Anonymita v prostředí internetu

Petr Kociňák

Bakalářská práce
2023

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav ochrany obyvatelstva

Akademický rok: 2022/2023

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Petr Kociňák**
Osobní číslo:	**L20356**
Studijní program:	**B1032A020002 Ochrana obyvatelstva**
Forma studia:	**Prezenční**
Téma práce:	**Anonymita v prostředí internetu**

Zásady pro vypracování

1. Proveďte rešerši literatury a elektronických zdrojů řešené problematiky.
2. Objasněte základní pojmy související s předmětnou problematikou.
3. Proveďte analýzu míry anonymity vybraných aplikací instant messagingu.
4. Navrhněte bezpečnou formu komunikace se zachováním anonymity v prostředí internetu.

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

Seznam doporučené literatury:

1. EVANS, Lester. *Cybersecurity: what you need to know about computer and cyber security, social engineering, the internet of things + an esential guide to ethical hacking for beginners.* [USA]: [Lester Evans], [2019], 218 s. ISBN 9781794647237.
2. JAN, Kolouch. *Cybersecurity.* Edice CZ.NIC, 2019, 1 online zdroj (560 stran). ISBN 978-80-88168-32-4.
3. MITNICK, Kevin D. a Robert VAMOSI. *The art of invinsibility: the world's most famous hacker teaches you how to be safe in the age of big brother and big data.* New York: Back Bay Books, Little, Brown and Company, 2019, x, 308 s. ISBN 978-0-316-38052-2.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **Ing. Petr Svoboda, Ph.D.**
Ústav ochrany obyvatelstva

Datum zadání bakalářské práce: **1. prosince 2022**
Termín odevzdání bakalářské práce: **5. května 2023**

PROHLÁŠENÍ AUTORA
BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 5. 5. 2023

Jméno a příjmení studenta: Petr Kociňák

.....
podpis studenta

ABSTRAKT

Bakalářská práce představuje současný stav anonymity v prostředí internetu se zachováním bezpečnosti. Práce informuje běžného uživatele o různých možnostech zabezpečení anonymity ve vybraných aplikacích instant messagingu. Dále práce komparuje aplikace z hlediska bezpečnosti tak, aby uživateli poskytly co nejlepší anonymitu a zabezpečení. Návrh bezpečné formy komunikace za využití správné mobilní aplikace. Kombinuje návrh a komparaci aplikací pro zachování anonymity a bezpečnosti. Práce je strukturována tak, aby přechod mezi tématy byl plynulý a tím poskytl čtenáři nejjasnější možný postup k dosažení anonymity v komunikaci přes mobilní aplikace.

Klíčová slova: anonymita, aplikace, bezpečnost, komunikace, šifrování.

ABSTRACT

The bachelor thesis presents the current state of anonymity in the Internet environment while maintaining security. The thesis informs the common user about various options for securing anonymity in selected instant messaging applications. Further, the thesis compares the applications in terms of security to provide the best anonymity and security to the user. Designing a secure form of communication using the right mobile application. It combines the design and comparison of applications to maintain anonymity and security. The work is structured in such a way that the transition between topics is seamless, thus providing the reader with the clearest possible approach to achieve anonymity in mobile application communication.

Keywords: anonymity, applications, security, communication, encryption.

Hlavní poděkování směřuje k panu Ing. Petrovi Svobodovi Ph.D., za poskytnutí důležitých rad, času a připomínek vedoucích ke zpracování této bakalářské práce.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

V dnešní době všechno, co je nebezpečné, není vůbec jednoduché kontrolovat. Podobné přirovnání platí i pro anonymitu. Dříve bylo pro identifikaci osob potřeba týmové spolupráce, dnes už není problém využít různé moderní technologie. Postupná digitalizace má za následek jednodušší práci k odhalení potřebné osoby. Postupné ubírání míry anonymity může vést k většímu zneužívaní ze strany útočníka, a proto je potřeba si dávat čím dál větší pozor na únik osobních informací.

K výběru tématu mě vedla otázka, jakým způsobem se v dnešní době zachází s osobními daty. Zda anonymita, jakou měl člověk dřív bez sociálních sítí, přes které komunikuje v jejich mobilních aplikacích, má stále stejnou hodnotu. Anonymita se stále vyvíjí, a v průběhu let bude těžké odhadnout, kam bude směřovat dále, a jak s ní bude zacházeno.

Bezpečí a anonymita začíná být čím dál větším aspektem, který uživatelé v prostředí aplikací vyhledávají. Postupné zavádění dvoufaktorového ověřování a zdokonalování šifrování napomáhá k ochraně osobních údajů a komunikace. Možností výběru správné aplikace přibývá. Trend směřuje k mobilním aplikacím, o kterých tato práce informuje.

Mobilní aplikace jsou často malé samotné softwarové moduly, nabízející desítky komunikačních aplikací pro mobilní zařízení s operačním systémem od společnosti Apple IOS nebo od konkurenčního systému Androidu. V dnešní době jsou základem běžné komunikace. Každá osoba žijící v moderní společnosti má alespoň jeden telefon, na kterém má nespočet aplikací pro využívání snadné komunikace. Vznikající kombinace mezi více aplikacemi má za následek menší obezřetnost k osobním údajům a informacím, které ne vždy jsou určené k vidění ostatním uživatelům nebo společnosti vlastnící danou aplikaci, přes kterou komunikace probíhá. Práce nepojednává o operačních systémech ani o poskytovatelích internetového připojení. Vztahuje se přímo na určené aplikace, jejich anonymitu a možnosti nabízeného zabezpečení pro případného uživatele.

Hlavním cílem bakalářské práce je návrh doporučení pro bezpečnou komunikaci formou instant messagingu (dále jen IM).

Dílčími cíli jsou rešerše problematiky anonymní komunikace v souvislosti s IM. Následně provést identifikaci kritérií pro posouzení vhodnosti aplikací IM v kontextu zachování anonymity. Analýza vhodnosti vybraných aplikací IM pro komunikaci se zachováním anonymity. Následné doporučení nejlepší aplikace z komparace pro bezpečnou formu komunikace.

I. TEORETICKÁ ČÁST

1 POJMOVÝ APARÁT

Internet je soubor distribuovaných sítí propojených sadou protokolů nazývaných TCP/IP. Královská akademie jazyků (RAE) ji definuje jako „celosvětovou počítačovou síť, která je decentralizovaná a tvořená přímým spojením mezi počítači prostřednictvím speciálních komunikačních protokolů“. (ARIMETRICS, 2022)

Jeho název pochází z anglického Interconnected Network (propojené sítě). Vyznačuje se schopností volně si vyměňovat a přistupovat k informacím bez ohledu na čas a prostor. Říká se, že to vedlo k určitému stupni „demokratizace“, protože k velkému množství dat lze přistupovat za relativně nízké nebo žádné náklady pomocí zdrojů mnoha veřejných institucí. (ARIMETRICS, 2022)

1.1 Historie internetu

První funkční obrázek internetu byl na počátku 60. let, kdy J.C.R. Licklider na MIT popularizoval myšlenku „intergalaktické sítě“ počítačů. Krátce poté vyvinuli počítačoví vědci koncept „přepínání paketů“, metodu efektivního přenosu elektronických dat, která se později stala jedním z hlavních stavebních kamenů internetu. První funkční prototyp internetu vznikl koncem 60. let, společně s vytvořením sítě ARPANET (Advanced Research Projects Agency Network). Síť ARPANET, původně financovaná ministerstvem obrany Spojených států, používala přepínání paketů, aby umožnila více počítačům komunikovat v rámci jedné sítě. (Andrews, 2019)

29. října 1969 odvysílal ARPANET svou první zprávu. Jednalo se o komunikaci z jednoho počítače do druhého. (První počítač byl v laboratoři UCLA, druhý na Stanfordské univerzitě, každý o velikosti malého domu.) Zpráva „přihlášení“ byla krátká a jednoduchá, ale přesto způsobila kolaps začínající sítě ARPA. Stanfordský počítač přijal pouze první dva znaky zprávy. (Andrews, 2019)

Daná technologie pokračovala ve vývinu v 70. letech poté, co výzkumníci Robert Kahn a Vinton Cerf vyvinuli komunikační model TCP/IP (Transmission Control and Internet Protocol), který vytvořil standardy pro přenos dat mezi více sítěmi. (Andrews, 2019)

Poté, v roce 1990, se online svět stal lépe rozpoznatelným, když počítačový vědec Tim Berners-Lee vynalezl World Wide Web. I když je často zaměňován se samotným internetem, je ve skutečnosti nejběžnějším prostředkem pro přístup k datům online ve formě webových stránek a hypertextových odkazů. (Andrews, 2019)

1.2 Budoucnost internetu

Svět se rychle posouvá směrem k všudypřítomné konektivitě a bude i nadále přetvářet, jak a kde se lidé připojují, shromažďují a sdílejí informace a konzumují média. (Anderson a Rainie, 2014)

Odborníci předpovídají, že přístup k internetu bude bezproblémový, a začne se používat informační prostředí, které většině lidí velmi usnadní připojení k internetu. Mobilní, nositelné a vestavěné počítače budou propojeny v internetu věcí, budou ukládat a sdílet informace v cloudu poháněném umělou inteligencí, aby z toho měli prospěch lidé a jejich okolí. (Anderson a Rainie, 2014)

Pokaždé, když někdo Alexu požádá, aby mu poslala další krmivo pro psy, poskytuje společnosti za miliardu dolarů informace o tom, kdo je. Hlavně to, že má psa, který moc rád jí. Poskytuje také informace o kreditní kartě, adresy, telefonní čísla atd. Bylo rozhodnuto obětovat některé z těchto potenciálně soukromých informací ve prospěch pohodlí. To se bude jen zvyšovat. Nové technologie si stále více uvědomují, co člověk chce. Pokud má určité návyky, (tato zařízení) mu pomůžou a předpoví je. Je to strašidelné, ale je to známé. (Blitz, 2021)

Většina odborníků předpokládá, že v budoucnosti bude pohlcující, neviditelné, globální, síťové, počítačové prostředí vytvořené neustálým šířením inteligentních senzorů, kamer, softwaru, databází a masivních datových center v rámci globální informační sítě známé jako internet věcí. Dále možnost „Rozšířené reality“ vylepšuje vstupy, které lidé vnímají v reálném světě, pomocí nositelných/přenosných technologií. (Anderson a Rainie, 2014)

Možnost narušení zavedených obchodních modelů 20. století (zejména v oblasti financí, zábavy, všech druhů vydavatelství a vzdělávání). značkování, vytváření databází a inteligentní analytické mapování fyzických a sociálních oblastí, jsou možnosti určitých budoucností, s kterými se bude muset člověk vypořádat. V rámci předpovídání a strategie lze přepokládat, že nezůstanou beze změny, a kde dnešní doba přepokládá něco, budoucnost může přinést úplně něco jiného. (Anderson a Rainie, 2014)

1.3 Prvky legislativy

„Zákon č. 110/2019 Sb. O zpracování osobních údajů.“ Hlavním cílem je zajištění osobních údajů v souladu s evropskými předpisy. V zákoně je obsaženo, že jakékoliv zpracování

osobních údajů, musí mít ze zákona určitou úroveň ochrany osobních údajů, aby nedošlo k jejich zneužívání, ztrátě, neoprávněnému přístupu a dalšímu nežádoucímu zpracování.

Subjekty zpravující osobní údaje dále musí zajistit osobám, jejichž údaje jsou zpracovány, potřebné informace, kdo bude jejich příjemcem, jaké jiné osoby budou mít přístup k těmto informacím, a jak s nimi bude zacházeno. (ČESKO, 2019)

„Zákon č. 412/2005 Sb. O ochraně utajovaných informací a o bezpečnosti způsobilosti.“ Hlavním účelem tohoto zákona je zajištění bezpečnostní způsobilosti osob a organizací, které s těmito informacemi pracují. Utajovanou informací se v zákoně rozumí informace, která je utajována podle právních předpisů určujících stupeň utajení důvěryhodných informací. Zákon také definuje postupy posuzování vhodnosti bezpečnosti a kritéria pro vydávání bezpečnostních certifikátů. (ČESKO, 2005)

„Zákon č. 181/2014 Sb. O kybernetické bezpečnosti a o změně souvisejících zákonů.“ Ukládá subjektům nakládajícím s citlivými informacemi jako jsou státní orgány, provozovatelé kritické infrastruktury a informačních systémů, povinnosti, aby zajistily ochranu těchto informací před zneužitím, ztrátou nebo poškozením. (ČESKO, 2014)

Zákon také ukládá poskytovatelům internetových služeb a vývojářům softwaru povinnost zajistit bezpečnost svých produktů a služeb. Představuje také nové instituce a nástroje pro zlepšení kybernetické bezpečnosti, jako jsou Kybernetický úřad a BIS. (ČESKO, 2014)

1.4 E-mail

S pomocí internetu a e-mailu je možné okamžitě posílat zprávy z jednoho systému do druhého. Dříve byly e-mailové zprávy dostupné pouze uživatelům na stejném počítači a vyžadovaly připojení k internetu. Dnes už víme, jak schránka vypadala. E-mail lze odeslat více příjemcům a uživatelé mohou zabránit ostatním v zobrazení jména příjemce přidáním jeho jména do pole skrytá kopie. (Pedamkar, 2023)

E-mailový klient pomáhá v tomto procesu připojením k serveru Simple Mail Transfer Protocol přes internet. Aby klient mohl odesílat e-maily, je serveru přiřazen specifický port. E-mailová adresa příjemce musí být správná, takže informace v záhlaví musí být zachovány. Protokol SMTP transformuje data pro předávání obsahu e-mailů přes porty. Protože symbol „@“ odděluje název poštovního serveru, SMTP hledá poštovní server za ním. (Pedamkar, 2023)

