BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Excel@FIT 2020
http://excel.fit.vutbr.cz

Pokročilá evaluace privátnosti na sociálních sítích

Filip Januš*

Abstrakt
V dnešní době stále přetrvává trend přesunu mezilidské komunikace do online prostředí. A to díky sociálním sítím a službám jimi poskytovanými. 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 bezpečnostních nastavení uživatelských účtů sociálních sítí a následné vyhodnocení tohoto 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 své nastavení soukromí na sociální síti. Což by mělo pomoci uživateli omezit množství uniklých citlivých informací.
Klíčová slova: Sociální síť — Soukromí — Bezpečnost — Skóre soukromí — Nastavení soukromí

Přiložené materiály: *N/A*

*xjanus08@stud.fit.vutbr.cz, *Faculty of Information Technology, Brno University of Technology*

1. Úvod

V dnešní době stále populárnějších sociálních sítí, se snadno stává, že bezpečnost soukromích informací na těchto sítích je až druhořadý nebo vůbec neřešený problém. Řada uživatelů má malé nebo žádné povědomí o možnostech nastavení a ochrany osobních údajů na sociálních sítích. Taktéž sociální sítě neposkytují uživatelům zpětnou vazbu na jejich nastavení a nakládání se svým soukromím. Nezbytnost řešit tyto problémy a poukazovat na ně dokazuje několik publikací [1, 2] nebo nedávno zveřejněný snímek "V síti".

Výzkumy ukazují, že díky klasifikačním technikám lze efektivně odhalit citlivé informace uživatelského profilu sociální sítě na základě ne mnoha informací, v kombinaci se znalostí příslušnosti do různých skupin nebo v kombinaci se znalostí o účasti v různých aktivitách na sociálních sítích.

Hlavním cílem práce je analyzovat možná nastavení soukromí na sociálních sítích. Tato nastavení vyčíslit pomocí modelů, aby bylo možné vyhodnotit získané informace o nastavení soukromí uživatele. Dále dát uživateli zpětnou vazbu na základě jeho nastavení a doporučit mu nápravná opatření. Přičemž informace budou získávány dvěma způsoby. Interním, při kterém informace o nastavení budou staženy přímo z přihlášeného účtu a nebo externí, při kterém budou informace o uživateli získány z veřejně dostupných zdrojů (vždy pro konkrétní sociální síť).

2. Existující práce

Již několik desítek prací bylo zaměřeno na oblast bezpečnosti na sociálních sítích. Tyto práce se tématem zaobíraly z několika různých pohledů. V [1] se autoři zabývají dolováním citlivých dat z publikovaných informací na sociálních sítích, definují zde anonymitu a popisují různé přístupy dolování dat a zabývají se možnými riziky vyzrazení citlivých informací. Jedna z prvních prací zaměřených na internetové sociální sítě [3] 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 [4] se zaměřovali na vy-

číslování soukromí mezi dvěma uživateli, dle nastavených atributů, prezentovali již dříve navrhované modely a následně je dále vylepšovány, tak aby lépe reflektovaly uživatelská nastavení.

V publikaci [5] se autoři věnovali vývoji aplikace zobrazující procentuální míru ohrožení soukromí uživatele sociální sítě. Tato aplikace získává data o uživateli z API sociální sítě Facebook. Autoři se zde rozhodli vyčíslovat ohrožení privátnosti na základě informací o vztazích s ostatními uživateli a na základě dostupných informacích o přátelích. Taktéž Becker a Chen [6] vyvíjeli nástroj na detekci potencionálních úniků soukromých informací, podobně jako v [5] 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 [2] 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. Naopak v práci [7] autoři zkoumají 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 nastavením.

3. Motivace

Cílem této 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 a 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.

Zatímco výše popisované práce pracovaly vždy s informacemi poskytovanými prostřednictvím API sociálních sítí nebo s informacemi veřejně dostupnými (členství ve skupinách, různé aktivity, spojení s přáteli), aplikace navrhovaná v této práci, pracuje s informacemi získanými přímo z nastavení profilu, díky čemuž lze dosahovat podstatně přesnějších a detailnějších výsledků než v předchozích pracích. Tato skutečnost je dána především skutečností, kdy API sociálních sítí neposkytují informace o nastavení zabezpečení a soukromí účtu.

Další předností navrhované práce je také podpora několika sociálních sítí, zatím co předešlé práce se zaměřovaly pouze na jednu specifickou síť.

