádaného spustitelného obsahu. Na druhou stranu ale může dojít k šíření podvržených nepravdivých informací, které může být pro uživatele nevyžádané.
- ve výsledku je efektivita rozšíření **Disconnect** a **DuckDuckGo Privacy Essentials** stejně vysoká oproti ostatním testovaným rozšířením. Při výběru může uživatel brát v potaz internetový vyhledávač zdarma, který **DuckDuckGo Privacy Essentials** nabízí.

## 5.3 Testování rozšíření blokujících spustitelný webový obsah

Rozšíření poslední testované skupiny se od sebe zásadně liší v ohledu funkcionality ihned po jejich nainstalování. I když ohledem na princip boje proti narušení bezpečnosti a soukromí implementují podobné metody a lze je zařadit do stejné kategorie, jejich provedení se od sebe výrazně odlišuje.

Rozšíření NoScript při prvotním nastavení blokuje všechna volání *JavaScriptových* metod. To znamená i volání metod první strany – navštěvované stránky. Zbavuje tak stánku

možnosti chovat se dynamicky. Na druhou stranu kompletně eliminuje možnost *fingerprintování* uživatele využitím *JavaScriptových* volání. Při jeho použití je tedy pravděpodobné, že funkcionalita navštěvované stránky bude zásadně narušena. Tento fakt může být nežádoucí zejména pro méně zkušené uživatele a pravděpodobně zásadně negativně ovlivní jejich požitek z prohlížení internetu. Nicméně je pomocí GUI rozšíření poměrně jednoduché volání *JavaScriptových* metod povolit. Rozšíření zobrazuje všechny domény, ze kterých jsou metody volány a dovoluje individuálně přidat zvolenou doménu na seznam domén, kterým uživatel důvěřuje.

Druhé rozšíření uMatrix ihned po instalaci blokuje všechna volání *JavaScriptových* metod, které nepochází z domény první strany. Funkcionalita stránky by tedy měla být ve velké míře zachována, uživatel ovšem není chráněn před voláním *fingerprintujích JavaScriptových* metod první strany. Pomocí GUI rozšíření lze nastavení pro každou doménu přítomnou na stránce upravit. Konfigurace není obtížná, ale pro většinového uživatele může být GUI rozšíření uMatrix velmi matoucí. V původní konfiguraci totiž nabízí uživateli i například možnost zakázat načtení obrázků nebo kaskádových stylů. Ve výsledku načtená stránka ztrácí svůj očekávaný vzhled.

JavaScript Restrictor v základní konfiguraci až na výjimky neblokuje žádná volání *JavaScriptových* metod. Rozlišuje potenciálně škodlivá volání a znemožní skriptu zjistit požadované informace. Místo blokování *JavaScriptových* metod v mnoha případech tedy přidává vlastní volání, kterým znemožní sbírat přesné informace o uživateli. Ve výsledku může proběhnout při náštěvě stránky více volání *JavaScriptu*, než bez rozšíření JavaScript Restrictor. Tento způsob ochrany přináší pohodlí uživateli, který nemusí zkoumat individuální domény nacházející se na navštívené stránce a obsah, který poskytují. Místo toho může uživatel jednoduše změnit úroveň ochrany kliknutím na tlačítko v GUI rozšíření. Funkce úrovně ochrany, které JavaScript Restrictor nabízí, byly popsány v kapitole 2.2.

Před popsáním výsledku testu je nutno zmínit, že při průchodu stránek v domácím prostředí (každodenní prohlížení internetu) narazí uživatel na stránky obsahující mnoho dalších připojených domén třetích stran. Stránky využité k testu často testují schopnost rozšíření zamezit *fingerprintování* uživatele výhradně využitím skriptů prvních stran. Výsledek testu je tedy značně zkreslený a spíše orientační za účelem demonstrace míry efektivnosti rozšíření v blokování spustitelného obsahu.

