VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV INTELIGENTNÍCH SYSTÉMŮ
DEPARTMENT OF INTELLIGENT SYSTEMS

POKROČILÁ EVALUACE ÚROVNĚ PRIVÁTNOSTI V SOCIÁLNÍCH SÍTÍCH

THESIS TITLE

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE **FILIP JANUŠ**
AUTHOR

VEDOUCÍ PRÁCE **Mgr. KAMIL MALINKA, Ph.D.**
SUPERVISOR

BRNO 2020

Vysoké učení technické v Brně
Fakulta informačních technologií

Ústav inteligentních systémů (UITS) Akademický rok 2019/2020

Zadání diplomové práce

Student: **Januš Filip, Bc.**
Program: Informační technologie Obor: Bezpečnost informačních technologií
Název: **Pokročilá evaluace úrovně privátnosti v sociálních sítích**
Advanced Evaluation of Privacy Level in Social Networks
Kategorie: Bezpečnost
Zadání:

1. Prostudujte stávající práce zabývající se popisem, analýzou, a evaluací privátnosti v sociálních sítí.
2. Navrhněte příslušné metodologie a algoritmy pro evaluace dvou typů privátnosti uživatelských dat v sociálních sítích: interního a externího uživatele. První algoritmus je specifický pro danou sociální síť, zatím co druhý algoritmus kombinuje všechny podporované sítě.
3. Implementujte příslušné nástroje aplikující všechny navržené algoritmy s využitím dat extrahovaných z nastavení ale i crawlovaní alespoň 7 zvolených sociálních sítí konzultovaných s vedoucím práce.
4. Aplikujte interní/externí nástroje na několika testovacích uživatelských účtech/identifikátorech.
5. Vyhodnoťte výsledky a zároveň analyzujte možnosti srovnání privátnosti interního uživatele napříč sociálními sítěmi.
6. Analyzujte a diskutujte nástroje a jejich aspekty privátnosti s ohledem na rozdílnost granularity dostupných informací s pohledu interního a externího uživatele.

Literatura:

- Comer, Ronan, Nigel McKelvey, and Kevin Curran. "Privacy and Facebook." *International Journal of Engineering and Technology* 2.9 (2012): 1626-1630.
- Zheleva, Elena, Evimaria Terzi, and Lise Getoor. "Privacy in social networks."*Synthesis Lectures on Data Mining and Knowledge Discovery* 3.1 (2012): s 47-62.
- Podle pokynů vedoucího.

Při obhajobě semestrální části projektu je požadováno:

- Body 1 a 2 zadání.

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

Vedoucí práce: **Malinka Kamil, Mgr., Ph.D.**
Konzultant: Homoliak Ivan, Ing., Ph.D., UITS FIT VUT
Vedoucí ústavu: Hanáček Petr, doc. Dr. Ing.
Datum zadání: 1. listopadu 2019
Datum odevzdání: 3. června 2020
Datum schválení: 31. října 2019

Abstrakt

V dnešní době stále přetrvává trend přesunu mezilidské komunikace do online prostředí. A to díky sociálním sítím a jejich službám. S tímto faktem souvisí i rostoucí počet uživatelů sociálních sítí. Mnoho uživatelů ovšem nevnímá rizika spojená s přítomností v internetovém prostředí. Tato práce se zaměřuje na analýzu nastavení soukromí uživatelských účtů na sociálních sítích a následné vyhodnocení těchto nastavení. Cílem práce je vytvořit nástroj poskytující možnost vyhodnotit bezpečnostní nastavení uživatelského účtu na sociální síti případně doporučit vhodnější nastavení s ohledem na soukromí uživatele. Aby bylo možné dosáhnout těchto cílů, je potřebné použít vhodný model provádějící vyčíslení skóre privátnosti. Výstupem práce bude návrh a implementace nástroje provádějící analýzu, vyhodnocení a doporučení, jak vylepšit nastavení soukromí na sociální síti. Což by mělo pomoci uživateli omezit množství uniklých citlivých informací.

Abstract

Nowadays persists a trend of moving interpersonal communication into the online environment. By the reason of the social networks and social network's services. Many users doesn't perceive threats connected with presence in internet environment. This thesis is focused on the analysis of the user's account privacy settings followed by the evaluation of these settings. The goal is to develop and create a tool providing ability to evaluate privacy settings of the user's account, eventually recommend more suitable settings given to user privacy. To achieve these goals is necessary to use a suitable model performing privacy evaluation. The output of the thesis will consist of a proposal and implementation of tool performing analysis, evaluation and recommendation of how to improve the social network's privacy settings. Which should help users reduce the amount of privacy information leakage.

Klíčová slova

sociální síť, soukromí, bezpečnost, Privacy score, nastavení soukromí, aplikační firewall, model

Keywords

social network, privacy, security, Privacy score, privacy settings, application firewall, model

Citace

JANUŠ, Filip. *Pokročilá evaluace úrovně privátnosti v sociálních sítích.* Brno, 2020. Diplomová práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Mgr. Kamil Malinka, Ph.D.

Pokročilá evaluace úrovně privátnosti v sociálních sítích

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně pod vedením pana doktora Kamila Malinky. Uvedl jsem všechny literární prameny, publikace a další zdroje, ze kterých jsem čerpal.

.....
Filip Januš
31. května 2020

Poděkování

Rád bych poděkoval vedoucímu své diplomové práce panu Mgr. Kamilu Malinkovi Ph.D. za čas a odborné rady, které mi při tvorbě této práce poskytl.

Obsah

Kapitola 1

Úvod do problematiky

V dnešní době se díky moderním technologiím stává internet stále dostupnější a populárnější platformou pro komunikaci, zábavu i práci a to i na odlehlých místech. Většina populace s internetem interaguje každý den. Důvodů k tomuto rozvoji může být několik, nicméně jedním z důležitějších je stále větší dostupnost mobilních dat. Zatímco dříve uživatelé využívali služeb internetu zejména z pohodlí domova, dnes není problém pracovat s internetem v mobilním zařízení téměř odkudkoliv, ani rychlost mobilních dat již není v dnešní době problém. Společně s rozvojem internetu a mobilních zařízení se stávají stále populárnějšími sociální sítě. Lidé spolu prostřednictvím těchto služeb mohou komunikovat, vyměňovat si své zážitky, sdílet fotografie, videa, hrát hry a provozovat řadu dalších aktivit. Řada uživatelů si ale dostatečně nebo vůbec neuvědomuje, že všechny tyto sítě mohou být potenciální hrozbou pro jejich soukromí. Neboť bez ostychu sdílí své osobní informace, čímž nad nimi ztrácí kontrolu. I pozornější uživatel může snadno o svá citlivá data přijít aniž by o tom věděl. A to především díky používání různých aplikací v mobilním zařízení připojeném k internetu. Příkladem hovořícím za vše může být situace, kdy si uživatel stáhne aplikaci, nepřečte si několikastránkové smluvní podmínky a dostává se do situace, kdy aplikace provádí sledování jeho polohy aniž by si toho byl vědom.

Motivací této práce je zmapování bezpečnostní situace na sociálních sítích, které zažívají dynamický vývoj. Dále prozkoumání situace uživatelského povědomí o možných rizicích spojených s používáním sociálních sítí, především v oblasti ochrany citlivých údajů.

Cílem práce je prostudovat možná nastavení soukromí a zabezpečení na různých sociálních sítích. Informace o nastavení vhodným způsobem agregovat a na základě navržených technik varovat uživatele před přílišnou důvěrou sociálním sítím potažmo internetu. Výsledkem by se měl stát nástroj, kterému uživatel svěří své přihlašovací údaje k sociálním sítím, ten provede kontrolu nastavení z pohledu přihlášeného uživatele, dále zkontroluje viditelné údaje z pohledu nepřihlášeného uživatele. Na základě těchto informací se pomocí matematických modelů provede výpočet míry ohrožení soukromí, dle dosaženého výsledku bude uživateli sděleno jak si stojí a popřípadě může být doporučeno, která nastavení upravit.

Práce je rozdělena na dvě základní části. První teoretická, se zabývá aktuální situací a již publikovanými texty z kterých čerpá. Taktéž se zde popisují jednotlivé sociální sítě jejich bezpečnostní nastavení a matematické modely pro vyčíslení soukromí. V druhé části práce se bude pojednávat o samotné realizaci nástroje jeho návrhu, implementaci a testování. V následující kapitole jsou základní definice soukromí, následované popisem sociálních sítí a jejich možnostmi nastavení zabezpečení.

Kapitola 2

Aktuální stav problematiky

V této kapitole budou nejprve prezentovány dosavadní práce, ze kterých tato kapitola z většiny čerpá. Dále budou definovány důležité pojmy v souvislosti se soukromím a sociálními sítěmi, taktéž bude uvedena definice sociální sítě, objeví se několik detailněji popsaných sociálních sítí, které byly vybrány s ohledem na popularitu. Poslední část kapitoly bude věnována modelům pro evaluaci privátnosti.

2.1 Privátnost

Privátnost nebo také soukromí lze definovat jako osobní oblast jedince nebo skupiny lidí, která zahrnuje právo a potřebu chránit informace o sobě před zveřejněním nebo zneužitím [11].

V kontextu této práce je spíše zajímavá definice internetové privátnosti resp. definice Informačního soukromí. Tento pojem definoval již v roce 1967 Alan Westin (Americký profesor práva), který jej formuloval jako : *informační soukromí je schopnost jedince určit, kdy, jak a do jaké míry budou jeho osobní informace sdělovány ostatním.* Pojem Informační soukromí lze také chápat jako ochranu osobních údajů před jejich zneužití organizací, které byly údaje poskytnuty. Ochranou se zde myslí kontrola nakládání s informacemi a možnost určení kdy, jak a kde budou informace zveřejňovány [15].

2.2 Stávající práce

Již několik desítek prací bylo zaměřeno na oblast bezpečnosti na sociálních sítích. Tyto práce se tématem zaobíraly z několika různých pohledů. V [21] se autoři zabývají dolováním citlivých dat z publikovaných informací na sociálních sítích, definují zde anonymitu a popisují různé přístupy dolování a zabývají se možnými riziky vyzrazení citlivých informací. Jedna z prvních prací zaměřených na internetové sociální sítě [9] si kladla za cíl změřit úroveň soukromí, cílem měl být nástroj, který každému uživateli řekne, jakého skóre soukromí dosahuje a popřípadě doporučí nastavení. Je třeba upozornit, že autoři chtěli evaluovat skóre soukromí skupině uživatelů na základě pravděpodobnostních modelů. Wang a jeho kolegové [19] se zaměřili na vyčíslování soukromí mezi dvěma uživateli, dle nastavených atributů, prezentovali již dříve navrhované modely a následně je dále vylepšovali, tak aby lépe reflektovaly uživatelská nastavení.

V publikacích [13, 6] se autoři věnovali vývoji aplikace zobrazující procentuální mírů ohrožení soukromí uživatele sociální sítě. Tato aplikace získává data o uživateli z API soci-

ální sítě Facebook. Autoři se zde rozhodli vyčíslovat ohrožení privátnosti na základě informací o vztazích s ostatními uživateli a dostupných informacích o přátelích. Taktéž Becker a Chen [12] vyvíjeli nástroj na detekci potencionálních úniků soukromých informací, podobně jako v [13, 20] pracovali s informacemi o vazbách mezi uživateli a na základě nich se snažili odhalovat soukromé atributy profilů. Z výsledků vyplývá, že při testování nástroje na 93 účastnících se podařilo odhalit necelých 60% soukromých informací. Všechny popsané přístupy se snaží na základě získaných informací odhadovat aktuální nastavení a následně doporučovat nastavení.

V článku [7] autoři popisují možná bezpečnostní rizika sociálních sítí, několik vybraných popisují detailněji, nejvíce prostoru je věnováno aplikacím nazývaným *Trojan applications*. Účelem těchto aplikací je především poskytnout jejich provozovateli informace z profilů uživatelů. Na závěr je zde navrhnuto také několik protiopatření.

Problematika dělení uživatelů do skupin dle ochoty sdílet své citlivé informace je diskutována v [2], v článku je pohlíženo na problematiku ochoty sdílet informace z několika pohledů, například s ohledem na věk a pohlaví respondentů. Naopak v práci [10] se zkoumá uživatelské povědomí o rizicích spojených se sociálními sítěmi. Dále se zde objevuje téma, kde jsou popsána některá úskalí nastavení zabezpečení a možné rozdíly mezi požadovaným a reálným nastavení.

V práci [14] jsou uvedeny metody získávání obsahu ze sociálních sítí za použití techniky *web scraping*. Popisují se zde výhody této technologie oproti přístupu k obsahu přes oficiální API. Autoři také prezentují různé nástroje pro extrakci webových dat.

Výše byly prezentovány dřívější výzkumy a nástroje zaměřující se na soukromí na sociálních sítích. Každá práce přistupuje k problému trochu odlišně, avšak žádná z nich nepracovala přesnými informacemi o nastavení soukromí. Publikované práce se snažily z veřejně dostupných informací nebo informací dostupných z API sítě predikovat ohrožení soukromí a detekovat potenciální atributy soukromí, které by mohly být prozrazeny. Tento přístup odlišuje dřívější práce od nástroje navrhovaného v této práci, který by měl pracovat s přesnými informacemi o soukromí extrahovanými přímo z nastavení účtu. I když nástroje publikované v [21, 18, 19] extrahují data odlišným způsobem než jaký je navrhovaný v této práci, evaluační postupy použité na získaná data se zdají být zajímavé v kontextu navrhované práce, proto budou detailněji popsány níže.

2.2.1 Ohrožení soukromí na sociálních sítích

Otázkou je proč uživatelé ochotně sdílí své osobní informace, aniž by věděli, kdo bude tyto informace číst. Dle [13] chtějí být propojeni s přáteli, hledat nové přátelé s podobnými zájmy a využívat společně množství dostupných aplikací sociálních sítí. Motivací sdílet osobní informace může být také snaha uživatelů nevybočovat a držet se trendů, jak uvádí autoři článku [9]. Dalším možným vysvětlením může být situace, kdy uživatel chce využívat určité funkcionality, která vyžaduje přístup k soukromým informacím, uživatel tedy souhlasí. A to i s vědomím toho, že takové chování vede k jisté ztrátě kontroly nad svým soukromím ve virtuálním prostředí. Neboť dokonalé smazání informace z webu může být neřešitelný problém.

Různé organizace mohou těžit z uživatelů, kteří dobrovolně zpřístupňují své osobní informace na sociálních sítích [5]. Aktuální a přesné informace o uživatelských profilech poskytují širokou škálu možností pro organizace provádějící dolování dat nebo doručování cílené reklamy. Taktéž informace ze sociálních sítí mohou využívat pojišťovací agenti či personalisté. Tyto informace jim mohou poskytnout vhled do soukromí člověka, který se uchází o za-

městnání nebo sjednává pojištění a na základě zveřejněných informací mohou rozhodnout v neprospěch klienta resp. uchazeče o zaměstnání.

I přes existenci těchto rizik lidé stále ochotně zveřejňují své osobní informace. Ve studii [10] prováděné ve Spojených státech vzhledem k sociální síti Facebook autoři prezentují výsledky, které ukazují uživatelskou nevědomost či lhostejnost ke svému soukromí na sociálních sítích. Na otázku, zda někdy uživateli na sociální síti unikla soukromá data, odpovědělo 91% respondentů studie negativně. Přičemž 85% z nich slyšelo z nějakého veřejného zdroje informace o soukromí na sociálních sítích a 25% z informovaných na základě získaných informací upravilo své nastavení zabezpečení nebo ho alespoň zkontrolovalo. Tyto informace lze interpretovat různými způsoby. Nabízí se ovšem výklad, kdy podstatná část uživatelů upřednostňuje maximální využití funkcionality sociální sítě a již se tolik nezajímá o únik soukromých informací.

Dalším zajímavým avšak ne nečekaným výsledkem studie je skutečnost, že každý zúčastněný této studie sdílel nechtěně alespoň jednu osobní informaci. Z těchto skutečností lze usuzovat, že nastavení soukromí na sociální síti není triviální záležitostí.

2.3 Bezpečnostní nastavení sociálních sítí

2.3.1 Sociální síť

Sociální síť lze popsat jako internetovou službu umožňující svým uživatelům vytvářet vlastní profily, sdílet informace, videa, fotografie, komunikovat, provozovat chat a mnoho další aktivit [16, 1]. Existuje celá řada sociálních sítí, které lze dělit dle obsahu, který uživatelé sdílí. Ale také podle lokality, některé sociální sítě jsou specifické jen pro svůj region, například v Číně existuje řada sociálních sítí, které jsou téměř neznámé v Evropě.

Stejně jako jsou sociální sítě různorodé svým obsahem a možnými aktivitami, tak i jednotlivé sítě dovolují různá nastavení zabezpečení a ochrany soukromí. Nejzásadnější rozdíly lze nalézt v granularitě jednotlivých nastavení, od velice obecných nastavení až po možnost detailního nastavení viditelnosti jednotlivých atributů uživatele. Zde se střetávají dva protichůdné názory na granularitu těchto nastavení.

Jedna strana má vizi několik málo nastavení, které lze upravit během pár kliknutí a tím pádem neobtěžuje uživatele, tedy potenciálního zákazníka zdlouhavým čtením a snahou o pochopení těchto nastavení. Příkladem této minimalistické strategie může být sociální síť *Tumblr*.

Druhá strana zastává názor na detailní nastavení soukromí a zabezpečení. Z čehož vyplývá, že uživatel musí věnovat více času porozumění a studiu nastavení. Příkladem jsou sociální sítě *Facebook* a *LinkedIn*.

Pro účely této práce bude vhodnější matematická definice sociální sítě, neboť později diskutované modely pracují na matematickém základu. Z matematického pohledu lze sociální síť považovat za graf, kde vrcholy jsou reprezentovány entitami a hrany vztahy mezi nimi [19]. Existují vztahy orientované či neorientované stejně jako v grafu hrany. U neorientovaných vztahů buď to vazba existuje či nikoli. U orientovaných se na vztahu podílí pouze jeden uživatel. Příkladem může být situace, kdy entita A zná entitu B, ale B nezná A. Většina sociálních sítí funguje na modelu přátelství, kdy vztah entit je obousměrný. Tj. entita A zná B a B zná A.