4. Sociální sítě

Sociální síť lze popsat jako internetovou službu umožňující svým uživatelům vytvářet vlastní profily, sdílet informace, videa, fotografie, komunikovat, provozovat chat a mnoho dalších aktivit [8, 9]. Existuje celá řada sociálních sítí, které lze dělit dle obsahu, který uživatelé sdílí. Dělení lze provádět 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.

Z matematického pohledu lze sociální síť považovat za graf, kde vrcholy jsou reprezentovány entitami a hrany vztahy mezi nimi [4]. 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.

Důležitým pojmem v kontextu vztahů na sociálních sítích je stupeň separace [4]. Pojem úzce souvisí s viditelností atributů entity. Definuje se jako *funkce h* určující počet kroků mezi entitou A_i a A_j.

$$d_{ij} = h(A_i, A_j) \tag{1}$$

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.

Z pohledu zabezpečení soukromých informací uživatele nabízí sociální sítě možnosti ovlivnit zveřejňované informace. Spektrum možných nastavení se různí napříč sociálními sítěmi. Od desítek možných kombinací nastavení až po malé jednotky. Například sociální síť Facebook umožňuje uživateli konfigurovat sedmnáct různých nastavení. Naproti tomu sociální síť Tumblr disponuje pouze 3 nastaveními. Všechny sociální sítě poskytují uživateli možnosti kontrolovat

své aktivity na síti, také dovolují uživateli stáhnout veškerá data, které uživatel síti poskytl. A to včetně chatových konverzací a záznamů všech akcí na sociální síti. Mezi akce lze zařadit příspěvky označené jako *To se mi líbí* v případě Facebooku. Žádná z analyzovaných sítí ovšem neposkytuje jakoukoli formu upozornění, zda zveřejnění určitého atributu má či nemá dopad na soukromí uživatele.

5. Privátnost a její vyčíslení

V průběhu této kapitoly bude popsána metrika privacy score. Dále několik modelů navržených autory v pracích [4], [10] a [3], které na základě údajů o nastavení účtů dokáží tuto metriku vyčíslit.

5.1 Privacy score

Aby bylo možné vhodným způsobem zpracovávat úroveň soukromí je potřeba mechanismus, který umožní tuto úroveň vyčíslit. Podobné mechanismy již spolehlivě fungují v různých odvětvích komerčního sektoru. Z toho důvodu byla jedna z metod převzata [3]. Metoda vychází z již fungujících technik pro určování skore entity. Tyto techniky se používají například v bankovnictví, kde se určuje bonita nebo důvěryhodnost klienta na základě jeho vlastností. Tato metoda se v kontextu soukromí na sociálních sítích nazývá Privacy score. Indikuje potenciální nebezpečí pro soukromí entity. Platí, že čím vyšší privacy score tím výšší 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, zatím co 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 [10, 2], 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.

5.2 Virtuální atribut

Jak bylo popsáno výše existují vlastnosti/atributy, které mají dopad na soukromí, i když se mohou zdát nepodstatné. V některých případech se jedná o tzv. virtuální nebo také kompozitní atribut, který se skládá z několika jiných atributů. Kombinace několika zdánlivě nepodstatných atributů může vést k odhalení podstatné části soukromí uživatele. Například v práci [10] 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.

5.3 Popis entity

Aby bylo možné jednoduše pracovat s jednotlivými položkami entity při evaluaci privátnosti v rámci OSN (Online social network), používá se u většiny modelů popis založený na maticích tzv. Odpovědní matice [3].

Přínos tohoto zápisu 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 R je odpovědní matice, i je uživatel (řádek matice), j je konkrétní vlastnost (sloupec matice) a 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 informaci sdílet.

5.4 Model citlivosti a viditelnosti

Prvním zástupcem modelů evaluace je základní model citlivosti a viditelnosti [3] 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 [10], z které vychází tabulka 1, 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.