Kontrola e-mailů je jednou z prvních věcí, kterou ráno uděláte. Můžete se obávat, zda někdo neviděl váš e-mail, a to není bezdůvodná obava. Pokud používáte e-mailovou službu, jako je Gmail nebo Outlook, řešení je děsivé a docela jednoduché. (Mitnick, 2019)

I když smažete e-mail z počítače nebo mobilního telefonu ihned po jeho přečtení, obsah nemusí být ztracen. Ještě někde je jeho kopie. E-mail je založen na cloudu, takže zálohování musí být dostupné z jakéhokoli zařízení, kdekoli a kdykoli. Pokud například používáte Gmail, Google uchovává kopie všech e-mailů, které odešlete a přijmete, na svých mnoha serverech po celém světě. (Mitnick, 2019)

1.5 Kyberprostor

Kyberprostor je definován jako virtuální a dynamické prostředí různých síťově propojených elektronických a komunikačních zařízení pro ukládání a používání elektronických dat. Struktura kyberprostoru připomíná strukturu lidského mozku. Lidský mozek se skládá z miliard neuronů, které se používají k přenosu signálů. Podobně se kybernetický prostor skládá z mnoha síťových připojení používaných pro komunikaci. Umožňuje existenci nehmotných médií (kyberprostoru) díky distribuci hmotných médií (síťové prvky, jednotlivé počítačové systémy, cloudová úložiště, propojené služby atd.). Pokud je hmotné médium poškozeno, přizpůsobuje se a mění se, ale pokud se fyzické médium nebo všechny jeho součásti zcela zhroutí, dojde k nenapravitelnému poškození nebo zničení samotného kyberprostoru. (Kolouch, 2019)

Identifikovat ho lze také jako prostor pro kybernetické aktivity nebo prostor vytvářený informačními a komunikačními technologiemi. Jeho hlavním účelem je sdílení informací a komunikace po celém světě. Obecně řečeno, kyberprostor se vztahuje na standardní kritéria aplikovaná v kontextu skutečného fyzického umístění dat nebo informací. Síťová zařízení v kyberprostoru zahrnují osobní počítače a servery, superpočítače, sítě a senzory. (Kolouch, 2019)

1.5.1 Internet věcí

Internet věcí (dále IoT) označuje miliardy fyzických zařízení po celém světě, která jsou nyní připojena k internetu a shromažďují a sdílejí data. Díky rozmachu superlevných počítačových čipů a bezdrátových sítí lze k IoT připojit vše od malého tabletu až po velikost letadla. Propojení všech těchto různých objektů a přidání senzorů k jinak hloupým zařízením dodává digitální inteligenci, která jim umožňuje přenášet informace v reálném čase bez

lidského zásahu. Díky IoT je svět kolem nás chytřejší a citlivější a propojuje digitální a fyzický vesmír. (Ranger, 2020)

Téměř jakýkoli fyzický objekt lze proměnit v zařízení IoT, pokud se dokáže připojit k internetu a ovládat nebo přenášet informace. Žárovka, která se rozsvítí pomocí aplikace pro chytré telefony, je zařízení IoT, stejně jako pohybový senzor nebo chytrý termostat v kanceláři nebo připojené pouliční osvětlení. Některé větší objekty mohou být osazeny menšími IoT komponentami, jako je tryskový motor, který je nyní nabitý za pomoci tisíci senzorů, které shromažďují a přenášejí data, aby zajistily efektivní fungování. V ještě větším měřítku jsou to projekty chytrých měst, které zaplňují celé oblasti senzory, a pomáhají porozumět, spravovat naše prostředí. (Ranger, 2020)

1.5.2 Umělá inteligence (AI)

Umělá inteligence (dále AI) je široké odvětví informatiky zabývající se vytvářením inteligentních strojů, které mohou provádět úkoly, které normálně vyžadují lidskou inteligenci. AI je multidisciplinární věda s mnoha přístupy, ale pokroky ve strojovém učení a hlubokém učení způsobují změny paradigmatu téměř ve všech oblastech technologického průmyslu. AI umožňuje strojům modelovat, a dokonce rozšiřovat schopnosti lidské mysli. Od počátku vývoje samořídících aut až po rozšíření chytrých asistentů jako Siri a Alexa se stává čím dál běžnější záležitostí. Mnoho technologických společností v různých odvětvích proto investuje do technologií AI. (Schroer a Glover, 2022)

Vzhledem k výpočetním nákladům a technické datové infrastruktuře je implementace AI složitá a nákladná záležitost. Naštěstí počítačová technika udělala obrovský pokrok. Podle Moorova zákona se počet tranzistorů na mikročipu zdvojnásobí zhruba každé dva roky a náklady na počítače budou poloviční. (Schroer a Glover, 2022)

Zatímco mnoho odborníků věří, že Moorův zákon pravděpodobně skončil v roce 2020, měl hluboký dopad na moderní technologii AI. Nedávný výzkum ukazuje, že inovace AI ve skutečnosti překonávají Moorův zákon a zdvojnásobují se zhruba každých šest měsíců po dobu dvou let. Podle této logiky jsou pokroky, kterých AI v posledních letech dosáhla v různých odvětvích, zásadní. A potenciál pro ještě větší dopady v příštích několika desetiletích se zdá být téměř nevyhnutelný. (Schroer a Glover, 2022)

1.6 Kybernetická bezpečnost

Zabezpečení domova se stává nekonečnou hrou na kočku a myš, kde investujete čas, peníze a úsilí do údržby nebo přístupu k určité oblasti. Vlastník může dojít k závěru, že nejlepší domácí zabezpečovací systémy jsou levné, pohodlné a nenápadné, ale fundovaného, odhodlaného a dobře infiltrovaného zloděje to neodradí. Zabezpečení každého je samostatné. Ukazuje se, že ochrana našich počítačů a sítí se řídí stejnými zásadami jako ochrana našich domovů, ale přístup je snazší než kdy jindy a sázky jsou vysoké. Vzdálení kybernetičtí útočníci se zlými úmysly můžou krást všechna data roky, aniž by si to kdokoliv uvědomil. (Evans, 2019)

Hlavní funkcí kybernetické bezpečnosti je ochrana zařízení používaných běžnými lidmi. To zahrnuje chytré telefony, tablety, počítače, notebooky a služby, ke kterým se přistupuje online a v práci. Cílem je zabránit možným útokům nebo přístupu. (Groot, 2022)

Kybernetická bezpečnost je důležitá, protože vládní, vojenské, podnikové, finanční a lékařské instituce shromažďují, zpracovávají a ukládají nebývalé množství dat v počítačích a dalších zařízeních. Většina těchto údajů jsou důvěrné informace, ať už se jedná o duševní vlastnictví, finanční údaje, osobně identifikovatelné informace nebo jakýkoli jiný typ dat, jejichž neoprávněný přístup nebo zveřejnění by nás mohlo nepříznivě ovlivnit. Firmy v rámci svého podnikání přenášejí citlivá data do sítí a dalších zařízení. Kybernetická bezpečnost představuje specialitu ochrany těchto informací a systémů používaných k jejich zpracování nebo ukládání. Vzhledem k tomu, že se kybernetické útoky stávají stále rozšířenějšími a sofistikovanějšími, podniky a organizace, zejména ty, které mají za úkol chránit informace související s národní bezpečností, lékařskou péčí a finančními záznamy, by měly chránit citlivé firemní a osobní informace. (Groot, 2022)

1.6.1 Původ hackerství

Slovník definuje slovo „hack“ jako řez s opakovanými nebo nepravidelnými seky, jedná se o správné slovo, protože hackeři používají jednoduché nástroje, vynakládají trochu úsilí a zbytek nechávají na setrvačnosti. (Evans, 2019)

Termín „hacking“ byl poprvé použit v roce 1955 na schůzi Klubu technických modelových železnic v souvislosti s využitím technického know-how. Zápis z jednání byl použit k popisu toho, jak členové změnili funkčnost high-tech železničních tratí. (Hiley, 2022)

Dnes se termín „hacker“ obvykle používá jako synonymum s „bezpečnostním hackerem“, ale může také označovat každého zkušeného počítačového programátora. Bezpečnostní hackeři využívají své technické znalosti o chybách a zranitelnostech k využívání zranitelných míst v počítačových systémech k získání přístupu k datům, ke kterým by jinak neměli oprávnění. Bezpečnostní hackerství je obvykle nezákonné a může vést k vysokým pokutám, a dokonce i vězení. (Hiley, 2022)

1.6.2 Kybernetické útoky

Kybernetický útok je pokus o neoprávněný přístup k počítači, počítačovému systému nebo počítačové síti za účelem poškození. Účelem kybernetických útoků je deaktivovat, narušit, zničit nebo převzít počítačové systémy nebo změnit, zablokovat, odstranit, manipulovat nebo ukrást data uložená v těchto systémech. Kybernetické útoky může provádět každý jednotlivec nebo skupina odkudkoli pomocí jedné nebo více různých strategií útoku. (Pratt, 2022)

Hrozby využívají různé techniky kybernetických útoků, především v závislosti na tom, zda provedou útok na cílovou entitu nebo jiné entity. (Pratt, 2022)

Náhodné útoky, při kterých se útočník pokouší proniknout do co největšího počtu zařízení nebo systémů, obvykle vyhledává zranitelnosti v softwarovém kódu, které umožňují pronikání, aniž by byly detekovány nebo blokovány. Případně lze použít phishing útoky. Při tomto útoku je velkému počtu lidí zaslán e-mail se sociálně pozměněnou zprávou navrženou tak, aby příjemce přiměl kliknout na odkaz, který stáhne škodlivý kód. (Pratt, 2022)

Při cílených útocích se útočníci zaměřují na konkrétní organizace a používají různé taktiky v závislosti na cíli útoku. Ke kybernetickým útokům často dochází, když hackeři začnou vyšetřovat nebo hledat zranitelnosti nebo vstupní body, zahájí počáteční kompromitaci a poté ukradnou cenná data, deaktivují počítačové systémy nebo obojí. (Pratt, 2022)

Otázkou pro většinu organizací není, zda dojde k úniku dat, ale kdy. Obvykle vícekrát. Pokud jde o detekci hrozeb, reakci a nápravu, čím rychleji, tím lépe. (Pratt, 2022)

2 ANONYMITA

Anonymita, řecky „bezejmenný“, je lidský psychologický zážitek. Je to koncept, který každý z nás má prezentovat světu, ale za určitých okolností ho můžeme vypnout a fungovat v naprostém utajení. (Lufkin, 2017)

Cokoli, co nelze ovládat, může být nebezpečné. To je přesně případ anonymity. Neautorská, nezávadná zpráva nebo akce znamená, že nikdo nebude stíhán. Může obsahovat pomluvy, diskriminace, nelegální obchod, teroristické útoky a mnoho dalších možností, kdy je potřeba provést identifikaci zdroje. Identifikace zdroje by však zasahovala do omezování svobody projevu. (Merzlikina, 2019)

2.1 Historie anonymity

V 19. století byla anonymita normou ve většině evropských zemí, i když v druhé polovině století začala upadat, zvláště když panovaly pochybnosti o tom, zda podepisovat literární recenze či nikoli. Rozhodujícím se stal i požadavek Napoleona III. V 50. letech 19. století francouzští novináři podepisovali kusy s politickým obsahem, aby měli pod kontrolou kritiku své vlády. Ať je to, jak chce, přechod z anonymity na podpis nebyl rychlý proces. Jak Reich podrobně rozebírá, podepisování článků se stalo běžným až ve druhé polovině 20. století. (Arrese, 2022)

Anonymita byla ve Spojeném království vždy velmi vzrušená debata. V roce 1867 publikoval John Morley jako redaktor The Fortnightly Review vlivný článek „Anonymní žurnalistika“ na obranu podpisů, ve kterém nadále hájil separatistického ducha novin, což oznámil jeden z jejich zakladatelů Anthony Trollope, „V anonymní literatuře“ (1865). Zde Morley uvedl své důvody, proč upřednostňuje osobnější formu žurnalistiky, kde každý reportér přebírá zásluhy a zodpovědnost za své psaní, bez závoje anonymity. (Arrese, 2022)

Pravdou ale je, že anonymita ve 30. letech minulého století do značné míry zmizela. V roce 1938 si Arthur Cummings, politický redaktor News Chronicle, stěžoval, že stále existují publikace, kde byla anonymita normou. Určitě byl pro podepsaný článek, kde si skutečný člověk musí hájit své názory. Odstraňte úvod „my“ a odstraníte velkou část okázalosti a falešného kouzla spojeného s anonymním vyjádřením redakčního názoru. (Arrese, 2022)

O deset let později, v roce 1948, Oscar Maurer Jr. uzavřel svou analýzu debaty o anonymitě v jedné z nejlepších historických studií na toto téma Solomonovým závěrem: *„Obecně pozitivní přijetí anonymity nepřineslo všechny výhody, které si její zastánci představovali.“*

Ani jeho odpůrci se nebojí novinářské destrukce. Od 70. let 20. století se rozsáhlá anonymita, která byla v žurnalistice praktikována, stala skutečnou raritou, doslovným reliktem minulosti. (Arrese, 2022)

Zájem o anonymní komunikaci v posledních desetiletích vzrostl s tím, jak se zvyšuje počet komunikačních kanálů využívaných občany. Kromě anonymity, které charakterizovala literární a publicistickou činnost v minulém století, nové technologie umožňují zamaskovat nebo utajit identitu původce informace (kterým může být nyní jakýkoli občan). Anonymita dnes znamená vše od úplného až po částečné skrytí identity. Jde tedy o míru, *„do jaké sdělovatel vnímá zdroj jako neznámý nebo neurčitý“*. Anonymita se posunula mimo svět tradičního obsahu (knihy, noviny atd.) do vysoce komplexních sociálních, ekonomických a technologických oblastí. Tento trend vyžaduje obecnou teorii fenoménu z pohledu odesílatelů i příjemců anonymních zpráv. (Arrese, 2022)