Nastavení v sociálních sítích	Facebook	Twitter	Youtube	LinkedIn	Instagram	Tumbir	Pinterest
Nastavení viditelnosti příspěvků	x	x			x		
Nastavení viditelnosti seznamu přátel	x			x			
Vyhledání pomocí e-mailu	x	x		x			
Vyhledání pomocí telefonního čísla	x	x		x			
Historie polohy	x	x	x				
Signalizace aktivity		x		x	x	x	
Kdo Vám může posílat zprávy		x		x			
Skrýt profil vyhledávačům	x						x

Tabulka 2.1: Vybraná nastavení soukromí a zabezpečení objevující se alespoň u dvou sociálních sítí

2.3.2 Stupeň separace

Důležitým pojmem v kontextu vztahů na sociálních sítích je stupeň separace [19]. Pojem úzce souvisí s viditelností atributů entity. Definuje se jako funkce h určující počet kroků mezi entitou A_i a A_j.

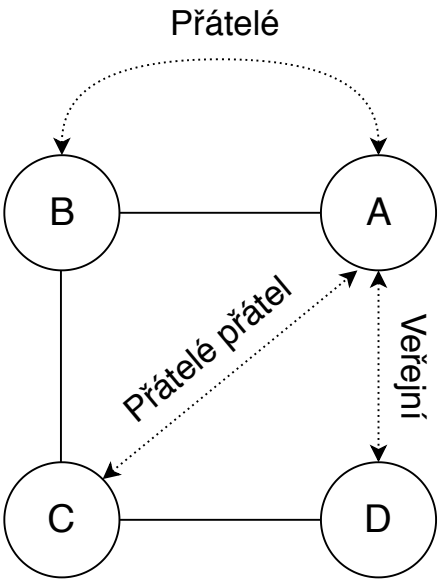
$$d_{ij} = h(A_i, A_j) \tag{2.1}$$

V závislosti na stupni separace se v modelech založených na přátelství rozlišují 3 skupiny přátel, tj. přátelé (hodnota funkce h rovna 1), přátelé přátel (hodnota funkce h rovna 2) a ostatní neboli veřejní, u kterých nabývá funkce h hodnoty 3 a více. Do poslední skupiny se řadí i ty entity, které mezi sebou nemají žádnou vazbu. Příklad tohoto modelu je znázorněn na obrázku 2.1. Na základě stupně separace jsou uživateli odkrývány informace o ostatních. To znamená, že uživatel A by měl zjistit více informací o uživateli B než o uživateli D viz obr. 2.1. Pokud se předpokládá standardní chování, tj. čím bližší osoba tím důvěrnější informace jsou poskytovány.

2.3.3 Úrovně viditelnosti v OSN

Tato práce si klade za cíl analyzovat uživatelský účet z pohledu externího a interního uživatele. Z pohledu uživatele sociální sítě, lze rozlišovat pohledy na profil dle toho, zda je uživatel přihlášený či nepřihlášený. Přihlášenému uživateli je zobrazen interní pohled na profil, nepřihlášenému se zobrazuje externí pohled.

V interní části si uživatelé nastavují a spravují svůj profil. Na druhou stranu externí část svého profilu nesledují tak často. Ale vidí ji ostatní uživatelé. Pro větší názornost nechť existují dva uživatelé A a B pracující se sociální sítí Facebook. Pokud se uživatel A úspěšně přihlásí dostává se do interní části sociální sítě. Pokud do vyhledávacího pole zadá jméno uživatele B a zobrazí si jeho profil, tak sleduje externí část profilu uživatele B. Stejně tak pokud se nepřihlášený uživatel B rozhodne pomocí internetového vyhledávače vyhledat uživatele A a nalezne ho, zobrazí se mu externí profil.



Obrázek 2.1: Stupně separace na sociálních sítích

Interní pohled

Interním pohledem, lze označit situaci či stav, kdy je uživatel přihlášen ke svému účtu a je mu dovoleno být aktivní na sociální síti, interagovat s ostatními účastníky, zobrazit si své nastavení účtu a v případě potřeby jej modifikovat. V rámci interního pohledu by mělo být uživateli umožněno editovat externí pohled.

Externí pohled

Externí pohled je možné definovat jako stav, kdy si nepřihlášený uživatel zobrazí svůj profil nebo kdy si přihlášený uživatel zobrazí profil někoho jiného.

Další variantou externího pohledu může být přístup k informacím o uživateli pomocí API sociální sítě. Tato rozhraní jsou velice komplexní systém, umožňující třetí straně přistupovat k informacím o uživateli. Je samozřejmé, že nejsou poskytovány všechny informace komukoliv. Většinou k informacím pomocí API přistupují aplikace, či webové stránky, kterým nejprve musí uživatel udělit přístup ke svým datům. Ale i tak nejsou prostřednictvím API dostupné informace o nastavení účtu.

2.4 Sociální sítě

V této části práce budou popsány jednotlivé sociální sítě. Nejprve bude u každé sítě popsán její účel a zaměření, dále bude následovat prezentace výchozí konfigurace nastavení soukromí a závěr bude vždy věnován drobné diskuzi ohledně nastavení soukromí. Zhodnocení výchozího nastavení sociálních sítí bude součástí následujících kapitol, kde bude tato problematika popsána detailněji a budou zde prezentovány výchozí nastavení soukromí těchto sítí. Dále prezentované sítě byly vybrány, tak aby zde byli zástupci jak těch nejznámějších sítí (Facebook, Twitter, Instagram, Google, LinkedIn), tak i zástupci sítí, které nejsou známé v takové míře (Tumblr, Pinterest).

2.4.1 Facebook

Facebook[1] v dnešní době s přibližně 2.45mld (srpen 2019) uživatelů zaujímá pozici nejpopulárnější sociální sítě. Jedná se o univerzální sociální síť dovolující sdílet fotografie, videa, události, posílat zprávy, hrát hry a mnoho dalších aktivit.

Nastavení	**Výchozí hodnota**
Jméno	Zadané při registraci
Nakládání s účtem po smrti	Nedefinováno
Dvoufázové ověření	Vypnuto
Kdo vidí vaše příspěvky	Přátelé
Kdo Vám může posílat žádosti o přátelství	Všichni
Kdo vidí seznam přátel	Veřejný
Kdo Vás může vyhledat podle e-mailu	Všichni
Kdo Vás může vyhledat podle telefonního čísla	Všichni
Propojení vyhledávačů mimo Facebook s profilem	Ano
Kdo může na Váš profil přidávat příspěvky	Přátelé
Kdo může vidět příspěvky na vašem profilu	Přátelé
Povolit ostatním sdílet vaše příspěvky	Zapnuto
Skrývat komentáře obsahující určitá slova	Vypnuto
Kdo může na vašem profilu vidět příspěvky kde jste označeni	Přátelé přátel
Kontrola příspěvků před zobrazením na profilu	Vypnuto
Kontrola označení ve vašich příspěvcích před zveřejněním	Vypnuto
Povolit sdílet vaše veřejné příběhy	Zapnuto
Povolit sdílet vaše příběhy lidem, které zmíníte	Vypnuto
Historie polohy	Vypnuto
Automatické rozpoznávání uživatelů	Vypnuto

Tabulka 2.2: Vybraná nastavení umožňovaná sítí Facebook

Za základní stavební kámen sítě lze považovat uživatelský účet neboli profil. Uživatelé mohou zakládat různé skupiny na základě svých názorů, aktivit, aj. Součástí Facebooku jsou také různé vestavěné aplikace jako například hry, počasí a jiné. Pro vytvoření účtu stačí vlastnit e-mailový účet, poskytnout datum narození a souhlasit s podmínkami sítě.

Ze strany bezpečnostních nastavení a nastavení soukromí se zde nabízí celá řada možných nastavení viz 2.2. Facebook disponuje výchozí konfigurací nastavení účtu, tím pádem je registrace rychlá a pokud má uživatel zájem, může svá nastavení modifikovat. Samozřejmostí je editace jména a kontaktů, správa aktivních zařízení a mnoho dalšího. Výchozí nastavení je zobrazeno v 2.2. Kromě těchto nastavení je dále možno nastavit blokování uživatelů, příspěvků, skupin, aplikací aj. Pro nově příchozího uživatele, bez předchozích zkušeností se sociálními sítěmi se může snadno stát, že uživatel není schopen identifikovat dopad příslušného nastavení na svůj profil.

[1] https://www.facebook.com/

2.4.2 Twitter

Twitter[2] je sociální síť, která je známá především svými tweety, což jsou textové příspěvky omezené na délku maximálně 280 znaků. Registrovaní uživatelé mohou vytvářet nové tweety nebo sdílet dál již ty vytvořené. Neregistrovaní uživatelé mohou tweety pouze číst. Přístup k tweetum je možné realizovat stejně jako u většiny ostatních sítí pomocí webového rozhraní, mobilní aplikace nebo netradičně pomocí SMS, díky čemuž je někdy Twitter označován jako *SMS internetu*. Dle odhadů je zde aktivních 321 milionů uživatelů.

V případě Twitteru jsou nastavování bezpečnostních pravidel obdobná jako u Facebooku, při registraci se účtu nastaví předem dané bezpečnostní nastavení viz 2.3. Twitter nabízí méně možností nastavení než Facebook.

Nastavení	**Výchozí hodnota**
Uživatelské jméno	Generované při registraci z jména a příjmení
Dvoufázové ověření	Vypnuto
Tweety vidí pouze sledující váš účet	Vypnuto
Přidávat lokalizační údaje k tweetum	Vypnuto
Kdo Vás může označit	Kdokoliv
Přijímání zpráv od kohokoliv registrovaného	Vypnuto
Signalizace přečtení zprávy	Zapnuto
Vyhledávání na základě e-mailu	Vypnuto
Vyhledávání na základě telefonního čísla	Vypnuto
Personalizace dat pro cílenou reklamu	Vypnuto

Tabulka 2.3: Vybraná nastavení umožňovaná sítí Twitter

2.4.3 Youtube

Youtube[3] je největším serverem pro sdílení videa. Umožňuje svým registrovaným uživatelům nahrávat, sledovat a hodnotit videa. Většina obsahu je nahrána individuálními uživateli, i když i některé mediální korporace využívají tohoto kanálu pro zveřejňování svých videi. Neregistrovaní uživatelé mohou videa pouze sledovat.

I když Youtube nezapadá zcela mezi sociální sítě, v kontextu této práce je tato služba zajímavá. Jelikož Youtube je vlastněno společností Google, tak i registrace, přihlašování a správa nastavení účtu a soukromí spadá pod správu Google účtu, resp. pro přihlášení do služby Youtube je zapotřebí mít registrovaný Google účet. Tento účet vlastní přibližně 1.5mld (březen 2019) lidí.

Z pohledu nastavení účtu je samozřejmostí možnost editace hesla, jména, příjmení, data narození, telefonního čísla a e-mailu. V nastavení lze také nalézt možnosti jako aktivita na webu a v aplikacích. Pokud je tato položka povolena, shromažďují se veškeré informace o aktivitě uživatele v rámci všech služeb Google. Jinými slovy pokud uživatel vlastní telefon se systémem Android a má toto nastavení aktivované veškerá aktivita se zaznamenává. Např. kdy uživatel telefonoval, místa hledaná na mapě, informace o používaných aplikacích, a mnoho dalšího. Další zajímavou položkou nastavení je historie používání Youtube nebo personalizace reklam. V souvislosti s nastavením kontaktů lze dohledat položku *Kontaktní údaje uložené z komunikace*, která je ve výchozím nastavení povolena viz 2.7.

[2] https://twitter.com/
[3] https://www.youtube.com/

Nastavení	Výchozí hodnota
Jméno, pohlaví, heslo	Definované při registraci
Primární a záložní e-mail	Definované při registraci
Telefonní číslo	Požadováno při registraci
Ukládání - Aktivita na webu a v aplikacích	Zapnuto
Aktivita na webu a v aplikacích včetně historie webu a aplikací	Zapnuto
Aktivita na webu a v aplikacích včetně nahrávek hlasu a zvuku	Vypnuto
Ukládání - Historie pozice	Vypnuto
Ukládání - Historie Youtube	Zapnuto
Historie Youtube včetně vyhledávání	Zapnuto
Ukládání - Kontaktní údaje z komunikace	Zapnuto
Ukládání - Kontaktní údaje z vašich zařízení	Zapnuto
Sdílení polohy	Vypnuto
Personalizace reklam	Zapnuto
Dvoufázové ověření	Vypnuto
Přihlášení pomocí telefonu	Vypnuto

Tabulka 2.4: Výchozí nastavení Google účtu

2.4.4 LinkedIn

LinkedIn[4] [1] je profesionální zaměstnanecky orientovaná sociální síť, kde se setkávají odborníci z různých odvětví, spravují své profily, které v mnoha případech slouží jako životopisy. Síť tedy spojuje na jedné straně odborníky, kteří možná hledají práci a na straně druhé zástupce firem popřípadě státních institucí hledající zaměstnance. LinkedIn stejně jako jiné sociální sítě poskytuje možnost vytvořit si vlastní profil a navazovat vztahy s ostatními uživateli. Jelikož je síť odborně a zaměstnanecky orientovaná, lze na profilu nalézt kromě standardních položek také položky jako vzdělání, pracovní zkušenosti, aktuální pracovní pozice, schopnosti aj. viz 2.5

Sociální síť LinkedIn používá pro označování vazeb mezi uživateli pojem *spojení*. Spojení mají stejně jako přátelství v případě sítě Facebook 3 úrovně, kde spojení prvního stupně odpovídá přátelům, spojení druhého stupně přátelům přátel, poslední úroveň je nazývána stejně veřejný. Díky této podobnosti, lze pro zjednodušení i v případě sítě LinkedIn používat již zavedený pojem přátelství.

2.4.5 Steemit

Steemit[5] je z části blogovací platforma, z části sociální síť. Tato platforma je založená na technologii blockchain. To znamená, že obsah není ukládán jako v případě jiných sociálních sítí přímo na serverech patřící dané sociální síti, ale je využíváno blockchainu. Základní funkcionalita spočívá v sledování zajímavých témat a poskytování kladné či záporné zpětné vazby prostřednictvím hlasování, samozřejmě uživatelé také mohou obsah vytvářet a diskutovat s ostatními účastníky. Platforma Steemit odměňuje své aktivní uživatele svou virtuální měnou. Aktivitou se zde rozumí zveřejňování nového obsahu, komentování, ale i hlasování o obsahu.

[4] https://www.linkedin.com/
[5] https://steemit.com/

Nastavení	Výchozí hodnota
E-mail, heslo	Nastaveno při registraci
Jméno, příjmení	Nastaveno při registraci
Telefonní číslo	Nedefinováno
Dvoufázové ověření	Vypnuto
Kdo může vidět vaši e-mailovou adresu	Přátelé
Kdo může zobrazit seznam přátel	Přátelé
Jak se má zobrazit vaše jméno	Celé
Zobrazovat mé jméno v souvislosti se zaměstnavateli	Zapnuto
Viditelnost profilu mimo LinkedIn	Zapnuto
Mód prohlížení vašeho profilu	Jméno a Motto
Kdo smí vědět, že jste aktivní na síti	Přátelé
Sdílet automaticky změny pozice, vzdělání	Zapnuto
Povolit označování	Zapnuto
Kdo může objevit Váš profil pomocí e-mailu	Všichni
Kdo může objevit Váš profil pomocí tel. čísla	Všichni
Sdělte náborářům, že hledáte novou pozici	Vypnuto
Kdo s vámi může navázat přátelství	Všichni
Kdo vám může posílat zprávy	Všichni

Tabulka 2.5: Vybraná nastavení sítě LinkedIn ve výchozí konfiguraci

Při registraci má uživatel volbu mezi okamžitou registrací, která je zpoplatněna nebo registrací, která je zdarma, ale údajně by měla proběhnout během dvou týdnů. Pro účely této práce bylo dva krát zažádáno o vytvoření účtu. Ale ani jedna z žádostí o registraci nebyla během několika měsíců sociální sítí vyřízena.

2.4.6 Tumblr

Tumblr[6] je sociální síť vzniklá v USA v roce 2007. Síť umožňuje uživatelům sdílet multimédia a další různý obsah formou krátkých blogů. Stejně jako u většiny jiných sociálních sítí existuje i zde možnost sledovat blogy ostatních uživatelů. Tumblr obsahuje přes 475 milionů uživatelských blogů (srpen 2019).

Co se týče rozmanitosti nastavení účtu, tak Tumblr nabízí pouze základní editaci registračního e-mailu a hesla. Z pohledu soukromí nabízí pouze 3 nastavení.

- Umožnit ostatním vidět, že je uživatel aktivní
- Umožnit sítí Tumblr přístup k historii vyhledávání
- Umožnit sběr dat z cookie

2.4.7 Instagram

Sociální síť Instagram[7] se zaměřuje především na sdílení fotek a krátkých videi. Instagram je především mobilní aplikací, která umožňuje svým uživatelům na pořízené fotografie aplikovat řadu filtrů a poté jednoduše sdílet. Sdílený obsah lze zpřístupnit buď to veřejně nebo

[6] https://www.tumblr.com/
[7] https://www.instagram.com/

předem schváleným uživatelům označovaným jako *sledující*. Sdílený obsah může být označen tagy a lokalizačními údaji. Jedná se o velice populární síť, počet uživatelů v roce 2019 přerostl jednu miliardu. V kontextu této sítě se krátká videa nazývají příběhy. Dalším indikátorem popularity je denní aktivita uživatelů. Denně sdílí průměru 500 milionů uživatelů svůj nový příběh.

Nastavení soukromí reprezentují tři položky:

- Soukromý účet - Pokud je váš účet soukromý, vaše fotky a videa na Instagramu uvidí jen lidé, které schválíte. Na lidi, kteří vás už sledují, to nebude mít vliv.
- Zobrazit stav aktivity - Umožněte účtům, které sledujete, a komukoli, komu napíšete, aby viděli, kdy jste byl(a) v instagramových aplikacích naposled aktivní. Když je tato funkce vypnutá, neuvidíte stav aktivity ostatních účtů.
- Povolit sdílení - Umožněte přátelům sdílet vaše příběhy jako zprávy

Ve výchozí konfiguraci sítě jsou povolena poslední dvě nastavení, nastavení *Soukromí účet* není aktivováno.

2.4.8 Pinterest

Pinterest[8] je sociální síť nabízející svým uživatelům možnost vytvářet kolekce obrázků, či fotografii. Ostatní uživatelé mohou tyto kolekce procházet, komentovat, označovat tlačítkem *Like* nebo si je přidat do vlastní kolekce. I zde je možná uživatelská interakce, která dovoluje vytvářet kolekce společně.