### AmIUnique

Stránka *AmIUnique* nabízí test *fingerprintu* prohlížeče pouze za využití skriptů domény první strany. Rozšíření NoScript a uMatrix mohou tedy volání metod pouze povolit, nebo zakázat. Tabulka 5.15 zobrazuje informace, které stránka *AmIUnique* zjistila o uživateli použitím *fingerprintujících* skriptů. Pro porovnání byly vybrány informace, které při průchodu bez rozšíření na stránce *AmIUnique* nejvíce odlišují uživatelovo zařízení od jiných zařízení v databázi poskytovatele stránky. V případě rozšíření NoScript a uMatrix nebylo možné voláním *JavaScriptových* metod zjistit žádné informace o uživateli, pokud bylo volání zakázáno. Navíc rozšíření uMatrix podvrhuje informace o aktivním blokování volání *JavaScriptových* metod, takže při jejich blokování se stránka nepřestala načítat a byla nepoužitelná. Tento výsledek je žádaný. Je ale nutné si uvědomit, že při každodenním prohlížení znamená zakázání skriptů prvních stran výrazné omezení funkcionality stránky. Zajímavější je výsledek rozšíření JavaScript Restrictor, které i bez blokování volání *JavaScriptových* metod bylo schopné zabránit získání informací zneužitím HTML elementu plátna.

| | NoScript | | uMatrix | | JavaScript Restrictor |
|---|---|---|---|---|---|
| | ✓ | × | ✓ | × | Úroveň ochrany 2 |
| Verze prohlížeče | ano | ne | ano | ne | ano |
| Jazyk | ano | ne | ano | ne | ano |
| Fonty | ano | ne | ano | ne | ano |
| Rozlišení obrazovky | ano | ne | ano | ne | ano |
| Grafická karta | ano | ne | ano | ne | ano |
| Element plátna | ano | ne | ano | ne | ne |

Tabulka 5.15: Tabulka popisující zabránění získání informací na stránce *AmIUnique* při použití testovaných rozšíření pro blokování spustitelného webového obsahu. Sloupec označený symbolem ✓popisuje situaci, ve které byla doméně první strany povolena volání *JavaScriptových* metod. Symbol × popisuje situaci, ve které byla volání zakázána.

### CoverYourTracks

Na rozdíl od stránky *AmIUnique* využívá *CoverYourTracks* pro sbírání informací volání *JavaScriptových* metod z domén třetích stran. Je tedy možné otestovat schopnost rozšíření NoScript a uMatix a zabránit *fingerprintingu* uživatele v kontextu jiné než první strany. Porovnávací metriky byly vybrány stejným způsobem, jako v případě stránky *AmIUnique*. *CoverYourTracks* zjišťuje verzi používaného prohlížeče uživatele pomocí HTTP hlaviček. Žádné rozšíření nebylo schopné zabránit získání této informace. Tabulka 5.16 zobrazuje informace, které byla stránka *CoverYourTracks* schopna přesně určit. Rozšíření NoScript zabránilo volání všech *JavaScriptových* metod včetně skriptů domény první strany. Nedovolilo stránce *CoverYourTracks* volat žádný *fingerprintující* skript ani po ruční konfiguraci (povolení volání všech domén přítomných na stránce). Sloupce uMatrix v tabulce 5.16 znázorňují chování v původní konfiguraci rozšíření ihned po nainstalování a po ruční konfiguraci ve formě zakázání veškerého obsahu třetích stran včetně obrázků a kaskádových stylů, které rozšíření v původní konfiguraci dovolovalo. Výsledek získání informací v obou případech je ale stejný. Rozšíření JavaScript Restrictor bylo schopné efektivně zamezit získání informace o elementu plátna uživatele.

### TorZillaPrint

Stránka *TorZillaPrint* funguje podobně jako *AmIUnique* pouze skrze volání *fingerprintujících* skriptů první strany. V původním nastavení rozšíření NoScript nebyla stránka schopna získat žádné informace, kromě rozlišení obrazovky a typu uživatelova prohlížeče. Po přidělení důvěry stránce ale rozšíření nezabránilo získání jakýchkoli informací. Obdobný případ lze pozorovat u rozšíření uMatrix, které však na rozdíl od NoScript při zakázání volání skriptů první strany nedovolilo stránce se v prohlížeči vůbec načíst. JavaScript Restric-

| | NoScript | uMatrix | | JavaScript Restrictor |
|---|---|---|---|---|
| | ✓ i × | ✓ | × | Úroveň ochrany 2 |
| Verze prohlížeče | ano | ano | ano | ano |
| Jazyk | ne | ano | ano | ano |
| Fonty | ne | ano | ano | ano |
| Rozlišení obrazovky | ne | ano | ano | ano |
| Grafická karta | ne | ano | ano | ano |
| Element plátna | ne | ano | ano | ne |
| WebGL fingerprint | ne | ano | ano | ano |