2.2 Adresa internetového protokolu a cookies

Adresa internetového protokolu (IP) je jedinečný číselný identifikátor pro jakékoli zařízení nebo síť připojenou k internetu. IP adresa, obvykle přidělená poskytovatelem internetových služeb (ISP), je e-mailová adresa zařízení používaného pro internetovou komunikaci. Na internetu se běžně používají dvě verze IP adres: IPv4 a IPv6. Adresa IPv4 je vyjádřena jako čtyři čárkovaná desetinná čísla s každým oktetem odděleným tečkou, například 192.168.35.4. Tři čísla v prvním oktetu představují konkrétní internetovou síť, zatímco ostatní čísla představují skutečnou adresu hostitele v místní síti, jako je pracovní stanice nebo server. Adresa IPv6 se skládá z osmi skupin čtyř hexadecimálních číslic oddělených dvojtečkami. (Yasar, 2023)

Každá adresa internetového protokolu může odesílat data na jiné adresy IP v samostatných částech nazývaných pakety. Každý síťový paket obsahuje jak odeslaná data, tak hlavičku obsahující metadata paketu. (Yasar, 2023)

IP adresa je součástí protokolu TCP/IP. Funguje v zákulisí a pomáhá zařízením a webovým stránkám propojit se navzájem na internetu. V souvislosti s každým požadavkem na použití webové stránky musí žádající počítač vědět, kde se webová stránka nachází a jak se k ní dostat. Zde vstupuje do hry IP adresa. Požadující počítač se připojí k síťovému routeru, který komunikuje s webovým serverem, který je hostitelem webové stránky. Webový server poté vezme informace o webové stránce a odešle je zpět do počítače, který si je vyžádal. Každé zařízení zapojené do tohoto procesu – včetně počítače, routeru

a webového serveru – nese jedinečnou IP adresu, bez které nemůže komunikace probíhat. (Yasar, 2023)

2.2.1 Typy IP adres

Čtyři hlavní typy IP adres jsou veřejné, soukromé, statické a dynamické. Veřejné a soukromé adresy jsou založeny na umístění v síti, přičemž soukromé adresy se používají v rámci sítí a veřejné adresy mimo sítě. Další dvě mají základní rozdíl, kdy dynamické se neustále mění a statické jsou neměnitelné. (Williams, 2023)

Soukromé IP adresy

Každé zařízení připojené k domácí nebo privátní síti má skrytou IP adresu. Soukromé IP adresy nesměřují do internetu a používají se pouze v rámci intranetu. Mezi zařízení se soukromou IP adresou mohou patřit počítače, chytré telefony, tablety, zařízení Bluetooth, chytré televize a tiskárny. S rostoucí popularitou produktů IoT bude pravděpodobně i nadále růst využívání privátních IP adres. (Williams, 2023)

Veřejné IP adresy

Tyto adresy, které umožňují směrovači komunikovat s internetem nebo vnější sítí, obstarává poskytovatel internetových služeb. Veřejné IP adresy pokrývají celou síť, z čeho vyplývá, že více zařízení sdílejících stejné internetové připojení také sdílí stejnou veřejnou IP adresu. (Yasar, 2023)

Dynamické IP adresy

Dynamické IP adresy se neustále mění. Jsou dočasné a přiřadí se k zařízení pokaždé, když se připojí k síti. Dynamické adresy IP mohou pocházet ze souboru adres IP sdílených mezi více počítači. Dynamické IP adresy jsou dalším důležitým typem adresy internetového protokolu. Jsou aktivní pouze po určitou dobu, poté už nebudou dále platné. (Williams, 2023)

Statické IP adresy

Statická IP adresa je neměnitelná. Naproti tomu dynamickou IP adresu přiděluje server DHCP (Dynamic Host Configuration Protocol), který ji může změnit. Statická IP adresa se nikdy nemění, ale lze ji změnit v rámci běžné správy sítě. Statická IP adresa je konzistentní a je přidělena jednou, takže zůstává stejná po celá léta. Tento typ IP adresy také pomáhá získat mnoho informací o zařízení. (Williams, 2023)

IP adresy webových stránek

Sdílená IP adresa se používá pro webové stránky malých firem, které ještě nemají mnoho návštěvníků nebo mnoho souborů či stránek. IP adresa není jedinečná a je sdílena s jinými webovými stránkami. (Williams, 2023)

Vyhrazená IP adresa je unikátní IP adresa přiřazená jednotlivým webovým stránkám. Soukromé IP adresy pomáhají vlastníkům webových stránek vyhnout se blokování, kterému mohou majitelé sdílených IP adres čelit, pokud se jiné webové stránky sdílející stejnou IP adresu chovají škodolibě. Vlastníci svých IP adres mají přístup na své webové stránky, i když čekají na převod domény. (Williams, 2023)

2.2.2 Cookies

Cookies jsou malé kousky dat, které fungují jako datové nosiče v prohlížeči a jsou odesílány na server s každým požadavkem. Jsou užitečné pro správu relací, přizpůsobení uživatele a sledování. (Ahn, 2021)

Soubory cookies mohou analyzovat a identifikovat každého návštěvníka webové stránky. Jejich praktické využití je vidět pokaždé, když se objednají produkty například z internetového obchodu a textové pole pro obsahující informaci je již předvyplněné. Celkově mohou šetřit spoustu času. (Čihák, 2020)

Dalším účelem jejich použití je pro různé statistiky měření síťového provozu nebo jiné systémy pro analýzu sítě. Cookies ukládají ID konkrétního návštěvníka, čas návštěvy, dobu trvání návštěvy, ze které webové stránky přišel, jaký hledaný výraz na internetu použil k nalezení určité webové stránky atd. Všechny tyto informace jsou následně shromažďovány pomocí nástrojů, jako je Google Analytics. (Čihák, 2020)

Běžného návštěvníka prakticky neovlivňují, ale jsou nezbytným zdrojem informací pro každého majitele webu, protože na základě těchto informací může zjistit, jaká cílová skupina jeho web navštěvuje nebo o jaký obor má web největší zájem. Tyto důležité statistické informace pak lze využít k přesnému a efektivnímu cílení reklam nebo zlepšení hodnocení ve vyhledávačích. Díky přesnému zacílení lze předpokládat, že investice do marketingu se mnohonásobně vrátí. (Čihák, 2020)

2.2.3 Typy cookies

Fragmenty dat nazývané cookies lze rozdělit do 5 základních typů, které mají své základní zobrazení a využití v internetovém prostředí. Každý jeden z daných typů je využíván pro specifické účely. Kombinace typů cookies přináší optimální výsledek pro obě strany řetězce. Vstupující uživatel odevzdává základní informace vlastníkovi webové stránky za účelem získaní určité výhody v podobě uložení dat pro příští přihlášení a dalších specifických možností. Druhá strana získává základní informace pro optimalizování své reklamy a usnadnění komunikace. (Ahn, 2021)

Soubory cookies relace

Soubory cookies relace, známé také jako dočasné soubory cookies, přestanou fungovat, když se uzavře nebo opustí prohlížeč. Webová stránka používá soubory cookies relace, pokud musí uživatel při každém otevření stránky zadávat své přihlašovací údaje. (Ahn, 2021)

Příkladem může být nákupní košík jakékoli online nákupní stránky. Soubory cookies relace pomáhají ukládat produkty do nákupního košíku, při kliknutí na produkt otevřete novou kartu. Bez souborů cookies si web nebude pamatovat položky. (Ahn, 2021)

Soubory cookies první strany

Web, který osoba navštíví, ukládá soubory cookies první strany přímo do jejího počítače. Webové stránky shromažďují analytická data a užitečné informace pro zlepšení uživatelské zkušenosti. (Ahn, 2021)

Při návštěvě určité stránky na internetu odešle web do počítače požadavek, který poskytne jedinečnou hodnotu souboru cookies určité doméně. Bez cookies první strany nemohou webové stránky automaticky přihlásit uživatele ani si zapamatovat jeho nastavení z předchozích relací. (Ahn, 2021)

Soubory cookies třetích stran

Soubory cookies třetích stran vytvářejí domény jiné než tu, kterou přímo uživatel používá. Soubory cookies třetích stran, které se obvykle používají pro účely sledování, se ukládají také po zavření prohlížeče. Jedním z nejčastějších použití je sledování reklam na jiných webech, které člověk obvykle navštěvuje. Když například prohlíží různé produktové stránky na webových stránkách elektronického obchodu, může narazit na soubory cookies třetích stran pocházejících z jiné domény, než je webová stránka, kterou navštěvuje. Později, když

zavře prohlížeč, může být použit soubor cookies třetí strany ke sledování, zda si zakoupil produkt prohlížený na webových stránkách. (Ahn, 2021)

Některé obrázky nebo jiné soubory stažené z webových stránek třetích stran mimo danou doménu mohou obsahovat soubory cookies třetích stran, které umožňují jiným doménám zasílat cílené e-maily nebo reklamy o produktech, které si osoba prohlížela, ale nezakoupila. (Ahn, 2021)

Zabezpečené soubory cookies

Zabezpečené soubory cookies zabraňují neoprávněným stranám ve sledování souborů cookies, které jsou odeslány novému uživateli jako součást odpovědi HTTP. S atributem Secure obsahují požadavky HTTP soubor cookies pouze v případě, že jsou odesílány přes zabezpečený kanál. (Ahn, 2021)

Zombie cookies

Účelem zombie cookies je vrátit se k životu, i když jsou smazány nebo byl uzavřen prohlížeč. Zombie cookies se ukládají na místech mimo samostatné úložiště cookies prohlížeče. Pokud uživatel cookies odstraní, zombie cookies můžou převzít kopii uloženou jinde a znovu ji propojit s úložištěm cookies uživatele. (Ahn, 2021)

V minulosti byly reklamní společnosti jako Quantcast žalovány za používání zombie cookies ke sledování uživatelů a ukládání osobních údajů. Státy jako Kalifornie považují používání zombie cookies za nelegální zásah do soukromí, kde může dojít ke zákonnému stíhání. (Ahn, 2021)

2.3 Heslo

Jak fungují hesla? Odpověď je celkem jednoduchá, možná i zřejmá: heslo se skládá z kombinace písmen, číslic a speciálních znaků, kterými prokazujete svou totožnost a přistupujete k určitým informacím, v tomto případě na internetu. (Moes, 2023)

Při vytváření silného hesla musí být použito více než jen známá slova, fráze nebo data. Jméno slavného předmětu, zvířete nebo narozeniny jsou nejhorší možné kombinace hesel. Silná hesla navíc obsahují alespoň osm znaků. Ačkoli je heslo omezeno na 64 znaků, je nejlepší omezit heslo na 16 znaků nebo méně. (Moes, 2023)

Projděte si v duchu všechny fotografie v telefonu, počítači a e-mailu. Ano, mnoho z nich je zcela neškodných. Nebylo by na škodu, kdyby každý viděl krásné západy slunce, roztomilé rodinné fotky a možná i zábavnou selfie. (Mitnick, 2019)

Co by se stalo, kdyby se všechny najednou objevily online? I když ne všechny osobní snímky jsou kompromitující, stále jde o dokumentaci soukromých událostí. Díky cloudovým službám je ne vždy kontrola nad tím, kdy, kde a jak je sdílíme. Proto existují hesla, která uživateli dokážou poskytnout určitou ochranu nad tím, aby se nemohl jen tak někdo dostat k osobnímu obsahu druhé osoby. (Mitnick, 2019)

3 ŠIFROVÁNÍ

Šifrování je kódování čitelného textu tak, aby jej mohl rozluštit pouze vlastník tajného kódu nebo dešifrovacího klíče. To pomáhá zajistit bezpečnost citlivých dat. Mnoho osobních údajů bývá uloženo online anebo na serverech s trvalým připojením k internetu nebo cloudu. Je téměř nemožné podnikat v jakémkoli odvětví, aniž by osobní údaje skončily v online počítačovém systému společnosti, takže je velmi důležité pochopit, jak chránit soukromí takových informací. (Rafter, 2022)

Šifrování zakóduje prostý text, jako je textová zpráva nebo e-mail, do „šifrovaného textu“, což je nesrozumitelný formát. To pomáhá zachovat soukromí digitálních dat přenášených přes síť (např. internet) nebo uložených v počítačových systémech. Data jsou převedena zpět do původní podoby, když zamýšlený příjemce přistoupí ke zprávě. Tento postup se nazývá dešifrování. Odesílatel i příjemce musí k odemknutí zprávy použít „tajný“ šifrovací klíč, což je sada algoritmů, které šifrují a znovu zakódují data do čitelného stavu. (Rafter, 2022)

Data jsou šifrována a dešifrována stejným heslem v symetrickém šifrování. V asymetrickém šifrování se pro šifrování a dešifrování používají dva klíče. Všichni uživatelé sdílejí veřejný klíč k šifrování dat. Data jsou dešifrována soukromým klíčem, který není sdílen. (Rafter, 2022)

End-to-End šifrování

Šifrování se provádí na úrovni zařízení v režimu end-to-end. Veřejný klíč, který je k dispozici komukoli, zašifruje zprávy a soubory předtím, než opustí telefon nebo počítač, ale lze jej dešifrovat pouze pomocí soukromého klíče příjemce, jakmile dosáhnou svého cíle. Protože soukromé klíče potřebné k dešifrování dat chybí, hackeři na serveru k nim nemají přístup. Místo toho jsou soukromé klíče uloženy na zařízení každého uživatele a jsou dostupné pouze jim. (Berlove, 2022)

Asymetrická kryptografie spočívá ve vytvoření páru veřejného a soukromého klíče. Zpráva je zašifrována a dešifrována pomocí samostatných šifrovacích klíčů. Veřejné klíče se používají k uzamčení nebo šifrování zprávy a jsou sdíleny globálně. Soukromé klíče se používají k otevření nebo dešifrování zprávy a zná je pouze jejich vlastník. Pro každého připojeného uživatele systém generuje veřejné a soukromé šifrovací klíče jako součást úplného šifrování. (Berlove, 2022)

3.1 Biometrické ověřování

Biometrie je analýza jedinečných biologických a fyziologických charakteristik k potvrzení identity osoby. Pět nejběžnějších typů biometrických údajů jsou: otisky prstů, obličej, hlas, duhovka a vzory žil na dlani nebo prstech. (Jiřík, 2021)

Banky například potřebují biometrické údaje k poskytování různých vzdálených služeb. Pokud si osoba chce nový účet založit, nebo si vzít půjčku, musí zajít na bankovní pobočku. V dnešní době není problém se k mnoha službám dostat přes telefon. (Jiřík, 2021)

Fyzická biometrie

Pomocí speciálních zařízení (skenery, senzory a další čtečky) se biometrické údaje člověka ukládají do databáze. Systém ukládá tyto informace jako otisky prstů a převádí je na digitální data. Když je prst znovu přiveden ke skeneru, systém porovná nové informace s informacemi uloženými v databázi. Nakonec systém buď potvrdí identitu osoby a udělí přístup, pokud je nalezena shoda, nebo odmítne požadavek, pokud není nalezena žádná shoda. (Jiřík, 2021)

V dnešní době fotoaparáty a videokamery chytrých telefonů snadno rozpoznávají obličeje pomocí vestavěných senzorů neuronové sítě. V tomto smyslu se obraz stává lidským identifikátorem. Tuto technologii lze využít nejen k odemykání telefonů, ale i ke složitějším úkonům, jako je potvrzování nákupů nebo přístup k finančním službám. (Jiřík, 2021)

Biometrie chování

Behaviorální biometrie je identifikační systém, který identifikuje osobu na základě dynamických nebo behaviorálních charakteristik. Tyto vlastnosti mohou zahrnovat dynamiku rukopisu a podpisu, rytmus hlasu a řeči, rozpoznávání gest, vlastnosti používání elektronických zařízení prostřednictvím rychlosti psaní, způsob, jakým člověk má uchopený chytrý telefon nebo tablet, a dokonce i způsob chůze. Tento typ se také nazývá pasivní biometrie, protože nevyžaduje, aby se uživatel aktivně účastnil procesu ověřování. (Jiřík, 2021)

Tyto dynamické metody autentizace jsou založeny na lidském chování. Oceňují jedinečné chování a podvědomé pohyby člověka opakováním jakékoli činnosti. Kombinací je rozpoznávání hlasu, kde se jedná o technologii, která kombinuje fyzickou i behaviorální biometrii, protože současně analyzuje dynamické a statické charakteristiky lidského hlasu. (Jiřík, 2021)

Skenování otisků prstů

Metoda skenování otisků prstů je typ elektronického bezpečnostního systému, který využívá otisky prstů k biometrické autentizaci a umožňuje uživateli přístup k informacím nebo potvrzení transakcí. (Goodner, 2021)

Vzhledem k tomu, že každý otisk je téměř jedinečný, jsou tyto otisky účinné při identifikaci osob. Databáze otisků prstů nevytvářejí a sledují pouze orgány činné v trestním řízení. Požadavek na snímání otisků prstů jako podmínka zaměstnání se týká mnoha profesí, které vyžadují profesní osvědčení (např. finanční poradci, makléři, realitní makléři, pedagogové, lékaři/zdravotní sestry, bezpečnostní služby, dodavatelé atd.). Otisky prstů mohou být požadované v notářsky ověřených dokumentech. (Goodner, 2021)

Pokrok v technologii umožnil přidat snímače otisků prstů – známé také jako „čtečky“ nebo „senzory“ – do mobilních zařízení jako (volitelnou) vrstvu ochrany. Seznam metod zamykání a odemykání smartphonů se neustále rozšiřuje a nově zahrnuje i snímače otisků prstů. Mezi další metody byly přidány kódy PIN, kódy vzorů, hesla, rozpoznávání obličeje, rozpoznávání polohy, skenování duhovky, rozpoznávání hlasu, důvěryhodná připojení Bluetooth nebo NFC. (Goodner, 2021)

Snímače otisků prstů snímají vzory na okrajích a spodní části prstu. Software pro analýzu/párování vzorů zařízení poté zpracuje data a porovná je s databázovým záznamem registrovaných otisků prstů. Úspěšná shoda znamená, že identita osoby byla ověřena, což umožňuje přístup. (Goodner, 2021)

Rozpoznávání obličeje

Biometrická technologie zvaná software pro rozpoznávání obličeje (FRS) se používá k přiřazování tváří z obrázků, obvykle fotografií a videí, k identitám již uloženým v databázi. Lze jej rozdělit do tří částí: rozpoznání obličeje (vyhledání obličeje na obrázku), mapování obličeje a rozpoznání obličeje (potvrzení identity). (Mohanakrishnan, 2021)

Funkce automatického označování Facebooku nebo dokonce Fotek Google je příkladem technologie rozpoznávání obličeje. Tyto typy sociálních sítí a technologických gigantů využívají svou stávající databázi nahraných obrázků k tomu, aby přiřazovali obrázek uživatele k jeho obličeji. Techniky FRS vyžadují pokročilou umělou inteligenci, protože rysy obličeje jsou podstatně složitější než jiná biometrická měření, jako jsou otisky prstů a duhovka. (Mohanakrishnan, 2021)

Rozpoznávání hlasu

Virtuální svět prošel obrovskou změnou díky softwaru pro rozpoznávání hlasu. Tento vynález využívá vlastní technologii k převodu lidského hlasu na písemnou reprezentaci. Díky softwaru pro rozpoznávání řeči je možné v dnešní době ovládat celý systém pouze svým hlasem. Tento program používá algoritmy k převodu lidského hlasu na text. Rozpoznávání hlasu nejprve poslouchá lidský hlas a poté reaguje. Přizpůsobuje svůj systém hlasu, který člověk používá. (Bennett, 2022)

Zpracování uživatelské řeči je přímou aplikací technologie hlasové biometrické autentizace v různých prostředích. Využití této biometrické technologie umožňuje zrychlit obsluhu a zároveň zjednodušit a zkvalitnit práci agentů. Aplikace pro tuto technologii zahrnují telekonference, forenzní systémy, rozpoznávání kreditních karet a bezpečnostní systémy. Rozpoznávání hlasu lze použít společně s jinou autentizační metodou, jako je rozpoznávání otisků prstů, ve větších projektech, zejména tam, kde je silná potřeba chránit citlivá data. (Jiřík, 2021)

Rozpoznávání duhovky

Duhovka je sval, který reguluje množství světla dopadajícího na sítnici. Navíc ovlivňuje barvu očí, která je dána množstvím pigmentu melaninu. Užitečnost identifikace duhovky, stejně jako jiné biometrie, spočívá ve vzácnosti a nemožnosti násobení duhovky. Podle výzkumů od 30. let 20. století má každý exemplář jedinečný vzor duhovky, který je téměř nemožné statisticky reprodukovat. Výsledkem je inherentní výhoda zabezpečení dat, protože snižuje počet falešných poplachů a umožňuje individuální párování. (Choi, 2022)

Technologie rozpoznávání duhovky snímá duhovku pomocí viditelného nebo blízkého infračerveného světla z kamery, která pak zkoumá přibližně 240 různých vzorů a znaků. Pro identifikaci nebo ověření jsou data převedena do modelu, což jsou matematické informace, které poskytují specifické informace o duhovce. (Choi, 2022)

Přestože se jedná o datově náročnou biometrii s menším počtem falešných poplachů než jiné metody, detekci duhovky lze oklamat prezentačním útokem pomocí vysoce kvalitní fotografie zaznamenané duhovky. Vzor může být pozměněn nekvalitním skenerem, posunem fotografie nebo zkreslením vlivem špatného osvětlení při psaní, což znesnadňuje další použití. Její implementace je však často nákladnější než jiné biometrické metody, jako jsou otisky prstů. (Choi, 2022)

Rozpoznávání rukopisu

Schopnost počítačů a mobilních zařízení přijímat a chápat ručně psaný vstup se nazývá rozpoznávání rukopisu (HWR). Možné jsou jak offline (papírové doklady, fotografie atd.), tak online účtenky (naskenované např. z pohybu pera speciálním digitizérem). Systém rozpoznávání rukopisu navíc zahrnuje formátování, segmentaci znaků a trénování jazykového modelu, který se učí tvořit srozumitelná slova a věty. (Baheti, 2022)

Nejlepší možné úložiště dat umožňuje rozpoznávání rukopisu. Mnoho dokumentů, smluv a osobních údajů obsahuje ručně psané informace, které lze ručně převést elektronicky pomocí metod HWR, jako jsou originální podpisy nebo poznámky. (Baheti, 2022)

Ve srovnání s fyzickým úložištěm souborů zabírají elektronická data méně fyzického prostoru a méně finančních prostředků. To šetří peníze a eliminuje potřebu ručního prosévání papírových dokumentů, aby byly nalezeny potřebné informace. (Baheti, 2022)

HWR lze využít ve formě formuláře, daňových dokladů a historie událostí. V pojišťovnictví a bankovnictví digitalizovány pomocí e-PDF a ověřování podpisů. Poskytovatelé zdravotní péče používají elektronické zdravotní záznamy a další opatření týkající se digitálních dat, aby zabránili chybám způsobeným nečitelnými recepty. Logistické organizace využívají technologie HWR ke skenování nákladních listů a třídění balíků na základě rozpoznávání štítků. (Baheti, 2022)

3.2 Instant messaging

IM je textová forma komunikace, kde se dva uživatelé počítačů nebo mobilních telefonů účastní jedné online konverzace. IM se odlišuje od "chatovací místnosti", kde uživatel vstupuje do otevřenější konverzace v reálném čase v chatovací místnosti, a všichni ostatní uživatelé kanálu vidí vše, co je řečeno. (Larson, 2023)

Ve své nejjednodušší podobě má IM za cíl dosáhnout dvou cílů: odesílání zpráv a sledování přítomnosti za účelem poskytování upozornění na základě přítomnosti uživatelům chatu. Program používá centrální server nebo servery ke sledování docházky. Systém rychlých zpráv detekuje přihlášení uživatele a upozorní ostatní uživatele sítě, kteří mají tuto adresu zadanou jako „kamaráda“ nebo „přítele“. Uživatelé mohou mezi sebou komunikovat synchronně a v reálném čase díky programu, který mezi nimi buduje přímé spojení. Přestože zasílání rychlých zpráv IM má dlouhou historii, aplikace pro rychlé zasílání zpráv se staly

populárními až koncem 90. let. 20. století v důsledku neustálých konfliktů mezi firmami podílejícími se na jejich rozvoji. (Larson, 2023)

3.3 Historie instant messagingu

IM se zrodila v roce 1971 jako chatovací místnost vládní počítačové sítě. Americký vědec v oblasti informačních technologií Murray Turoff vyvinul IM pro Agenturu nouzové připravenosti jako součást Emergency Management Information Systems and Reference Index (EMISARI). Jeho původním účelem bylo usnadnit výměnu informací, které by byly užitečné pro americkou vládu během krize. Jednou z prvních aplikací systému EMISARI bylo zlepšit mezi agenturní komunikaci na podporu úsilí Nixonovy administrativy zajistit protiinflační kontrolu mezd a cen. Uživatelé systému EMISARI používali pro přístup do systému terminály psacího stroje připojené k sálovému počítači. Až do roku 1986 používala americká vláda systém EMISARI ke zvládání mimořádných událostí. Party Line, chatovací funkce systému EMISARI, byla původně vytvořena jako náhrada telefonu. (Larson, 2023)

První veřejný chatovací software se objevil v 70. letech 20. století. Aby uživatelé mohli používat „Talk“, museli se přihlásit ke stejnému počítači, který byl vytvořen pro operační systém UNIX. Vzhledem k tomu, že uživatelé mohli posílat zprávy libovolnému uživateli v systému a zpráva se objevovala na terminálu uživatele, byl to vlastně předchůdce systémů pro rychlé zasílání zpráv. Tento program byl často kombinován s nástrojem „Finger“, který uživatelům umožňoval zjistit, zda je ten či onen uživatel online. (Larson, 2023)

America Online byla vydavatelem první velké IM publikace (AOL). V roce 1988 prohlížeč AOL zavedl seznamy kontaktů, které uživatelům AOL umožňovaly vědět, kdy jsou jejich přátelé, příbuzní nebo jiní známí, kteří také používají AOL, online. Po spuštění AOL Instant Messenger (AIM) v roce 1997 se tyto seznamy staly známými jako „seznamy přátel“. AIM vzkvétal a jak se internet rozšiřoval, rostla i poptávka po softwaru, který umožňoval komunikaci v reálném čase. (Larson, 2023)

V závěru 80. let byl také představen software pro skupinovou konverzaci IRC a v polovině 90. let se staly alternativní IM programy jako ICQ (nebo „I Seek You“) dostupné i uživatelům internetu, kteří nejsou AOL. ICQ bylo poprvé spuštěno v roce 1996 izraelskou společností Mirabilis, jako bezplatná služba pro zasílání zpráv. Ačkoli ICQ konkurovalo vlastnímu systému okamžitých zpráv AOL. Společnost AOL později koupil ICQ a ponechal si rozhraní ICQ. Na počátku 21. století se na internetu používalo několik platforem pro IM,

z nichž existovaly různé verze pro různé počítačové platformy (Windows, Mac OS, Linux). (Larson, 2023)

Zahrnuje se mezi ně Google Talk (také známý jako Gchat nebo Google Chat), který byl poprvé integrován do Gmailu v roce 2005, a Apple iChat, který debutoval v roce 2002 třetí edicí OS X Jaguar. Jedná se o verzi operačního systému Apple pro Mac OS X. Se zavedením MySpaceIM od MySpace v roce 2006, Facebook Chat od Facebooku v roce 2008 a Facebook Messenger v roce 2011 byly komunikační nástroje propojeny s platformami sociálních médií. (Larson, 2023)

Dílčí závěr

Teoretická část pojednává o základním pojmovém aparátu v prostředí internetu, navazující na historii anonymity. Adresy internetového protokolu spolu se soubory cookies zajišťují skrytý server a shromažďují informace o návštěvníkovi. Základem pro ochranu je heslo, využívané pro vstup do aplikace. Práce dál pokračuje plynulým přechodem do kapitoly šifrování, kde jsou základní možnosti šifrování souborů a biometrické ověřování uživatele. IM základní informace obsažené v teoretické části, fungují jako vstupní bod do problematiky řešené v praktické části, kde budou využité pro praktické účely. Analýza a komparace IM aplikací, bude pracovat s těmito informacemi, aby dovršila požadovaného závěru.

II. PRAKTICKÁ ČÁST

4 APLIKACE INSTANT MESSAGINGU

V běžném životě se komunikuje více prostřednictvím obrázků, videí, GIFŮ, emotikonů a dalších médií. Zdá se, že doby, kdy byly zprávy doručovány přes poslíčka, už jsou dávno pryč, a proto stále více lidí používá mobilní možnosti. Níže jsou uvedeny některé z nejoblíbenějších aplikací pro rychlé zasílání zpráv, které lidé používají k doplnění nebo nahrazení textových zpráv. (Moreau, 2021)

4.1 Facebook messenger

Uživatelé si mohou vytvořit speciální uživatelské jméno, pomocí kterého se v Messengeru identifikují. Protože uživatelé nejsou nuceni používat svá skutečná jména, může to poskytnout určitý stupeň anonymity. (Meta, © 2023)

End-to-end šifrování: Messenger nabízí end-to-end šifrování pro chaty, což znamená, že zprávy jsou chráněny od okamžiku, kdy opustí zařízení odesílatele, dokud se nedostanou do zařízení příjemce. To ztěžuje ostatním zachytit nebo číst vaši komunikaci a pomáhá to udržet konverzaci v soukromí. (Meta, © 2023)

Režim inkognito: Messenger také nabízí možnost „anonymní“, která uživatelům umožňuje vést konverzace, které nejsou uloženy na žádném zařízení ani nejsou viditelné v historii chatu. Uživatelům, kteří chtějí mít soukromý chat, může tato funkce poskytnout větší anonymitu. (Meta, © 2023)

Integrace s třetími stranami: Messenger umožňuje integraci se službami třetích stran, jako je Spotify nebo Uber, což někdy narušuje důvěrnost uživatelských dat. Tyto služby mohou shromažďovat informace o aktivitě uživatele v Messengeru a používat je pro marketingové nebo jiné účely. (Meta, © 2023)

Závěrem lze konstatovat, že Facebook Messenger svým uživatelům nabízí určitou anonymitu a soukromí, ale není zcela soukromý ani anonymní. Anonymita a soukromí uživatelů mohou být ohroženy, protože Facebook je dokáže identifikovat a shromažďovat informace o jejich online aktivitách. Pokud si uživatelé chtějí zachovat anonymitu, měli by si být vědomi omezení anonymity Facebook Messengeru a přijmout vhodná opatření na ochranu svého soukromí. (Meta, © 2023)

4.2 iMessage

Společnost Apple nabízí iMessage na svých produktech, mezi ty nejznámější zahrnuje iPhony, iPady a Macy. End-to-end šifrování v aplikaci zajišťuje důvěryhodnost a bezpečnost zpráv zasílaných mezi uživateli. To ztěžuje celkové zachycení a čtení přenášených zpráv. (Apple, © 2023)

Tím, že je možné si vytvořit účet s přezdívkou nebo pseudonymem namísto skutečného jména, zajišťuje iMessage určitou úroveň anonymity. Pro vytvoření účtu však uživatelé musí poskytnout některé osobní údaje, jako je telefonní číslo nebo e-mailová adresa. Dané informace jsou potřebné k připojení účtu iMessage k účtu Apple ID a k závěrečnému ověření uživatele. (Apple, © 2023)

Zprávy odeslané prostřednictvím služby lze navíc propojit se zařízením odesílatele, to ubírá na anonymitě. Apple může ukládat metadata, jako je IP adresa odesílatele a informace o zařízení, a na základě náležité žádosti je může sdělit orgánům činným v trestním řízení. Celkové zabezpečení je poměrně slušné, ale uživatel si vždy musí uvědomit, že není zcela anonymní. (Apple, © 2023)

4.3 WhatsApp

End-to-end šifrování je funkce poskytovaná aplikací WhatsApp pro všechny zprávy, která zajišťuje, že obsah zpráv nemůže číst nikdo jiný než odesílatel a příjemce. Toto šifrování pomáhá chránit online transakce tím, že zvyšuje anonymitu uživatelů a zajišťuje soukromí a důvěrnost. (WhatsApp, © 2023)

WhatsApp však shromažďuje některá uživatelská data, jako jsou telefonní čísla, kontaktní údaje a informace o zařízení. Tyto informace lze mimo jiné využít ke zlepšení a personalizaci uživatelského zážitku. (WhatsApp, © 2023)

WhatsApp zjevně podniká kroky k ochraně soukromí uživatelů, ačkoli tento software tají přesné techniky, které používá k anonymizaci uživatelských dat. WhatsApp například neukládá zprávy na svých serverech po jejich doručení a řídí komunikaci mezi uživateli pomocí náhodných identifikátorů, nikoli telefonních čísel. (WhatsApp, © 2023)

WhatsApp má obecně vysokou úroveň anonymity, zejména ve srovnání s jinými službami pro zasílání zpráv, které nenabízejí úplné šifrování. Protože žádná online služba nezaručuje úplnou anonymitu, měli by uživatelé vždy chránit své soukromí a osobní údaje. (WhatsApp, © 2023)

4.4 WeChat

Když si zaregistrujete účet WeChat, obdržíte uživatelské jméno spojené s vaším telefonním číslem. To znamená, že vaši přátelé vás mohou kontaktovat na WeChat a zobrazit si vaše uživatelské jméno. Lze však provést změnu na vlastní uživatelské jméno, které není spojeno s vaším telefonním číslem. Díky tomu může být aplikace více anonymní. (Wechat, © 2023)

Uživatelé aplikace WeChat mohou upravit svá nastavení ochrany osobních údajů tak, aby omezili, kdo je může kontaktovat a zobrazit informace o jejich profilu. Můžete například omezit použití své profilové fotky a přezdívky nebo ponechat své Momenty (funkce podobná News Feed na Facebooku) soukromé pro určité kontakty. Úroveň anonymity aplikace lze zvýšit změnou nastavení soukromí. (Wechat, © 2023)

WeChat umožňuje podnikům a organizacím vytvářet veřejné účty, které mohou uživatelé sledovat pro novinky a nabídky. Uživatelé mohou přestat sledovat nebo deaktivovat účty, aby si zachovali anonymitu, ale veřejné účty mají přístup k osobním informacím a ke komunikaci uživatele. (Wechat, © 2023)

Uživatelé WeChatu se mohou také připojit ke službám a aplikacím třetích stran, jako je online bankovnictví a nakupování. Tyto aplikace mohou shromažďovat a vyměňovat uživatelská data, což může ohrozit anonymitu. (Wechat, © 2023)

Celková úroveň anonymity v aplikaci se může měnit v závislosti na nastavení uživatele a způsobu používání aplikace. Existují kroky, které mohou uživatelé udělat, aby posílili svou anonymitu na WeChatu, i když služba shromažďuje údaje o uživateli a vyžaduje telefonní číslo pro vytvoření účtu. (Wechat, © 2023)

4.5 Telegram

Aplikace pro zasílání zpráv Telegram nabízí end-to-end šifrování pro ochranu uživatelské komunikace. Je také známá svým důrazem na soukromí a anonymitu, nabízí funkce jako soukromé chaty, sebezničující zprávy a možnost vytvářet anonymní kanály a skupiny. (Telegram, © 2023)

Při registraci účtu musí uživatelé poskytnout telefonní číslo pro ověření. I když to může zvýšit bezpečnost a snížit počet spamových účtů, znamená to také, že uživatelé nemohou používat platformu zcela anonymně. (Telegram, © 2023)

Uživatelé si mohou, ale nemusí, vytvořit uživatelské jméno a profilový obrázek. Když se uživatel rozhodne vytvořit profil, může se rozhodnout, zda chce, aby byl viditelný pro všechny, pouze pro jeho kontakty, nebo pro nikoho. Pokud si uživatel neudělá profil, je pro ostatní uživatele viditelný pouze jako řada čísel. (Telegram, © 2023)

Uživatelé Telegramu mají možnost vytvářet veřejné nebo soukromé skupiny a kanály. Zatímco tajné skupiny a kanály musí být připojeny prostřednictvím odkazu na pozvání, veřejné skupiny a kanály může najít kdokoli na webu. Při vytváření veřejných skupin nebo kanálů se uživatelé mohou rozhodnout odhalit svou identitu nebo zůstat v anonymitě. (Telegram, © 2023)

Telegram nabízí různé možnosti zasílání zpráv, včetně soukromých, skupinových a individuálních chat kanálů. Soukromé i skupinové chaty jsou šifrované, ale šifrovací klíče zůstávají na serveru. Na druhé straně tajné chatovací místnosti používají šifrování typu end-to-end a jsou přístupné pouze těm, kteří jsou pozváni, aby se k nim připojili. Další funkcí tajných chatovacích místností, která dále zvyšuje anonymitu, je sebezničení komunikace. (Telegram, © 2023)

Pokud uživatelé využijí nástroje ochrany osobních údajů Telegramu, jako je vytváření anonymních kanálů a používání skrytých chat kanálů, může být celková anonymita platformy vysoká. Možnost uživatelů vytvořit si uživatelské jméno a profilový obrázek a povinnost ověřit své telefonní číslo jim brání zůstat v naprosté anonymitě. (Telegram, © 2023)

4.6 Line

Hlasové hovory a videohovory, textové zprávy a nástroje sociálních médií jsou jen některé z možností, které mají uživatelé Line k dispozici. Stupeň anonymity se může lišit v závislosti na tom, jak uživatelé aplikaci používají. Line nabízí určitou ochranu soukromí, která uživatelům umožňuje chatovat, aniž by odhalili svou identitu. (Line, © 2023)

Uživatelé Line si mohou zaregistrovat anonymní účty, aniž by odhalili svou skutečnou identitu nebo jiné osobní údaje. Aplikace umožňuje uživatelům anonymně komunikovat s ostatními. Pro registraci účtu však uživatelé musí poskytnout funkční telefonní číslo, které lze za určitých podmínek použít k jejich identifikaci. (Line, © 2023)

Zprávy odeslané přes Line jsou také end-to-end šifrovány, takže je nemůže přečíst nikdo jiný než odesílatel a příjemce. Uživatelé mají zisk z vysoké úrovně soukromí a anonymity, protože nikdo jiný nevidí jejich zprávy. (Line, © 2023)

Nástroje sociálních médií společnosti Line jako Timeline a Skupiny jsou však méně soukromé. Tyto funkce umožňují uživatelům vybrat si sdílení svých skutečných jmen a profilů, což může zviditelnit jejich identitu ostatním. V podmínkách služby Line je také uvedeno, že mohou shromažďovat a sdílet uživatelská data s třetími stranami pro různé účely, včetně reklamy. (Line, © 2023)

Line obecně nabízí určité soukromí uživatelům, kteří chtějí chatovat soukromě. Úroveň anonymity se však může lišit v závislosti na tom, jak aplikaci používají. Při používání aplikace pro anonymní komunikaci je třeba vzít v úvahu zásady ochrany osobních údajů a metody shromažďování dat společnosti Line. (Line, © 2023)

4.7 Viber

Viber nabízí šifrování, ale nesmí se zapomenout, že nezaručuje úplnou anonymitu. Uživatelé aplikace si musí zaregistrovat účet s platným telefonním číslem pro identifikaci a ověření. Viber nyní může sledovat aktivitu uživatelů v aplikaci, včetně toho, s kým a jak často komunikují, a má přístup k jejich telefonním číslům. (Viber, © 2023)

End-to-end šifrování je funkce softwaru pro zasílání zpráv a volání Viber, která zajišťuje, že všechny zprávy, hovory a sdílená média jsou bezpečné a že k jejich obsahu mají přístup pouze účastníci. (Viber, © 2023)

Kromě toho Viber shromažďuje metadata, která lze použít k identifikaci uživatelů a sledování jejich online aktivity, jako je IP adresa uživatele, informace o zařízení a informace o poloze. Podle prohlášení o ochraně osobních údajů společnosti Viber může být anonymita uživatelů ohrožena, když jsou uživatelská data sdílena s přidruženými společnostmi a poskytovateli služeb třetích stran pro marketingové a reklamní účely. (Viber, © 2023)

Uživatelé by si měli uvědomit, že zatímco Viber šifruje zprávy a chaty, jejich identita a aktivity v aplikaci mohou být stále spojeny s jejich telefonním číslem a dalšími metadaty shromážděnými aplikací. (Viber, © 2023)

4.8 Signal

Aplikace nabízí end-to-end šifrování, což znamená, že jakmile jsou zprávy zašifrovány, může je dešifrovat pouze určený příjemce. Protože nikdo, včetně samotného Signalu, nemá oprávnění pro přečtení zprávy, je zajištěna vysoká úroveň anonymity. (Signal, © 2023)

Pro zachování anonymity uživatelů, Signal při registraci účtu nepožaduje od uživatele jméno, telefonní číslo ani e-mailovou adresu. Uživatelé mohou používat uživatelské jméno nebo telefonní číslo k rozpoznání mezi svými kontakty, ale dané informace jsou uložené pouze v lokální podobě na zařízení. (Signal, © 2023)

V aplikaci lze najít funkce skupinového chatu, která vyžaduje, aby jednotlivce pozval stávající člen skupiny, což může oboustranně odhalit identitu. Aby byla anonymita zachována ve skupinových chatech, má Signal k dispozici funkci automatického mazání zpráv po uplynutí nastavené doby. (Signal, © 2023)