Sekce nastavení soukromí v případě této sítě obsahuje pouze jednu položku *Skrýt profil před externími vyhledávači (Google).*

2.4.9 Shrnutí

Jak naznačují výše popsané možnosti zabezpečení na sociálních sítích, nelze předpokládat existenci jednoho přenosného nastavení pro všechny sítě. Tato skutečnost plyne z toho, že stejně jako má každá sociální síť svá specifika, tak i možností nastavení jejich zabezpečení jsou různorodá, také granularita nastavení je síť od sítě různá. Z těchto důvodu nelze všechna bezpečnostní nastavení z jedné sítě očekávat i v síti jiné.

2.5 Entita

Definice sociální sítě byla společně s přehledem několika sociálních sítí popsána výše. Než bude možné přejít dále k mechanismům provádějícím vyčíslení soukromí entit. Je potřeba definovat entitu a model popisující entitu.

Entitu [3] lze definovat, jako libovolný objekt reálného světa, který je zaznamenán v objektovém modelu. Entita musí být v rámci modelu jedinečná. V kontextu této práce se entita definuje specifičtěji, jako uživatel sociální sítě nebo skupina těchto uživatelů.

Model popisující entitu

Pro jednoduchý a jednotný přístup k jednotlivým položkám entity při evaluaci privátnosti v rámci OSN(Online social network), se u většiny modelů používá popis založený na maticích tzv. *Odpovědní matice* [9]. Tento popis definuje entitu jako vektor vlastností V_0 až V_n

[8] https://www.pinterest.com/

o velikosti n, kde V_k (k $\in$ <0,n>) je číselná hodnota interpretována specificky na základě použitého modelu. Odpovědní matice následně vznikne složením jednotlivých vektorů. Výsledkem je tedy matice MxN, kde řádky odpovídají jednotlivým entitám a sloupe jejich vlastnostem.

Nejčastěji ovšem udává míru ochoty uživatele sdílet informaci o dané vlastnosti, V_k je kladné reálné číslo. Platí, že čím vyšší hodnota V_k, tím ochotněji entita vlastnost sdílí. Na druhou stranu pokud je hodnota příliš malá, lze usuzovat, že se jedná o privátní atribut entity.

Přínos tohoto popisu spočívá v jednotném přístupu k popisování vlastností entity v OSN napříč různými výpočetními modely. Pro evaluaci konkrétní hodnoty atributu konkrétní entity bude v rámci práce používán následující zápis. R(i,j)=x, kde *i* je uživatel tedy řádek matice, *j* je konkrétní vlastnost - sloupec matice, *x* je příslušná hodnota z odpovědní matice. Příkladem může být interpretace: uživatel *i* je ochotný vlastnost *j* sdílet s ohledem na *x*, kde *x* udává míru ochoty tuto informaci sdílet. Například při použití dvoustavového nastavení *0* označuje neochotu sdílet tuto informaci, na druhé straně hodnota *1* udává ochotu sdílet. Tato situace je znázorněna na 2.2, kde uživatel **i** sdílí jméno a E-mail, naopak příjmení a PSČ se rozhodl nesdílet.

$$\text{R} = (\text{Jméno, Příjmení, PSČ, E-mail})$$
$$\text{R(i)} = (1, 0, 0, 1)$$

Obrázek 2.2: Příklad vektoru uživatele v odpovědní matici

2.6 Vyčíslení privátnosti

V této části práce bude nejprve představena metrika *Privacy score* používaná pro reprezentaci míry ohrožení soukromí, zmíněn bude kompozitní atribut a následně budou prezentovány jednotlivé metody nebo-li modely pro výpočet *Privacy score* prezentované v [19, 18, 9].

2.6.1 Privacy score

Aby bylo možné vhodným způsobem zpracovávat úroveň soukromí je potřeba mechanismus, který tuto úroveň umožní vyčíslit. Podobný mechanismus již spolehlivě funguje v různých odvětvích komerčního sektoru. Z toho důvodu byla metoda převzata [9]. Metoda vychází z již fungujících technik pro určování skóre entity. Tyto techniky se používají například v bankovnictví, kde se určuje bonita nebo důvěryhodnost klienta na základě jeho vlastností. Metoda se v kontextu soukromí na sociálních sítích nazývá Privacy score. Indikuje potenciální nebezpečí pro soukromí entity. Platí, že čím vyšší Privacy score tím vyšší riziko.

Evaluace privátnosti/soukromí není zcela triviální disciplínou. Již definice privátnosti může být problematická neboť je subjektivní a různí lidé mohou chápat privátnost odlišně. Také váha jednotlivých vlastností soukromí může být napříč populací různá. Například jeden člověk považuje telefonní číslo za velmi citlivou informaci zatímco jiný může považovat tuto informaci za naprosto nepodstatnou.

Ovšem z druhé strany, ač se mohou uživateli zdát některé z vlastností nepodstatné, opak může být pravdou. Toto dokazují například publikace [18, 7, 8], kde jsou jednoznačně definovány některé atributy, které mají značný dopad na soukromí uživatele bez ohledu na subjektivní vnímání.

Na základě těchto znalostí vznikla řada přístupů a modelů pro evaluaci privátnosti a výpočet Privacy score.

2.6.2 Virtuální atribut

Virtuální nebo také kompozitní atribut se skládá z několika jiných atributů. Kombinace několika zdánlivě nepodstatných atributů může vést k odhalení podstatné části soukromí uživatele. Například v práci [8] se poukazuje na skutečnost, že 87% obyvatel Ameriky lze identifikovat na základě poštovního směrovacího čísla, pohlaví a data narození. Ačkoliv každý z těchto atributů samostatně pro soukromí nepředstavuje značné riziko, dohromady mohou vést k unikátní identifikaci jedince. Jednou z metrik dále prezentovaných modelů je právě odhalování virtuálních atributů.

2.6.3 Model citlivosti a viditelnosti

Prvním zástupcem modelů evaluace je základní model citlivosti a viditelnosti [9] využívaný i dalšími pokročilejšími modely. Základními složkami pro výpočet Privacy score tímto modelem jsou:

- citlivost nebo-li privátnost vlastnosti **i** je označována jako β_i. Problematikou nastavení vah jednotlivých atributů se zabývá práce [18], z které vychází tabulka 2.6, kde jsou zobrazeny váhy vybraných atributů. Pro tento výpočetní model platí, že se zvyšující se citlivostí vlastnosti **i** roste také Privacy score entity.
- viditelnost vlastnosti **i** entity **j** se značí V(i,j), kde funkce V je definována pomocí stupně separace. Viz definice níže. Platí, že s rostoucím počtem uživatelů, se kterými je informace o vlastnosti sdílena, roste i Privacy score entity.

$$\text{V(i,j)}=\begin{cases} 0, & \text{pokud i vidí pouze sám} \\ 1, & \text{pokud i vidí přátelé} \\ 2, & \text{pokud i vidí přátelé přátel} \\ 3, & \text{pokud i vidí všichni} \end{cases} \tag{2.2}$$

Na základě výše definovaných vlastností se Privacy score definuje jako monotonně rostoucí funkce dvou parametrů, citlivosti (privátnosti) a viditelnosti informací o entitě. Příkladem poukazující na důležitost parametru citlivosti může být scénář, kdy entita **j**, v tomto případě uživatel sdílí dvě osobní informace, telefonní číslo x a vzdělání y. Situace R(x,j) = 1 && R(y,j) = 0 je mnohem nebezpečnější z pohledu citlivosti sdílených informací než R(x,j) = 0 && R(y,j) = 1. V tomto případě i když velká skupina lidí bude znát vzdělání uživatele **j** není to stejné jako kdyby stejná skupina lidí znala jeho telefonní číslo.

Privacy score entity **j** je vypočítáno na základě následujícího vztahu:

$$PR(j) = \sum_{i=1}^{n} PR(i,j) = \sum_{i=1}^{n} \beta_i * V(i,j) \tag{2.3}$$

2.6.4 PIDX (Privacy Index)

Dalším z modelů vyčíslující soukromí entity resp. Privacy score je PIDX [19]. Měří úroveň publicity jedné entity vzhledem k jiné. Model PIDX pracuje se třemi metrikami: známé atributy, jejich citlivost a viditelnost. Na základě kombinací těchto metrik se určí míra

Atribut	**Váha atributu**[%]
Jméno	15
Vzdělání	15
Stav	25
Rodinní příslušníci	25
Pohlaví	25
Město	45
Stát	45
Fotografie	45
List přátel	60
E-mail	65
Domovské město	65
Navštívená místa	65
Datum narození	65
Telefonní číslo	70
Aktuální pozice	80
Rodné číslo	90

Tabulka 2.6: Tabulka citlivostí atributů (Zdroj:[18])

ohrožení soukromí entity. Dle zvolené kombinace a kombinačního přístupu k metrikám se rozlišují tři typy: w-PIDX váhovaný PIDX, m-PIDX (maximum PIDX) a c-PIDX (composite PIDX).

Aby byla brána v potaz citlivost atributu, je každému atributu přidělen PIF (privacy impact factor). PIF je numerická hodnota mezi 0 a 1, kde 1 znamená maximální citlivost atributu. Pro výpočet PIF se použije vzorec 2.4, kde **i** značí konkrétní atribut a W_{max} maximální hodnotu citlivosti, konkrétní hodnoty lze nalézt v dříve prezentované tabulce vah 2.6.

$$PIF(i) = \frac{W(i)}{W_{max}} \tag{2.4}$$

Všechny varianty PIDX pracují s viditelností atributů resp. se stupněm separace a s výše definovaným PIF. Jednotlivé metody se liší pouze postupem výpočtu.

Index privátnosti PIDX je definován jako míra vyzrazení soukromí entity A_j směrem k entitě A_i. V rámci této práce bude vždy zkoumán jeden konkrétní účet sociální sítě vůči okolí, tím pádem lze zápis funkcí modelu mírně zjednodušit oproti definicím uvedeným v [18]. Funkce PIDX nabývá hodnot z intervalu $< 0, 100 >$. Vysoká hodnota PIDX znamená vysoké prozrazení soukromých informací entity.

Nechť existuje množina $S = \{s_1, s_2, ..., s_n\}$ obsahující PIF váhy pro jednotlivé atributy a vektor $V = (v_1, v_2, ..., v_n)$ obsahující hodnoty viditelnosti, které odpovídají jednotlivým atributům entity. Jak bylo zmíněno výše existují 3 různé varianty indexu privátnosti PIDX:

1. w-PIDX vyčísluje privátnost vztahem

$$w - PIDX(V, S) = \frac{\sum_{j=1}^{n} V(j)s_j}{\sum_{j=1}^{n} s_j} \tag{2.5}$$

2. m-PIDX měří maximální možné odhalení privátnosti entity A_j směrem k A_i

$$m - PIDX(V, S) = \max(V(1)s_1, .., V(n)s_n) \tag{2.6}$$

kde funkce max vrací ze zadaných hodnot tu maximální.

	Název nastavení	Nastavení	Viditelnost	Váha[%]
1	Web & App Aktivita	Zapnuto	1	65
2	Historie polohy	Pozastaveno	0	65
3	YouTube historie	Zapnuto	1	60
4	Kontakty z interakcí	Zapnuto	1	60
5	Kontakty ze zařízení	Pozastaveno	0	60

Tabulka 2.7: Příklad nastavení účtu Google

3. c-PIDX nebo-li kompozitní PIDX, jak napovídá název tato metoda v sobě kombinuje dva předchozí přístupy w-PIDX a m-PIDX, což může být zapsáno jako:

$$c - PIDX(V,S) = m - PIDX(V,S) + \\ (100 - m - PIDX(V,S)) \cdot \frac{w - PIDX(V,S)}{100} \tag{2.7}$$

Zatímco, w-PIDX reflektuje inkrementální změny atributu, m-PIDX se hodí spíše pro hodnocení aktuálního soukromí, těchto dvou vlastností využívá poslední zástupce c-PIDX a snaží se kombinovat výhody obou přístupů [19].

Příkladem použití může být aplikace modelu C-PIDX na výchozím nastavení Google účtu, které je zobrazeno v tabulce 2.7. Pro výpočet Privacy score je zapotřebí množina V_i, která je reprezentována sloupcem *viditelnost* a množina vah S_i. Váhy se vypočtou dle vztahu 2.4. Například pro nastavení *Historie polohy*:

$$PIF(2) = \frac{60}{65} \tag{2.8}$$

Dále se již jen dosadí známé hodnoty do rovnic 2.5, 2.6 a 2.7, čímž se získá výsledné Privacy score modelem C-PIDX.

2.6.5 IRT

Matoda Item Response Theory (IRT) byla původně používána pro vyhodnocování dotazníků a testů [9]. Hlavní cílem bylo na základě pravděpodobností určit schopnosti zkoušených, obtížnost otázky a pravděpodobnost, že zkoušený odpoví na otázku správně. Vstupem do tohoto mechanismu je množina otázek a množina zkoušených, na druhé straně výstupem je odpovědní matice NxM, kde

$$R(i,j) = 1 \tag{2.9}$$

v případě správné odpovědi. i zde reprezentuje testovaného, j otázku. Naopak v případě nesprávné odpovědi obsahuje matice hodnotu 0, tj.

$$R(i,j) = 0 \tag{2.10}$$

Tento výpočetní model určuje skóre privátnosti jako pravděpodobnost.

$$P(R(i,j) = 1) \tag{2.11}$$

Jelikož původně model pracuje s testovanými a otázkami, v případě určování skóre privátnosti se mapuje zkoušený na uživatele a otázka na atribut uživatele.

Kapitola 3

Návrh systému evaluace privátnosti

V této kapitole bude nejprve prezentováno již existující řešení, poté bude představena architektura navrhovaného systému, stručně budou popsány její stavební kameny a jejich funkcionalita. Následně budou jednotlivé části popsány detailněji včetně všech vstupů a výstupů potřebných pro práci nástroje. Taktéž budou postupně definovány potřebné konstanty na základě dostupných prací zabývajících se těmito tématy.

3.1 Existující řešení

Jak již bylo popsáno výše tématem soukromí na sociálních sítí se zabývalo již několik prací. Některé z nich prezentovaly pouze teoretické modely nebo prováděly analýzy a studie, jiné se naopak zabývaly stejně jako tato práce vývojem nástroje pro měření potenciálního úniku informací.

Aplikace *Privometr* (obr. 3.1) publikovaná v [13] je prezentovaná jako první funkční prototyp nástroje provádějící měření soukromí na sociální síti. Aplikace využívala jako zdroj informací API sociální sítě Facebook. Bohužel dnes již tato aplikace není dostupná. Patrně díky změně API sítě Facebook. Dle autorů aplikace prováděla predikci soukromích atributů uživatele na základě informací o přátelích a členstvích ve skupinách. A poté určovala pravděpodobnost vyzrazení privátních informací. Zatímco tato práce přistupuje k problematice odlišně. Klade si tyto cíle:

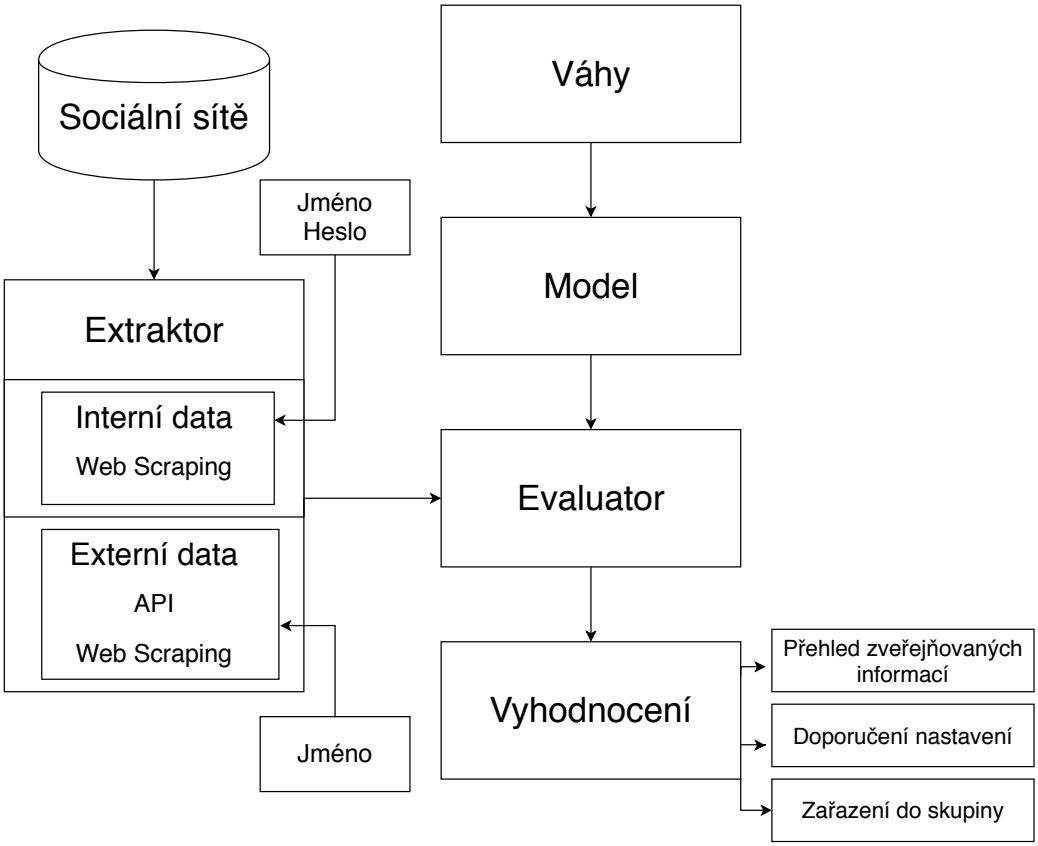
- číst přímo uživatelská nastavení jedné konkrétní sociální sítě, pracuje tedy s naprosto přesnými informacemi. Vyhodnotí je, prezentuje výsledky a následně doporučit nastavení na základě získaných informací o nastavení právě přihlášeného uživatele.
- získat informace o uživateli z více různých sociálních sítí, agregovat je, provést analýzu dostupných informací a následně prezentovat výsledky.

3.2 Architektura systému

Navrhovaný systém by se měl skládat ze tří hlavních částí, z extraktoru, evaluatoru a modulu vyhodnocení. Vstupním bodem do nástroje bude extraktor, v závislosti na jeho výstupu bude pracovat evaluator a nakonec bude modul vyhodnocení prezentovat výsledky uživateli.

Obrázek 3.1: Náhled nástroje Privometr (Zdroj:[13])

Kompletní schéma systému je zobrazeno na obr. 3.2. Funkcionalita jednotlivých částí bude podrobněji popsána v průběhu kapitoly.