Tabulka 5.16: Tabulka popisující zabránění získání informací na stránce *CoverYourTracks* při použití testovaných rozšíření pro blokování spustitelného webového obsahu.

tor znovu potvrdil svou schopnost zabránit zjištění informace o elementu plátna uživatele. Navíc zabránil čtení přesné informace o datu a času pomocí zaokrouhlení výsledku volání API. Informací poskytnutých stránkou *TorZillaPrint* je výrazně více. Do výsledku porovnání rozšíření jsou zahrnuta jen některá vybraná kritéria. Tabulka 5.17 porovnává schopnost rozšíření zabránit získání informací o uživatelově zařízení. Stejně jako v případě *AmIUnique* je nutno zmínit, že pokud rozšíření zabrání zjištění informací zabráněním volání veškerých *JavaScriptových* metod první strany, při každodenním prohlížení pravděpodobně výrazně omezí funkcionalitu stránky.

### BrowserLeaks

Stránka *BrowserLeaks* poskytuje podobné služby, jako stránky *AmIUnique* a *TorZillaPrint*. Rozšíření lze v tomto případě testovat pouze v kontextu první strany. Obdobně jako u předchozích testů rozlišuje tabulka 5.18 v testu rozšíření NoScript a uMatrix případy, kdy bylo povoleno doméně první strany *BrowserLeaks* volat *JavaScriptové* metody. Obě rozšíření NoScript i uMatrix podala očekávaný a požadovaný výsledek, stejně jako v případě předchozích stránek testujících pouze pomocí domény první strany. Také JavaScript Restrictor demonstroval schopnost manipulovat s časem čteným z uživatelova zařízení a podvržením dat získaných z elementu plátna uživatele. Celkově je výsledek srovnatelný s testem na stránce *TorZillaPrint*.

### JavaScript Restrictor Test Page

Poslední využitá stránka v testu nabízí volání *JavaScriptových* metod pouze z domény první strany. Obsahuje ale množství alternativních metrik v porovnání s předchozími testovacími stránkami. Stránka je navržena převážně pro potřeby týkající se testování rozšíření

| | NoScript | | uMatrix | | JavaScript Restrictor |
|---|---|---|---|---|---|
| | ✓ | × | ✓ | × | Úroveň ochrany 2 |
| Druh prohlížeče | ano | ano | ano | nelze určit | ano |
| Verze prohlížeče | ano | ne | ano | nelze určit | ano |
| Jazyk | ano | ne | ano | nelze určit | ano |
| Informace o datu | ano | ne | ano | nelze určit | ne |
| Fonty | ano | ne | ano | nelze určit | ano |
| Rozlišení obrazovky | ano | ano | ano | nelze určit | ano |
| Element plátna | ano | ne | ano | nelze určit | ne |
| WebGL fingerprint | ano | ne | ano | nelze určit | ano |

Tabulka 5.17: Tabulka popisující zabránění získání informací na stránce *TorZillaPrint* při použití testovaných rozšíření pro blokování spustitelného webového obsahu.

JavaScript Restrictor, čemuž odpovídají i porovnávané informace. Možnost otestovat schopnost geolokace uživatele byla vynechána, i bez rozšíření je totiž taková informace poskytnutá stránkou velice nepřesná. Tabulka 5.19 opět zohledňuje případy, ve kterých bylo doméně *polcak.github* povoleno volat *JavaScriptové* metody při testování rozšíření NoScript a uMatrix. Kromě informace o výkonu nebylo ani jedno z dvou jmenovaných rozšíření schopné po povolení volání *JavaScriptových* metod zabránit sběru informací o uživateli. V případě zákazu volání sice nebylo možné žádné informace získat, ale testová stránka celkově přestala pracovat. Přesné informace o výkonu nebylo možné získat spíše kvůli použití prohlížeče *Mozilla Firefox*, než účinkem rozšíření. Rozšíření JavaScript Restrictor splnilo všechny nároky kladené stránkou, která nebyla schopna o uživateli zjistit přesné informace i v případě, že doméně *polcak.github* byla povolena volání *JavaScriptových* metod.