Míra anonymity v aplikaci Signal je na velmi vysoké úrovni, a i přesto, že se řadí mezi jednu z méně známých, neměla by se podceňovat a určitě stojí za vyzkoušení. (Signal, © 2023)

4.9 Snapchat

Snapchat je známá sociální síť, která uživatelům umožňuje zveřejňovat obrázky a krátká videa, která po uplynutí nastavené doby zmizí. Software má také nástroje, které uživatelům umožňují upravovat fotografie včetně filtrů, čoček a zástupných symbolů. (Snapchat, © 2023)

Snapchat nabízí svým uživatelům určitou úroveň anonymity a soukromí. Když uživatel zveřejní fotografii, má možnost ji poslat konkrétním lidem nebo skupinám, dále má možnost ji umístit do svého příběhu, kde bude po krátkou dobu dostupná všem svým přátelům. Uživatelé však mají možnost sdílet obrázky anonymně pomocí funkce anonymního zasílání zpráv aplikace, která uživatelům umožňuje komunikovat mezi sebou, aniž by prozradili svá jména. (Snapchat, © 2023)

I když tato funkce může nabízet určitou anonymitu, je důležité si uvědomit, že Snapchat stále sleduje chování svých uživatelů online. To zahrnuje informace, jako je IP adresa uživatele, typ zařízení a informace o poloze. Prohlášení o ochraně osobních údajů Snapchatu také umožňuje aplikaci sdílet informace o uživatelích s dalšími partnery a reklamními agenturami třetích stran. (Snapchat, © 2023)

Přestože Snapchat nabízí svým uživatelům určitou anonymitu, je důležité, aby uživatelé věděli, jaké informace se shromažďují a jak je může aplikace a její partneři používat. (Snapchat, © 2023)

4.10 Instagram

Instagram umožňuje uživatelům zůstat do jisté míry, i když ne zcela, anonymní. Uživatel si může pro svůj instagramový účet vybrat vlastní uživatelské jméno, které není podmíněno jeho reálným jménem. Mají také možnost nastavit svůj profil jako soukromý, což omezuje počet lidí, kteří mohou vidět jejich příspěvky a další aktivity, na to, co povolí. (Instagram, © 2023)

Pokud se uživatel rozhodne zveřejnit svůj profil, jeho sledující, komentáře a přímé zprávy budou viditelné pro všechny uživatele platformy. Kromě toho Instagram shromažďuje informace o uživateli, jako jsou informace o zařízení a poloze. (Instagram, © 2023)

Instagram přidal několik funkcí pro zvýšení anonymity, včetně možnosti anonymně přispívat do příběhů Instagramu a posílat mizející zprávy. Je však třeba poznamenat, že tyto funkce nezaručují úplnou anonymitu, protože je lze sledovat a zpětně propojit s účtem uživatele. (Instagram, © 2023)

V důsledku toho lze míru anonymity Instagramu považovat za mírnou, přičemž uživatelé mají určitou kontrolu a anonymitu, nikoli však úplnou anonymitu. Uživatelé by si měli být vždy vědomi toho, že jejich aktivita a obsah na Instagramu mohou být propojeny s jejich účtem, a měli by přijmout vhodná opatření k zachování svého soukromí. (Instagram, © 2023)

4.11 Tik tok

Na sociální síti TikTok mohou uživatelé sdílet krátké filmy s širokou veřejností. Jak anonymní uživatelé mohou zůstat při používání sociální sítě TikTok, je určeno úrovní anonymity platformy. (TikTok, © 2023)

Uživatelé si musí vytvořit účet na sociální síti TikTok, aby mohli nahrávat videa a komunikovat s ostatními uživateli. Uživatelé mají možnost se zastupovat výběrem uživatelského jména a profilového obrázku, ale mohou si zvolit i pseudonym nebo zůstat v anonymitě. (TikTok, © 2023)

Přestože uživatelé mohou na TikToku vytvářet anonymní profily, aplikace nenabízí úplnou anonymitu. Pro vytvoření účtu musí uživatelé poskytnout e-mailovou adresu nebo telefonní

číslo, které TikTok používá k ověření identity uživatele. Aplikace také shromažďuje informace o interakcích uživatelů s ostatními uživateli a o videích, která sledují na platformě. (TikTok, © 2023)

TikTok čelil kritice kvůli shromažďování uživatelských dat a obavám o soukromí. Indie aplikaci zakázala v roce 2020 kvůli obavám o soukromí a národní bezpečnost. Podobné obavy přiměly Spojené státy, aby zvážily zákaz aplikace, ale federální soudce nakonec rozhodnutí zrušil. (Porter, 2023)

Závěrem lze konstatovat, že ačkoli TikTok umožňuje uživatelům vytvořit si anonymní identitu, stránka nadále sleduje chování uživatelů a vyžaduje určité množství osobních údajů. Uživatelé by si měli být vědomi informací shromážděných o nich pomocí této aplikace. (TikTok, © 2023)

5 KOMPARACE INSTANT MESSAGING APLIKACÍ

V rámci komparace bezpečnosti IM aplikací jsem si vybral tyto aplikace: Signal, WhatsApp, Telegram, Facebook Messenger, iMessage, Viber, Line, WeChat, TikTok, Instagram, Snapchat.

5.1 Kritéria

Při přípravě na komparaci zvolených IM aplikací, jsem si zvolil 6 důležitých kritérií, která mají za úkol rozdělit aplikace podle jejich zabezpečení a přiřadit jim potřebné bodové ohodnocení.

Šifrování End-to-End: Aplikace, které poskytují end-to-end šifrování, které zajišťuje, že obsah zprávy může číst pouze odesílatel a příjemce, jsou hodnoceny (Ano = 10, Částečně = 5, Ne = 0).

Dvoufaktorové ověřování: Aplikace, které nabízejí dvoufaktorovou autentizaci, která přidává další úroveň zabezpečení tím, že vyžaduje druhý faktor, například kód zaslaný prostřednictvím SMS nebo kód vygenerovaný autentizační aplikací, jsou hodnoceny (Ano = 10, Ne = 0).

Zásady zpracování údajů: Aplikace, které zpracovávají uživatelská data, jako je historie zpráv nebo metadata, pro určitou dobu nebo je neukládají, jsou hodnoceny (Neuchovává = 10, Uchovává se po dobu 30 dnů = 5, Uchovává si uživatelská data = 0).

Otevřený zdrojový kód: Aplikace, které poskytují otevřený zdrojový kód, umožňují vývojářům procházet kód a identifikovat potenciální bezpečnostní hrozby, jsou hodnoceny (Ano = 10, Částečně = 5, Ne = 0).

Peníze: Aplikace obsahující možnost používání úplně zadarmo nebo s poplatky, jsou hodnoceny (Zdarma = 10, Zdarma/Placené = 5, Placené = 0).

CVE: Hodnocení se odvíjí od počtu chyb, ale zároveň je kladen velký důraz na chyby, které byly velkého rázu. Pokud má aplikace více malých chyb než druhá aplikace, neznamená, že bude mít horší skóre, pokud druhá aplikace obsahovala nějaké závažné chyby. Hodnocení u této kategorie je subjektivní. (Bodové hodnocení od 0 do 10)

5.2 Bodové rozdělení

Ke každé aplikaci je potřeba rozdělit příslušné bodové ohodnocení na základě dříve zvolených kritérií.

Zásady zpracování údajů

Signal: V základním nastavení si neuchovává žádnou historii zpráv ani metadat. Je zde i možnost pro uživatele si nastavit vlastní dobu pro zmizení zpráv. (Skóre 10)

WhatsApp: Uchovává historii zpráv a metadat, pokud si je uživatelé nechtějí odstranit ručně. Aplikace taky shromažďuje určité údaje uživatelů pro marketingové a reklamní účely. (Skóre 0)

Telegram: V základním nastavení uchovává historii zpráv a metadat. Aplikace taky shromažďuje určité údaje uživatelů pro marketingové a reklamní účely. (Skóre 0)

Facebook Messenger: Uchovává historii zpráv a metadat, pokud si je uživatelé nechtějí odstranit ručně. Aplikace taky shromažďuje určité údaje uživatelů pro marketingové a reklamní účely. (Skóre 0)

iMessage: V základním nastavení uchovává historii zpráv a metadat s možností ručního mazání. Aplikace taky shromažďuje určité údaje uživatelů pro marketingové a reklamní účely. (Skóre 0)

Viber: Uchovává historii zpráv a metadat po dobu 30 dní, s možností nastavení vlastní doby mazání. (Skóre 5)

Line: V základním nastavení uchovává historii zpráv a metadat s možností ručního mazání. Aplikace taky shromažďuje určité údaje uživatelů pro marketingové a reklamní účely. (Skóre 0)

WeChat: Uchovává historii zpráv a metadat, pokud si je uživatelé nechtějí odstranit ručně. Aplikace taky shromažďuje určité údaje uživatelů pro marketingové a reklamní účely. (Skóre 0)

TikTok: V základním nastavení uchovává uživatelská data, včetně videí, zpráv a dalšího obsahu, s možností ručního mazání. Aplikace taky shromažďuje určité údaje uživatelů pro marketingové a reklamní účely. (Skóre 0)

Instagram: Uchovává uživatelská data, včetně fotografií, videí, zpráv a dalšího obsahu, s možností ručního mazání. Aplikace taky shromažďuje určité údaje uživatelů pro marketingové a reklamní účely. (Skóre 0)

Snapchat: Uchovává uživatelská data, včetně fotografií, videí, zpráv a dalšího obsahu, s možností ručního mazání. Aplikace taky shromažďuje určité údaje uživatelů pro marketingové a reklamní účely. (Skóre 0)

Dvoufaktorové ověřování

Všechny IM aplikace zahrnuté v komparaci mají dvoufaktorové ověřování, které je k dispozici, a uživatelé si ho můžou povolit v nastavení dané aplikace. (Skóre 10)

Peníze

Mezi aplikace, které jsou zadarmo jsou zařazeny: Signal, WhatsApp, Telegram, Facebook Messenger, iMessage, Viber, TikTok a Instagram. (Skóre 10)

Aplikace se základním nastavení, které je neplacené, ale nabízí možnosti placených funkcí a předplatných: Line, Snapchat a WeChat. (Skóre 5)

Otevřený zdrojový kód

Aplikace Signal a Telegram nabízí otevřený zdrojový kód, takže kdokoliv má právo a možnost si zkontrolovat kód a ověřit si, zda neobsahuje zadní vrátka nebo jiné bezpečnostní chyby. Velmi důležité pro zachování soukromí a bezpečnosti uživatelů. (Skóre 10)

WhatsApp, Facebook Messenger, iMessage, Viber, Line, WeChat, TikTok, Instagram a Snapchat nemají otevřený zdrojový kód, a tím pádem uživatel nemá možnost si ověřit bezpečnost kódu a existují zde rizika zadních vrátek nebo jiných bezpečnostních chyb. (Skóre 0)

End-to-End šifrování

Signal: Používá end-to-end šifrování pro všechny zprávy, hovory a videochaty, což zajišťuje, že daný obsah může číst nebo si zobrazit pouze odesílatel a chtěný příjemce. Signal byl také nezávisle ověřen pro zajištění bezpečného šifrování. (Skóre 10)

iMessage: Jedná se o exkluzivní službu od společnosti Apple. Veškerá komunikace mezi IOS zařízeními je šifrována. (Skóre 10)

WhatsApp: WhatsApp používá Signalizační protokol, který zajišťuje, že všechny zprávy, hovory a média sdílená ve službě jsou dobře chráněna. Na hodnocení ale má vliv vlastník Facebook, který se často dostává pod palbu kvůli svým praktikám ochrany osobních údajů. (Skóre 5)

Telegram: Šifrování je v aplikaci Telegram volitelné a nevztahuje se na všechny formy komunikace. (Skóre 5)

Viber: Nabízí plné šifrování pro všechny zprávy, hovory a média sdílená v rámci aplikace. Uživatelé však musí samotné šifrování povolit, protože ve výchozím nastavení není povolené. (Skóre 10)

Instagram: Šifrování není dostupné pro veškerou interní komunikaci. Přestože poskytuje šifrování aspoň pro některé funkce, není ani tak vždy aktivováno. Instagram navíc vlastní Facebook, který se často dostává pod palbu kvůli svým praktikám ochrany osobních údajů.