Obrázek 3.2: Architektura navrhovaného systému pro evaluaci privátnosti

Extraktor

Hlavním úkolem extraktoru je získat uživatelská data ze sociálních sítí a poskytnout je v jednotném formátu na výstup pro další zpracování. Samotný proces získání dat spočívá v jednoduchém stažení obsahu stránky. Ale jelikož navrhovaná aplikace si klade za cíl podporovat analýzu různých sociálních sítí, stává se nutností extrahování z různých zdrojů v různých formátech. Proto samotný extraktor bude složen z několika modulů, kde každý modul bude obsluhovat jednu sociální síť. Tento přístup také zajistí snadnou rozšiřitelnost v případě potřeby analyzovat další doposud nepodporovanou sociální síť.

Pro případ, kdy je analyzováno několik různých zdrojů informací obsahuje extraktor modul pro agregaci informací. Cílem tohoto modulu je identifikovat jednoho uživatele tj. sama sebe napříč různými sociálními sítěmi a získat informace o jeho nastavení. Tyto informace se následně budou agregovat a poskytovat ve stejném formátu jako by pocházely pouze z jedné sítě.

Evaluator

Do komponenty evaluatoru budou vstupovat data z dříve popsané komponenty extraktoru. Za další vstupy se budou považovat váhy jednotlivých nastavení a model provádějící samotné vyčíslení soukromí na základě informací získaných v předchozí komponentě. Z důvodu nalezení nejvhodnějšího výpočetního modelu, ale také opět kvůli snadné rozšiřitelnosti aplikace bude možné použít různé modely popsané v 2.6 nebo definovat další bez zasahování do samotného evaluatoru.

Modul vyhodnocení

Poslední částí nástroje bude logika vyhodnocující a prezentující výsledky na základě obdržených dat od evaluatoru. Případně bude tato část provádět export dat v jednotném formátu pro další zpracování.

3.3 Extrakce nastavení účtu

Ačkoliv sociální sítě poskytují API aplikacím třetích stran pro přístup k informacím, nejsou touto cestou poskytovány všechny dostupné informace a to informace o nastavení účtu a především informace o nastavení soukromí. Proto získávání informací ze sociálních sítí navrhovanou aplikací bude rozděleno na dva přístupy. Prvním z nich bude zajištění informací prostřednictvím API. Druhý přístup bude o něco náročnější neboť bude potřeba prostudovat strukturu stránek obsahující nastavení nedostupná přes API a následně vyextrahovat požadované informace. Zatímco první přístup bude aplikován především na získání dat z externího prostředí sociální sítě, druhý přístup bude aplikován na získání informací z interního prostředí účtu a získání nedostupných informací z API.

3.3.1 Interní pohled

Jak bylo popsáno výše některé informace o nastavení není možné získat prostřednictvím API, proto bude pro získání informací o nastavení soukromí použita technika *Web scraping*.

Web scraping

Pojmem Web scraping se rozumí proces získávání dat z internetu [14]. Tato technika se široce využívá pro získávání znalostí z webových dat, monitorování změn na webu, extrahování kontaktů, porovnávání cen různých e-shopů a mnoho dalšího. Existuje mnoho přístupů k extrakci informací, několik základních bude prezentováno níže:

- Hledání vzorů - jednoduchý přístup založený na vyhledávání vzorů ve webových stránkách pomocí regulárních výrazů
- HTML parsing - přístup založený na extrakci jednotlivých elementů HTML dokumentu
- DOM parsing - přístup založený na prohledávání DOM, který je definovaný W3C

3.3.2 Externí pohled

Pro získávání informací o uživateli z externího pohledu lze brát v úvahu několik různých přístupů. Každý z dále prezentovaných postupů extrakce informací má kladné i záporné stránky, z toho důvodu zde boudou popsány 3 různé návrhy přístupu.

API

Sociální sítě, které poskytují oficiální API pro vývojáře aplikací většinou požadují registraci klientské aplikace a vygenerování autentizačního tokenu, pomocí kterého je následně API přístupné. Tato akce vyžaduje souhlas dotčeného uživatele sociální sítě s tím, že aplikace bude přistupovat k jeho uživatelským údajům. Za pozitivní lze považovat široké spektrum poskytovaných informací o uživateli prostřednictvím rozhraní, které poskytuje data ve standardizovaných formátech. Také jednoduchá sémantika a dokumentace rozhraní jsou značně pozitivní vlastnosti.

Ovšem z pohledu použitelnosti navrhované aplikace tento přístup nese jistá úskalí. Jelikož si práce klade za cíl vytvořit aplikaci, která bude provádět analýzu soukromí hned na několika sociálních sítích (alespoň 7), tak by nebylo pro uživatele nejkomfortnější zadávat pro každou z podporovaných sociálních sítí jméno a heslo. U některých uživatelů může již představa zadávání jména a hesla do aplikace 3. strany vyvolávat pochyby. A jak bylo popsáno výše pro přístup k API je potřeba součinnost uživatele v podobě přihlášení se ke svému účtu a odsouhlasení přístupu k informacím pro navrhovanou aplikaci.

Extrakce informací přes přihlášeného uživatele

Dalším uvažovaným přístupem je vyhledávání informací přímo ve webovém rozhraní sociální sítě. Pro tento účel by byl vytvořen přístupový účet, přes který by se přistupovalo k informacím o ostatních uživatelích. Tento přístup by zahrnoval zdokumentování rozhraní webové služby sociální sítě, aby bylo možné klást dotazy a následné použití techniky scrapovaní pro extrakci získaných dat, která je popsána výše 3.3.1.

Za kladnou stránku tohoto přístupu lze brát skutečnost, že uživatel pro spuštění aplikace a provedení analýzy soukromí není nucen zadávat své heslo. Na druhou stranu použití tohoto přístupu značně limituje rozmanitost získaných informací. Dalším negativním aspektem je potřeba přesně určit analyzovaný účet. Neboť na sociálních sítích není výjimkou existence několika účtů, které nejsou rozlišitelné na základě jména a příjmení. Proto by byla potřeba

	Váha atributu[%]	Skupina I	Skupina II	Skupina III
Jméno	15	1	1	1
Vzdělání	15		1	1
Stav	25			1
Rodinní příslušníci	25			1
Pohlaví	25	1	1	1
Město	45		1	1
Stát	45		1	1
Fotky	45			1
List přátel	60			1
E-mail	65			1
Domovské město	65			1
Navštívená místa	65			1
Datum narození	65			1
Telefonní číslo	70			1
Aktuální pozice	80			1
Rodné číslo	90			

Tabulka 3.1: Konfigurace výchozích hodnot vah, definice typů uživatelů (Zdroj:[18])

další interakce s uživatelem, aby identifikoval správný účet tedy svůj, což v určitých případech může být také značný problém. Pokud uživatel nemá profilovou fotografii a žádné další informace o sobě neposkytuje je nemožné od sebe jednoznačně odlišit dva nebo více stejně se jmenujících účtů bez dalších informací.

Extrakce informací bez interního uživatele

Poslední navrhovaný přístup se velice podobá předchozímu, až na skutečnost, že k informacím je přistupováno pomocí veřejného rozhraní sociální sítě. Tento přístup lze považovat za nejméně účinný co se týče množství získaných informací. Z pohledů výhod a nevýhod platí stejná fakta jako u předchozího přístupu až na situaci, kdy se webové rozhraní sociální sítě pokouší zabránit automatizovanému přístupu. Sociální sítě disponují celou řadou detekčních mechanismů, které se snaží hlídat, aby přes webové rozhraní k sociální síti přistupovali pouze skuteční uživatelé (lidé). V případě detekce robota sociální síť například zamkne účet a je vyžadována reaktivace účtu pomocí kódu zaslaného e-mailem. Zatímco tento problém je potřeba u předešlého přístupu aktivně řešit, v případě vyhledávání informací bez přihlášení jen pomocí veřejného rozhraní se řešit nemusí.

3.4 Evaluace soukromí

Jak napovídá 2.6 existuje celá řada výpočetních modelů snažících se vyčíslit úroveň resp. skóre privátnosti. Většina používaných metod používá jako vstup dvě proměnné, viditelnost atributu a jeho váhu. Zatímco viditelnost se určuje relativně snadno na základě stupně separace 2.3 přímo z dat, tak pro nastavení jednotlivých vah atributů je zapotřebí tyto váhy definovat. Přiřazením vah k jednotlivým atributům byl v práci [18] použit statický model s hodnotami viz 3.1, hodnoty byly pravděpodobně získány experimentálním způsobem. Stejný model je použit i v [19]. Výsledky obou prací potvrzují vhodnost tohoto konkrétního nastavení. Z toho důvodu bude použito i v této práci.

V 2.6 bylo popsáno několik modelů pro evaluaci privátnosti, ačkoli metoda IRT eliminuje problém s určováním vah jednotlivých atributů, díky čemuž by mohla být značným přínosem

pro tuto práci, tak nelze použít jelikož pro její aplikaci je nutné pracovat s množinou uživatelů.

Pro tuto práci bude zvolen jeden z modelů PIDX nebo model váhy a viditelnosti. Volba bude záviset na testování modelů v různých situacích. Výběr modelu bude detailněji popsán v kapitole implementace.

3.5 Vyhodnocení nastavení

Poslední částí navrhovaného nástroje je modul vyhodnocení, na základě získaných informací o uživateli ze sociální sítě a výsledku práce evaluačního modelu budou uživateli poskytnuty výstupy. Na jejichž základě se bude moci uživatel rozhodnout, zda nastavení jeho profilu odpovídá jeho představám či nikoliv a provede úpravu svého nastavení. Nástroj bude poskytovat tyto výsledky:

- Detailní výpis poskytovaných informací
- Procentuální míru možného ohrožení privátnosti - vizualizovaný výsledek použitého evaluačního modelu
- Zařazení do níže definované třídy uživatelů

3.5.1 Třídy uživatelů

V návaznosti na předešlých pracích byly v [2] definovány skupiny uživatelů sociálních sítí. Tyto skupiny byly vytvořeny na základě uživatelského přístupu k citlivým informacím. Existuje dělení do tří základních skupin. První a nejstriktnější skupinou jsou tzv. *fundamentalisté* (Skupina I) , nejsou ochotni sdílet téměř žádné informace. Druhou skupinou jsou uživatelé (Skupina II) , kteří informace sdílí, ale snaží se kontrolovat co a komu sdílí. Poslední skupinu (Skupina III) reprezentují uživatelé sdílející většinu svých informací. Detailní informace o poskytovaných informacích jednotlivými skupinami jsou zobrazeny v tabulce 3.1.

Kapitola 4

Implementace

Tato kapitola bude dokumentovat průběh implementace navrhovaného nástroje. Budou zde popsány problémy, které bylo třeba řešit v rámci jednotlivých komponent. První část kapitoly se bude zabývat především komponentou extraktoru, která bude zmíněna detailněji, neboť zde probíhá interakce s internetovým prostředím, díky čemu vzniká množství problematických situací. V této části kapitoly bude dále pojednáváno o použitých prostředcích pro získávání webového obsahu a bude zdokumentována struktura dat v jaké jsou uloženy informace o nastavení soukromí na jednotlivých sociálních sítích.

Druhá část kapitoly bude věnována vyhodnocení a evaluaci získaných dat. Bude se zde pojednávat o problematice výběru vhodného modelu a konverze modely naměřených hodnot do uživatelsky pochopitelné podoby.

Navrhovaný nástroj byl implementovaný jako konzolová aplikace s možností rozšíření o grafické rozhraní. Pro implementaci byl zvolen jazyk Python, protože disponuje širokou škálou modulů umožňujících práci s webovými stránkami. Taktéž podporuje framework Selenium, což je nástroj dovolující automatizované testování webových aplikací. Tato technologie a její použití v rámci práce bude blíže popsáno v rámci kapitoly.

Jak bylo zmíněno v kapitole Návrh, nástroj by měl provádět externí a interní analýzu soukromí sociálních sítí. Celý proces běhu aplikace je pro oba přístupy velice podobný pouze s drobnými rozdíly. Tyto odlišnosti budou popsány v závěru kapitoly.

4.1 Extraktor

Jelikož cílem práce je automatizovaně a s co nejmenším uživatelským úsilím vyhodnotit uživatelské nastavení zabezpečení na sociální sítí, musí se navrhovaný nástroj nejprve na sociální síť přihlásit a poté nalézt potřebná data. Ač se může zdát tento úkol triviální a šlo by se domnívat, že celý problém vyřeší několik HTTP dotazů, přináší tento úkol řadu úskalí a problémů:

- Nutnost extrahovat konkrétní HTTP dotazy
- Nutnost překonat aplikační firewally webových aplikací
- Rozdílná struktura dat sociálních sítí

4.1.1 Extrakce dotazů

Jednou z variant interakce s webovou aplikací je použití knihovny *urllib*. Tato knihovna poskytuje rozhraní pro práci s HTTP protokolem. Knihovna umožňuje odesílání HTTP požadavků, udržování relace a práci s cookies. Aby bylo možné interagovat s webovým rozhraním sociální sítě, je potřeba nejprve extrahovat položky odesílané v HTTP dotazech. Pro extrakci položek z dotazů, je možné použít nástroj Wireshark, který se používá pro analýzu webového provozu. Dalšími možnostmi je použití vývojářského prostředí webových prohlížečů nebo nástroj Burp Suite[1]. V rámci této práce byla vybrána druhá varianta. I když Wireshark nabízí širší spektrum funkcí, pro účely této práce postačilo i omezenější vývojářské prostředí.

4.1.2 Ochrana webových aplikací před automatizovanými nástroji

Sociální sítě se stejně jako řada jiných webů snaží omezovat automatizované procházení, přihlašování a stahování informací ze svých webů. A právě pro naplnění cílů této práce je nutné se automatizovaně přihlásit na sociální síť, vyhledat zde potřebné informace a uložit je pro další zpracování. Během implementace bylo zmapováno několik různých technik, které mají za úkol zabraňovat nebo alespoň znepříjemňovat potencionálnímu útočníkovi jeho snažení o automatizované zpracování obsahu. Z pochopitelných důvodu k těmto proprietálním opatřením neexistuje veřejně dostupná dokumentace. Některé principy aplikačních firewallů jsou popsány v publikacích [4, 17].

V následující pasáži této podkapitoly bude prezentováno několik bezpečnostních opatření webů, které bylo nutné překonat.

Hlavička prohlížeče

Součástí HTTP dotazů je položka *User-Agent* identifikující internetový prohlížeč. Některé webové aplikace tuto položku v dotazech kontrolují a pokud se zde objeví identifikace knihoven, které bývají často používány pro webové roboty, je požadavek na serveru zamítnut. Příkladem takové knihovny v jazyce Python může být *urllib*.

Pro překonání takového opatření postačí manuálně změnit v hlavičce požadavku identifikaci odpovídající prohlížeči viz obrázek 4.1.

```
User-Agent: Python-urllib/3.6
User-Agent: Mozilla/5.0 (X11; Linux i686) Gecko/20100101 Firefox/39.0
```

Obrázek 4.1: Ukázka změny nastaveni HTTP hlavičky

Skryté vstupní pole formuláře

Servery sociálních sítí zpracovávající HTTP dotazy generované z webových formulářů za účelem přihlášení, počítají s množinou položek resp. informací, na základě kterých požadavek buď to zamítnou nebo akceptují a uživatele přihlásí. Tyto informace se odesílají po stisku tlačítka *přihlásit* na server, kde se validuje, zda byly odeslány všechny povinné a zda obsahují validní data. Všechny sociální sítě zde samozřejmě očekávají uživatelské jméno a heslo. Dále se již rozcházejí a každá ze svého formuláře generuje jiné HTTP dotazy.

[1] https://portswigger.net/burp

Příkladem tohoto bezpečnostního opatření je sociální síť Facebook. Po načtení přihlašovací stránky může uživatel vidět vstupní políčka pro zadání e-mailu/telefonního čísla a hesla. Ovšem samotný formulář obsahuje dále několik dalších skrytých elementů *input*. Některé z nich si již ze serveru nesou vygenerovanou hodnotu v atributu *value* viz obrázek 4.2. Po potvrzení formuláře uživatelem se odešlou spolu s vyplněným e-mailem a heslem i tyto předgenerované hodnoty.

```
<form id="login_form" ...>
   .
   .
   <input type="hidden" name="jazoest" value="2769" autocomplete="off" />
   <input type="hidden" name="lsd" value="AVolpvaH" autocomplete="off" />
   <input type="hidden" name="lgnrnd" value="091555_dgWS" />
   .
   .
</form>
```

Obrázek 4.2: Ukázka skrytých elementů přihlašovacího formuláře sociální sítě Facebook

Je otázkou k čemu tento mechanismus slouží, ale pro úspěšné přihlášení do sociální sítě je nezbytné tyto speciální hodnoty v nezměněném stavu odeslat společně s e-mailem a heslem na server.

V rámci implementace navrhované aplikace byly tyto informace extrahovány ze zdrojového HTML kódu a následně přidány do HTTP dotazu.

Javascript generující cookies

Některé sociální sítě používají mechanismus, kdy pomocí javascriptu vygenerují přístupový *token*, který společně s přihlašovacími údaji tvoří kombinaci, na jejímž základě se uživatel přihlásí a je mu umožněno vstoupit do prostředí sociální sítě.

Příkladem sociální sítě využívající tento mechanismus je Twitter. Po stažení webové stránky do webového prohlížeče se spustí javascript, který vygeneruje token, bez kterého je nemožné se přihlásit. Nad zdrojovým souborem tohoto scriptu byl použit obfuskační nástroj. Tudíž reverzní inženýrství je značně znesnadněno a bylo by časově velmi náročné, jelikož zdrojový soubor obsahuje desítky tisíc řádků zdrojového kódu v nečitelné formě viz 4.3.

Existuje několik možných přístupů, vedoucím k prolomení popisovaného zabezpečení. Výše popsané reverzní inženýrství je z několika důvodů nevyhovující. I úspěšný pokus by vedl pouze k proniknutí přes ochranu jedné konkrétní webové aplikace. Tudíž tomuto přístupu chybí univerzalita a má nedostatek v podobě časové náročnosti.

Dalším uvažovaným přístupem je jednorázové vykonání javascriptu pomocí nějakého interpretu např. pomocí *Node.js* serveru a frameworku *jsdom*. Tento přístup bohužel by byl použitelný pro sociální síť Twitter. Ale bohužel v prostředí účtu Google je situace komplikovanější. Google za pomoci svého javascriptu dynamicky mění cookies v určitém časovém intervalu. Což by znamenalo nepřetržitý běh Node.js serveru a tím pádem potřebnou synchronizaci s navrhovanou aplikací.

```
function(e, t, n) {
       "use strict";
       n.d(t, "a", (function() {
           return r
       })), n.d(t, "b", (function() {
           return i
       })), n.d(t, "e", (function() {
           return
o~})), n.d(t, "c", (function() {
           return
a~}));
```

Obrázek 4.3: Část obfuskovaného javascript kódu generujícího cookies pro Twitter

Dalším řešením,které by mohlo vést k překonání popisovaných forem zabezpečení je použití frameworku Selenium, který dokáže vyřešit všechny výše popisované potíže za cenu mírně delšího běhu programu.

V této práci je kladen důraz na univerzalitu, tudíž byl zvolen poslední z navrhovaných přístupů. A to použití frameworku Selenium, který je popsán níže.

Selenium

Selenium[2] je testovací platforma zaměřená na testování webových aplikací. Platforma byla vyvinuta Jasonem Hugginsem v roce 2004 a skládá se z několika částí, z Selenium IDE, Selenium RC, Selenium Web driver a Selenium Grid. Každá z částí má svou funkčnost a řeší různé problémy. Selenium je multiplatformní open source řešení, podporující řadu prohlížečů (Firefox, Chrome a Internet Exploler). Tato platforma má podporu v několika programovacích jazycích (Python, Java).

V rámci této práce je zajímavá pouze část Selenium Web driver, která komunikuje přímo s webovým prohlížečem prostřednictvím API, což dovoluje programově definovat posloupnost kroků vykonaných v prohlížeči. Díky této funkcionalitě je tedy možné v programu zadefinovat posloupnost akcí, které je nutné provést pro přihlášení a nalezení potřebných informací. Taková posloupnost přesně kopíruje kroky uživatele. Tedy načtení přihlašovací stránky, zadání přihlašovacích údajů, potvrzení formuláře tlačítkem a následné vyhledání potřebných informací.

Detekce frameworku Selenium

Některé webové služby do svých bezpečnostních opatření přidaly i přímo detekci frameworku Selenium. Z množiny sociálních sítí, se kterými je interagováno v rámci této práce, se popisovaný způsob ochrany vyskytuje u sítě Google. Existuje mnoho různých řešení, která se snaží různými způsoby Selenium detekovat. Některé pouze skenují HTTP hlavičky a hledají zde některá klíčová slova, která identifikují tento farmework. Sofistikovanější řešení pomocí Javascriptu prohledávají proměnné a v nich hledají klíčová slova. Jistě existuje celá řada dalších přístupů a pokusů jak tuto detekci provádět.

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

V této práci bylo potřeba tento problém řešit pouze u přihlašováni do sítě Google. Byl zvolen odlišný způsob obejití těchto bezpečnostních opatření než opatření, která byla prezentována výše. Přihlašovací stránka na Googlu detekuje Selenium a nedovolí uživateli přihlásit se, tedy není mu vytvořen přístupový token a jako bonus je uživatel přesměrován na výstražnou stránku. Ale jelikož se lze pomocí Google účtu přihlásit na řadu jiných webů, například na *stackoverflow.com*, kde tyto bezpečnostní opatření nejsou. Lze tuto situaci vyřešit tak, že se uživatel resp. Selenium přihlásí na *stackoverflow*, zde získá přístupový token od Google, který je platný ve všech aplikacích, které podporují Google přihlašování. A dále již může přistupovat na jakákoli místa v nastavení Google účtu, zde se již detekce neprovádí.

4.1.3 Změna CSS selektorů a HTML struktury webu

Pro extrakci informací z HTML struktury, je v jazyce Python dostupných několik knihoven. V této práci byla použita knihovna *BeautifulSoap*, která poskytuje možnosti vyhledávání na základě CSS selektorů a názvů HTML elementů. Nebo přímo selenium integruje možnosti vyhledávání a navíc umí vyhledávat pomocí Xpath. V případě CSS selektorů hledanou položku specifikuje její *id* nebo třída. V případě Xpath se požadovaná položka specifikuje přesnou cestou k položce.

Použití těchto přístupů s sebou nese jeden nepříjemný problém. Se stává, že sociální síť změní CSS selektory nebo změní strukturu své stránky a tím pádem se stává celé vyhledávání nepoužitelným. V průběhu implementace byl tento problém řešen přibližně jednou za dva měsíce. Tento problém pramení, z toho že se provádí interakce s internetem, kde se vše může rychle měnit. Změny CSS selektorů a struktury webu jsou ale také jednou z technik ochrany webu proti automatickému stahování obsahu. Přidání několika elementu *div* bez jakékoli další konfigurace uživatel nijak nepozná, ale již nefunguje technologie Xpath. Stejně jako změna názvu CSS třídy, uživatel ji nepozoruje, ale vyhledávání na stránce na základě této třídy selhává.

4.1.4 Struktura a extrakce dat

Na základě způsobu implementace webové služby, lze webové aplikace sociálních síti rozdělit na 2 kategorie.

První z nich po přihlášení stáhne veškeré dostupné informace z webového serveru a následně interaguje s uživatelem pouze pomocí javascriptu a technologie *AJAX*. Tudíž data jsou ihned po přihlášení připravena ve standardizovaném formátů ke stažení. Většinou ve formátu *JSON*. Zástupcem této kategorie je sociální síť Twitter.

Druhá kategorie webových aplikací používá přístup, kdy na každou stránku se lze dostat pomocí odkazu. Přechody mezi stránkami zajišťuje HTTP dotazem *GET*. To znamená, že uživatel se serverem komunikuje při každé interakci. V této kategorii sociálních sítí jsou většinou bezpečnostní nastavení rozdělena mezi několik stránek. A konkrétní informace jsou serverem přímo generovány do HTML struktury. Tudíž pro extrakci potřebných informací musí navrhovaný nástroj projít všechny stránky obsahující důležité informace a z každé z nich vyextrahovat požadovaná data. Zástupci tohoto klasičtějšího modelu jsou Facebook, LinkedIn a Google.

4.2 Evaluator

V rámci popisu komponenty evaluatoru bude detailněji ověřeno chování výpočetních modelů v různých situacích. Na základě dosažených výsledků bude zvolen výchozí model pro tuto práci.

Díky tomu, že sociální sítě nedovolují u všech atributů modifikovat možnosti zveřejňování, je nutné tyto nemodifikovatelné položky vhodným způsobem reflektovat. Příkladem takového atributu je u většiny sociálních sítí profilová fotografie. Pokud by chtěl uživatel svou profilovou fotografii skrýt, nezbývá mu než ji změnit. Zde je nutno dodat, že ani tato akce není v některých případech dostačující. Tak již zbývá jen úplné smazání. Problém začlenění těchto položek je řešen jejich přidáním k datům sesbíraným extraktorem před aplikací modelu.

V následující pasáži budou detailně pro každou podporovanou sociální síť popsány vstupy a výstupy testovacího scénáře. Vstupní konfigurace testovacích nastavení jsou zobrazeny v tabulkách, přičemž potřebná číselná ohodnocení tabulkových hodnot obsahuje každá tabulka na svém posledním řádku.

4.2.1 Výběr výchozího modelu

V rámci práce byly implementovány všechny níže prezentované modely. Pro finální verzi aplikace je potřeba zvolit model, který bude co možná nejlépe reflektovat nastavení soukromí. Pro hodnocení modelů byly zvoleny dva testovací scénáře. Prvním z nich je reakce modelů na inkrementální změny nastavení. Druhý scénář ověřuje, zda model dokáže reflektovat nastavení, která by mohla mít pozitivní efekt na Privacy score.

Na základě stávajících prací, kde byla publikována řada evaluačních modelů byly do testování a výběru zahrnuty 4 modely:

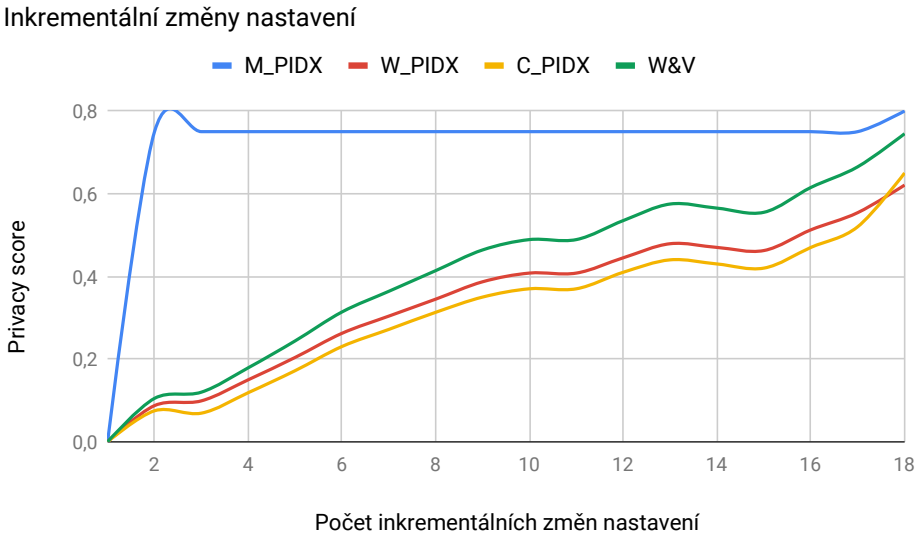
- Model váhy a viditelnosti
- M-PIDX
- W-PIDX
- C-PIDX

Všechny tyto modely byly popsány v první části práce. V rámci testování a výběru nejvhodnějšího modelu pro tuto práci byly použity dva testovací scénáře. Jelikož pro výběr modelu není důležitý význam vyhodnocovaných dat, ale spíše chování modelů, tak není potřeba provádět tento typ testování na všech podporovaných sociálních sítích. Díky tomu, že sociální síť Facebook poskytuje rozmanitou škálu nastavení, byla tato síť vybrána pro testování.

4.2.2 Inkrementální změny

V rámci prvního přístupu je sledováno chování modelu při inkrementálních změnách atributů. Inkrementální změnou atributů je myšleno postupné přidávání resp. zveřejňování jednotlivých atributů. Jinými slovy: test T_1 zveřejňuje informace jednoho atributu, T_2 informace dvou atributů až T_n. Počet testů v rámci diskutovaného přístupu je roven počtu nastavovaných atributů. Tyto atributy byly označeny T_1 až T_{17}, společně s příslušnými váhami jsou zobrazeny v tabulce 4.1. Zdrojem tabulky jsou bezpečnostní nastavení sítě Facebook. Protože v rámci testování vlastností modelů je význam jednotlivých položek

nastavení irelevantní, byly názvy pominuty. Testování tohoto přístupu bylo postupně provedeno na všech čtyřech prezentovaných modelech a výsledky byly vyneseny do grafu. Díky tomu, že modely pracují v různých intervalech, bylo nutné hodnoty před vynášením do grafu normalizovat.



Obrázek 4.4: Výsledek testování inkrementálních změn

Tento postup byl již použit pro modely třídy PIDX v práci [19]. V rámci této práce byl výsledek ověřen a přidán jeden další model. Na základě naměřených hodnot byly potvrzeny dříve publikované závěry a to, že model W-PIDX dobře reflektuje inkrementální změny, ale má jisté potíže s reflektováním aktuálně zveřejněného atributu. Dále bylo vypozorováno, že W-PIDX má tendenci vyhlazovat skokové změny. Naproti tomu model M-PIDX dobře odráží skokové změny, ale neumí pracovat s inkrementálními změnami atributů. Což je vidět na obrázku 4.4, kdy většina výstupních hodnot modelu je stejná až na skokové změny. Výhody obou těchto modelů by měl kombinovat model C-PIDX. Dobře reflektuje inkrementální změny a také reflektuje změny aktuálního atributu. Tento fakt lze vidět na obrázku 4.4 a to zejména v okolí třetího a sedmnáctého testu.

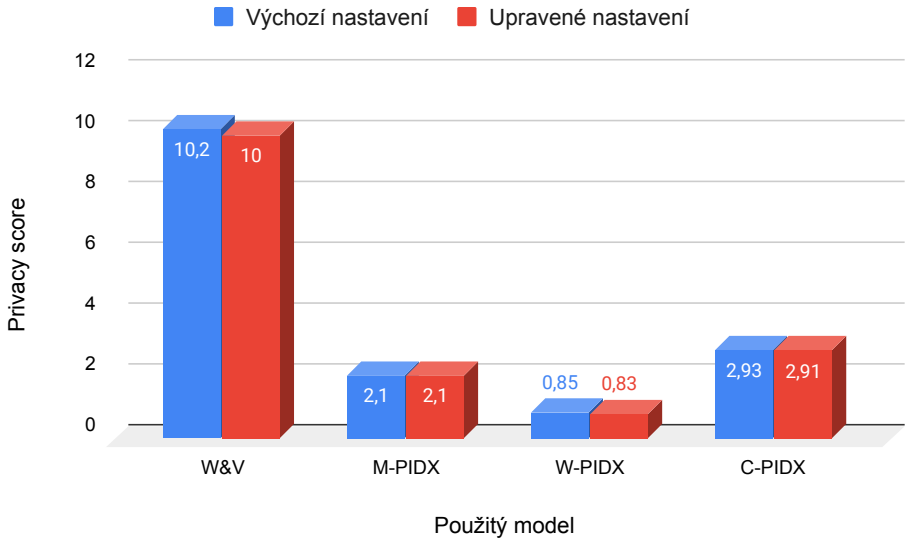
Položka	**váha**[%]	**Položka**	**váha**[%]
T1	25	T10	80
T2	60	T11	80
T3	50	T12	20
T4	50	T13	30
T5	0	T14	40
T6	-10	T15	80
T7	-10	T16	25
T8	80	T17	15
T9	20		

Tabulka 4.1: Testovací data vycházející z výchozího nastavení sítě Facebook

Posledním testovaným modelem je model váhy a viditelnosti zobrazený zeleně na obrázku 4.4. Model se chová velice podobně jako W-PIDX a taktéž má problém se skokovými změnami.

4.2.3 Reflektování nastavení zlepšující skóre

V možnostech nastavení některých sociálních sítí se objevují nastavení, která jdou protichůdným směrem oproti klasickým nastavením atributů. Za klasické nastavení atributu se považuje situace, kdy se nastavuje, zda atribut sdílet či nikoli, tedy při sdílení s okolím má různě velký negativní dopad na soukromí. Naopak tato protichůdná nastavení by měla aktivací soukromí uživatele chránit. Příkladem takového nastavení (tab. 4.1 položka T_7) je v síti Facebook: *Chcete kontrolovat příspěvky, ve kterých vás někdo označil, než se budou moct zobrazit na vaší timeline?*. Nastavení umožňuje uživateli ovlivňovat a kontrolovat co se mu zobrazí na profilu, resp. provádět „cenzuru“ svého profilu. V rámci práce jsou tato nastavení považována za přínosná a mohou mírně pozitivně ovlivnit soukromí. Aby bylo docíleno pozitivního přínosu nastavení, je jeho váha nastavena na zápornou hodnotu.



Obrázek 4.5: Výsledek testování nastavení s pozitivním efektem

Podstatným kriteriem při výběru vhodného modelu pro nástroj je schopnost reflektovat výše popsané nastavení. Pro testování tohoto scénáře byly nejprve aplikovány všechny prezentované modely na výchozí nastavení sítě Facebook, kde jsou nastavení T_6 a T_7 z tabulky 4.1 vypnuty. Poté bylo přidáno nastavení: *Chcete kontrolovat příspěvky, ve kterých vás někdo označil, než se budou moct zobrazit na vaší timeline?* (T_7). Nad takto upravenou konfigurací nastavení byly opět provedeny výpočty všech podporovaných modelů. Výsledky jsou graficky znázorněny na obrázku 4.5.

Lze si zde všimnout, že model M-PIDX pravděpodobně nesplňuje požadavky na reflektování popisovaných nastavení, jelikož model v obou případech dojde ke stejné hodnotě Privacy score. U ostatních modelů lze vidět mírné zlepšení (snížení Privacy score) po aplikování výše diskutovaných nastavení.

4.2.4 Vyhodnocení pokusů

Jako výchozí model byl pro tuto práci zvolen C-PIDX. Jelikož inkrementální testování potvrdilo předešlé výsledky publikované v [19] a také ukázalo, že ani model váhy a viditelnosti neposkytuje lepší výsledky z pohledu reflektování skokových změn.

Při hodnocení modelů na základě nastavení, která by měla pozitivně ovlivňovat privátní skóre se vyloučil model M-PIDX, ostatní modely se chovaly velice podobně.

Byl také brán zřetel na závěry autorů modelů PIDX, kteří uvádí v [19], že C-PIDX nejlépe z navrhovaných modelů reflektuje kompozitní atributy.

4.3 Modul vyhodnocení

Modul vyhodnocení je komponenta připravující data k prezentaci uživateli. Jejím výstupem je jedna JSON struktura, která se odesílá grafické části aplikace. Součástí odesílaných dat jsou:

- Minimální, maximální a výchozí hodnota Privacy score pro každou analyzovanou sociální síť
- Nápověda pro každou analyzovanou sociální síť
- Výsledky interní a externí analýzy

Aby bylo možné uživateli zobrazit výsledné Privacy score v kontextu, bylo potřeba určit pro každou sociální síť hranice této metriky. Předmětem následující pasáže bude detailní popis procesu získávání těchto mezí u vybraných sociálních sítí, mechanismus tvorby nápovědy, dělení uživatelů do skupin a zhodnocení výchozích nastavení sociálních sítí.

4.3.1 Hranice Privacy score

Aby bylo později možné naměřené hodnoty přesněji interpretovat, pro každou sociální síť je zapotřebí určit interval, ve kterém vybraný model (C-PIDX) v kontextu dané sociální sítě pracuje. Proto bylo provedeno měření extrémních situací bezpečnostních nastavení, tj. situace kdy uživatel sdílí veškeré informace v co nejširším okruhu ostatních účastníků a kdy uživatel omezí sdílení informací na co nejmenší množství podle možností sociální sítě. Toto měření bylo rozšířeno o určení hodnoty Privacy score u výchozího nastavení, což může poskytnout jistou míru srovnání, jak sociální sítě chrání své uživatele.

Facebook

V rámci sociální sítě Facebook byly hodnoty Privacy score vypočítány z nastavení uvedených v tabulce 4.2, výše popisované nemodifikovatelné atributy jsou označeny **X**.

Vstupem pro experimentální měření byly tři základní konfigurace: minimální, maximální a výchozí nastavení. Všechna potřebná vstupní data pro výpočet Privacy score jsou zobrazena v 4.2.