### Závěr testu rozšíření blokujících spustitelný obsah

Rozšíření NoScript a uMatrix splnila očekávání testu. Pokud uživatel zakázal volání *JavaScriptových* metod nenastal případ, ve kterém by byť jedno z těchto rozšíření selhalo. Lze tedy usoudit, že jsou v tomto ohledu obě rozšíření stejně efektivní. Jediný zásadní rozdíl je původní konfigurace rozšíření bez dalšího zásahu uživatele. V případě použití rozšíření uMatrix by měla být zachována celková funkcionalita všech navštívených stránek, což v mnoha případech eliminuje nutnost uživatele volit metodu „pokus-omyl“ při snaze získat zpět všechny žádané služby stránky. Navíc má rozšíření uMatrix ihned po instalaci vlídnější GUI, které je sice na první pohled složité, ale nabízí v porovnání s GUI rozšíření

| | NoScript | | uMatrix | | JavaScript Restrictor |
|---|---|---|---|---|---|
| | ✓ | × | ✓ | × | Úroveň ochrany 2 |
| Verze prohlížeče | ano | ano | ano | ano | ano |
| Jazyk | ano | ne | ano | ne | ano |
| Informace o datu | ano | ne | ano | ne | ne |
| Fonty | ano | ne | ano | ne | ano |
| Rozlišení obrazovky | ano | ne | ano | ne | ano |
| Grafická karta | ano | ne | ano | ne | ano |
| Element plátna | ano | ne | ano | ne | ne |
| WebGL fingerprint | ano | ne | ano | ne | ano |
| Operační systém | ano | ne | ano | ne | ano |

Tabulka 5.18: Tabulka popisující zabránění získání informací na stránce *BrowserLeaks* při použití testovaných rozšíření pro blokování spustitelného webového obsahu.

| | NoScript | | uMatrix | | JavaScript Restrictor |
|---|---|---|---|---|---|
| | ✓ | × | ✓ | × | Úroveň ochrany 2 |
| Informace o datu | ano | ne | ano | ne | ne |
| Informace o výkonu | ne | ne | ne | ne | ne |
| Element plátna | ano | ne | ano | ne | ne |
| Informace o hardware | ano | ne | ano | ne | ne |
| Informace periferiích | ano | ne | ano | ne | ne |

Tabulka 5.19: Tabulka popisující zabránění získání informací na stránce *polcak.github* při použití testovaných rozšíření pro blokování spustitelného webového obsahu.

NoScript bez konfigurace mnohem více možností. Zároveň je obohaceno vlídným barevným zpracováním, které zvyšuje jeho přehlednost.

V případě rozšíření JavaScript Restrictor testy dokázaly jeho kompetenci ve všech ohledech, které zmiňuje jeho dokumentace. Velkou výhodou je jeho uživatelská přívětivost ve formě přehledného GUI, ve kterém se lehce na první pohled zorientuje i všední uživatel. Dále není ve většině případů nutné rozšíření konfigurovat pro dosažení ochrany i zachování funkcionality navštívených stránek. Na druhou stranu nemůže uživatele ochránit před profilováním pomocí *fingerprintujících JavaScriptových* metod tak efektivně, jako v případě předchozích rozšíření, která volání celkově zakáží. Po porovnání rozšíření této kategorie vzniklo následující doporučení pro uživatele:

- rozšíření **NoScript** a **uMatrix** jsou stejně efektivní ve své slíbené funkcionalitě. Jejich použití ale není doporučeno pro nezkušené uživatele, může totiž při špatné konfiguraci negativně ovlivnit požitek z prohlížení.
- v otázce vyvážení ochrany před *fingerprintingem* a zachování funkcionality navštívených stránek je vhodnější využít rozšíření **uMatrix**.
- uživatel musí ale přijmout, že ve většině případů při používání internetu nelze dosáhnout perfektní ochrany a zachování kompletní funkcionality stránek najednou.
- rozšíření **uMatrix** nabízí v původní konfiguraci příjemnější a přehlednější uživatelské rozhraní, než rozšíření **NoScript**.
- **JavaScript Restrictor** nabízí alternativu ke kompletnímu blokování všech volání *JavaScriptových* metod, ve kterém je podle testů úspěšný. Lze jej použít jako doplněk k prohlížení v závislosti na potřebách uživatele. Při jeho použití nebude ve většině případů negativně ovlivněna funkcionalita navštívené stránky. Jeho užití by měl uživatel zvážit po nastudování možností ochrany, které rozšíření nabízí.