(Skóre 5)

Snapchat: Pouze určité funkce v aplikaci nabízejí end-to-end šifrování. Skupinová diskuse a otevřené příběhy nemají žádné krytí. (Skóre 5)

Facebook Messenger: Nemá šifrování ve výchozím nastavení a varianta volitelného tajného chatu podporuje pouze šifrování zpráv mezi jedním párem zařízeni. Z rodiny aplikací od společnosti Facebook se jedná o nejslabší zabezpečení. (Skóre 0)

Line: Dostupnost end-to-end šifrování není pro všechny formy komunikace. Využití funkce „skrytý chat“ dává největší smysl. (Skóre 5)

WeChat: Nemá k dispozici šifrování pro všechny komunikace, a i ty co má, nejsou ve výchozím nastavení povoleny. K tomu ji vlastní Tencent, který je známý zpronevěřováním osobních údajů. (Skóre 0)

TikTok: Aplikace pro sociální média nenabízí šifrování pro žádnou komunikaci. K tomu má světové problémy kvůli sdílení uživatelských dat s čínskými úřady. (skóre 0)

CVE od roku 2018

Signal: Má od roku 2018 zaznamenaných 5 CVE. Aplikace měla dříve drobné chyby. Společnost reagovala okamžitě, a dané problémy vždy vyřešila. (Skóre 9)

iMessage: Má od roku 2018 zaznamenaných 9 CVE. Chyby CVE byly drobného charakteru, a jejich vyřešení netrvalo dlouho. Oproti aplikaci Signal jich bylo o něco více, proto menší hodnocení. (Skóre 8)

WhatsApp: Má od roku 2018 zaznamenaných 42 CVE. Největší identifikovanou zranitelností je CVE-1019-3568, která útočníkům umožnila spustit škodlivý kód na zařízení oběti prostřednictvím jednoduchého volání v aplikaci. Tato zranitelnost byla zneužita proti aktivistům za lidská práva a novinářům. Během let se objevily další CVE, které nebyly úplně nejmenší, ale podařily se vyřešit. WhatsApp získává nejmenší možné hodnocení. (Skóre 0)

Telegram: Má od roku 2018 zaznamenaných 31 CVE. Hrozby nebyly nikdy velkého rázu a k jejich vyřešení docházelo velmi rychle. Telegram získává horší hodnocení než aplikace s menším počtem CVE zahrnující drobné chyby. (Skóre 7)

Viber: Má od roku 2018 zaznamenaných 6 CVE. V průběhu let se vyskytlo pár menších chyb v aplikaci, které ale vývojáři velmi rychle vyřešili. Viber je se svým zabezpečením na tom podobně jako aplikace iMessage, ale oproti Signalu nemá až tak propracované zabezpečení, proto získává stejné hodnocení jako aplikace iMessage. (Skóre 8)

Instagram: Má od roku 2018 zaznamenaných 8 CVE. Společnost bere zabezpečení vážně a pracuje na řešení všech zranitelností, které se mohou objevit. Hodnocení velmi dobré, ale aplikace Signal je stále lepší v daném kritérii. (Skóre 8)

Snapchat: Nemá od roku 2018 zaznamenáno žádné CVE. Podle toho zaslouženě dostává nejlepší hodnocení ze všech aplikací v daném kritérii. (Skóre 10)

Facebook Messenger: Má od roku 2018 zaznamenáno pouze 1 CVE. Nejednalo se o nijak zvlášť velkou chybu. Vývojáři pracují velmi dobře, aby nedošlo k žádným zranitelnostem v aplikaci. Hodnocení na stejné úrovni jako Signal, ne-li o něco kvalitnější, ale na bezchybnost aplikace Snapchatu to nemá. (Skóre 9)

Line: Má od roku 2018 zaznamenaných 6 CVE. Aplikace dělá velmi podobné kroky k vyřešení problémů jako Viber, a i proto je její hodnocení stejné. (Skóre 8)

WeChat: Má od roku 2018 zaznamenaných 22 CVE. Nejedná se o velké chyby, ale množství a časté opakovaní některých z nich není dobrou vizitkou pro společnost. Hodnocení velmi průměrné, je potřeba zapracovat na zabezpečení, aby nedocházelo k zranitelnostem tak často. (Skóre 5)

TikTok: Má od roku 2018 zaznamenané 4 CVE. Měl jednu větší zranitelnost CVE-2019-14319, kdy nebylo prováděné šifrování obrázků a videí. Daný problém umožňuje útočníkovi získat informace za použití odposlouchávání síťového provozu. Aplikace není perfektní, ale zároveň nelze konstatovat na základě jejího CVE, že by nebyla bezpečná, proto dostává podobné hodnocení jako WeChat. (Skóre 5)

Veškerá data v bodovém rozdělení lze dohledat v nastavení každé konkrétní aplikace s možností náhledu do internetových zdrojů použitých v analýze IM aplikací.

Tabulka 1 – Komparace IM aplikací

Instant Messaging Aplikace	End-to-End šifrování	Dvoufaktorové ověření
Signal	Ano	Ano
WhatsApp	Částečně	Ano
Telegram	Částečně	Ano
Facebook Messenger	Ne	Ano
iMessage	Ano	Ano
Viber	Ano	Ano
Line	Částečně	Ano
WeChat	Ne	Ano
TikTok	Ne	Ano
Instagram	Částečně	Ano
Snapchat	Částečně	Ano

Tabulka 1 popisuje výčet vybraných aplikací pro IM komparaci. V prvním sloupci je kritérium End-to-end šifrování, kde je uvedeno, jestli aplikace má úplné šifrování, částečné, nebo ho nepodporuje. Druhý sloupec obsahuje dvoufaktorové ověření. Všechny konkrétní aplikace ho mají k dispozici.

Tabulka 2 – Komparace IM aplikací

Aplikace IM	Otevřený zdrojový kód	Peníze	CVE	Zásady zpracování údajů
Signal	Ano	Zdarma	9	Neuchovává
WhatsApp	Ne	Zdarma	0	Uchovává
Telegram	Ano	Zdarma	7	Uchovává
Facebook Messenger	Ne	Zdarma	9	Uchovává
iMessage	Ne	Zdarma	9	Uchovává
Viber	Ne	Zdarma	8	30 dní
Line	Ne	Zdarma/Placené	8	Uchovává
WeChat	Ne	Zdarma/Placené	5	Uchovává
TikTok	Ne	Zdarma	5	Uchovává
Instagram	Ne	Zdarma	8	Uchovává
Snapchat	Ne	Zdarma/Placené	10	Uchovává

Tabulka 2 je pokračováním tabulky 1. Z tabulky 2 vyplývá, že ne všechny aplikace mají otevřený zdrojový kód. U některých aplikací, jako například Snapchat, existují 2 verze zpeněžení. Jedna z nich je dostupná zadarmo a druhá má placený plán. Třetím kritériem jsou CVE, kde už jsou zobrazena jejich závěrečná hodnocení. Posledním měřítkem jsou zásady zpracování údajů. Z možností vyplývá, že většina vybraných aplikací data zpracovává, ale jsou zde i případy s určitou dobou uchování nebo v nejlepším případě bez jakéhokoliv uchování.

Tabulka 3 – Bodové hodnocení IM aplikací

Instant Messaging Aplikace	End-to-End šifrování	Dvoufaktorové ověření
Signal	10	10
WhatsApp	5	10
Telegram	5	10
Facebook Messenger	0	10
iMessage	10	10
Viber	10	10
Line	5	10
WeChat	0	10
TikTok	0	10
Instagram	5	10
Snapchat	5	10

V tabulce 3 je bodové skóre, jaké každá aplikace dostala v daném kritérii. Bodové ohodnocení se pohybuje od 0 do 10 a z toho lze vyčíst, že Signal, iMessage a Viber si odnáší plný počet bodů z daných kritérií. Ostatní aplikace vždy nějaké body ztratily z důvodů uvedených v bodovém rozdělení práce.

Tabulka 4 – Bodové hodnocení IM aplikací

Aplikace IM	Otevřený zdrojový kód	Peníze	CVE	Zásady zpracování údajů
Signal	10	10	9	10
WhatsApp	0	10	0	0
Telegram	10	10	7	0
Facebook Messenger	0	10	9	0
iMessage	0	10	9	0
Viber	0	10	8	5
Line	0	5	8	0
WeChat	0	5	5	0
TikTok	0	10	5	0
Instagram	0	10	8	0
Snapchat	0	5	10	0

Tabulka 4 je pokračováním tabulky 3, kde jsou zobrazeny další 4 kritéria a jejich bodové ohodnocení vztahující se ke konkrétní aplikaci z tabulky 3. Nejlépe z daných kritérií vychází aplikace Signal a Telegram, které dokázaly získat nejvíce bodů z většiny kritérií, pouze u Telegramu je menší ztráta v podobě minimálního počtu bodů z kategorie zásad zpracování údajů.

Tabulka 5 – Finální skóre IM aplikací

Instant Messaging Aplikace	Finální skóre
Signal	59
WhatsApp	25
Telegram	42
Facebook Messenger	29
iMessage	39
Viber	43
Line	28
Wechat	20
TikTok	25
Instagram	33
Snapchat	30

Z tabulky 5 vyplývá, že nejlepší aplikací z IM komparace je Signal, kdy se s 59 body jedná o hladký průchod všemi kritérii. Aplikace zaznamenala pouze 1 ztrátu za CVE. Na druhém místě se umístila aplikace Viber, která si vedla o poznání hůře, ale stále se jedná o velmi slušný výsledek. Její hlavní slabinou je uzavřený zdrojový kód a 30denní uchovávání údajů. V rámci CVE kategorie neměla žádný velký problém, ale i malé chyby ji stály pár bodů. Na třetím místě se umístila aplikace Telegram z důvodu částečného šifrování a uchovávání údajů. Kategorie CVE rozhodla o její finální pozici, z důvodu většího počtu menších chyb než Viber, si odnesla o 1 bod méně. Za zmínku stojí i aplikace od společnosti Apple iMessage, která bodově ztratila pouze 3 body na třetí pozici a z hlediska zabezpečení je stále velmi slušná. Ostatní aplikace jako Facebook Messenger, Line, Instagram a Snapchat většinou dopadly průměrně a z pohledu bezpečí a anonymity se nejedná o žádnou výhru. Nejhůře však dopadla aplikace WeChat, kdy její bodové ohodnocení bylo napříč všemi kategoriemi velmi špatné. S o kousek lepším výsledkem skončily aplikace TikTok a WhatsApp, ale i u nich se dá konstatovat, že mají velmi slabé zabezpečení a podporu anonymity.

5.3 Návrh bezpečné formy komunikace

V dnešní době vytvoření bezpečného a anonymního způsobu komunikace v mobilních aplikacích je zásadní. Většina informací je sdílena veřejně a určitého soukromí začíná být čím dál těžší dosáhnout. Proto pro zajištění důvěrnosti, integrity a správnosti přenášených dat je nutné při návrhu bezpečné formy komunikace pro mobilní aplikace kombinovat několik taktik.

Základem při online komunikaci je, aby nedošlo ke sdílení osobních údajů, které by vás mohly identifikovat. To zahrnuje vaše jméno a příjmení, adresu nebo místo, kde se nacházíte, telefonní číslo a veškeré další osobní údaje. Je potřeba být opatrný při sdílení informací zejména s cizími lidmi.

Využívání pseudonymu: Při online konverzaci je nejlepší používat vlastní přezdívku nebo krycí jméno. Tento způsob napomáhá chránit identitu a dělá sledování vaší online aktivity těžší.

Dvoufaktorové ověření: Abyste zajistili, že k aplikaci budou mít přístup pouze oprávnění uživatelé, je potřeba využít dvoufaktorového ověřování. To může zahrnovat jak heslo, tak biometrické ověřování (jako je otisk prstu nebo rozpoznávání obličeje). Jejich kombinace se odvíjí od uživatelské preference, ale zároveň i od aplikace, která poskytuje tyto možnosti.

Správce hesel: Ochrana vašich účtů vyžaduje velmi silná hesla. Chcete-li si usnadnit vytváření a správu silných hesel, zvažte vyzkoušet známé správce hesel, jako jsou LastPass nebo 1Password. Není potřeba si dále pamatovat složitá hesla, jelikož tyto programy je vytvářejí a ukládají za vás. Je potřeba dát si pouze pozor na to, aby se do vašeho programu nemohl dostat kdokoliv jen tak po přihlášení do vašeho počítače.

Šifrování: Jedním z neúčinnějších bezpečnostních opatřeních v rámci komunikace je šifrování. Vaše zprávy jsou zakódované, tím pádem je může dešifrovat pouze konkrétní příjemce, kterému dané zprávy byly poslány. Implementování vypršení platnosti zprávy tak, aby byly zprávy smazány okamžitě po zadané době, snižuje pravděpodobnost, že se někdy nechtěná osoba dostane k soukromým informacím.

Aktualizace softwaru: Mezi základní věc, která ohrožuje účty a zařízení lze zařadit zastaralý software. Je potřeba se vždy ujistit, že váš operační systém, aplikace a antivirový software jsou aktuální, protože pokud nejsou, můžou se začít objevovat mezery v zabezpečení, a to může mít za následek možný útok hackera.

Veřejné sítě Wi-Fi: Při online komunikaci není dobré používat veřejnou Wi-Fi. Tyto sítě nemají často žádné zabezpečení, což znamená že vaše konverzace může odposlouchávat úplně kdokoliv. Pokud je opravdu potřeba používat veřejnou Wi-Fi, není nic lepšího něž využít VPN (virtuální soukromou síť) nebo prohlížeč s anonymním režimem.

Phishingové podvody: Klasickou metodou využívanou kyberzločinci pro získání osobních údajů je phishingový podvod. Hlavní je si dát pozor na nevyžádané e-maily, textové zprávy nebo telefonní hovory, které vyzívají ke kliknutí na určitý odkaz, a tam od vás získají osobní informace bez vašeho vědomí.

Ve zkratce lze konstatovat, že vytvoření bezpečného způsobu komunikace při zachování anonymity v online prostředí vyžaduje mnohostrannou strategii. Soukromí a bezpečnost lze zvýšit pomocí šifrování, dvoufaktorového ověřování, minimalizace zveřejňování osobních údajů, používání pseudonymů, vyhýbání se veřejným Wi-Fi, implementace anonymních platebních metod a celková opatrnost před phishingovými podvody.

Doporučením z této práce je používání aplikace Signal. Mezi její hlavní výhody pro zachování anonymity a bezpečnosti uživatele jsou důležité systémy. Signal má k dispozici nejmodernější šifrovací protokol Signal Protocol, který zabezpečuje obsah zpráv, hovorů nebo přenosů souborů. Přístup k daným souborům nemá ani samotná společnost Signal. Další výhodou je, že Signal nespadá pod žádného giganta v oboru technologických společností. Jedná se o neziskovou organizaci podporovanou garanty a finančními příspěvky od běžných lidí. V aplikaci se nenachází žádné reklamy ani marketingové spolupráce, tím pádem nejsou lidem vnucovány žádné produkty, které by mohly být případnou hrozbou.