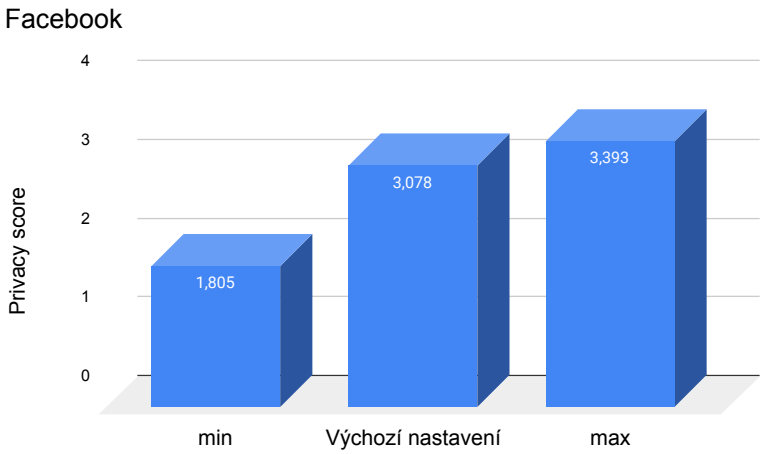
Výsledky experimentálního měření nastavení sítě Facebook jsou zobrazeny na obrázku 4.6. Lze zde vidět velký skok mezi minimálním sdílením informací a výchozím nastavením a dále již menší nárůst mezi výchozím nastavením a maximálním sdílením. Což odráží realitu, neboť ve výchozí konfiguraci Facebook zakazuje pouze sdílení polohy, rozpoznávání obličeje a několik méně podstatných položek, které nemají přílišný dopad na soukromí, ale

Nastavení	Váha	Min	Max	Výchozí
X Jméno a příjmení	0.05	Veřejný	Veřejný	Veřejný
X Profilová fotografie	0.55	Veřejný	Veřejný	Veřejný
Kdo vidí vaše příspěvky	0.25	Jen já	Veřejný	Přátelé
Kdo Vám může posílat žádosti o přátelství	0.15	PP	Všichni	Všichni
Kdo vidí seznam přátel	0.60	Jen já	Veřejný	Veřejný
Kdo Vás může vyhledat podle e-mailu	0.65	Jen já	Všichni	Všichni
Kdo Vás může vyhledat podle telefonního čísla	0.70	Jen já	Všichni	Všichni
Propojení vyhledávačů mimo Facebook s profilem	0.50	Vypnuto	Zapnuto	Zapnuto
Kdo může na Váš profil přidávat příspěvky	0.50	Jen já	Přátelé	Přátelé
Kdo může vidět příspěvky na vašem profilu	0.50	Jen já	Všichni	Přátelé
Povolit ostatním sdílet vaše příspěvky	0.25	Vypnuto	Zapnuto	Zapnuto
Skrývat komentáře obsahující určitá slova	0.00	Vypnuto	Zapnuto	Vypnuto
Kdo může na vašem profilu vidět příspěvky kde jste označeni	0.45	Jen já	Všichni	PP
Kontrola příspěvků před zobrazením na profilu	-0.10	Zapnuto	Vypnuto	Vypnuto
Kontrola označení ve vašich příspěvcích před zveřejněním	-0.10	Zapnuto	Vypnuto	Vypnuto
Povolit sdílet vaše veřejné příběhy	0.25	Vypnuto	Zapnuto	Zapnuto
Povolit sdílet vaše příběhy lidem, které zmíníte	0.30	Vypnuto	Zapnuto	Vypnuto
Historie polohy	0.80	Vypnuto	Zapnuto	Vypnuto
Automatické rozpoznávání obličejů uživatelů	0.80	Vypnuto	Zapnuto	Vypnuto

* PP - Přátelé přátel

Zakázáno|Vypnuto|Jen já = 0, Přátelé|Zapnuto = 1, Přátelé přátel = 2, Veřejné|Všichni = 3

Tabulka 4.2: Nastavení atributů při mezních konfiguracích a při výchozí konfiguraci bezpečnostního nastavení sociální sítě Facebook



Obrázek 4.6: Naměřené hodnoty na síti Facebook při výchozí konfiguraci a při mezních konfiguracích

položky s velkým dopadem jako *Kdo vás může vyhledat pomocí telefonního čísla, které jste zadali?* jsou povoleny.

Twitter

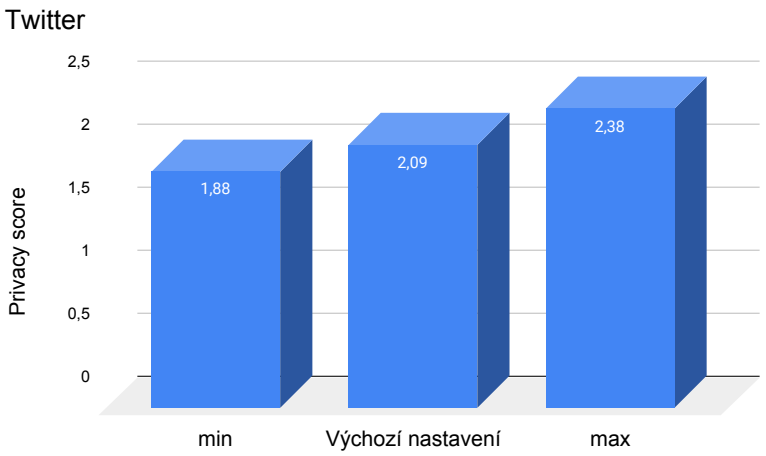
Vstupní data pro určení mezních hodnot Privacy score pro sociální síť Twitter jsou zobrazeny v 4.3. Na vstupní data byl postupně aplikován model C-PIDX a výsledky byly vyneseny do grafu 4.7. Výsledkem měření je stejně jako u předchozí sociální sítě interval

hodnot, kterých může Privacy score nabývat. Zároveň lze z výsledků usoudit, že výchozí nastavení soukromí je položeno přibližně ve středu tohoto intervalu, což lze považovat za nejlepší variantu z pohledu vyváženosti ochrany soukromí a použitelnosti sociální sítě.

Nastavení	**Váha**	**Min**	**Max**	**Výchozí**
X Jméno a příjmení	0.05	Veřejné	Veřejné	Veřejné
X Profilová fotografie	0.55	Veřejné	Veřejné	Veřejné
Tweety vidí pouze sledující váš účet	-0.15	Zapnuto	Vypnuto	Vypnuto
Přidávat lokalizační údaje k tweetům	0.80	Vypnuto	Zapnuto	Vypnuto
Kdo Vás může označit	0.45	Nikdo	Všichni	Všichni
Vyhledávání na základě e-mailu	0.65	Vypnuto	Zapnuto	Vypnuto
Vyhledávání na základě telefonního čísla	0.70	Vypnuto	Zapnuto	Vypnuto

Nikdo|Vypnuto = 0, Sledující|Zapnuto = 1, Veřejné|Všichni = 3

Tabulka 4.3: Nastavení atributů při mezních konfiguracích a při výchozí konfiguraci bezpečnostního nastavení sociální sítě Twitter



Obrázek 4.7: Naměřené hodnoty na síti Twitter při výchozí konfiguraci a při mezních konfiguracích

LinkedIn

V případě profesní sociální sítě LinkedIn se pracuje s jedenácti možnými bezpečnostními nastaveními, které lze upravovat a třemi nemodifikovatelnými. LinkedIn disponuje oproti ostatním sítím jedním zvláštním nastavením, které umožňuje skrýt příjmení. Vstupní konfigurace testovaných účtů je zobrazena v tabulce 4.4. Výsledky měření 4.8 ukazují podobně jako v případě sítě Facebook značný skok mezi minimální hodnotou privacy skore a hodnotou získanou při měření výchozího nastavení. Důvodem tohoto výsledku je, že ve výchozím nastavení se sdílí řada citlivých informací se všemi ostatními uživateli sociální sítě. Například telefonní číslo, ač není přímo viditelné na profilu, lze pomocí něj uživatele vyhledat, tudíž při vynaložení jistého úsilí lze ke konkrétnímu uživateli telefonní číslo přiřadit.

Nastavení	Váha	Min	Max	Výchozí
X Jméno	0.02	Veřejný	Veřejný	Veřejný
X Profilová fotografie	0.55	Veřejný	Veřejný	Veřejný
X Vzdělání	0.15	Veřejný	Veřejný	Veřejný
Kdo může zobrazit seznam spojení	0.60	Jen vy	Spojení	Spojení
Zobrazit vaše příjmení	0.03	Ne	Ano	Ne
Zobrazovat mé jméno v souvislosti se zaměstnavateli	0.40	Ne	Ano	Ano
Viditelnost profilu mimo LinkedIn	0.50	Ne	Ano	Ano
Kdo smí vědět, že jste aktivní na síti	0.05	Jen já	Všichni	Spojení
Sdílet automaticky změny pozice, vzdělání	0.40	Vypnuto	Zapnuto	Zapnuto
Povolit označování	0.45	Ne	Ano	Ano
Kdo může vidět Váš e-mail	0.65	Skrytý	Všichni	Spojení první úrovně
Kdo může objevit Váš profil pomocí e-mailu	0.65	Jen já	Všichni	Všichni
Kdo může objevit Váš profil pomocí tel. čísla	0.70	Jen já	Všichni	Všichni
Mód prohlížení profilů	0.50	Skrytý	Odhalený	Odhalený

Ne|Skrytý| Jen vy = 0, Ano|Spojení|Zapnuto = 1, Spojení první úrovně = 2, Odhalený| Všichni = 3

Tabulka 4.4: Nastavení atributů při mezních konfiguracích a při výchozí konfiguraci bezpečnostního nastavení sociální sítě LinkedIn

Nastavení	Váha	Min	Max	Výchozí
X Jméno	0.05	Zapnuto	Zapnuto	Zapnuto
X Telefonní číslo	0.70	Zapnuto	Zapnuto	Zapnuto
Ukládání kontaktů z vašich zařízení	0.60	Vypnuto	Zapnuto	Zapnuto
Ukládání kontaktů z interakce	0.60	Vypnuto	Zapnuto	Zapnuto
Historie polohy	0.80	Vypnuto	Zapnuto	Vypnuto
Ukládání aktivity na webu a v aplikacích	0.70	Vypnuto	Zapnuto	Zapnuto
Historie Youtube	0.60	Vypnuto	Zapnuto	Zapnuto
Spojení účtu s reklamami	0.40	Vypnuto	Zapnuto	Vypnuto

Zapnuto = 1 , Vypnuto = 0

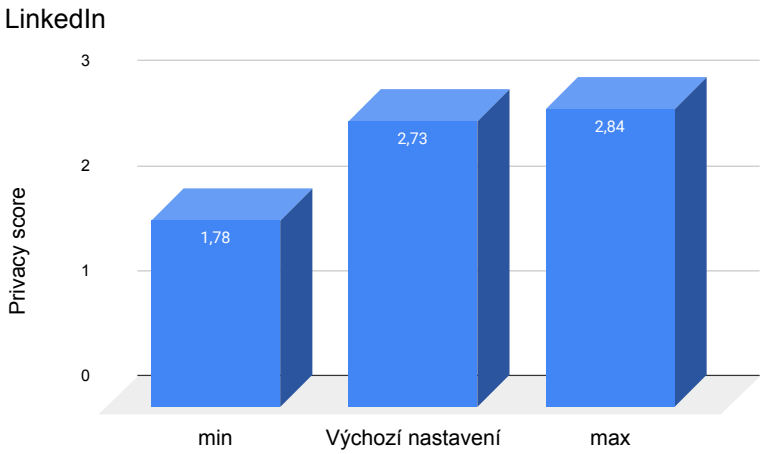
Tabulka 4.5: Nastavení atributů při mezních konfiguracích a při výchozí konfiguraci bezpečnostního nastavení sociální sítě Google

Google

Platforma Google je díky svým službám odlišná oproti jiným sociálním sítím. Na rozdíl od ostatních sociálních sítí Google nedisponuje externím rozhraním, které by dovolovalo vyhledat každého registrovaného uživatele a zobrazit si jeho profil. Vyhledání uživatele a nahlédnutí na jeho profil lze pouze u uživatelů, kteří jsou aktivní v aplikaci Youtube. Proto bylo Privacy score pro tuto síť určováno na základě informací, které uživatel může síti poskytovat. Platforma Google byla do práce zahrnuta i přes své odlišnosti jelikož může mít přístup k velice citlivým informacím, ke kterým se žádná z dříve diskutovaných sítí nemůže tak snadno dostat. Příkladem takto citlivých dat jsou například SMS konverzace, výpis telefonních hovorů a veškeré data uložená v zařízeních se systémem Android. Na základě možných nastavení budou i pro tuto síť vypočítány meze pro Privacy score. A také bude určeno Privacy score u výchozího nastavení sítě. Vstupní data jsou zobrazeny v tabulce 4.5

4.3.2 Třídy uživatelů

Proto aby bylo možné snadno rozdělit uživatele do několika skupin, je definována procentuální míra ohrožení soukromí v konkrétní sociální síti. Procentuální výsledek je určen na základě mezních hodnot Privacy score. U každé sociální sítě bylo určeno maximální



Obrázek 4.8: Naměřené hodnoty na síti Facebook při výchozí konfiguraci a při mezních konfiguracích

možné Privacy score a minimální Privacy score. Přičemž maximální bylo vypočítáno na základě nastavení soukromí, které umožňuje sdílet vše, minimální na druhou stranu odráží co nejrestriktivnější konfiguraci nastavení. Všechna prováděná měření konkrétní sítě se budou nacházet v intervalu $< min, max >$. Dále jsou hodnoty posunuty, tak aby minimum odpovídalo nule. Nyní lze z vypočítaného a posunutého Privacy score určit procentuální vyjádření udávající míru ohrožení.

Jedním z cílů práce je zařadit uživatele do skupiny obsahující uživatele s obdobným nastavením. Dělení do skupin se provádí z vypočteného Privacy score. Na základě normálního rozložení byly vytvořeny 3 skupiny uživatelů:

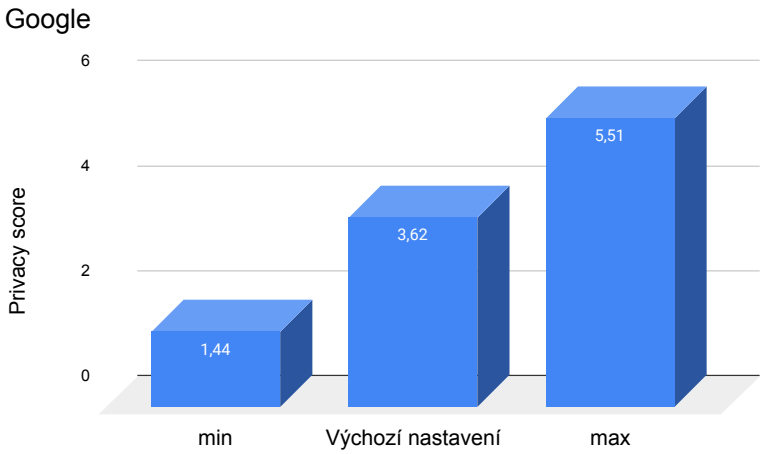
- Defensivní uživatel - Procentuální výsledek naleží do intervalu $< 0, 15.9 >$
- Většinový uživatel - Procentuální výsledek náleží do intervalu $(15.9, 68.2 >$
- Neopatrný uživatel - Procentuální výsledek náleží do intervalu $(68.2, 100 >$

4.3.3 Poskytnutí nápovědy

Mechanismus nápovědy vyhledá v uživatelském nastavení soukromí, položky které by bylo možné upravit tak, aby se snížila hodnota Privacy score. Tyto položky se seřadí dle své váhy a uživateli jsou nejprve doporučovány úpravy atributů s vysokou váhou a tím pádem s co největším dopadem na soukromí, až po atributy s minimálním vlivem na Privacy score. V případě minimálního nastavení účtu, tedy nastavení kdy již nelze Privacy score více snížit, mechanismus nápovědy tuto skutečnost oznámí uživateli.

4.4 GUI

Implementovaná aplikace se skládá ze dvou částí. První z nich je konzolová aplikace, která byla popisována doposud. Provádí sběr informací jejich vyhodnocení a připravuje data



Obrázek 4.9: Naměřené hodnoty na síti Facebook při výchozí konfiguraci a při mezních konfiguracích

k prezentaci. Druhou částí aplikace je grafické uživatelské rozhraní. Tato část aplikace byla přidána aby bylo možné výsledky měření doručit uživateli v co nejintuitivnější podobě.

Grafické uživatelské rozhraní je využíváno pouze pro prezentaci výsledků, celá aplikace je ovládána prostřednictvím terminálové části.

Pro vzhled webové části bylo použito volně dostupné řešení[3].

4.4.1 Architektura

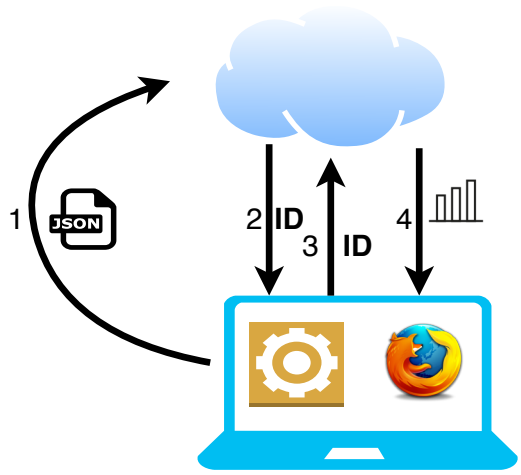
Aby bylo docíleno toho, že uživatel aplikace není nucen instalovat knihovny umožňující vykreslování grafiky a aby výsledná práce měla co nejméně závislostí, byla pro reprezentaci grafického rozhraní vytvořena jednoduchá webová aplikace zobrazující hodnoty zaslané ve formátu JSON.

Uživateli tedy stačí webový prohlížeč pro zobrazení výsledků. Tato webová aplikace je dostupná z [4].

Jelikož webová aplikace potřebuje získat data od konzolové aplikace, je potřeba všechny informace k prezentování odesílat z konzolové do webové aplikace ideálně protokolem HTTP. Metoda GET protokolu HTTP umožňuje přenášet pouze omezené množství dat. Z toho důvodu byl zvolen způsob, kdy se nejprve použije metoda POST k nahrání dat na server. Pro tato data se vygeneruje pseudonáhodný identifikátor (generovaný pseudonáhodným generátorem). Identifikátor je odeslán konzolové aplikaci jako odpověď, na základě které se odesílá požadavek GET s tímto identifikátorem a webová aplikace otevře dříve nahraná data a vizualizuje je. Celý proces je zobrazen na obrázku 4.10. Proces interakce aplikace s uživatelem je popsán níže:

1. Uživatel je vyznán k výběru sociální sítě pro analýzu
2. Uživatel je vyzván k zadání svých přihlašovacích údajů

[3] https://github.com/BlackrockDigital/startbootstrap-sb-admin
[4] http://www.stud.fit.vutbr.cz/ xjanus08/privchecker/index.php



Obrázek 4.10: Architektura GUI

3. Aplikace extrahuje data
4. Opakuje se bod 1, dokud uživatel nezadá všechny sítě, pro které požaduje analýzu
5. Aplikace provede evaluaci
6. Aplikace otevírá webový prohlížeč a zobrazuje výsledky

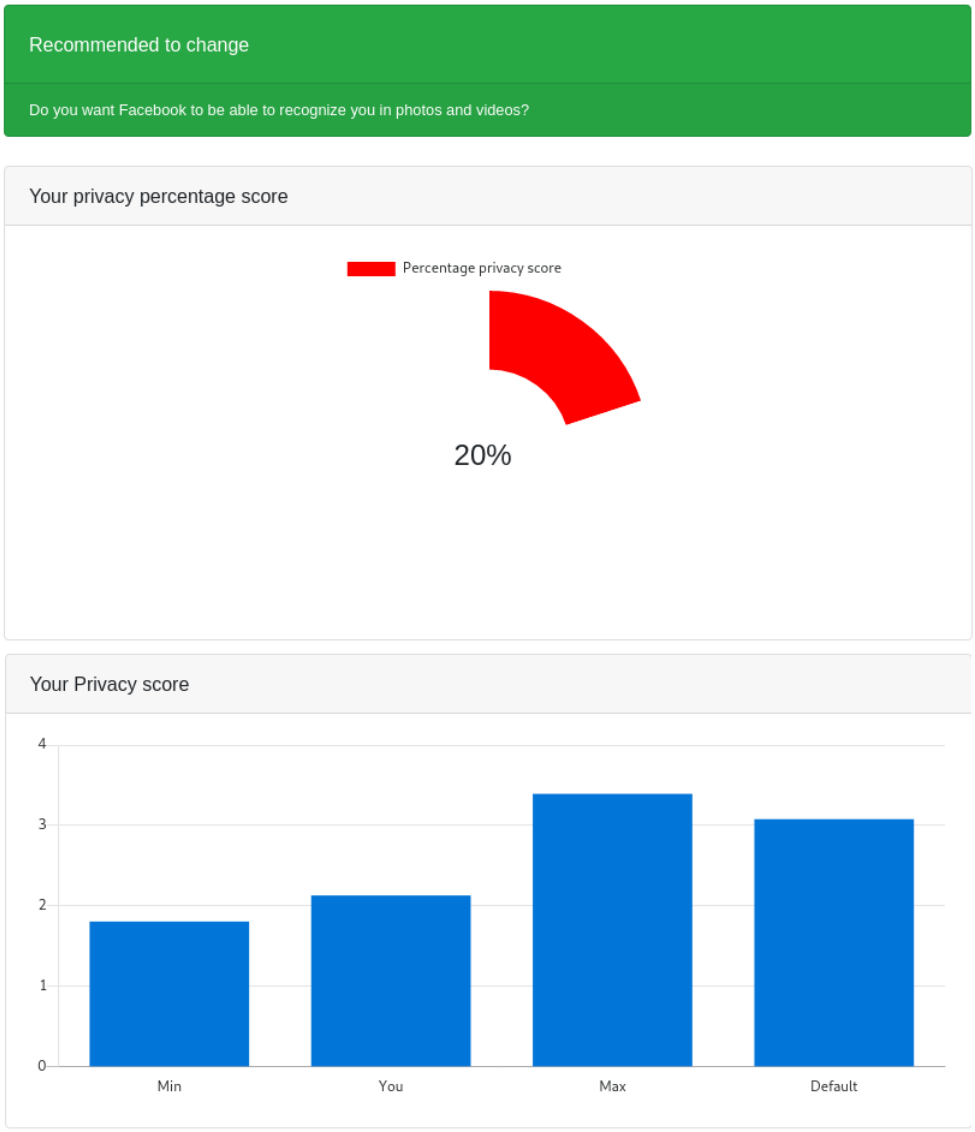
4.4.2 Zobrazovaná data

Výsledek měření pro každou sociální síť se skládá ze 2 grafů a nápovědy, což je zobrazeno na obrázku 4.11. První graf uživateli prezentuje naměřenou hodnotu v procentech, kde nula procent reprezentuje minimální možnou hodnotu Privacy score pro danou síť, zatímco sto procent reprezentuje maximální možnou hodnotu Privacy skore. Tato vizualizace se snaží informovat uživatele o výsledku na první pohled bez nutností čtení a interpretace matematických hodnot.

Druhý graf se již zaměřuje na detailnější zobrazení dosažené hodnoty Privacy skore. Dále obsahuje hodnoty k porovnání, výchozí hodnotou pro danou sociální síť, minimální a maximální hodnotou pro tuto síť.

4.5 Interní a externí uživatel

V průběhu implementace externího režimu byl řešen problém s identifikací správného uživatelského účtu. Jednoznačná identifikace profilu na základě jména a příjmení není možná, jelikož na sociálních sítích se stejně jako v populaci objevují lidé se stejným jménem a příjmením. Tato práce si klade za cíl vytvořit nástroj s co možná nejmenší mírou nutné interakce s uživatelem. Díky tomuto požadavku není vhodné nechat uživatele označovat své účty. Každá sociální síť má pro každého uživatele jednoznačný identifikátor, který většina uživatelů znát nebude, ale lze jej získat po přihlášení. Proto byl zvolen přístup, kdy při provádění interní analýzy účtu se získá tento identifikátor, který je později použit pro externí analýzu.



Obrázek 4.11: Náhled GUI

Jakmile je dokončena extrakce interních informací, provede se extrakce externích informací o uživateli. Externí informace jsou získávány a doplňovány postupně z poskytnutých účtů sociálních sítí. Předpokládá se, že všechny účty patří uživateli, který provádí kontrolu svých údajů.

Dále se již použije stejný postup pro evaluaci interních a externích informací, pouze při prezentaci je výsledek externího měření oddělen od interních závěrů.

Následující scénář ilustruje běh aplikace: Uživatel zadá k analýze dva účty (např. Facebook a Linkedin). U obou účtů se postupně provede extrakce interních informací a jednoznačného identifikátoru účtu. Poté se na základě získaného identifikátoru zobrazí veřejný profil uživatele. V tomto příkladu se zjistí, že uživatel na síti Facebook veřejně poskytuje

jméno a příjmení (implicitně) a dále své zájmy. U sítě LinkedIn je opět dostupné jméno, ale na rozdíl od Facebooku se zde navíc objevují informace o zaměstnání a vzdělání. V toto chvíli se spouští evaluace na základě získaných informací, provede se vyhodnocení a uživatel obdrží informace o interní analýze každé sociální sítě a externí analýze, která mimo Privacy score uživateli sděluje, že sdílí své jméno, záliby, pracovní pozici a vzdělání.

4.6 Možnosti srovnání výsledků

V následující pasáži budou představeny problémy, které provází srovnání Privacy score z různých sociálních sítí. U každého problému bude jeho popis a příklad. Diskutován bude jak interní, tak i externí režim a úskalí pramenící z různé granularity nastavení.

4.6.1 Interní pohled

Porovnání Privacy skore interního uživatele napříč různými sociálními sítěmi je obtížnou disciplínou, neboť si s sebou nese řadu problémů.

Různé povahy sociálních sítí

Různé sociální sítě mají různá zaměření například LinkedIn je sociální sítí, která se zaměřuje na sdílení informací o vzdělání a pracovních zkušenostech. Naopak sociální síť Tumblr se zaměřuje na publikaci krátkých článků. Těmto zaměřením odpovídají i možná bezpečnostní nastavení těchto sítí. Zatímco nastavení platformy LinkedIn klade důraz spíše na práci s kontaktními informacemi, tak Tumblr disponuje jedním nastavením *Umožnit ostatním vidět, že jsem aktivní*. O uživateli tato sociální síť mnoho neví, jelikož při registraci je požadován pouze e-mail a jakákoli přezdívka. Zde je patrné, že pokud by síť LinkedIn věděla o uživateli jen to co ví Tumblr, poté by síť LinkedIn postrádala smysl a byla by naprosto nepoužitelná. Situace kdy se budoucí zaměstnavatel rozhoduje koho osloví pouze na základě přezdívky není příliš reálná.

Dalším příkladem rozporu mezi povahami sítí může být kombinace Google a ostatní sítě. V tabulce 4.5 lze vidět možná bezpečnostní nastavení platformy Google. Zde se klade velký důraz na možnosti ukládání citlivých dat jako jsou kontakty, aktivity na webu, Youtube a dalších. Například položka *Ukládání aktivity na webu a v aplikacích* by se dala označit za exotickou, jelikož obdobné nastavení by se hledalo obtížně u jiné sociální sítě. A to především z důvodu, že jiná síť nemá přístup k tolika datům jako právě Google prostřednictvím platformy Androind a webového prohlížeče Chrome.

Z tohoto pohledu by se daly za porovnatelné považovat sociální sítě Facebook, Twitter a Instagram. I když Instagram slouží pro sdílení multimediálního obsahu (fotografii, videa), tak způsob jeho používání je velice podobný síti Facebook.

Různá množství nastavení

I v tomto případě lze vzít za příklad sociální síť Tumblr nebo Pinterest, které disponují jedním bezpečnostním nastavením, naopak Facebook jich má sedmnáct. Bez ohledu na význam nastavení, by při porovnávání těchto dvou extrémních situací docházelo ke ztrátě informací. Mohlo by nastat několik situací: Jediné nastaveni Tumblr by odpovídalo jednomu z mnoha nastavení sítě Facebook. Pokud by potom byla snaha tyto sítě porovnávat, znamenalo by to opomenout zbylých šestnáct položek nastavení sítě Facebook, což by vedlo k naprosto zkresleným hodnotám Privacy score.

Druhou o něco lepší situací by bylo, pokud by se v jediném nastavení Tumblr kombinovalo několik nastavení platformy Facebook. Příkladem by mohla být modelová situace, kdy Facebook by měl nastavení *Sdílet e-mail* a *Sdílet telefonní číslo*, naopak Tumblr by disponoval pouze nastavením *Sdílet kontaktní údaje*. V tomto případě by došlo k menší ztrátě informací než v předchozím případě, ale vyvstává zde problém, zda by bylo vhodné porovnávat situaci, kde na jedné straně by se sdílelo jen telefonní číslo a na straně druhé obě informace. Porovnání by v tomto případě bylo možné pokud by se správně nastavily váhy atributů. Tj. suma vah (telefonní číslo a e-mail) v síti Facebook by se měla rovnat váze jednoho nastavení v síti Tumblr. Jediným nedostatkem by bylo, že Privacy score sociální sítě Facebook by mohlo nabývat více hodnot než Privacy score sítě Tumblr.

Příklad popisovaných situací lze nalézt na sociální sítí LinkedIn. Jako jediná ze studovaných sítí umožňuje zakázat zveřejňování příjmení. Ostatní sociální sítě, které s jménem a příjmením pracují zveřejňují jméno i s příjmením bez možnosti skrytí.

Různá nastavení

Ač jsou si některé sociální sítě velice podobné svým použitím, tak i přes svou podobnost mají taková nastavení, která nemohou být přenosná. Příkladem mohou být Facebook a Twitter, zatímco Facebook disponuje nastavením *Povolit ostatním sdílet vaše příspěvky ve vlastním příběhu?*, tak Twitter takové nastavení mít nemůže, jelikož nezná pojem příběh ani nic podobného. Zkrátka Facebook podporuje více funkcionalit a tím pádem dovoluje i více možností nastavení, které nelze nalézt v sítích se skromnější funkcionalitou.

Druhým případem rozdílných možností nastavení může být *Chcete, aby se vyhledávače mimo Facebook propojily s vaším profilem?*. Obdobné nastavení se také nevyskytuje u sítě Twitter, i když profil lze vyhledávačem nalézt. Z toho plyne, že Twitter má tuto volbu implicitně povolenou, ale neumožňuje ji uživateli nastavovat.

První popisovaný problém by bylo možné řešit zanedbáním nastavení, která jsou přítomná pouze v jedné síti a tím pádem by byly ztraceny cenné informace. Druhý případ by se dal vyřešit bez ztráty informace a to přidáním implicitní hodnoty tam, kde není umožněna modifikace. Toto řešení je ale možné pouze díky tomu, že daná funkcionalita je podporována v obou sociálních sítích, ale pouze v jedné je možné ji modifikovat.

Vyhodnocení

V ideálním případě by všechny sociální sítě měly stejná nastavení soukromí a bylo možné snadno porovnávat bezpečnostní nastavení resp. vypočítané Privacy score napříč sociálními sítěmi. Bohužel v této práci neexistují dvě sociální sítě se stejným počtem nastavení, některé sociální sítě mají několik obdobných nastavení, která by bylo možné považovat za stejná při jisté míře benevolence.

Tabulka 2.1 zobrazuje jednotlivé sítě a jejich bezpečnostní nastavení. Jsou zde zahrnuta pouze nastavení, která se vyskytují ve více sociálních sítích. V tabulce si lze všimnout, že ani jedno nastavení není přítomné ve všech sociálních sítích. V nejvíce sítích je přítomno nastavení *Signalizace aktivity*, které patří mezi nastavení s minimálním dopadem na soukromí. Facebook se svými sedmnácti možnými nastaveními obsazuje pomyslnou první příčku co do počtu možných nastavení, následovaný platformou LinkedIn, která má třináct možností. Nabízela by se tedy úvaha, že právě tyto dvě sociální sítě budou mít nejširší shodu v nastaveních. Z tabkulky lze vidět, ze tomu tak není. Čtyři společná nastavení mají dvojice: Facebook, Twitter a Twitter, LinkedIn, což je maximum. Tedy pokud by byla snaha aplikovat porovnávání na tyto čtyři nastavení muselo by se na straně sítě Facebook zanedbat

dalších třináct položek a na straně sítě Twitter jedno. Lze předpokládat, že výsledek takového srovnání by byl zavádějící.

Na základě výše popsaných faktů, lze konstatovat, že nelze porovnávat přímo nastavení soukromí mezi dvěma sociálními sítěmi bez ztráty informací. S rostoucím počtem srovnávaných sociálních sítí, se zvyšuje také počet informací, které by bylo potřeba zanedbat. Z tabulky 2.1 lze vidět, že analýza napříč všemi analyzovanými sítěmi v této práci by nebyla možná, jelikož neexistuje ani jedno nastavení, které by měly všechny podporované sociální sítě společné.

Aby bylo možné porovnávat výsledky měření napříč sociálními sítěmi, byla zavedena procentuální míra definované výše společně s třídami uživatelů.

Modelovou situací pro porovnání procentuálních měr může být situace: Nechť existují dvě měření, sítě X a sítě Y. Přičemž procentuální míra X = 40%, Y = 60%. Potom X < Y, což lze interpretovat, tak že X má restriktivnější nastavení než Y. Hodnoty žádným způsobem neudávají jakým způsobem bylo dosaženo hodnot. Pouze říkají že síť X je v rámci svých nastavení nastavena restriktivněji než Y.

4.6.2 Externí pohled

Jak bylo popsáno výše, externí režim nástroje pracuje s informacemi z více různých zdrojů, jako by informace pocházely z jednoho zdroje. Tudíž externí analýza několika sítí vrací jeden výsledek stejně jako externí analýza jedné sítě. Více analyzovaných sítí znamená pro externí režim více informací, na základě kterých může poskytnout přesnější výsledek. Proto lze bez potíží porovnávat výsledky externího Privacy score (z různých běhů aplikace).

4.6.3 Srovnání přístupů

Implementovaná aplikace podporuje dva režimy analýzy, externí a interní. Zatímco interní analýza je detailnější a specifická pro každou sociální síť, tak externí analýza kombinuje informace z více různých sociálních sítí. V rámci interního režimu se pracuje s různou granularitou nastavení, z čehož pramení řada problémů, které byly popsány výše. Na druhé straně externí režim se nemusí potýkat s problémy rozdílné granularity nastavení, díky tomu že agreguje více zdrojů do jednoho.

I když oba přístupy vyčíslují Privacy score, tak tyto výsledky prezentují soukromí z různých úhlů pohledů.

Externí režim zkoumá informace veřejně dostupné na internetu, dosažitelné bez jakéhokoliv přihlašování do sociálních sítí. Sociální sítě umožňují tímto způsobem prezentovat jen některé uživatelské informace. Většinou se jedná o jméno, zájmy, zaměstnání, vzdělání a profilovou fotografii.

Naopak interní režim zkoumá soukromí na základě dostupných nastavení. Tato nastavení ovlivňují kromě položek veřejně dostupných i to jak se bude uživatelský účet chovat v rámci sociální sítě. Zda bude možné uvnitř sítě objevit příslušnost k zájmovým skupinám, seznamy přátel a další informace, které nemohou být dostupné mimo sociální síť. Počet a povaha těchto informací úzce souvisí s granularitou nastavení sociální sítě a také s orientací této sítě. Například bude obtížné v sociální síti LinkedIn hledat nastavení ohledně sdílení příběhů, které existuje v síti Facebook, ale LinkedIn funkcionalitou příběhů nedisponuje.

I když interní a externí Privacy score spolu úzce souvisí, mohou nastat situace, kdy budou výsledky naprosto odlišné až protichůdné. Například může nastat situace, kdy výsledek externí analýzy bude alarmující, ale interní analýzy jednotlivých sítí nebudou vykazovat žádné náznaky nadměrného sdílení informací. Konkrétně může nastat situace, kdy externí

analýza odhalí sdílení *jména, fotografie, vzdělání, zaměstnání a místa bydliště*. Na základě těchto informací bude uživatel zařazen do skupiny *neopatrných uživatelů*. Ovšem tyto informace jsou rozptýleny na pěti různých sociálních sítích, kde u každé sítě se uživatel při interní analýze řadí mezi *defensivní uživatele*. A to díky tomu, že tyto informace jsou separátně méně nebezpečné z pohledu soukromí než pokud se spojí dohromady. Tento problém je příkladem virtuálního atributu, který byl definovaný v první kapitole.

Kapitola 5

Testování

V průběhu kapitoly budou popsány testovací scénáře, které by měly ověřit funkcionalitu implementované aplikace. Dále bude prezentováno uživatelské testování, které by mělo v omezené míře poskytnout informaci o aktuální situaci soukromí na sociálních sítích.