## 5.4 Závěr testu webových rozšíření zaměřených na bezpečnost a soukromí

Z testů rozšíření zaměřených na bezpečnost a soukromí bylo možné vyhodnotit jejich individuální efektivitu v oblastech ochrany, kterou nabízí. V případě rozšíření na bázi sledovacích prvků se podle provedených testů stalo vítězem rozšíření *uBlock Origin*. Rozšíření demonstrovalo schopnost rozeznat a blokovat nevyžádané HTTP požadavky zasílané klientem, potenciálně škodlivá volání *JavaScriptových* metod a *cookies* třetích stran, které mohou uživatele při prohlížení internetu ohrozit. Hlavním důvodem jsou seznamy, které v původní konfiguraci rozšíření obsahuje. Jeho největší výhodou je právě implementace vhodných seznamů ihned po jeho instalaci bez další nutné konfigurace uživatelem – například ověřený seznam *EasyPrivacy*, který jiné testované rozšíření v základu nepoužívá. Tento fakt jej staví před konkurenci hlavně proto, že interakce s rozšířením tohoto typu pro většinového uživatele končí u jeho instalace. S využitými seznamy souvisí i absence placeného programu, který ostatní testovaná rozšíření nabízí. Rozšíření *uBlock Origin* tak není udržováno za účelem výdělku a nepoužívá vlastní seznamy blokovacích prvků, které v případě ostatních rozšíření nejsou podle testů tak efektivní. Motivace ostatních rozšíření této kategorie je tedy spíše monetární, pro nejlepší poskytnutí služby musí uživatel využít některého z nabízených placených programů.

V otázce blokování nevyžádaných HTTP přesměrování se ale na prvním místě ocitá rozšíření *AdGuard AdBlocker*. Rozšíření této kategorie se nedoporučuje používat současně.

Přes odlišnost používaných seznamů se v jejich obsahu v mnoha případech shodují a používáním vícero rozšíření probíhá filtrace jednoho prvku zbytečně vícekrát.

Rozšíření druhé testované skupiny se od sebe liší výrazněji, než v případě skupiny první. V oblasti nabízených služeb prokázala v provedeném testu největší efektivitu rozšíření *Disconnect* a *DuckDuckGo Privacy Essentials*. Výsledky testů obou rozšíření jsou na porovnatelné úrovni a při rozhodování mezi nimi záleží spíše na preferenci uživatele. Rozšíření *DuckDuckGo Privacy Essentials* ihned po instalaci změní vyhledávač prohlížeče na svůj vlastní *DuckDuckGo*, což může být uživatelům nepříjemné. *Privacy Possum* po zrušení programu učenlivého blokování [21] nenabízí žádnou výhodu a jeho efektivita není výrazně vysoká. Pokud vývojáři program v budoucnu obnoví, přinese snad rozšíření v ohledu bezpečného prohlížení více výhod. *Privacy Possum* přináší do boje o internetové soukromí nové zajímavé metody. Jejich využití ale může uživatele negativně ovlivnit, měl by tedy zvážit, zda chce, aby byly po internetu šířeny podvržené informace. Efektivita rozšíření *First Party Isolation* není vysoká a je otázkou, zda není jeho použití v prohlížeči *Mozilla Firefox* spíše redundantní. Rozšíření této kategorie je vhodné využít za doprovodu s rozšířeními kategorie první, jelikož při ochraně soukromí implementují rozdílné metody a v jejich obsahu se nepřekrývají.

Poslední testovaná skupina – rozšíření blokující spustitelný webový obsah – ve všech případech prokázala schopnost implementovat metody slíbené vývojáři. Kromě rozšíření *JavaScript Restrictor* nejvýrazněji ovlivňují každodenní prohlížení internetu a jejich použití není doporučeno nezkušeným uživatelům. Výběr mezi rozšířením *NoScript* a *uMatrix* znovu závisí spíše na preferenci uživatele, jelikož je funkcionalita obou rozšíření téměř totožná. Rozšíření *JavaScript Restrictor* lze použít jako vhodný doplněk prohlížení, který nemá ve většině případů negativní dopad na požitek uživatele a do jisté míry slíbené vývojáři chrání uživatelovo soukromí při pohybu po internetu. Rozšíření této kategorie lze využít samostatně i v doprovodu s rozšířeními předchozích kategorií, jelikož jejich funkcionalita se od ostatních zásadně odlišuje.