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

	Váha atributu[%]
Jméno	15
Vzdělání	15
Stav	25
Rodinní příslušníci	25
Pohlaví	25
Město	45
Stát	45
Fotky	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 1. Tabulka citlivostí atributů (Zdroj:[10])

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:

$$PR(j) = \sum_{i=1}^{n} PR(i,j) = \sum_{i=1}^{n} \beta_i * V(i,j) \qquad (3)$$

5.5 PIDX (Privacy Index)

Dalším z modelů vyčíslující soukromí entity resp. privacy score je PIDX [4]. 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 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 4, kde **i** značí konkrétní atribut a W_{max} maximální hodnotu citlivosti, konkrétní hodnoty lze nalézt v dříve prezentované tabulce vah 1.

$$PIF(i) = \frac{W(i)}{W_{max}} \qquad (4)$$

	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. Příklad nastavení účtu Google

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 [10]. 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

$$w - PIDX(V,S) = \frac{\sum_{j=1}^{n} V(j)s_j}{\sum_{j=1}^{n} s_j} \qquad (5)$$

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

$$m - PIDX(V,S) = \max(V(1)s_1, .., V(n)s_n) \qquad (6)$$

   kde funkce max vrací ze zadaných hodnot tu maximální.

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:

$$c - PIDX(V,S) = m - PIDX(V,S) + \qquad (7)$$
$$(100 - m - PIDX(V,S)) \cdot \frac{w - PIDX(V,S)}{100}$$

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 [4].

Příkladem použití může být aplikace modelu C-PIDX na výchozím nastavení Google účtu, které je

zobrazeno v tabulce 2. Pro výpočet privacy score je zapotřebí množina V_i, která je reprezentována sloupcem viditelnost a množina vah S_i. Váhy se vypočtou dle vztahu 4. Například pro nastavení *Historie polohy*:

$$PIF(2) = \frac{60}{65} \tag{8}$$

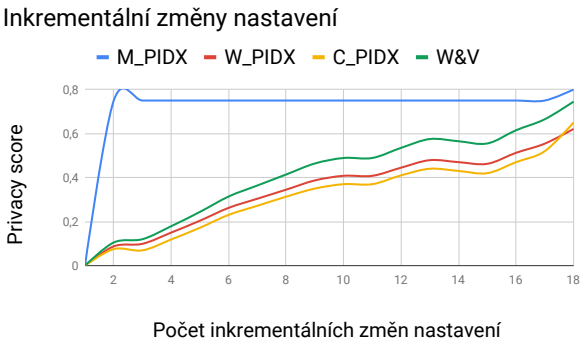
Dále se již jen dosadí známé hodnoty do rovnic 5, 6, 7, čímž se získá výsledné privacy score modelem C-PIDX.

6. Výběr modelu

Aby bylo možné vybrat co nejvhodnější model pro vyčíslení privátního skóre, bylo provedeno testování a vyhodnocení chování modelu v různých situacích.

6.1 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 3. 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 1. Výsledek testování inkrementálních změn

Tento postup byl již použit pro modely třídy PIDX v práci [4]. 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 1, 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 1 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		

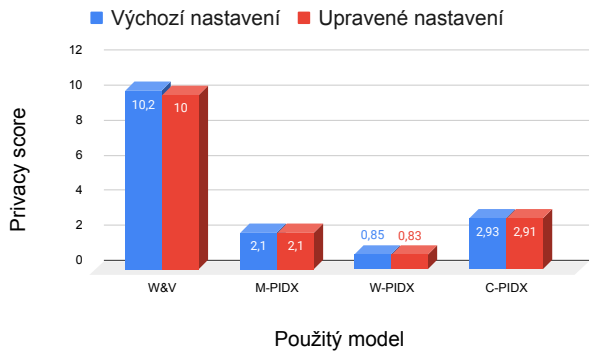
Tabulka 3. Testovací data vycházející z výchozího nastavení sítě Facebook

Posledním testovaným modelem je model váhy a viditelnosti zobrazený zeleně na obrázku 1. Model se chová velice podobně jako W-PIDX a taktéž má problém se skokovými změnami.

6.2 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. 3 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.

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 3 vypnuty. Poté bylo přidáno nastavení:



Obrázek 2. Výsledek testování nastavení s pozitivním efektem

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 2.

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

6.3 Vyhodnocení

Jako výchozí model byl pro tuto práci zvolen C-PIDX. Jelikož inkrementální testování potvrdilo předešlé výsledky publikované v [4] 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 a ostatní modely se chovaly velice podobně.

Byl také brán zřetel na závěry autorů modelů PIDX, kteří uvádí v [4], že C-PIDX nejlépe z navrhovaných modelů reflektuje kompozitní atributy.

7. Návrh řešení

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, což bude stěžejní komponenta celého nástroje, neboť bude na základě dostupných informací a za pomoci dříve vybraného modelu provádět vyčíslování skóre soukromí. Poslední v řetězci bude modul vyhodnocení prezentující výsledky uživateli. Kompletní schéma systému je zobrazeno na obr. 3.

Nástroj bude podporovat dva základní režimy: Interní a externí. V interním režimu aplikace provede přihlášení na sociální síť, zde vyhledá a extrahuje informace o nastavení soukromí, které jsou následně vyhodnoceny a prezentovány uživateli. Externí přístup zjišťuje informace o uživateli z pohledu třetí osoby a na základě zjištěných informací se dedukuje aplikované nastavení účtu.

Prezentace výsledku spočívá v zařazení uživatele do skupiny s obdobným nastavením soukromí účtu. Uživateli bude také poskytnuta možnost nechat si poradit, které položky nastavení upravit za účelem zlepšení zabezpečení soukromí.

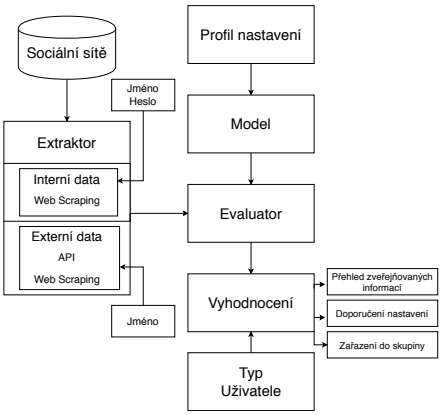
Cílové řešení by měla představovat aplikace, které uživatel poskytne přihlašovací údaje k účtu sociální sítě. Aplikace se přihlásí, zjistí aktuální nastavení zabezpečení a soukromí. Tyto informace vyhodnotí a sdělí uživateli procentuální míru ohrožení jeho citlivých informací. V případě nespokojenosti uživatele s výsledkem mu bude nabídnuta pomoc ve formě jednoduché nápovědy. Tato nápověda by měla uživateli sdělit, které položky nastavení představují největší hrozbu pro jeho soukromí. A uživatel se již sám bude moci rozhodnout, zda nastavení upraví či nikoli.

8. Implementace a testování

Navrhovaný nástroj byl prozatím implementovaný jako konzolová aplikace s ohledem na plánované rozšíření o grafické rozhraní.

Aplikace aktuálně podporuje funkcionalitu, která byla popsána v 7, přičemž se používá vybraný model C-PIDX. Momentálně je plně podporována sociální síť Facebook. Tj. na základě přihlašovacích údajů poskytnutých uživatelem, provede extrakci informací z jeho účtu, evaluuje nastavení, sdělí uživateli míru ohrožení, případně doporučí, která nastavení by šla upravit tak, aby bylo soukromí uživatele více chráněno.

Pro implementaci byl zvolen jazyk Python jelikož



Obrázek 3. Navrhovaná architektura systému

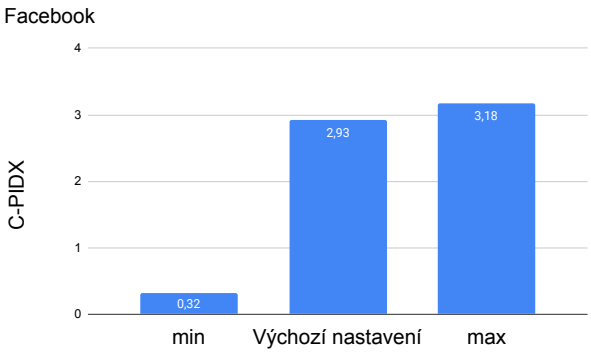
disponuje širokou škálou modulů umožňujících práci s webovými stránkami. Taktéž podporuje framework Selenium, což je nástroj dovolující automatizovaně procházet webu skrze webový prohlížeč. Tato technologie byla použita z důvodu potřeby překonat aplikační firewally sociálních sítí.

Dosavadní testování probíhalo pouze 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. Testování proběhlo na dvou testovacích účtech pro každou podporovanou sociální síť. Na jednom účtu byla ponechána výchozí konfigurace. Příkladem tohoto vstupu je tabulka 3. Na účtu druhém byly náhodné položky nastavení pozměněny. Nakonec byla data získaná nástrojem 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. 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.

Testování proběhlo pro sociální sítě Facebook, Twitter, LinkedIn a platformu Google. Během testování byl odhalen pouze problém popsaný výše i s jeho případným řešením.

Dále bylo provedeno za pomoci dříve vybraného modelu experimentální měření privátnosti pro výchozí nastavení sítě Facebook. Také byly měřeny extrémní situace 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.

Výsledky experimentálního měření v síti Facebook jsou zobrazeny na obrázku 4. 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 a několik méně podstatných položek, které nemají přílišný dopad na soukromí, ale položky s velkým dopadem jako *Kdo vás může vyhledat pomocí telefonního čísla, které jste zadali?* jsou povoleny.



Obrázek 4. Naměřené hodnoty na síti Facebook při výchozí konfiguraci a při mezních konfiguracích

9. Shrnutí a pokračování práce

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 rámci práce byly analyzovány jednotlivé sociální sítě a jejich nastavení. Hlavním cílem práce je tato nastavení vyčíslit, tak aby bylo možné použít nějakou míru a orientační stupnici, dle které si bude uživatel moci upravit svá nastavení. Popřípadě uživateli doporučit, které položky nastavení upravit.

Aktuálním výsledkem je konzolová aplikace použitelná pro měření privátnosti v sociální síti Facebook s možností poskytnout nápovědu, jakým způsobem upravit nastavení. Pro jiné sociální sítě zatím není podporována nápověda.

Další pokračování práce bude spočívat v rozšíření kompletní funkcionality pro další sociální sítě (Twitter, Google, LinkedIn) a poté se bude zabývat především testováním, zejména uživatelským testováním. Předpokládá se, že do testování bude zahrnuto dvacet uživatelů se svým nastavením soukromí na různých sociálních sítích. Výsledkem by mělo být pravděpodobnostní rozložení skóre soukromí. Dále budou určeny extrémy skóre privátnosti pro další sociální sítě. Na základě těchto testů by se měli dle skóre soukromí rozdělit uživatelé do několika skupin, do kterých bude následně prováděna klasifikace.

10. Poděkování

Tímto bych chtěl poděkovat vedoucímu své práce Mgr. Kamilu Malinkovi Ph.D. za odborné vedení a cenné rady.

Literatura

[1] Elena Zheleva, Evimaria Terzi, and Lise Getoor. Privacy in social networks. In *Synthesis Lectures on Data Mining and Knowledge Discovery*, volume 3, pages 1–85, 2012-03-31.

[2] Fredrik Erlandsson, Martin Boldt, and Henric Johnson. Privacy threats related to user profiling in online social networks. In *2012 International Conference on Privacy, Security, Risk and Trust and 2012 International Confernece on Social Computing*, pages 838–842. IEEE, 2012.

[3] Kun Liu and Evimaria Terzi. A framework for computing the privacy scores of users in online social networks. In *ACM Transactions on Knowledge Discovery from Data*, volume 5, pages 1–30, 2010-12-01.

[4] Yong Wang, Raj Kumar Nepali, and Jason Nikolai. Social network privacy measurement and simulation. In *2014 International Conference on Computing, Networking and Communications (ICNC)*, pages 802–806. IEEE, 2014.

[5] Nilothpal Talukder, Mourad Ouzzani, Ahmed K. Elmagarmid, Hazem Elmeleegy, and Mohamed Yakout. Privometer. In *2010 IEEE 26th International Conference on Data Engineering Workshops (ICDEW 2010)*, pages 266–269. IEEE, 2010.

[6] Justin Lee Becker and Hao Chen. Measuring privacy risk in online social networks. 2009. Dostupné z `https://web.cs.ucdavis.edu/~hchen/paper/w2sp2009.pdf`.

[7] Michelle Madejski, Maritza Johnson, and Steven Bellovin. The failure of online social network privacy settings. 01 2011. Dostupné z `https://www.researchgate.net/publication/229046080_The_Failure_of_Online_Social_Network_Privacy_Settings`.

[8] Joon S. Park, Kevin A. Kwiat, Charles A. Kamhoua, Jonathan White, and Sookyung Kim. Trusted online social network (osn) services with optimal data management. volume 42, pages 116–136, 2014.

[9] Česká terminologická databáze knihovnictví a informační vědy (tdkiv), 2003.

[10] Yong Wang and Raj Kumar Nepali. Privacy measurement for social network actor model. In *2013 International Conference on Social Computing*, pages 659–664. IEEE, 2013.