5.1 Testování funkcionality

Ověřování funkcionality pobíhalo na testovacích účtech. Neboť pro ověření funkcionality nebylo zapotřebí pracovat s reálnými daty. Tato část testování se zaměřovala především na komponentu extraktoru, která zajišťuje vstupní data pro práci nástroje, tj. stažení a parsování dat. Zde dochází k interakci s vnějším světem a může zde nastat řada problémů, nejpodstatnějším z nich je již dříve zmíněná změna struktury HTML stránky.

Testování proběhlo na dvou testovacích účtech pro každou podporovanou sociální síť. Na jednom účtu byla ponechána výchozí konfigurace. Příkladem těchto vstupů jsou tabulky 4.2, 4.3, 4.5 a 4.4. Na druhém účtu byly položky nastavení inkrementálně měněny. Tento přístup byl již použit při výběru modelu. Při prvním testu byla použita minimální konfigurace (definováno výše) a postupovalo se směrem k maximální konfiguraci. Takto získaná data byla manuálně porovnávána s daty na sociální síti. Jelikož bylo nezbytné při použití frameworku Selenium pracovat s prodlevou mezi stažením a kompletním načtením stránky včetně provedení všech scriptů, tak bylo testování prováděno opakovaně. Při několika běžích testů bylo zjištěno, že tato prodleva může způsobovat potíže při hledání HTML elementů stránky. Pro zamezení tomuto problému byl přidán mechanismus, kdy při detekci tohoto chování je přidána prodleva dvě sekundy a poslední chybná akce se opakuje s takto nastavenou prodlevou. V případě opětovného neúspěchu se tento mechanismus opakuje znovu. Hodnota dvě sekundy byla zvolena na základě pozorování během testování. Dalším faktorem ovlivňující toto chování je rychlost připojení k internetu. Pokud uživatel disponuje nízkou rychlostí internetového připojení, načítání stránky trvá déle a proto je potřeba zvyšovat dobu čekání na načtení stránky.

Další krokem testování aplikace bylo testování celé aplikace, přičemž se zároveň otestovaly i zbývající komponenty. Opět byly použity dříve vytvořené účty a již ověřené inkrementální testování. Opět byla u každé sociální sítě zvolena počáteční konfigurace, tj. minimální a postupovalo se směrem k maximu. Po každém běhu aplikace bylo sledováno, zda se výsledné Privacy score pohybuje dle předpokladů. Se zvyšujícím se Privacy score souvisí i dělení uživatelů do skupin. I zde se ověřovalo, zda jsou uživatelé klasifikováni správně. Nakonec se při každém testu ověřila kompletnost dat odesílaných grafické části aplikace.

	U1	U2	U3	U4	U5	U6	U7	U8	U8	U9	U10	U11	U12
Facebook	3.16	2.48	1.79	2.54	1.79	1.97	3.16	3.02	1.88	2.67	2.83	1.81	1.93
Google	3.62				3.62	3.62		3.62	2.35	3.62			
Instagram			1.29	1.08			1.29	1.28			0.06		
Twitter			1.88			2.21				2.09			
LinkedIn		2.73				2.37							
Tumblr						0.07							
Externí analýza	0.32	1.32	0.32	0	1.14	1.32	0.32	1.46	1.14	0.32	1.46	1.32	1.32
SU - Facebook	III	II	I	II	I	I	III	II	I	II	II	I	I
SU - externí	II	III	II	I	II	III	II	III	II	II	III	III	III

SU - skupina uživatelů, I - Defensivní uživatel, II - Většinový uživatel, III - Neopatrný uživatel

Tabulka 5.1: Výsledky uživatelského testování

Tato skutečnost je ověřitelná na základě zobrazených dat, pokud by se data odeslala nekompletní, část grafického výstupu by chyběla.

5.2 Uživatelské testování

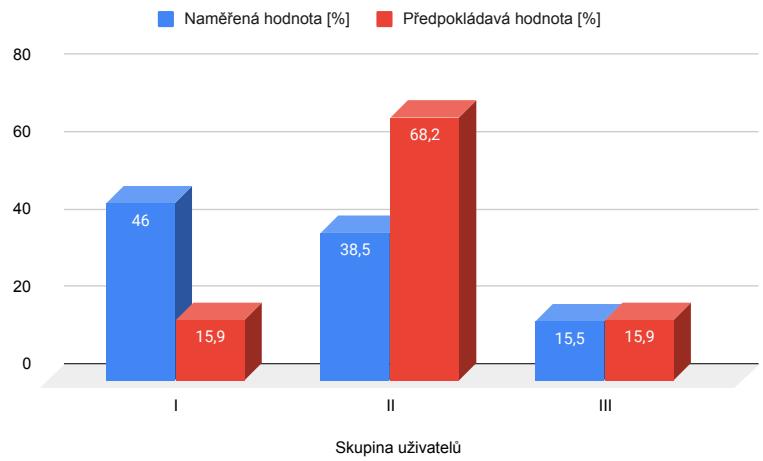
Uživatelské testování bylo naplánováno ze dvou důvodu, prvním z nich je ověření funkčnosti implementace uživateli. Druhým cílem tohoto přístupu bylo zjistit jak jsou uživatelé opatrní při nakládání s privátními informacemi.

Pro účely testování byla aplikace umístěna na server s veřejnou IP adresou. Na tomto serveru byl vytvořen uživatelský účet s předinstalovanou aplikací. Toto řešení bylo zvoleno tak aby bylo umožněno testování co nejširší skupině uživatelů. Pro běh aplikace na konkrétní stanici je nutné instalovat řadu Python modulů, stáhnout ovladač webového prohlížeče a nakonfigurovat ho. Tento proces by jistě odradil řadu uživatelů. Další možností bylo vytvoření jednoho spustitelného souboru. Ač se tento přístup zdál být nejjednodušší, ukázalo se, že řada uživatelů používá starší systémy, díky čemuž se objevily problémy se závislostmi. Proto byl zvolen přístup, kdy se aplikace nainstaluje na jeden server s aktuálním operačním systémem, všemi potřebnými moduly, uživatel se pouze přihlásí a může aplikaci využívat dle libosti. Testování se zúčastnilo třináct technicky založených respondentů ve věku 20-25 studujících informatiku.

5.3 Vyhodnocení testování

V rámci testování funkcionality nebyly objeveny žádné nedostatky a to především díky testování, které probíhalo v rámci implementace, kdy byly nedostatky odhalovány a operativně opravovány. Testování se zúčastnilo třináct respondentů, přičemž všichni z nich vlastnili účet na síti Facebook, pět z nich na síti Google a Instagram, dva LinkedIn a tři Twitter. Zbylé sociální sítě měly zastoupení po jednom respondentovi až na Pinterest, kde nevlastnil žádný z účastníků účet. Výsledky měření jsou zobrazeny v tabulce 5.1. Hodnoty buněk tabulky udávají výsledné Privacy score. Jelikož pro vyhodnocování výsledků není u všech sociálních sítí dostatek informací bude dále pracováno pouze se sítí Facebook a výsledky externí analýzy.

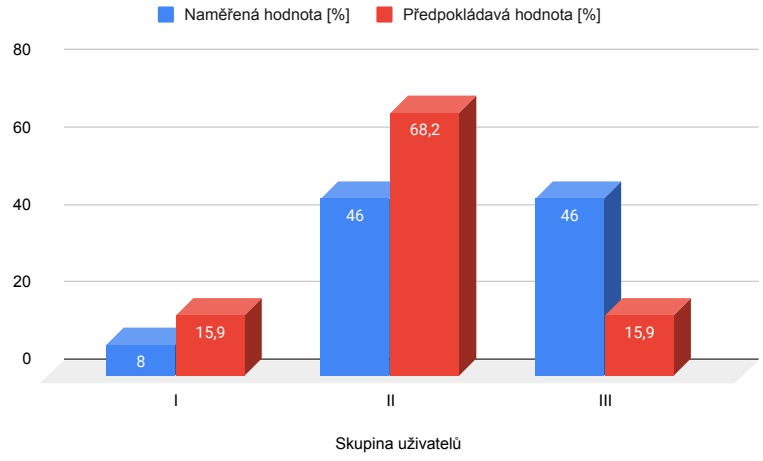
Z výsledků interní analýzy (5.1) sítě Facebook lze určit, že 46% účastníků testování má defenzivní nastavení soukromí na síti, 38.5% spadá do skupiny *Většinový uživatel* (II) a 15,5% uživatelů se řadí mezi neopatrné uživatele (III). Zde lze vidět (obr. 5.1), že procento neopatrných uživatelů odpovídá s jistou tolerancí předpokladu. Tj. na základě normálního



Obrázek 5.1: Výsledné rozložení uživatelů sítě Facebook v porovnání s předpokládaným rozložením

rozložení pravděpodobnosti by mělo těchto uživatelů být 15,9%. Naopak opatrných uživatelů je přibližně o 30% více oproti předpokladu na úkor většinovým uživatelům. Z čehož by šel vyvodit závěr, že zúčastnění uživatelé jsou spíše opatrnější na své soukromí. Tento výsledek ovšem nelze považovat za směrodatný z důvodu relativně malého počtu respondentů.

Výsledky externí analýzy ukázaly mírně opačný trend (obr. 5.2). Zde skupina opatrných uživatelů (I) dosáhla pouze 8% , skupina většinových uživatelů obsahuje (II) shodně jako skupina neopatrných uživatelů (III) 46% respondentů. Zde lze vidět celkový posun rozložení směrem k neopatrnosti při nakládání se soukromím.



Obrázek 5.2: Výsledné rozložení uživatelů externí analýzy v porovnání s předpokládaným rozložením

Kapitola 6

Závěr

Práce se zabývá soukromím na internetu resp. na sociálních sítích, což je velmi diskutované téma v dnešní době. V rámci práce byl vytvořen nástroj/aplikace, která pomůže běžnému uživateli zorientovat se v poměrně novém prostředí. Taktéž může být tento nástroj považovaný za varovný prostředek pro některé uživatele, kteří si ne zcela uvědomují skrytá nebezpečí internetu. Aplikace umí sbírat informace přímo z nastavení uživatele, což je hlavní předností této práce. Díky této funkcionalitě se pracuje s nejpřesnějšími daty a je poskytováno přesné zhodnocení soukromí a tím pádem i přesná doporučení, jak zlepšit nastavení zabezpečení privátních informací účtu.

V průběhu práce bylo nutné provést analýzu sociálních sítí, především analýzu nastavení soukromí. Dalším nezbytným krokem bylo nastudovat přístupy evaluace nastavení, což zahrnovalo studium evaluačních modelů.

Implementace práce zahrnovala studium rozhraní a struktur webových rozhraní sociálních sítí. Nejpodstatnějším problémem v průběhu implementace byly aplikační firewally těchto webů. Jelikož v této oblasti neexistují z pochopitelných důvodů veřejně dostupné dokumentace, bylo nezbytné nejprve tyto ochranné mechanismy identifikovat, otestovat jejich reakce na různé scénáře a detekovat jejich chování. Na základě zjištěných poznatků byly pro všechny podporované sítě navrženy a implementovány mechanismy, které tato opatření překonávají. Jelikož se sociální sítě snaží chránit sebe a své uživatele před automatizovanými nástroji, nebylo by bez této části možné provádět interní analýzu jelikož nese rysy automatizovaného přístupu k webu.

Testování funkcionality výsledné aplikace neprokázalo žádné chyby. Dále probíhalo uživatelské testování. Pro tyto účely byla konečná verze aplikace zveřejněna na platformě **Github**[1] včetně návodu ke stažení a spuštění binární verze nebo instalaci potřebných modulů a spuštění aplikace ze zdrojových souborů. Uživatelské testování potvrdilo výsledky předchozího testování funkcionality. A mimo to ukázalo, že uživatelé, kteří se zúčastnili testování se snaží v rámci sítě chránit své soukromé informace, ale na druhou stranu externí analýza ukázala, že ti stejní uživatelé sdílí veřejně, mimo sociální sítě, řadu soukromých informací.

Zadání kladlo práci za cíl na základě získaných znalostí ze stávajících prací navrhnout, implementovat a otestovat nástroj pro evaluaci soukromí z interního, externího pohledu. Dále diskutovat možnosti srovnání různých nastavení napříč sociálními sítěmi a na závěr provést srovnání interního a externího přístupu. Navržená a implementovaná aplikace dokáže analyzovat sedm sociálních sítí (Facebook, Twitter, Google, LinkedIn, Tumbrl, In-

[1] https://github.com/fila43/Master-thesis

stagram, Pinterest) jak z externího tak i interního pohledu. Zatímco interní analýza je prováděna pro každou konkrétní sociální síť separátně, tak externí analýza sbírá a agreguje data z více zdrojů a tím postupně informace o uživatelském nastavení zpřesňuje. Kvůli rozdílné granularitě nastavení a dalším problémům popisovaným v práci není vhodné porovnávat výsledky interní analýzy napříč sociálními sítěmi, jelikož porovnání by vedlo k značnému zkreslení výsledku zanedbáním části dostupných informací. Naopak díky tomu, že externí analýza agreguje informace z více zdrojů a přistupuje k množině sociálních síti jako k jediné je možné tyto výsledky porovnávat.

Další pokračování práce by mohlo směřovat k rozšíření funkcionality komponenty extraktoru. Data by mohla být extrahována vhodným doplňkem v prohlížeči popřípadě by mohla být extrahována data z cookies prohlížeče. Tyto přístupy by odstranily nutnost zadávání uživatelských údajů do aplikace. Další možnou cestou pokračování práce je přidání podpory pro účty s dvoufázovým ověřením. V souvislosti s automatizovaným získáváním informací z webů, které využívají změn HTML jako obrany, by bylo vhodné navrhnout a implementovat automatizovaný mechanismus detekce těchto změn a následné úpravy cest ke změněným elementům.

Literatura

[1] *Česká terminologická databáze knihovnictví a informační vědy (TDKIV)*. 2003. Dostupné z: https://aleph.nkp.cz/F/?func=direct&doc_number=000015947&local_base=KTD.

[2] Ackerman, M., Cranor, L. a Reagle, J. Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences. *Proceedings of the ACM Conference in Electronic Commerce*. Září 2000.

[3] Bruckner, T. *Tvorba informačních systémů: principy, metodiky, architektury*. Praha: Grada, 2012. ISBN 978-80-247-4153-6.

[4] Clincy, V. a Shahriar, H. Web Application Firewall: Network Security Models and Configuration. In: *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*. 2018, s. 835–836.

[5] Hanna Krasnova, K. K. T. H. *ONLINE SOCIAL NETWORKS: WHY WE DISCLOSE* [online]. [cit. 2019-11-02]. Dostupné z: http://ssrn.com/abstract=2050898.

[6] E. M. Maximilien, T. S. D. R. S. G. a Liu, K. Privacy-as-a-Service: Models, Algorithms, and Results on the Facebook Platform. In:. Web 2.0 Security and privacy workshop, 2009, 2009. Dostupné z: http://www.ieee-security.org/TC/W2SP/2009/papers/s4p2.pdf.

[7] Erlandsson, F., Boldt, M. a Johnson, H. Privacy Threats Related to User Profiling in Online Social Networks. In:. Září 2012.

[8] Golle, P. Revisiting the Uniqueness of Simple Demographics in the US Population. In: *Proceedings of the 5th ACM Workshop on Privacy in Electronic Society*. New York, NY, USA: Association for Computing Machinery, 2006, s. 77–80. WPES '06. Dostupné z: https://doi.org/10.1145/1179601.1179615. ISBN 1595935568.

[9] KUN LIU, E. T. *A Framework for Computing the Privacy Scores of Users in Online Social Networks* [online]. 2010 [cit. 2019-11-02]. Dostupné z: http://cs-people.bu.edu/evimaria/papers/tkdd-pr.pdf.

[10] Madejski, M., Johnson, M. a Bellovin, S. The Failure of Online Social Network Privacy Settings. Leden 2011.

[11] Oldřich, M. *Slovník sociální práce*. 2. vyd. Portál, 2008.

[12] Chen, J. B. H. *Measuring Privacy Risk in Online Social Networks* [online]. [cit. 2019-12-02]. Dostupné z: https://web.cs.ucdavis.edu/~hchen/paper/w2sp2009.pdf.

[13] Nilothpal Talukder, Mourad Ouzzani, Ahmed K. Elmagarmid, Hazem Elmeleegy, and Mohamed Yakout. *Privometer: Privacy Protection in Social Networks* [online]. 2010 [cit. 2019-11-02]. Dostupné z: https://ieeexplore.ieee.org/document/5452715.

[14] Renita Crystal Pereira, V. T. *Web Scraping of Social Networks* [online]. [cit. 2019-11-02]. Dostupné z: http://www.ijircce.com/upload/2015/sacaim/43_710.pdf.

[15] SIGMUND, T. *Ambiguous Character of Information Privacy and Its Possible Solution. Journal of Information Ethics. 26 (2).* McFarland Company, 2017. ISBN 978-1-4766-2189-0.

[16] Joon S. ParkKevin, A. K. J. W. K. *Trusted Online Social Network (OSN) serviceswith optimal data management* [online]. [cit. 2019-11-02]. Dostupné z: https://www.sciencedirect.com/science/article/pii/S0167404814000236.

[17] Tekerek, A., Gemci, C. a Bay, O. F. Development of a hybrid web application firewall to prevent web based attacks. In: *2014 IEEE 8th International Conference on Application of Information and Communication Technologies (AICT).* 2014, s. 1–4.

[18] Wang, Y. a Nepali, R. K. Privacy Measurement for Social Network Actor Model. In: *2013 International Conference on Social Computing.* IEEE, 2013, s. 659–664. Dostupné z: http://ieeexplore.ieee.org/document/6693396/. ISBN 978-0-7695-5137-1.

[19] Wang, Y., Nepali, R. K. a Nikolai, J. Social network privacy measurement and simulation. In: *2014 International Conference on Computing, Networking and Communications (ICNC).* IEEE, 2014, s. 802–806. Dostupné z: http://ieeexplore.ieee.org/document/6785440/. ISBN 978-1-4799-2358-8.

[20] Zheleva, E. a Getoor, L. To join or not to join: The illusion of privacy in social networks with mixed public and private user profiles. In:. Leden 2009, s. 531–540.

[21] Zheleva, E. T. a Getoor, L. *Privacy in social networks. Synthesis Lectures on Data Mining and Knowledge Discovery 3.1.* Morgan publishers Claypool publishers, 2012. ISBN 9781608458622.