# Kapitola 6

# Závěr

Práce v teoretické části umožnila čtenáři vhled do „ekosystému“ internetového obchodu s informacemi a podtrhla význam sběru osobních údajů uživatelů, stejně jako nebezpečí, která s sebou přináší 1. Seznámila čtenáře s principem seznamů sledovacích prvků a způsobem jejich využití. Představila nejpopulárnější rozšíření zaměřená na bezpečnost a soukromí dostupná na webu, která orientačně zařadila do kategorií podle jejich funkce 2. Dále nastínila hrozby, se kterými se uživatel každodenním prohlížením internetu může setkat, čímž podtrhla důležitost rozšíření zaměřených na bezpečnost a soukromí 3. Teoretickou část zakončila návrhem implementace testovacího prostředí pro porovnání zmíněných webových rozšíření 4.

V praktické části byla analyzována data získaná použitím nástroje *OpenWPM* a pomocí ručního testování rozšíření. Databáze získané nástrojem byly podrobeny analýze pomocí *SQL* dotazování a výsledek porovnání byl promítnut do přehledných grafů a tabulek. Testy vyzdvihují oblasti funkcionality, ve kterých se rozšíření překrývají. Důraz je kladen na schopnost omezení nevyžádaného internetového provozu a zamezení sledování uživatele po internetu za účelem jeho profilování. Při ručním testování rozšíření byl kladen důraz na splnění funkce, kterou rozšíření nabízí. Test každé skupiny rozšíření byl zakončen krátkým doporučením pro uživatele v závislosti na jeho potřebách 5.

Výsledkem práce je doporučení konkrétních webových rozšíření se zaměřením na bezpečnost a soukromí všednímu uživateli internetu. Práce shrnuje podstatné informace, které uživateli pomohou při výběru rozšíření v závislosti na jeho potřebách a preferencích.

# Literatura


[1] *About Adblock Plus* [online]. [cit. 2021-1-3]. Dostupné z: https://adblockplus.org/en/about.

[2] *Acxicom.* [online]. [cit. 2020-3-24]. Dostupné z: https://www.acxiom.com/.

[3] *Adblock Plus filters explained* [online]. [cit. 2020-12-24]. Dostupné z: https://adblockplus.org/filter-cheatsheet.

[4] *Adblock Plus now sells ads* [online]. [cit. 2021-1-3]. Dostupné z: https://www.theverge.com/2016/9/13/12890050/adblock-plus-now-sells-ads.

[5] *Cookie Matching* [online]. [cit. 2021-3-2]. Dostupné z: https://developers.google.com/authorized-buyers/rtb/cookie-guide.

[6] *Cross-Origin Identifier Unlinkability* [online]. [cit. 2021-1-3]. Dostupné z: https://2019.www.torproject.org/projects/torbrowser/design/#identifier-linkability.

[7] *DuckDuckGo Founding Member in Global Privacy Control (GPC) Standards Effort* [online]. [cit. 2021-3-1]. Dostupné z: https://spreadprivacy.com/announcing-global-privacy-control/.

[8] *Firefox Browser Add-ons, Privacy  Security* [online]. [cit. 2021-3-1]. Dostupné z: https://addons.mozilla.org/en-US/firefox/extensions/category/privacy-security/.

[9] *GPC: Take Control Of Your Privacy* [online]. [cit. 2021-3-1]. Dostupné z: https://globalprivacycontrol.org/#about.

[10] *How does Privacy Badger work?* [online]. [cit. 2021-1-2]. Dostupné z: https://privacybadger.org/#How-does-Privacy-Badger-work.

[11] *Online Privacy: Using the Internet Safely* [online]. [cit. 2021-3-1]. Dostupné z: https://privacyrights.org/consumer-guides/online-privacy-using-internet-safely.

[12] *Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities.* [cit. 2021-3-18]. Dostupné z: https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-52019-interplay-between-eprivacy_en.

[13] *Personalized Marketing: The Ultimate Guide to WOW Your Prospects and Customers.* [online]. [cit. 2020-3-24]. Dostupné z: https://moosend.com/blog/personalized-marketing/.

[14] *Privacy Possum: Browser Fingerprinting* [online]. [cit. 2021-1-3]. Dostupné z: https://github.com/cowlicks/privacypossum.

[15] *Schema Documentation* [online]. [cit. 2021-1-3]. Dostupné z: https://github.com/mozilla/OpenWPM/blob/master/docs/Schema-Documentation.md.

