UNIVERZITA PARDUBICE

FAKULTA ELEKTROTECHNIKY A INFORMATIKY

BAKALÁŘSKÁ PRÁCE

2017 Radek Pištínek

Univerzita Pardubice

Fakulta elektrotechniky a informatiky

Analýza eroze soukromí uživatelů mobilních operačních systémů a geolokačních aplikací

Radek Pištínek

Bakalářská práce

2017

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: **2016/2017**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Radek Pištínek**
Osobní číslo:	**I14159**
Studijní program:	**B2646 Informační technologie**
Studijní obor:	**Informační technologie**
Název tématu:	**Analýza eroze soukromí uživatelů mobilních operačních systémů a geolokačních aplikací**
Zadávající katedra:	**Katedra informačních technologií**

Zásady pro vypracování:

Cílem bakalářské práce je vyhodnotit při různých modelech geolokačních služeb míru tzv. eroze soukromí uživatelů u současných mobilních operačních systémů a mobilních aplikací využívající geolokaci. Bakalářská práce bude zahrnovat analýzu geodat, které jsou odesílané na servery poskytovatelům vybraných mobilních operačních systémů (např. Android, Windows Mobile, iOS) a mobilních aplikací využívající geolokaci uživatele (např. geosociální sítě). Bakalářská práce také bude zkoumat modely predikce pohybu uživatelů na základě sbíraných geodat. Součástí práce bude i srovnání přesnosti současných WiFi geolokačních služeb (od Google, Microsoft, Apple, Mozilla). Výstupem bakalářské práce bude metodika pro maximalizaci ochrany před erozí soukromí uživatelů při zachování možnosti využívat lokálně kontextové služby uživatelem.

Rozsah grafických prací:

Rozsah pracovní zprávy: **30**

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

KYSELA, J.: Comparison of Web Applications Geolocation Service. In: IEEE 15th International Symposium on Computational Intelligence and Informatics (CINTI 2014). Budapešť: Óbuda University, 2014. ISBN 978-1-4799-5338-7.
KYSELA, J.: Analysis of Privacy Erosion of Geosocial Networks. In: IEEE 16th International Symposium on Computational Intelligence and Informatics (CINTI 2015). Budapešť: Óbuda University, 2015. ISBN 978-1-4673-8520-6.

Vedoucí bakalářské práce: **Ing. Jiří Kysela, Ph.D.**
Katedra informačních technologií

Datum zadání bakalářské práce: **31. října 2016**

Termín odevzdání bakalářské práce: **12. května 2017**

Ing. Zdeněk Němec, Ph.D.
děkan

L.S.

Mgr. Josef Horálek, Ph.D.
pověřený vedením katedry

dne

Prohlášení autora

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 08. 12. 2017

podpis autora
Radek Pištínek

PODĚKOVÁNÍ

Rád bych poděkoval svému vedoucímu práce, Ing. Jiřímu Kyselovi, Ph.D., za ochotu, vstřícnost, trpělivost, cenné rady a materiály, které mi poskytl v průběhu zpracování bakalářské práce. Dále bych chtěl poděkovat rodině, přátelům a přítelkyni za trpělivost a podporu nejen při psaní bakalářské práce, ale i v průběhu studia.

ANOTACE

Bakalářská práce se zabývá problematikou eroze soukromí uživatelů mobilních operačních systémů a geolokačních aplikací. V práci jsou popsány modely predikce uživatelů. Dále jsou měřeny přesnosti jednotlivých WiFi geolokačních služeb a zanalyzovány geolokační údaje, které si o uživatelích vyžadují servery geolokačních aplikací. Nakonec je popsána metodika maximalizace ochrany před erozí soukromí.

KLÍČOVÁ SLOVA

eroze soukromí, geolokace, WiFi, geosociální sítě, analýza, predikce

TITLE

Analysis of privacy erosion of mobile operating system and geolocation applications users

ANNOTATION

Bachelor thesis focuses on problematics of privacy erosion of mobile operating system and geolocation applications users. The thesis describes prediction models of users. Additionally, there are measures of WiFi geolocation services and geolocation data, which are requested by geolocation application servers are also analyzed. Finally, there is described method for maximizing protection against privacy erosion.

KEYWORDS

privacy erosion, goelocation, WiFi, geosocial networks, analysis, prediction

OBSAH

SEZNAM ILUSTRACÍ A TABULEK

SEZNAM ZKRATEK A ZNAČEK

API	Application Programming Interface
ARP	Address Resolution Protocol
BSS	Base Station Subsystem
BTS	Base Transceiver Station
DPO	Data Protection Officer
DVD	Digital Versatile Disc
EU	Evropská unie
GDPR	General Data Protection Regulation
GPS	Global Positioning System
HW	Hardware
IP	Internet protocol
LBQID	Location Based Quasi-Identifier
LBS	Location Based Service
LBSN	Location Based Social Network
OS	Operační Systém
SSID	Service Set Identifier
SW	Software
SWOT	Strengths, Weaknesses, Opportunities, Threats
WiFi	Wireless Fidelity

ÚVOD

Tato práce má za cíl vyhodnotit pří různých modelech geolokačních služeb míru tzv. eroze soukromí uživatelů u současných mobilních operačních systémů a mobilních aplikací využívající geolokaci. Znění zadání této práce se jevilo jako více než zajímavé, protože nikdo nemá rád narušení vlastního soukromí a už vůbec ne, když je to narušení bez jeho vědomí. Ochrana soukromí a jeho respektování vychází z uznání, že každému náleží rovná práva a že každý člověk má přirozenou důstojnost. Nikdo nesmí být vystaven svévolnému zasahování do soukromého života, rodiny nebo korespondence a každý má nárok na ochrany proti takovým zásahům.

V první části této práce se čtenář seznámí s typy mobilních operačních systémů. Dále také s geolokací, časoprostorovými otisky a geosociálními sítěmi. K vyhodnocení této problematiky poslouží SWOT analýza.

První praktickou částí, jež se práce zabývá je přesnost WiFi geolokačních služeb. Ta byla naměřena pomocí JavaScriptového kódu ve webových prohlížečích Google Chrome, Microsoft Edge a Mozilla Firefox. Měření proběhlo tzv. *indoor* na notebooku ve třech městech České republiky, v Praze, Brně a Pardubicích.

Druhou praktickou částí byla analýza odesílaných dat serverům nadřazených společností mobilních operačních systémů a mobilních aplikací využívající geolokaci uživatele. Přibližný postup této analýzy probíhal simulací útoku *man in the middle* pomocí notebooku s OS Kali linux, kde se zachytávala komunikace mezi tabletem s OS Android a směrovačem připojeným dále na internet.

V poslední části je shrnuta metodika pro maximalizaci ochrany před erozí soukromí pro běžné uživatele mobilních zařízení. Dále jsou zmíněny obecná doporučení, která plynou ze všech měření a zjištění této práce.

1 MOBILNÍ OPERAČNÍ SYSTÉMY

Mobilní operační systém je operační systém pro chytré telefony, tablety, nebo jiná mobilní zařízení. Výjimkou jsou laptopy, které bychom sice mohli za mobilní zařízení považovat, ale většinou mají instalovaný operační systém určený pro stolní počítače.

Poskytuje uživatelské rozhraní, přístup k aplikacím, komunikuje s hardwarem a umožňuje uživateli manipulaci s daty a programy. Je pravdou, že je to právě operační systém, co dělá z telefonu telefon chytrý. Politika jednotlivých výrobců mobilních zařízení poté určuje, zdali je operační systém koncipován přímo na míru daného zařízení (iOS), nebo je více zobecňován (Android). V dnešní době jsou primárně navrženy pro zařízení s dotykovou obrazovkou.

Zdroje: [1], [2].

1.1 Android

Mobilní operační systém Android je v současnosti vyvíjen společností Google. Systém je založen na linuxovém jádře. Správu a stahování dalšího softwaru zastřešuje aplikace Google Play. Android byl od roku 2003 vyvíjen pod společností Android Inc. a měl být na trhu rivalem operačního systému Symbian. Google jej koupil v roce 2005 a odhalil široké veřejnosti roku 2007 s cílem vyvinout první skutečně otevřenou a komplexní platformu pro mobilní zařízení. Prvním chytrým telefonem s Androidem byl HTC Dream, také známý jako T-Mobile G1, ohlášen 23. září 2008. Zajímavostí také zůstává, že poté, co prošla první verze Androidu velkou řadou aktualizací a opravami, byly všechny další verze Androidu pojmenovány podle sladkých dezertů v pořadí abecedy. Během ohlášení Androidu KitKat v roce 2013 to Google objasnil tím, že „*Tato chytrá zařízení dělají náš život sladší, proto je každá verze Androidu pojmenována po sladkém dezertu.*“.

Zdroj: [3].

Zdrojový kód systému Android je vydán pod *open source* licencí, přestože si většina zařízení s Androidem razí cestu kombinací právě *open source* a proprietárního software. Android je populární mezi technologickými společnostmi požadující dokončený, nízkonákladový a upravitelný operační systém pro tzv. *high-tech* zařízení.

Obrovská hardwarová flexibilita Androidu má také svoje úskalí a tím je fakt, že softwarové aktualizace nových verzí operačního systému a bezpečnostní aktualizace mají ve většině případů výrazné zpoždění. Toto zpoždění vůči koncovým uživatelům je z praxe vyčísleno v řádu měsíců a objevily se i případy, kdy tyto aktualizace nedorazily vůbec.

Mezi další SW produkty z dílny společnosti Google se řadí například Android TV, Android Auto, jejichž názvy celkem intuitivně napovídají, že se jedná o systémy pro televize a auta. Dále také Android *wear* pro náramkové chytré hodinky. Všechny tyto zmíněné systémy mají od mobilní verze androidu speciálně upravené uživatelské rozhraní.

Zdroje: [1], [4].

Version	Codename	API	Distribution
2.3.3 - 2.3.7	Gingerbread	10	0.5%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	0.5%
4.1.x	Jelly Bean	16	2.2%
4.2.x		17	3.1%
4.3		18	0.9%
4.4	KitKat	19	13.8%
5.0	Lollipop	21	6.4%
5.1		22	20.8%
6.0	Marshmallow	23	30.9%
7.0	Nougat	24	17.6%
7.1		25	3.0%
8.0	Oreo	26	0.3%

Obrázek 1 - přehled zastoupení jednotlivých verzí Androidu na trhu (k 9. 11. 2017, verze se zastoupením 0,1 % a více)

Zdroj: [5].

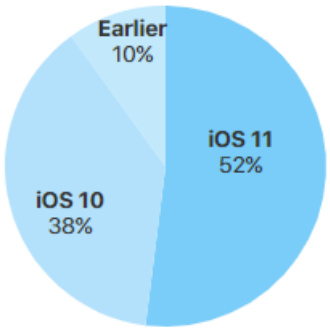
1.2 iOS

Operační systém iOS je vyvíjen společností Apple, a to speciálně pro jejich hardware. V praxi to znamená, že vychází přibližně jeden telefon ročně, za to ale s plně odladěným softwarem. Nevýhodou pro běžné uživatele je pak cenová dostupnost, neboť se tyto zařízení ihned po vydání cenově pohybují na hranici 15 až 20 tisíc Kč. Po hardwarové stránce razí Apple nekompromisní politiku nekompatibility svých zařízení s dostupnými standardy, např. napájecí a zároveň datové konektory používá odlišného typu (USB-C), než ostatní společnosti a v posledních verzích iPhonu nenalezneme audio konektor typu *Jack* atp.

Globálně je iOS druhým nejoblíbenějším, hned za právě zmíněným Androidem. Obsluhuje několik mobilních zařízení včetně iPhone, což je řada chytrých mobilních telefonů, iPad je řada tabletů a v neposlední řadě iPod, který zastřešuje řadu mobilních zařízení známou jako vylepšené MP4 přehrávače. Verze operačních systémů pro osobní počítače od společnosti Apple se pak nazývá macOS.

Prvně byl představen v roce 2007 pro iPhone, ještě tentýž rok pro iPod a v roce 2010 i pro iPad. Stejně jako Android, má iOS speciální službu pro stahování dalšího software, která se nazývá App Store. Uživatelské rozhraní tohoto systému dovoluje ovládat dané zařízení pomocí *multi-touch* gest, tedy více dotyky najednou. V neposlední řadě dokáže zařízení díky akcelerometru reagovat na tzv. *shaking*, neboli zahrkání. Společnost Apple je výjimečně vyzdvihována za dostupnost svých zařízení pro lidi např. s poruchou vidění nebo poruchou sluchu, kteří mohou svoje zařízení, i přes svůj hendikep, plnohodnotně využívat.

Zdroje: [6], [7].



Obrázek 2 - přehled zastoupení jednotlivých verzí iOS na trhu (k 6. 11. 2017)

Zdroj: [8].

1.3 Windows Phone

Mobilní operační systém Windows Phone je vyvíjen společností Microsoft čistě pro chytré telefony.

Byl to úspěšný nástupce Windows Mobile, který byl zaměřen spíše pro firemní trh a jehož počátky se datují k roku 2003. Kolem roku 2007 byl ve Spojených Státech Amerických nejvíce oblíbený, nicméně jeho popularita časem vypršela. Díky silné konkurenci iOS a Android v září 2010 byl Microsoft donucen vyvinout nástupce, kterým je právě zmiňovaný Windows Phone. Ten ale nebyl s Windows Mobile zpětně kompatibilní, Microsoft tuto větev absolutně „odřízl“ a začal opět s „čistým štítem“.

Windows Phone přišel na trh se zbrusu novým uživatelským rozhraním *Metro* a cílovou skupinou byli nově běžní uživatelé. Byl nasazen v říjnu 2010 a jeho první verzí byl Windows Phone 7. Názvy mobilních operačních systémů společnosti Microsoft se shodovali s aktuálními verzemi variant osobních počítačů, proto dalšími verzemi byly Windows Phone 8 a 8.1.

V roce 2015 vznikla idea, že by Microsoft mohl mnohem více propojit právě varianty osobních počítačů s mobilními zařízeními a vznikla tak další větev vývoje – Windows 10 Mobile, který byl prvně použitelný i pro tablety. Pro stahování a správu aplikací sloužil Microsoft Store, který se objevil i na variantách osobních počítačů Windows 10. Nutno podotknout, že ne všechny aplikace byly kompatibilní na obou variantách těchto systémů.

Mobilní zařízení s tímto operačním systémem měly největší výhodu v cenové dostupnosti. Hardwarově, až na výjimky, nebyla tyta zařízení nijak průlomová, ale poměr cena/výkon byl velmi příjemný. Dokázaly tak obstojně konkurovat na trhu, hlavně díky více odladěnému operačnímu systému. Pod ikonou lupy v navigační liště se vyhledával online obsah přes službu Bing, vlastněnou také Microsoftem. Toto nastavení nešlo nijak změnit a uživatelé byli nuceni používat tento vyhledávací *engine*, který je, podle počtu požadavků, druhý nejvyužívanější na světě hned za vyhledávací službou Google.

V říjnu roku 2017 byl ohlášen ukončený vývoj Windows 10 Mobile pro nedostatek poptávky na trhu a také pro nezájem široké veřejnosti dostatečně zásobovat Microsoft Store aplikacemi třetí strany. Od té doby funguje pouze jakási údržba současného systému ve formě vydávání aktualizací vůči bezpečnostním rizikům.

Zdroje: [9], [10].

2 ČASOPROSTOROVÉ OTISKY A PREDIKCE UŽIVATELŮ

2.1 Geolokace

Geolokací se chápe zjištění zeměpisné polohy cílového objektu, v případě této práce právě mobilních zařízení. Nejjednodušší forma geolokace je pomocí zeměpisných souřadnic, nicméně účel geolokace, je rozšířit tyto zeměpisné informace k určení smysluplné lokace, jako je například název ulice.

Geolokačních metod je samozřejmě více a patří mezi ně např.:

- GPS,
- BSS, BTS (systém základnových stanic),
- IP lokace (podle veřejné IP),
- WiFi poziční systém,
- Datový otisk (fingerprint).

Zdroj: [11].

2.2 Datový otisk

Datovým otiskem jsou myšleny veškeré nashromážděné informace vzdáleného zařízení pro účel identifikace. Základní nastavení internetového prohlížeče jsou s pomocí skriptovacích jazyků na straně klienta shromažďována analytickou webovou službou (například www.infobyip.com) pro získání důvěrných parametrů, jako např.:

- název prohlížeče,
- název operačního systému,
- rozlišení obrazovky,
- zapnuté služby jako Java, Flash, WebGL,
- název poskytovatele internetu.

Tyto získané informace pak mohou vést, kromě špehování běžných uživatelů, i k dopadení a prevenci online zločinu, jako například krádež identity nebo podvody s platebními kartami.

Zdroje: [12], [13].

2.3 Geosociální sítě

Patří do skupiny LBS (služby založené na poloze), respektive podmnožiny LBSN (lokalizační sociální sítě). Nová generace sociálních sítí, kde se sdílejí data a souřadnice, které vrací aktuální pozici zařízení uživatele. Tyto data se nazývají *geodata* a jsou spojeny s každou

uživatelskou zprávou, nebo tzv. *check-in* zveřejněným v LBSN. Respektovaný expert přes sociální média Marshall McLuhan napsal: „*Zveřejnění je napadení soukromí sebe sama*“.

Zdroj: [14].

Princip LBSN aplikací je v šíření lokálních informací k uživateli závisících na faktorech, které vyplývají z podmínek, ve kterých se uživatel právě nachází. LBSN požadující osobní informace mohou přinášet nové příležitosti, ale zároveň riziko. Proto se tato práce v této části zabírá tzv. SWOT (silné stránky, slabé stránky, příležitosti, hrozby) analýzou.

Zdroj: [15].

2.3.1 SWOT analýza

Mezi silné stránky LBSN patří:

- Všechny zkoumané LBSN (Foursquare, Google+, Facebook) v současné době používají zabezpečený HTTPS protokol, kterým je možnost zachycení citlivých dat minimalizována.
- LBSN poskytuje lokální informace založení na zjištěných pozicích uživatele i přes absenci GPS technologie. WiFi geolokace nebo jiné bezdrátové technologie (bluetooth) jsou v tomto případě přesné přibližně na 30 metrů.
- LBS funkčnost nevyžaduje permanentní připojení k internetu, nebo geolokaci.
- Použití LBS k poskytování místních informací o cestovním ruchu není závislé na přihlašování uživatele do jeho účtu nebo poskytnutí osobních informací na tomto účtu.
- Relevantnost a obsah místních informací, obsažených v POI (bod zájmu) je zaručeno jejich správci (také nazývanými starosty), které jsou např. v případě Foursquare nejčastější návštěvníci POI (statut starosty je přenosný, takže automaticky odstraní toto oprávnění v případě pasivity). Existuje také interní kontrola LBSN, která např. na Foursquare označuje podvodné „návštěvy“ od stejného uživatele, jehož frekvence je nejméně 5 „návštěv“ za minutu nebo méně, 8 „návštěv“ za 15 minut nebo méně, 49 „návštěv“ za 24 hodin a 90 „návštěv“ nebo méně po dobu maximálně 72 hodin. Podvodníci jsou také klasifikováni jako „odbavení“ na POI, jejichž souřadnice jsou vzdáleny více než 200 m od aktuálních souřadnic uživatele, stejně je tomu tak i při rychlosti běžného uživatele, jehož rychlost překračuje:
    - 4 kilometry za minutu vzhledem k poslednímu navštívenému bodu zájmu v rozmezí méně než 100 km,
    - 25 kilometry za minutu vzhledem k poslednímu navštívenému bodu zájmu v rozmezí více než 100 km.

Slabé stránky LBSN jsou:

- Počet možných dotazů prostřednictvím rozhraní API LSBN je omezen (např. Foursquare umožňuje pouze 500 dotazů za hodinu při používání informací o profilu uživatele).
- Dlouhodobé používání GPS, WiFi nebo jiné geolokační technologie rychle snižuje životnost baterií mobilních zařízení, kde se jedná v průměru přibližně o čtvrtinu až k méně než polovině času ve srovnání se zařízeními bez těchto technologií.

LBSN nabízí příležitosti jako:

- Pokročilé systémy doporučení LBS mohou poskytnout uživatelům lokální informace v závislosti na prostorovém faktoru (realizované poptávkou po geolokaci uživatele), časovém faktoru (určeném v místě, kde se uživatel nachází), možnost profilových dat z uživatelských účtů LBSN a také další okolnosti uživatelské lokality (např. aktuální počasí).
- LBSN jsou zdrojem informací s výrazně vyššími úplnostmi informací o studovaných předmětech cestovního ruchu (restaurace a barové podniky), než tradiční informační zdroje v cestovním ruchu.
- Pro dobré osobní doporučení je systém LBS dostatečným přístupem k LBQID (lokalizační kvazi identifikátor). Jedná se o prostorotemporální vzorec tvořený opakovanými sekvencemi pohybu uživatele v omezeném prostoru a čase. V životě uživatelů LBS existuje vysoký stupeň prostorových a časových pravidel pravidelnosti. Použitím LBQID z uživatelského profilu (zejména historie jeho navštíveného POI) umožňuje útočníkovi předpovědět s 93% úspěšností další navštívený POI. Konkrétně s přibližně 63% mírou úspěšnosti může být předpovězeno další navštívené POI s přibližně 93% mírou úspěšnosti pro identifikaci skupiny pěti POI, do kterých patří. Další studie dokonce uvádí, že pouze čtyři prostorově vzdálené datové otisky postačují k jednoznačné identifikaci dalších 95 % uživatelů ze vzorku 1,5 milionu uživatelů. Tyto skutečnosti lze použít jako součást pokročilého systému doporučování používaného pro marketingové účely.

Nakonec hrozby LBSN:

- Možnost sledování uživatelů díky geolokaci aplikací LBS, které získají informace o velmi přesné poloze. Toto je poskytováno uživatelům nejen ze seznamu přátel, ale i úplně cizím osobám (např. V případě „návštěvy“ POI na LBSN).
- Hrozba krádeže identity z uživatelského účtu LBSN. Důvody mohou být následující:
    - Odhad slabých hesel útočníkem. Útočník požaduje obnovení hesla na základě odhadované odpovědi na otázku kontroly pro přihlášení do služby LBSN nebo odesláním do již nefunkční poštovní schránky.
    - Majitel účtu zapomíná na odhlášení počítače, ke kterému mají cizinci přístup.
    - Zachycení hesla pomocí hardwarového nebo softwarového *keyloggeru* nainstalovaného v počítači, na který se přihlašovatel přihlásí.

    - *Phishing*, většinou vytvořením falešné přihlašovací stránky k LBSN, která je odkazována na držitele účtu e-mailu.
    - Vytvoření účtu externím napodobováním jména a příjmení jiné osoby.
- Kyberšikana, včetně slovních útoků uživatelů LBS (u českých dětí se vyskytuje ve 34,3 % případů), ohrožení, zastrašování a vydírání (u českých dětí ve 25,8 % případů), ponížení, hanba šířením fotografií, videa nebo zvuku (u českých dětí ve 24,1 % případů).
- Schopnost LBSN záměrně zasahovat nepravdivými informacemi, nebo geodat. Tyto POI jsou pak vyznačeny jako *venue attack* (místo útočníka) a klamou tak uživatele, nebo škodí reputaci POI.

Uvedené kvadranty s využitím metody SWOT analýzy byly identifikovány na základě vědeckých zdrojů, rozsáhlých statistik a vlastních výzkumných sil, nedostatků, příležitostí a ohrožení využívání LBS a LBSN. Tato analýza má zásadní význam pro další výzkum LBSN, zejména pro navrhování modelu systému doporučení a přístupu k citlivým osobním informacím uživatelů, pokud se autor snaží minimalizovat dopad výskytu hrozeb a nedostatků LBSN.

Zdroje: [16], [17], [18].

3 PŘESNOST WIFI GEOLOKAČNÍCH SLUŽEB

3.1 WiFi geolokace

WiFi poziční systém (WPS) je termín zavedený společností Skyhook Wireless, nicméně v dnešní době používají společnosti Google, Apple, Microsoft a Mozilla stejnou metodiku. Jde o využití GPS k určení polohy WiFi sítí, podle čehož pak lze určit polohu uživatele čistě na základě WiFi sítě.

Určení polohy na základě bezdrátových sítí je oproti GPS lokalizaci mnohem přesnější v uzavřených oblastech, kde má GPS lokátor malý signál na jednoznačné určení polohy a zároveň je v okolí více WiFi sítí. Nicméně výhody jsou ještě větší za okolností, kdy je příliš těžké vůbec zachytit GPS signál, např.:

- v podzemních garážích,
- ve velkých nákupních centrech, nebo obchodech,
- ve výškových budovách.

Je důležité mít ale na paměti, že WPS mimo dosah WiFi sítí nemůže a nebude fungovat.

Zařízení, která mají GPS i WiFi přijímače, mohou být využita k zasílání informací ohledně bezdrátové sítě zpět nadřazené společnosti (Google, Microsoft, Apple, Mozilla), která najednou má informace, kde se na ní uživatel připojil. Zařízení posílá BSSID (MAC adresu) přístupového bodu společně s lokací zjištěnou pomocí GPS. Když je služba GPS zapnutá, skenuje také sítě v dosahu pro veřejně dostupné informace, které můžou vést k identifikaci sítě. Jakmile je lokace a okolní sítě objeveny, informace se odesílají online. Pokud je v dosahu někdo bez GPS, služba může sloužit k rozpoznání přibližné lokace podle WiFi, protože tato síť již byla v minulosti lokalizována.

Tyto informace jsou konstantně obnovovány všemi dostupnými nadřazenými společnostmi a všechny další získané informace o bezdrátových sítích vzhledem ke geolokaci slouží k upřesnění polohy daného přístupového bodu pro jejich uživatele.

Anonymní sběr dat o uživateli je vždy uveden v souboru podmínek služeb daného mobilního zařízení, nicméně u většiny těchto zařízení lze tuto metodiku sběru geodat vypnout. Zajímavostí je, že Google ve svých službách tohoto typu implementoval skutečnost, že správci přístupových bodů WiFi mohou přidat na konec názvu sítě „_nomap“ (např. „mojesit_nomap“) a Google tak skutečně nebude ukládat o tomto přístupovém bodě

informace na jejich serverech a tím tedy nebude možné tuto popisovanou geolokační metodu na těchto přístupových bodech využívat.

Zdroje: [19], [20].

3.1.1 Google

Tato společnost nabízí API pro využití svých geolokačních služeb přes html odkaz: *https://www.googleapis.com/geolocation/v1/geolocate?key=%GOOGLE_API_KEY%*. Toto API je využito hlavně v jejich prohlížeči Google Chrome, ale i v dalších internetových prohlížečích, které jsou odvozeny od *open-source* projektu Chromium. Jsou jimi např.:

- Yandex,
- Cent Browser,
- Opera,
- Slimjet,
- Vivaldi,
- UC Browser,
- Sleipnir.

Zdroj: [21].

3.1.2 Microsoft

Microsoft vlastní také svojí databázi polohy přístupových bodů WiFi spojenou s vlastní geolokační službou. Tato služba je dostupná pouze pro jejich prohlížeče Microsoft Edge a Internet Explorer.

Zdroj: [20].

3.1.3 Apple

Společnost Apple má stejně jako Microsoft svojí databázi poloh přístupových bodů WiFi a svojí geolokační službu a umožňuje také pouze povolit, nebo vypnout služby pro detekci polohy. Služba je dostupná pro prohlížeč Safari.

Zdroj: [22].

3.1.4 Mozilla

Mozilla ve výchozím nastavení používá geolokační služby společnosti Google, nicméně také disponuje svým rozhraním a databázemi, které dává široké veřejnosti k dispozici na html adrese: *https://location.services.mozilla.com/v1/geolocate?key=%MOZILLA_API_KEY%*. Lokalizační službu lze změnit přes URL adresu *about:config*, kde se vyhledá řádek

konfigurace *geo.wifi.uri* a změní se jeho hodnota na html API společnosti Mozilla. Proprietárním internetovým prohlížečem je samozřejmě Mozilla Firefox, který ale, stejně jako Chromium, disponuje několika alternativami, kterými jsou např.:

- Waterfox,
- Pale Moon,
- SeaMonkey,
- Iceweasel,
- IceCat,
- Wyzo.

Předpokládá se, že co se týče nastavení lokalizačních služeb budou na tom stejně jako Mozilla Firefox.

Zdroj: [23].

3.2 JavaScript

Je to skriptovací jazyk, který je vedle značkovacích jazyků HTML a CSS jedním ze základních technologii pro vývoj internetových stránek. Jedním z hlavních důvodů, proč je JavaScript tak rozšířeným jazykem, je skutečnost, že všechny moderní internetové prohlížeče jej podporují bez potřeby nějakého zásuvného modulu nebo pluginu. Je implementován na straně klienta, čímž rozumíme, že k provozování JavaScriptu není zapotřebí režie nějakého serveru, kam se pouze odesílají požadavky na uživatelův pokyn, mezi které patří např. zjištění zeměpisných souřadnic.

Zdroj: [24].

Pro zjištění geolokace pomocí WiFi v této práci byly využity následující zdrojové kódy.

```
//funkce na zjištění polohy z prohlížeče
function getLocation(){
     //vestavěná proměnná v prohlížeči
     if(navigator.geolocation) {
          //první/druhý parametr je funkce, která se má zavolat, když
            nenastane/nastane chyba a předá se do ní proměnná s daty
          //třetí parametr je objekt, který představuje možnosti získání
            polohy, zobrazovat čerstvá data a používat vysoká přesnost
          navigator.geolocation.getCurrentPosition(getPosition, getError, {
               maximumAge: 0, enableHighAccuracy: true
          });
     } else {
          //když prohlížeč nepodporuje zjištění polohy, vypíše se na stránku
            chyba
          res.innerHTML = "Geolocation not supported by this browser.";
     }
}
```

Zdroje: *vlastní*, [25].

Pro určení přesnosti WiFi geolokace je potřeba zjistit reálnou vzdálenost mezi dvěma souřadnicemi.

```
// funkce pro počítání vzdálenosti mezi dvěma body, vrací vzdálenost v
kilometrech
function distance (lat1, lon1, lat2, lon2) {
     var theta = lon1 - lon2;
     var dist = Math.sin(Math.deg2rad(lat1)) *
                Math.sin(Math.deg2rad(lat2)) + Math.cos(Math.deg2rad(lat1))
                * Math.cos(Math.deg2rad(lat2)) *
                Math.cos(Math.deg2rad(theta));
     dist = Math.acos(dist);
     dist = Math.rad2deg(dist);
     var miles = dist * 60 * 1.1515;
     //vrací vydálenost v km
     return miles * 1.609344;
}
```

Zdroje: *vlastní*, [25].

3.3 Měření přesnosti WiFi geolokačních služeb

Veškeré prováděné měření na prohlížeči Mozilla Firefox jsou samozřejmě přes databáze společnosti Mozilla, nikoli přes lokační služby Googlu, které jsou ve výchozím nastavení. Měření proběhlo na notebooku se síťovou kartou *Qualcomm Atheros QCA61x4A*, vždy uvnitř nějaké budovy, tedy tzv. *indoor*.

Poslední verze Safari, která je pro OS Windows k dispozici, je 5.1.4 z roku 2012, na které po spuštění JavaScriptového kódu prohlížeč vrací chybu: „Permission Error Constructor: position unavailable“. Z tohoto důvodu byl tedy z měření vynechán.

Všechny WiFi přístupové body mají kolísavý průběh vysílání signálu v čase, a proto byla zapotřebí synchronizační bariéra, která se stará o to, aby se vždy spustilo měření ve všech prohlížečích najednou a měření tak bylo relevantní.

Parametr *coords.accuracy* indikuje přibližnou přesnost udávanou API od vydavatele daného webového prohlížeče. Parametr *real.accuracy* pak ukazuje reálnou vzdálenost vypočítanou skriptem.

Měření proběhlo ve 3 městech České republiky s následujícími výsledky.

- Praha

Tabulka 1 - měření WiFi přesnosti v Praze (Zdroj: vlastní.)

původní souřadnice		50.080036, 14.394024		
počet AP v okolí		7		
číslo měření	parametry	Mozilla Firefox	Microsoft Edge	Google Chrome
1.	coords.accuracy [m]	194,31	55	30
	real.accuracy [m]	92,93	22,64	28,36
2.	coords.accuracy [m]	100,42	58	38
	real.accuracy [m]	86,79	33,22	32,98
3.	coords.accuracy [m]	166,01	58	37
	real.accuracy [m]	84,65	24,13	34,6
4.	coords.accuracy [m]	115,73	57	39
	real.accuracy [m]	79,56	23,09	30,75
5.	coords.accuracy [m]	104,33	60	30
	real.accuracy [m]	88,36	29,33	28,73

Tabulka 2 - průměr naměřených hodnot v Praze (Zdroj: vlastní.)

webový prohlížeč	Mozilla Firefox	Microsoft Edge	Google Chrome
průměr z reálné vzdálenosti [m]	86,458	26,482	31,084

- Brno

Tabulka 3 - měření WiFi přesnosti v Brně (Zdroj: vlastní.)

původní souřadnice		49.226877, 16.574929		
počet AP v okolí		4		
číslo měření	parametry	Mozilla Firefox	Microsoft Edge	Google Chrome
1.	coords.accuracy [m]	128,58	63	67
	real.accuracy [m]	64,04	14,07	15,92
2.	coords.accuracy [m]	119,59	68	50
	real.accuracy [m]	62,15	19,75	12,35
3.	coords.accuracy [m]	123,62	63	63
	real.accuracy [m]	63,95	15,97	12,05
4.	coords.accuracy [m]	139,34	63	54
	real.accuracy [m]	68,5	16,22	17,91
5.	coords.accuracy [m]	136,43	66	49
	real.accuracy [m]	65,84	16,75	10,43

Tabulka 4 - průměr naměřených hodnot v Brně (Zdroj: vlastní.)

webový prohlížeč	Mozilla Firefox	Microsoft Edge	Google Chrome
průměr z reálné vzdálenosti [m]	64,896	16,552	13,732

- Pardubice

Tabulka 5 - měření WiFi přesnosti v Pardubicích (Zdroj: vlastní.)

původní souřadnice		50.048851, 15.763302		
počet AP v okolí		10		
číslo měření	parametry	Mozilla Firefox	Microsoft Edge	Google Chrome
1.	coords.accuracy [m]	237,63	63	60
	real.accuracy [m]	144,21	13,91	20,61
2.	coords.accuracy [m]	293	61	39
	real.accuracy [m]	160,14	5,27	17,97
3.	coords.accuracy [m]	228,72	61	49
	real.accuracy [m]	158,45	3,55	20,29
4.	coords.accuracy [m]	318,04	61	68
	real.accuracy [m]	246,92	6,55	4,95
5.	coords.accuracy [m]	236,01	61	106
	real.accuracy [m]	165,46	3,71	5,02

Tabulka 6 - průměr naměřených hodnot v Pardubicích (Zdroj: vlastní.)

webový prohlížeč	Mozilla Firefox	Microsoft Edge	Google Chrome
průměr z reálné vzdálenosti [m]	175,036	6,598	13,768

Z výsledků měření v jednotlivých městech je jasně patrné, že přesnost WiFi geolokace u prohlížeče Mozilla Firefox není zdaleka tak přesné jako u služeb Microsoftu, nebo Googlu. Zato Microsoft Edge a Google Chrome mají geolokační API mnohem přesnější, proto není divu, že Mozilla Firefox používá ve výchozím nastavení Google API.

Tabulka 7 - průměr všech naměřených hodnot (Zdroj: vlastní).

webový prohlížeč	Mozilla Firefox	Microsoft Edge	Google Chrome
Celkový průměr z reálné vzdálenosti [m]	108,7966667	16,544	19,528

Přesnost WiFi geolokace v nějaké lokalitě závisí vždy na počtu WiFi v okolí, ale také na tom, kolik lidí se kdy připojilo na tyto AP s GPS lokátorem. Proto bylo měření v Brně, co se týče přesnosti, úspěšnější než v Praze, protože se předpokládá, že fakultu VUT Brno navštíví se zapnutým GPS lokátorem více lidí než strahovské koleje v Praze. Pro přesnost geolokace pomocí WiFi na jednotky metrů je tedy zapotřebí najít optimální bod mezi počtem AP v okolí a počtem připojení na AP s GPS lokátorem.

Zdroj: *vlastní*.

4 ANALÝZA GEOLOKAČNÍCH ÚDAJŮ

4.1 GDPR

Obecné nařízení o ochraně osobních údajů je nařízení Evropské unie s cílem posílit a sjednotit ochranu dat pro všechny občany EU. Toto nařízení bylo přijato 27. dubna 2016, vejde v platnost 25. května 2018 a nevyžaduje od vlád států EU schvalování jakékoli legislativy, čímž je tedy přímo závazná a použitelná. Má za cíl hájit práva občanů proti neoprávněnému zacházení s osobními údaji a jejich daty.

Navrhovaný nový režim EU pro ochranu údajů rozšiřuje oblast působnosti zákona EU o ochraně údajů na všechny zahraniční společnosti, které zpracovávají údaje o obyvatelích EU. V případě porušení jakýchkoli pravidel GDPR musí viníci počítat s přísnými sankcemi až do výše 4 % celosvětového obratu. Dále také nařizuje větším zpracovatelům dat zřídit kontrolní funkci DPO (pověřenec pro ochranu údajů), jehož úkolem bude dohlížet na řádné zacházení s osobními daty a hlásit možné porušení zákona, nebo úniky dat.

Zdroj: [26].

4.2 Man in the middle

Zjednodušeně jde o typ útoku, kde se útočník vloží do komunikace mezi dvě strany, kdy se vydává pro jednu zúčastněnou stranu za tu druhou a naopak, čímž získá přístup k informacím, které se obě strany pokoušely poslat sobě navzájem.

Zdroj: [27].

4.3 ARP spoofing

Kapitolu ARP spoofing popsal výborně ve své práci Jiří Danielka:

„*Protokol ARP má v počítačových sítích důležitou roli. Používá se pro překlad síťové IP adresy na adresu fyzickou. ARP spoofing je technika, kdy útočník podvrhne tyto adresy, konkrétně fyzickou adresu, kterou zvolí vlastní, například svého zařízení. To mu umožní stav, kdy veškerá komunikace mezi zařízeními proudí přes něj.*“.

Zdroj: [28].

4.4 Odposlech odesílaných dat

Pro analýzu odesílaných dat vůči poskytovatelům vybraných mobilních operačních systémů byl použit nástroj *mitmproxy*, což je interaktivní MITM proxy pro protokoly HTTP a HTTPS

s konzolovým rozhraním. Analýza proběhla kompletně na linuxové distribuci Kali linux 2016.2, která je odvozená od linuxové distribuce Debian.

Nejprve se použil nástroj *arpspoof* k podvrhnutí adres, jednoduše tak, aby si mobilní zařízení uživatele „myslelo“, že útočník je směrovač, přes který proudí veškerá data na systémové servery. Byl k tomu využit následující příkaz, kde první IP adresa je cílové zařízení a druhá IP adresa směrovač.

```
arpspoof -i wlan0 -t 192.168.1.3 192.168.1.1
```

```
root@kali:~/.mitmproxy# arpspoof -i wlan0 -t 192.168.1.3 192.168.1.1
58:0:e3:e3:4b:97 0:0:0:0:0:0 0806 42: arp reply 192.168.1.1 is-at 58:0:e3:e3:4b:97
58:0:e3:e3:4b:97 0:0:0:0:0:0 0806 42: arp reply 192.168.1.1 is-at 58:0:e3:e3:4b:97
```

Obrázek 3 - výpis nástroje arpspoof

Zdroj: *vlastní*.

Dále bylo potřeba nastavit tzv. IP přesměrování, které umožní průchod paketů přes útočníkovo zařízení.

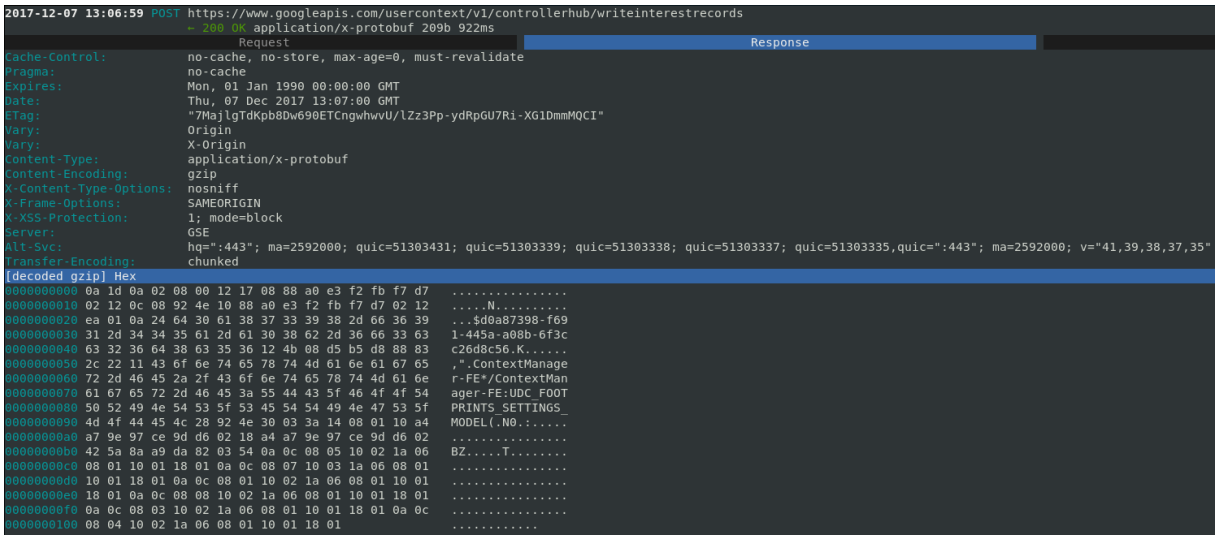
```
sysctl -w net.ipv4.ip_forward=1
```

V neposlední řadě se musela přesměrovat komunikace do portů nástroje *mitmproxy*, a to následujícími příkazy.

```
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-
port 8080
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 443 -j REDIRECT --to-
port 8080
```

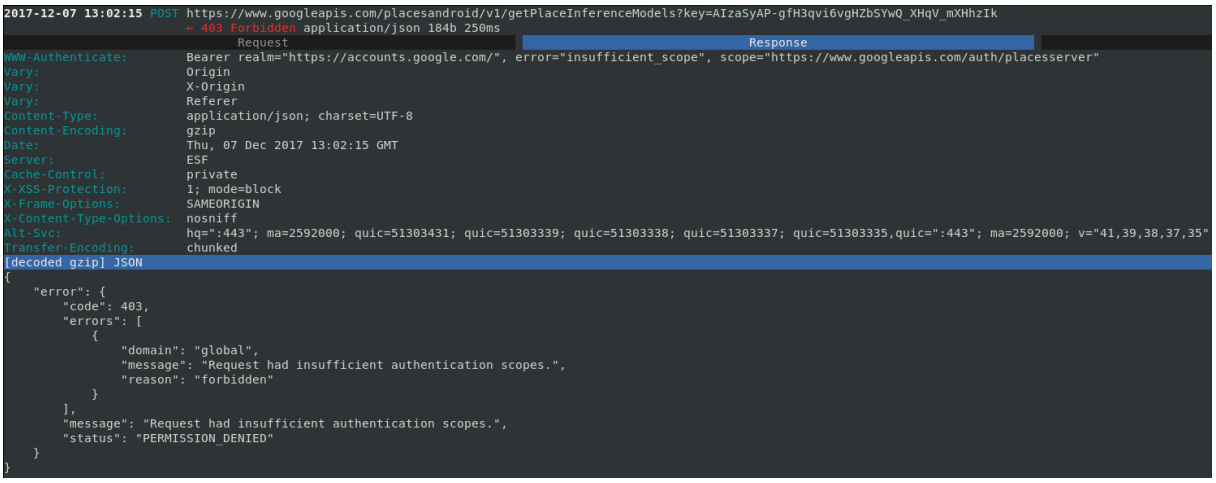
Poté stačilo jen zapnout nástroj *mitmproxy*, který zachytává a dešifruje veškerou HTTPS komunikaci a podvrhuje HTTP variantu protokolu. Tímto by ale uživatel, který chce otevřít například aplikaci Foursquare, byl informován o možné hrozbě MITM útoku, proto je potřeba podvrhnout ještě *mitmproxy* certifikát, který je vytvořen při instalaci tohoto nástroje. Soubor je pojmenován jako *mitmproxy-ca-cert.pem*. Na zařízení uživatele se potom tento certifikát nainstaluje a uživatel tím tedy potvrzuje věrohodnost překladu SSL vrstvy.

Zdroj: [29].



Obrázek 4 - komunikace se servery Googlu

Zdroj: *vlastní*.



Obrázek 5 - komunikace se servery Googlu

Zdroj: *vlastní*.

Komunikace se servery Googlu byla i přes SSL vrstvu dále šifrovaná. Někdy dokonce servery poznali, že komunikace proudí přes třetí stranu a načítání aplikace tak znemožnili přes chybovou hlášku.

S velkou pravděpodobností je toto zapříčiněno skandály, které vyšly najevo koncem listopadu roku 2017, jak informoval server root.cz následující zprávou:

„*I když má uživatel chytrého telefonu s Androidem vypnuté lokalizační služby i mobilní připojení (dokonce i když nemá vloženou SIM kartu), jeho chytrý telefon shromažďuje lokalizační data na základě mobilních vysílačů (kódy Cell ID) a posílá je Googlu. S tímto*

zjištěním přišel Quartz a má jít o chování platné pro všechna zařízení s Androidem někdy od počátku tohoto roku. Tiskový mluvčí Googlu měl na dotaz odpovědět v tom smyslu, že Cell ID informace nejsou nijak využívány a jsou zahazovány ihned po obdržení. Společnost se pouze zabývala analýzou využití takových dat pro urychlení doručování zpráv. Firma přislíbila, že tuto praktiku ukončí, telefony s Androidem by měly Cell ID přestat odesílat Googlu. Ačkoli obecně nelze předpokládat, že by šlo o reálně nebezpečnou praktiku kompromitující zásadně soukromí konkrétních uživatelů, je nebezpečná a špatná v tom, že jde opět o shromažďování dat uživatelů bez jejich vědomí, které navíc nemá uživatel možnost ovlivnit a které je před ním maskováno falešnou indikací vypnutých služeb.".

Zdroj: [30].

Komunikace se servery aplikace Foursquare, jakožto aplikace geosociální sítě byla k přečtení v JSON formátu. Při odposlechu komunikace se servery aplikace Foursquare došlo na zjištění, že si o napadeném zařízení nechají posílat mimo jiné informace jako:

- značka zařízení,
- typ zařízení,
- země, ve které je zařízení připojeno,
- typ OS,
- jazyk OS,
- typ síťového připojení,
- časový otisk prvního spuštění aplikace,
- IP lokace (pozice vlastníka ISP),
- lokální IP adresa,
- rozlišení obrazovky.

Zdroj: *vlastní*.

```
JSON
{
    "app_version": "2017.11.10",
    "branch_key": "key_live_nmm2Ae8J1GbSQXu22I7FTohhuwnTL9R0",
    "brand": "LENOVO",
    "country": "CZ",
    "device_fingerprint_id": "467296809862411772",
    "hardware_id": "b027ab4bdcd8f3dd",
    "identity_id": "467296809925094482",
    "instrumentation": {
        "v1/close-qwt": "0",
        "v1/open-brtt": "1252"
    },
    "is_hardware_id_real": true,
    "language": "cs",
    "local_ip": "192.168.1.3",
    "metadata": {},
    "model": "Lenovo YT3-X50F",
    "os": "Android",
    "os_version": 23,
    "retryNumber": 0,
    "screen_dpi": 213,
    "screen_height": 1216,
    "screen_width": 800,
    "sdk": "android2.11.1",
    "session_id": "467299613813261069",
    "wifi": true
}
```


Obrázek 6 - komunikace se servery aplikace Foursquare

Zdroj: *vlastní*.


```
"locale": "cs-CZ",
"subject_location": {
    "latitude": 49.99202619,
    "longitude": 15.82174637,
    "type": "location"
},
```

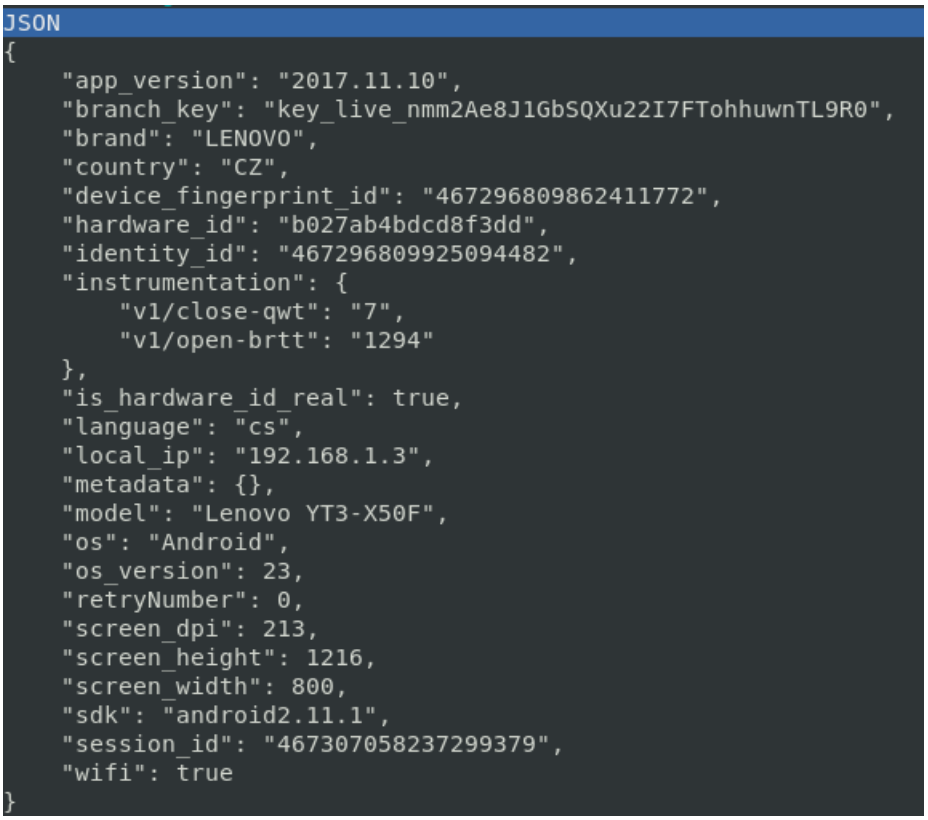

Obrázek 7 - komunikace se servery aplikace Foursquare

Zdroj: *vlastní*.


```
"locale": "cs-CZ",
"subject_location": {
    "latitude": 50.0496826171875,
    "longitude": 15.768896102905273,
    "name": "Áčko",
    "type": "location"
},
```


Obrázek 8 - komunikace se servery aplikace Foursquare

Zdroj: *vlastní*.



Obrázek 9 - komunikace se servery aplikace Foursquare

Zdroj: *vlastní*.

Při zapnutí GPS lokátoru poté zařízení odesílalo i svoje GPS souřadnice a v případě prokliku v aplikaci na vybraný bod zájmu i jeho souřadnice a název. Veškeré informace se po zavření aplikace odesílaly znovu.

Zdroj: *vlastní*.

5 METODIKA MAXIMALIZACE OCHRANY PŘED EROZÍ SOUKROMÍ

Z hrozeb SWOT analýzy v části predikce uživatelů jasně vyplývá fakt, že pokud chce uživatel maximalizovat svoje soukromí před erozí, měl by dodržovat tyto doporučení:

- Uživatel by měl mít v seznamu přátel dané LBSN lidi, kterým důvěřuje a zároveň by si měl dávat pozor, u jakého POI svojí pozici zveřejňuje.
- Před krádeží identity se dá bránit následujícími způsoby:
    - robustní heslo,
    - být na pozoru vůči pokusu o útok zvaný *phishing* ze strany útočníka (např. resetování hesla přes podvodný e-mail),
    - odhlašovat se z veřejných zařízení.
- Uživatel by měl mít na vědomí, že veškerá autorská práva zveřejněného obsahu již nepatří jemu, ale geosociální síti a měl by tím předejít kyberšikaně.

Zdroj: [18].

Uživatel by měl mít na paměti, že při zjišťování polohy lze využít například tyto údaje:

- Veřejná IP adresa zařízení, ze které se dá dále vysledovat například záznamem o majiteli IP adresy v databázi *whois*.
- Nastavení jazyka, času a časové zóny webového prohlížeče, nebo OS.
- Možnou erozi soukromí přes podrobnosti o systému uživatele zjištěné například pomocí služeb JavaScript, Adobe Flash.
- Metadata v obrázcích, tzv. *exif data* také mohou obsahovat citlivé informace.
- Při placení na nezabezpečených portálech se dají využít informace o platební kartě, například banka, která kartu vydala, je zjistitelná z jejího čísla.

Zdroje: [19], [20].

Obecná doporučení, která plynou z výsledků této práce jsou:

- Vypínat GPS lokátor, WiFi nebo bluetooth, když uživatel tyto služby momentálně nepotřebuje.
- Jako administrátor sítě přidávat do názvů WiFi AP na konec SSID „_nomap“, který zaručí, že se tento WiFi AP neobjeví v databázi společnosti Google.
- Změnit výchozí nastaveni nově pořízených zařízení, které mají většinou zapnuté možnosti geolokace.
- Nepřijímat podezřelé SSL certifikáty.
- Udržovat aktuální OS vůči možným softwarovým chybám.

- Používat robustní hesla na geosociálních sítích s dvojí autentizací, tj. potvrzení přes mobil nebo druhý e-mail.
- Nepřipojovat se bezhlavě do veřejných sítí bez zašifrovaného lokálního obsahu.
- Neklikat na neznámé odkazy a vždy si jejich přesměrování zkontrolovat přes stavový řádek.
- Nezobrazovat externí obrázky, které mohou obsahovat škodlivý kód.
- Zkontrolovat, které aplikace mají přístup k citlivým informacím a pokud možno tento přístup odepřít.
- Nastavit automatické zamykání zařízení při neaktivitě.
- Mazání historie webového prohlížeče.

Zdroj: [31].

Každý by měl mít na paměti slova Edwarda Snowdena: „*Nezajímat se o ochranu soukromí s tvrzením, že stejně nemám co skrývat, je podobné jako nezajímat se o svobodu projevu, protože stejně nemám co říct.*“.

Zdroj: [32].

ZÁVĚR

Cílem této práce bylo vyhodnotit pří různých modelech geolokačních služeb míru tzv. eroze soukromí uživatelů u současných mobilních operačních systémů a mobilních aplikací využívající geolokaci.

Výsledky SWOT analýzy ukázaly, že v životě uživatelů LBS existuje vysoký stupeň prostorových a časových pravidel pravidelnosti. Použitím LBQID z uživatelského profilu umožňuje útočníkovi předpovědět s 93% úspěšností další navštívený POI. Další studie dokonce uvádí, že pouze čtyři prostorově vzdálené datové otisky postačují k jednoznačné identifikaci dalších 95 % uživatelů ze vzorku 1,5 milionu uživatelů.

V části měření přesnosti WiFi geolokačních služeb bylo zjištěno, že nejpřesnější služby mají společnosti Google a Microsoft, které byly schopné uživatele lokalizovat vždy na pár desítek metrů, zatímco služby společnosti Mozilla, které jsou v ranném vývoji, byly přesné spíše na stovky metrů. Geolokační API bohužel společnost Apple neposkytovala, tudíž nemohlo měření proběhnout, neboť byl použit notebook s OS Microsoft Windows 10, který webový prohlížeč Safari nepodporuje. Zde je nutné se pozastavit nad faktem, že pro přesnost geolokace pomocí WiFi na jednotky metrů těch nepřesnějších služeb je zapotřebí najít optimální bod mezi počtem AP v okolí a počtem připojených uživatelů na AP s GPS lokátorem v minulosti.

Z výsledků části analýzy geolokačních údajů vyšlo najevo, že Google si odesílaná data po nedávných skandálech šifruje ještě mimo SSL vrstvu, což z nich dělá data na první pohled nečitelná. Foursquare ale uživatelova data přeposílá na servery v JSON formátu, a tak bylo zjištěno, že při každém prokliku v aplikaci se odesílají v podstatě veškerá data o typu zařízení a OS, na kterém je aplikace spuštěna. Při zapnuté GPS je pak odesílaná mimo jiné i pozice uživatele zároveň s pozicí POI, který si právě prohlíží.

Pro maximalizaci ochrany soukromí uživatelů slouží poslední část této práce, kde je shrnutá metodika pro běžné uživatele, kteří nejsou znalí možnostem dnešních vyspělých technologií a zručnosti možných útočníků.

POUŽITÁ LITERATURA

1. VINCENT, James. 99.6 percent of new smartphones run Android or iOS. *The Verge* [online]. 2017 [cit. 2017-12-01]. Dostupné z: https://www.theverge.com/2017/2/16/14634656/android-ios-market-share-blackberry-2016/
2. HOLWERDA, Thom. The second operating system hiding in every mobile phone. *OSnews* [online]. 2013 [cit. 2017-12-01]. Dostupné z: http://www.osnews.com/story/27416/The_second_operating_system_hiding_in_every_mobile_phone/
3. MENON, K. Murali. Android Nougat: Here's why Google names the OS after sweets. *The Indian Express* [online]. 2016 [cit. 2017-12-01]. Dostupné z: http://indianexpress.com/article/lifestyle/food-wine/from-donut-to-nougat-why-are-android-versions-named-after-sweets-2887237/
4. EADICICCO, Lisa. THE RISE OF ANDROID: How a flailing startup became the world's biggest computing platform. *Business Insider* [online]. 2015 [cit. 2017-12-01]. Dostupné z: http://www.businessinsider.com/how-android-was-created-2015-3
5. Android Dashboards: Platform Versions. *Android Developers* [online]. 2017 [cit. 2017-12-01]. Dostupné z: https://developer.android.com/about/dashboards/index.html
6. ROUSE, Margaret. Apple iOS. *Search Mobile Computing* [online]. 2016 [cit. 2017-12-01]. Dostupné z: http://searchmobilecomputing.techtarget.com/definition/iOS
7. CLOVER, Juli. Apple Releases iOS 11.2. *MacRumours* [online]. 2017 [cit. 2017-12-01]. Dostupné z: https://www.macrumors.com/2017/12/02/apple-releases-ios-11-2/
8. App Store. *Apple Developer* [online]. 2017 [cit. 2017-12-01]. Dostupné z: https://developer.apple.com/support/app-store/
9. ZIEGLER, Chris. Microsoft talks Windows Phone 7 Series development ahead of GDC. *Engadget* [online]. 2010 [cit. 2017-12-01]. Dostupné z: https://www.engadget.com/2010/03/04/microsoft-talks-windows-phone-7-series-development-ahead-of-gdc/
10. WARREN, Tom. Windows Phone dies today: An end of an era. *The Verge* [online]. 2017 [cit. 2017-12-01]. Dostupné z: https://www.theverge.com/2017/7/11/15952654/microsoft-windows-phone-end-of-support
11. IONESCU, Daniel. Geolocation 101: How It Works, the Apps, and Your Privacy. PCWorld [online]. 2010 [cit. 2017-12-01]. Dostupné z: https://www.pcworld.com/article/192803/geolo.html
12. ECKERSLEY, Peter. How Unique Is Your Web Browser? *Electronic Frontier Foundation* [online]. [cit. 2017-12-01]. ISSN 1062-9424. Dostupné z: https://panopticlick.eff.org/static/browser-uniqueness.pdf

13. PANGAM, Rahul. 7 Leading Fraud Indicators: From Fresh Cookies to Null Values. *Simility* [online]. 2016 [cit. 2017-12-01]. Dostupné z: https://simility.com/device-recon-results/
14. FOREMSKI, Tom. Social Media Is Not About Conversations.. It's About Something Much More Amazing. *Silicon Valley Watcher* [online]. 2010 [cit. 2017-12-01]. Dostupné z: http://www.siliconvalleywatcher.com/mt/archives/2010/03/social_media_is.php
15. ZHENG, Yu. Location-Based Social Networks. *Microsoft* [online]. 2011 [cit. 2017-12-01]. Dostupné z: https://www.microsoft.com/en-us/research/project/location-based-social-networks/
16. KOPECKÝ, K., KOŽÍŠEK, M. Výzkum rizikového chování českých dětí v prostředí internet. [Online]. 2014 [cit. 2017-12-10]. Dostupné z: http://www.e-bezpeci.cz/index.php/ke-stazeni/doc_download/61-vyzkum-rizikoveho-chovani-eskych-dti-v-prostedi-internetu-2014-prezentace/
17. JIN, L., TAKABI, H., Venue Attacks in Location-Based Social Networks, *ACM International Conference on Advances in Geographic Information Systems*, Dallas: ACM/University of North Texas/University of Florida, 2014 [cit. 2017-12-10]. ISBN 978-1-4503-3134-0.
18. KYSELA, Jiří. Analysis of Privacy Erosion of Geosocial Networks. *Computational Intelligence and Informatics (CINTI), 2015 16th IEEE International Symposium*. Budapest, Hungary, 2015 [cit. 2017-12-10]. ISBN: 978-1-4673-8520-6.
19. ZAHRADNIK, Fred. An Explanation of Wi-Fi Triangulation. *Lifewire* [online]. 2017 [cit. 2017-12-01]. Dostupné z: https://www.lifewire.com/wifi-positioning-system-1683343
20. Microsoft Privacy. Zjišťování polohy a ochrana osobních údajů ve Windows 10. *Microsoft* [online]. 2017 [cit. 2017-12-01]. Dostupné z: https://privacy.microsoft.com/cs-cz/windows-10-location-and-privacy
21. RAYMONDCC. 7 Chromium Based Browsers With Extra Features. *RaymondCC* [online]. 2017 [cit. 2017-12-01]. Dostupné z: https://www.raymond.cc/blog/chromium-browser-alternatives-with-extra-features/
22. YANDEX. Geolocation settings in Safari. *Yandex Support* [online]. 2016 [cit. 2017-12-01]. Dostupné z: https://yandex.com/support/common/browsers-settings/geo-safari.html
23. HOFFMAN, Chris. 6 Alternative Browsers Based on Mozilla Firefox. *How To Geek* [online]. 2012 [cit. 2017-12-01]. Dostupné z: https://www.howtogeek.com/108608/6-alternative-browsers-based-on-mozilla-firefox/
24. FLANAGAN, David. JavaScript: The Definitive Guide (6th ed.). 2011, O'Reilly & Associates. ISBN 978-0-596-80552-4.
25. KYSELA, Jiří. Comparison of Web Applications Geolocation Services. *Computational Intelligence and Informatics (CINTI), 2014 15th IEEE International Symposium*. Budapest, Hungary, 2014 [cit. 2017-12-10]. ISBN: 978-1-4799-5338-7.
26. ŠKORNIČKOVÁ, Eva. Co je GDPR? *GDPR.CZ* [online]. 2017 [cit. 2017-12-11]. Dostupné z: https://www.gdpr.cz/gdpr/

27. DUPAUL, Neil. MAN IN THE MIDDLE (MITM) ATTACK. *Veracode* [online]. [cit. 2017-12-11]. Dostupné z: https://www.veracode.com/security/man-middle-attack
28. DANIELKA, Jiří. Penetrační testování bezdrátových sítí. *Univerzita Pardubice* 2016 [cit. 2017-12-10]. Diplomová práce (Bc.), Fakulta elektrotechniky a informatiky.
29. HECKEL, C. Philipp. How To: Use mitmproxy to read and modify HTTPS traffic. *Philipp's Tech Blog* [online]. 2013 [cit. 2017-12-11]. Dostupné z: https://blog.heckel.xyz/2013/07/01/how-to-use-mitmproxy-to-read-and-modify-https-traffic-of-your-phone/
30. JEŽEK, David. Android posílá svou polohu, i když je lokalizační služba vypnuta. *Root.cz* [online]. 2017 [cit. 2017-12-11]. Dostupné z: https://www.root.cz/zpravicky/android-posila-svou-polohu-i-kdyz-je-lokalizacni-sluzba-vypnuta
31. KAJZAR, Petr. Ochrana soukromí v roce 2017: zákony přitvrzují, šifrujte. *Root.cz* [online]. 2017 [cit. 2017-12-11]. Dostupné z: https://www.root.cz/clanky/ochrana-soukromi-v-roce-2017-zakony-pritvrzuji-sifrujte/
32. GOODQUOTES. Edward Snowden: Quotable Quote. Goodreads [online]. [cit. 2017-12-11]. Dostupné z: https://www.goodreads.com/quotes/7308507-arguing-that-you-don-t-care-about-the-right-to-privacy

PŘÍLOHY

Příloha A – *DVD se zpracovanou bakalářskou prací*

- soubor PistinekR_AnalyzaEroze_JK_2017.pdf