Aplikace dále podporuje dvoufaktorové ověření a její otevřený zdrojový kód dovolující uživateli si zkontrolovat, zda aplikace neobsahuje žádné skryté bezpečnostní chyby. V historii aplikace nebyly nalezeny ani žádné velké CVE případy a u těch pár menších se nejednalo o nebezpečí pro uživatele, a jejich následné vyřešení trvalo krátkou dobu. V celkovém obalu má Signal jedno z nejlepších zabezpečení na trhu a váží si anonymity svých uživatelů.

ZÁVĚR

Tato bakalářská práce obsahuje hned několik dílčích cílů, a to analyzovat míru anonymity vybraných aplikací IM. Poté rozdělit základní aplikace obsažené v této práci, a provést u nich analýzu míry anonymity. Dílčím cílem je také komparovat mezi sebou vybrané aplikace IM z pohledu zabezpečení a anonymity, navrhnout bezpečnou formu komunikace se zachováním anonymity a bezpečnosti u mobilní aplikace a zakomponovat do ní výsledky komparace s výběrem vhodné aplikace.

Na začátku práce je definován pojmový aparát a jeho základní prvky, jako jsou internet, jeho historie a vývoj, dále kyberprostor a útoky ohrožující anonymitu a bezpečnost. Poté další kapitola pojednává o anonymitě a její historii. Adresy internetového protokolu představují jedinečný číselný identifikátor pro jakékoliv zařízení nebo síť připojenou k internetu. Rozdělení těchto IP adres má své náležitosti a různě se mění podle druhu připojení. Přidání souborů cookies zaručuje identifikaci každého návštěvníka, a podle rozdělení ukládají určité informace o návštěvníkovi.

Další kapitola se zabývá šifrováním textových zpráv a dat tak, aby pomáhaly zachovat soukromí digitálních dat přenášených přes síť. End-to end šifrování zašifruje zprávy a soubory před tím, než opustí náš telefon. Plynulým přechodem pokračuje biometrickým ověřováním identity osoby. Biometrie má hned několik různých charakteristik, za pomoci, kterých může rozpoznat osobu pro ověření její identity a povolit vstup do požadovaného zařízení. Kombinací hesel a otisku prstu lze zajistit násobně vyšší ochranu před nechtěným vniknutím cizí osoby.

V praktické části se práce soustředí na zodpovězení otázek uvedených v úvodu práce. Byla provedena analýza míry anonymity vybraných aplikací IM. Jejich základní rozdělení a analýza bezpečnosti a anonymity. Všechny dané aplikace byly vloženy do tabulky, a byla u nich provedena metoda komparace, která zahrnuje 6 kritérií. Ze zvolených kritérií vyšlo, že nejlépe s anonymitou a bezpečností zachází aplikace Signal, a další v pořadí se umístily aplikace Viber a Telegram. Nejhůře si vedly aplikace Wechat a TikTok, které nezachází s osobními údaji velmi dobře a jejich zabezpečení není na požadované úrovni. V závěru byl proveden návrh bezpečné formy komunikace v prostředí mobilní aplikace. Návrh bral ohled na výsledek komparace a doporučuje využití aplikace Signal s dalšími možnými bezpečnostními zabezpečeními pro ochranu osobních dat a anonymity. Cíle bakalářské práce byly naplněny a je na uživateli, aby si pečlivě vybíral, kterou aplikaci bude používat k běžné

komunikaci přes internet a mobilní zařízení. Anonymitu má každý z nás, a proto nesmí být podceněno, jak s ní aplikace IM zachází. Slepě důvěřovat, že jsme v bezpečí a v plné anonymitě, není už dnes možné, protože nikdy nevíte, kdo se dívá a má přístup k vaším osobním informacím.

SEZNAM POUŽITÉ LITERATURY

AHN, Joshua. *Educative: What are HTTP cookies? [*online]. 29. 10. 2021 [cit. 2023-04-01]. Dostupné z: https://www.educative.io/blog/http-cookies

ANDERSON, Janna a Lee RAINE. Pew Research Center: Digital Life in 2025 [online]. 11. 3. 2014 [cit. 2023-01-30]. Dostupné z: https://www.pewresearch.org/internet/2014/03/11/digital-life-in-2025/

ANDREWS, Evan. *HISTORY: Who Invented the Internet?* [online]. 28. 10. 2019 [cit. 2023-01-30]. Dostupné z: https://www.history.com/news/who-invented-the-internet

Apple: *Messages & Privacy* [online]. © 2023 [cit. 2023-04-30]. Dostupné z: https://www.apple.com/legal/privacy/data/en/messages/

ARIMETRICS: *What is internet* [online]. © 2022 [cit. 2023-01-29]. Dostupné z: https://www.arimetrics.com/en/digital-glossary/internet

Arrese, Ángel. *The evolution of anonymity in The Economist. Media History* 28, 111–124. 2022. Dostupné z: https://doi.org/10.1080/13688804.2021.1888703

BAHETI, Pragati. *V7 Labs: Handwriting Recognition: Definition, Techniques & Uses* [online]. 2. 3. 2022 [cit. 2023-04-10]. Dostupné z: https://www.v7labs.com/blog/handwriting-recognition-guide

BENNETT, Richard. *Filmora: 8 Best Voice Recognition Software for Windows, Mac, and Online* [online]. 1. 9. 2022 [cit. 2023-04-10]. Dostupné z: https://filmora.wondershare.com/audio/best-voice-recognition-software.html?psafe_param=1&gclid=Cj0KCQjwocShBhCOARIsAFVYq0iJjK8iAThDfsVftpKgnOXUkoQflGsQez--WoyYYdfuTC-RIPj-X7saAgx1EALw_wcB

BERLOVE, Orlee. *PREVEIL: What is end-to-end encryption & how does it work?* [online]. 31. 12. 2022 [cit. 2023-04-20]. Dostupné z: https://www.preveil.com/blog/end-to-end-encryption/

BLITZ, Matt. *Popular Mechanics: What Will the Future of the Internet Look Like?* [online]. 30. 9. 2021 [cit. 2023-01-30]. Dostupné z: https://www.popularmechanics.com/technology/infrastructure/a29666802/future-of-the-internet/

ČESKO: *Zákon č. 110/2019 Sb., Zákon o zpracování osobních údajů* [online]. 2019 [cit. 2023-04-20]. Dostupné z: https://www.zakonyprolidi.cz/cs/2019-110

ČESKO: *Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů* [online]. 2014 [cit. 2023-04-20]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

ČESKO: *Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti* [online]. 2005 [cit. 2023-04-20]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-412

ČIHÁK, Lukáš. *CDR: Co jsou cookies a proč vás s nimi každý web otravuje?* [online]. 3. 3. 2020 [cit. 2023-04-01]. Dostupné z: https://cdr.cz/clanek/co-jsou-cookies-proc-vas-s-nimi-kazdy-web-otravuje

EVANS, Lester. *Cybersecurity: what you need to know about computer and cyber security, social engineering, the internet of things + an esential guide to ethical hacking for beginners.* [USA]: [Lester Evans], [2019], 218 s. ISBN 9781794647237.

GOODNER, Stanley. *Lifewire: What Are Finger Scanners and How Do They Work?* [online]. 29. 8. 2021 [cit. 2023-04-08]. Dostupné z: https://www.lifewire.com/understanding-finger-scanners-4150464

GROOT, Juliana De. *Digital Guardian: What is Cyber Security? Definition, Best Practices & Examples* [online]. 20. 12. 2022 [cit. 2023-02-02]. Dostupné z: https://digitalguardian.com/blog/what-cyber-security

HILEY, Catherine. *Cybernews: Brief history of cybersecurity and hacking* [online]. 4. 10. 2022 [cit. 2023-03-04]. Dostupné z: https://cybernews.com/security/brief-history-of-cybersecurity-and-hacking/

CHOI, Tyler. *BIOMETRICUPDATE.COM: Iris recognition reaches the mainstream for identification, authentication* [online]. 13. 6. 2022 [cit. 2023-04-10]. Dostupné z: https://www.biometricupdate.com/202206/iris-recognition-reaches-the-mainstream-for-identification-authentication

Instagram: *Privacy Policy* [online]. © 2023 [cit. 2023-04-30]. Dostupné z: https://privacycenter.instagram.com/policy/

JAN, Kolouch. *Cybersecurity.* Edice CZ.NIC, 2019, 1 online zdroj (560 stran). ISBN 978-8088168324

JIŘÍK, Pavel. *PHONEXIA: 5 Popular Types of Biometric Authentication: Pros and Cons* [online]. 9. 9. 2021 [cit. 2023-04-07]. Dostupné z: https://www.phonexia.com/blog/5-popular-types-of-biometric-authentication-pros-and-cons/

LARSON, Gary W. *Encyclopedia Britannica: instant messaging* [online]. 20. 3. 2023 [cit. 2023-04-13]. Dostupné z: https://www.britannica.com/topic/instant-messaging

Line: *LINE Privacy Policy* [online]. © 2023 [cit. 2023-04-30]. Dostupné z: https://line.me/en/terms/policy/

LUFKIN, Bryan. *BBC Future: The reasons you can't be anonymous anymore* [online]. 29. 5. 2017 [cit. 2023-02-05]. Dostupné z: https://www.bbc.com/future/article/20170529-the-reasons-you-can-never-be-anonymous-again

MERZLIKINA, Sofia. *Ethicontrol: Anonymity – what do we know about it?* [online]. 8. 12. 2019 [cit. 2023-02-21]. Dostupné z: https://ethicontrol.com/en/blog/anonymity

Meta: *Protecting privacy and security* [online]. © 2023 [cit. 2023-04-30]. Dostupné z: https://about.meta.com/actions/protecting-privacy-and-security/?utm_source=about.facebook.com&utm_medium=redirect

MITNICK, Kevin D. a Robert VAMOSI. *The art of invinsibility: the world's most famous hacker teaches you how to be safe in the age of big brother and big data. New York: Back Bay Books, Little, Brown and Company,* 2019, x, 308 s. ISBN 9780316380522.

MOES, Tibor. SoftwareLab: *What is a Password? Types & Examples You Need to Know* [online]. 2023 [cit. 2023-04-20]. Dostupné z: https://softwarelab.org/what-is-a-password/

MOHANAKRISHNAN, Ramya. Spiceworks: *Top 11 Facial Recognition Software in 2021* [online]. 2. 9. 2021 [cit. 2023-04-07]. Dostupné z: https://www.spiceworks.com/it-security/identity-access-management/articles/facial-recognition-software/

MOREAU, Elise. *Lifewire: 9 Popular and Free Instant Messaging Apps* [online]. 11. 3. 2021 [cit. 2023-04-30]. Dostupné z: https://www.lifewire.com/popular-and-free-instant-messaging-apps-3485937

PEDAMKAR, Priya. *Software Development Basics: What is Email?* [online]. © 2023 [cit. 2023-04-20]. Dostupné z: https://www.educba.com/what-is-email/

PORTER, Jon. *The Verge: TikTok ban: all the news on attempts to ban the video platform* [online]. 18. 4. 2023 [cit. 2023-04-30]. Dostupné z: https://www.theverge.com/23651507/tiktok-ban-us-news

PRATT, Marry K. *TechTarget: cyber attack* [online]. © 2022 [cit. 2023-02-02]. Dostupné z: https://www.techtarget.com/searchsecurity/definition/cyber-attack

RAFTER, Dan. Norton: *What is encryption and how does it protect your data?* [online]. 15. 3. 2022 [cit. 2023-04-20]. Dostupné z: https://us.norton.com/blog/privacy/what-is-encryption

RANGER, Steve. ZDNET: *What is the IoT? Everything you need to know about the Internet of Things right now* [online]. 3. 2. 2020 [cit. 2023-03-08]. Dostupné z: https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/

SCHROER, Alyssa a Ellen GLOVER. *Builtin: Artificial Intelligence* [online]. 19. 9. 2022 [cit. 2023-02-01]. Dostupné z: https://builtin.com/artificial-intelligence

Signal: *Signal Terms & Privacy Policy* [online]. © 2023 [cit. 2023-04-30]. Dostupné z: https://signal.org/legal/

Snapchat: *Privacy Policy* [online]. © 2023 [cit. 2023-04-30]. Dostupné z: https://values.snap.com/privacy/privacy-policy

Telegram: *Telegram Privacy Policy* [online]. © 2023 [cit. 2023-04-30]. Dostupné z: https://telegram.org/privacy?setln=fa

TikTok: *Zásady ochrany osobních údajů* [online]. © 2023 [cit. 2023-04-30]. Dostupné z: https://www.tiktok.com/legal/page/eea/privacy-policy/cs-CZ

Viber: *Viber Privacy Policy* [online]. © 2023 [cit. 2023-04-30]. Dostupné z: https://www.viber.com/en/terms/viber-privacy-policy/

Wechat: *WECHAT PRIVACY POLICY* [online]. © 2023 [cit. 2023-04-30]. Dostupné z: https://www.wechat.com/en/privacy_policy.html

WhatsApp: *WhatsApp Privacy Policy* [online]. © 2023 [cit. 2023-04-30]. Dostupné z: https://www.whatsapp.com/legal/privacy-policy/?lang=en

WILLIAMS, Lawrence. *GURU99: Types of IP Address in Computer Network: What is & Full Form* [online]. 25. 3. 2023 [cit. 2023-03-31]. Dostupné z: https://www.guru99.com/types-of-ip-addresses.html

YASAR, Kinza. *TechTarget: IP address (Internet Protocol address)* [online]. 2023 [cit. 2023-03-31]. Dostupné z: https://www.techtarget.com/whatis/definition/IP-address-Internet-Protocol-Address

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AIM – AOL Instant messeging

BIS – Bezpečnostní informační služba

CVE – Common vulnerabilities and exposures

FRS – Facial recognition software

GPG – GNU Privacy Guard

HTTP – Hypertext Transfer Protocol

HWR – Handwriting recognition

IM – Instant messaging

IoT – Internet of Things

IP – Internet Protocol

PDF – Portable document format

PGP – Pretty Good Privacy

SMTP – Simple Mail Transfer Protocol

VPN – Virtual private network

SEZNAM TABULEK