[16] *Search ads and self-promotion* [online]. [cit. 2021-3-1]. Dostupné z: https://kb.adguard.com/en/general/search-ads-and-self-promotion?utm_source=browser_extension&utm_medium=options_screen&utm_campaign=self_promotion.

[17] *Types of Cookies* [online]. [cit. 2021-1-3]. Dostupné z: https://cookiepedia.co.uk/types-of-cookies.

[18] *Understanding Redirection-Based Tracking* [online]. [cit. 2021-1-3]. Dostupné z: https://brave.com/redirection-based-tracking/.

[19] *Identity Matching in Programmatic – What Publishers Need to Know?* [online]. 2020 [cit. 2021-3-2]. Dostupné z: https://headerbidding.co/identity-matching-adtech/.

[20] Acar, G., Englehardt, S. a Narayanan, A. No boundaries: data exfiltration by third parties embedded on web pages. *Sciendo*. sv. 4, [cit. 2021-1-2]. Dostupné z: https://content.sciendo.com/view/journals/popets/2020/4/article-p220.xml?language=en.

[21] Arrieta, A. a Cyphers, B. *Privacy Badger Is Changing to Protect You Better* [online]. 2020 [cit. 2020-12-24]. Dostupné z: https://www.eff.org/deeplinks/2020/10/privacy-badger-changing-protect-you-better.

[22] Brinkmann, M. *UMatrix development has ended* [online]. 2020 [cit. 2020-12-24]. Dostupné z: https://www.ghacks.net/2020/09/20/umatrix-development-has-ended/.

[23] Crane, C. *3 Cyber Fraud Tactics Targeting Seniors And Why They're So Effective* [online]. [cit. 2020-12-24]. Dostupné z: https://cybersecurityventures.com/3-cyber-fraud-tactics-targeting-seniors-and-why-theyre-so-effective/.

[24] Doty, N. *Mitigating Browser Fingerprinting in Web Specifications* [online]. [cit. 2021-1-2]. Dostupné z: https://w3c.github.io/fingerprinting-guidance/.

[25] Englehardt, S. a Narayanan, A. Online tracking: A 1-million-site measurement and analysis. In: *Proceedings of ACM CCS 2016*. 2016 [cit. 2021-1-3].

[26] Goodin, D. Adblockers installed 300,000 times are malicious and should be removed now. *Arstechnica*. [cit. 2020-3-24]. Dostupné z: https://arstechnica.com/information-technology/2020/10/popular-chromium-ad-blockers-caught-stealing-user-data-and-accessing-accounts/.

[27] Goodman, M. *Future Crimes*. 2016. ISBN 978-0-8041-7145-8.

[28] Gray, S. *Understanding Session Replay Scripts - a Guide for Privacy Professionals* [online]. [cit. 2021-1-2]. Dostupné z: https://fpf.org/blog/understanding-session-replay-scripts-a-guide-for-privacy-professionals/.

[29] Heaton, R. *Identity Graphs: how online trackers follow you across devices* [online]. 2017 [cit. 2021-3-2]. Dostupné z: https://robertheaton.com/2017/11/24/identity-graphs-how-online-trackers-follow-you-across-devices/.

[30] Jelínek, L. *Firefox 57: zbrusu nový engine Quantum, nové GUI, konec starých rozšíření* [online]. [cit. 2020-3-24]. Dostupné z: https://www.linuxexpres.cz/novinky/firefox-57-zbrusu-novy-engine-quantum-nove-gui-konec-starych.

[31] Polčák, L. Soukromí uživatelů v prostředí internetové reklamy na českém webu. *DSM*. 2020, [cit. 2021-3-2]. Dostupné z: https://www.fit.vut.cz/research/publication-file/12175/dsm.pdf.

[32] Rouse, M. *Supercookie* [online]. [cit. 2021-1-2]. Dostupné z: https://searchsecurity.techtarget.com/definition/supercookie.

[33] Traverso, S. *Benchmark and Comparison of Tracker-blockers: Should You Trust Them?* [online]. [cit. 2021-1-2]. Dostupné z: https://ieeexplore.ieee.org/abstract/document/8002898.

[34] Turow, J. a Hannesy, M. *The Tradeoff Fallacy* [online]. [cit. 2021-1-3]. Dostupné z: https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf.