Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Anonymita a bezpečnost na internetu

Albina Makisheva

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Albina Makisheva

Informatika

Název práce

Anonymita a bezpečnost na internetu

Název anglicky

Anonymity and security on the internet

Cíle práce

Hlavním cílem práce je porovnání způsobů ochrany svých osobních údajů před třetími osobami. V teoretické části budou vysvětleny metody ochrany, jak fungují a jejich výhody. Závěrem práce je vytvoření schématu kroků, které by měl uživatel dodržovat.

Metodika

Metodika dané práce bude založena na informaci získané z odborných informačních zdrojů a dokumentace. Vybrané způsoby ochrany budou vyhodnoceny z hlediska složitosti použití v praxi, vhodnosti v různých situacích a předpokládané úrovně bezpečnosti. Na základě získané informace bude vytvořeno schéma, které pomůže uživateli být co nejvíce opatrným a zároveň ochráněným.

Doporučený rozsah práce

50

Klíčová slova

ochrana dat, šifrování, prohlížeč, anonymita, důvěrnost

Doporučené zdroje informací

Gritzalis Stefanos. 2006. Privacy and anonymity in the digital era. ISBN 9781845449643
Paul Baka, Jeremy Schatten, Hollie Acres. 2020. SSL/TLS Under Lock and Key. Keyko books. ISBN 9780648931638
Paul C. van Oorschot. 2020. Computer Security and the Internet. Information Security and Cryptography. ISBN 9783030336486
William Pollock. Linux Basics. 2019. OccupyTheWeb. ISBN 9781593278557

Předběžný termín obhajoby

2022/23 LS – PEF

Vedoucí práce

Ing. Tomáš Vokoun

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 14. 7. 2022

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 27. 10. 2022

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 30. 11. 2023

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Anonymita a bezpečnost na internetu" jsem vypracovala samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci uvedeny v seznamu použitých zdrojů na konci práce. Jako autorka uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 30.11.2023 _____

Poděkování

Ráda bych touto cestou poděkovala Ing. Tomášovi Vokounovi za vedení této bakalářské práce.

Anonymita a bezpečnost na internetu

Abstrakt

Tato bakalářská práce se zaměřuje na bezpečnostní technologie a jejich využití v současném digitálním prostředí. Práce je rozdělena do dvou hlavních částí: teoretické a praktické.

Teoretická část obsahuje komplexní přehled o bezpečnostních technologiích, šifrovacích algoritmech a bezpečnostních funkcích prohlížečů a charakterizuje principy jejich fungování. Tato část je základem pro porozumění aspektům bezpečnosti ve digitálním světě a také pro vytvoření schématu kroků.

Praktická část této práce obsahuje porovnání šifrovacích algoritmů a bezpečnostních funkcionalit internetových prohlížečů. Cílem této části je provést porovnání a poskytnout cenné poznatky o aktuálním stavu bezpečnosti v oblasti šifrování a mechanismů prohlížečů. Jako výsledek bude vytvořeno schéma, které pomůže koncovým uživatelům zlepšit svá vlastní bezpečnostní opatření.

Klíčová slova: ochrana dat, šifrování, prohlížeč, anonymita, důvěrnost

Anonymity and security on the internet

Abstract

This bachelor's thesis focuses on security technologies and their uasge in the contemporary digital environment. The work is divided into two main parts: theoretical and practical.

The theoretical part contains a comprehensive overview of the security technologies, encryption algorithms and security features of browsers and characterize the principles of their operation. This section is a foundation for understanding aspects of security in the digital world and schema of steps creation.

The practical part of this work contains a comparison of encryption algorithms and security functionalities in internet browsers. The aim of this section is to compare and provide valuable insights into the current state of security regarding encryption and browser mechanisms. As the result schema will be created to assist end-users in enhancing their own security measures.

Keywords: data protection, encryption, browser, anonymity, confidentiality

Obsah

1 Úvod 10

2 Cíl práce a metodika 11

2.1 Cíl 11

2.2 Metodika 11

3 Teoretická východiska 12

3.1 Anonymita 12

3.2 Kryptografie 13

3.2.1 Šifrování 13

3.2.2 Algoritmy 15

3.3 Síťový model 18

3.3.1 TCP/IP model 18

3.3.2 Úroveň datového kanálu 21

3.3.3 Síťová vrstva 24

3.3.4 Transportní úroveň 27

3.3.5 Úroveň aplikace 28

3.4 Anonymní prohlížení 30

3.4.1 Směrovací řešení 31

3.4.2 Prohlížeče 33

Tor Browser 33

4 Vlastní práce 37

4.1 Porovnání algoritmů 37

4.2 Porovnání Linken Sphere a Tor 43

4.2.1 BeEF 43

4.2.2 Sběr dat 43

4.2.3 Safari 44

4.2.4 Tor 46

4.2.5 Linken Sphere 48

4.2.6 Porovnání Linken Sphere a Tor 49

4.3 Schéma kroků 50

4.4 Závěr 52

5 Seznam zdrojů 54

6 Přílohy 56

Seznam tabulek 56

Použité zkratky 57

1 Úvod

V dnešní době roste problém bezpečnosti a anonymity uživatelů na internetu. Internetová komunita se rychle mění a vyvíjí, protože firmy, lidi a služby přecházejí do online komunikace. Většina lidí nechápe důležitost ohleduplného využití světové sítě, ochrany své virtuální stopy a své osobní informace. Bezohlední lidé mohou využít naivity ostatních a vytvářet problémy.

Anonymita je navíc důležitým prvkem práva na svobodu sdružování a shromažďování online a práva na osvobození od diskriminace. Relativní anonymita, kterou internet nabízí, umožňuje se jednotlivcům a menšinovým skupinám sdružovat v citlivých záležitostech, jako je sexuální orientace nebo náboženství. Soukromí poskytuje lidem příznivé prostředí pro vytváření vztahů a hledání podpory pro jejich problémy, které mají sociální stigma.

Svoboda projevu a anonymita byly vždy důležitými společenskými otázkami v reálném světě. Tyto problémy jsou stále důležité, protože více lidí objevuje digitální svět a v této nové společnosti potřebují soukromí. V posledních letech probíhá mezi uživateli internetu intenzivní diskuse ohledně otázky, zda by měla být zachována anonymita online. První část lidí se podobných technologií vzdává kvůli snazší a nelegální možnosti prodeje drog, hrozbě terorismu a nelegálním informacím. Druhá část nechce být kontrolována a sledována vládou a ostatními uživateli. Bez ohledu na stranu, je zřejmé, že technologie pro anonymitu je snadno dostupná. A v této bakalářské práci bude probráno, jaké způsoby existují a jak fungují.

2 Cíl práce a metodika

2.1 Cíl

Hlavním cílem práce je porovnání způsobů ochrany svých osobních údajů před třetími osobami. V teoretické části budou vysvětleny metody ochrany, jak fungují a jejich výhody. Závěrem práce je vytvoření schématu kroků, které by měl uživatel dodržovat.

2.2 Metodika

Metodika dané práce bude založena na informaci získané z odborných informačních zdrojů a dokumentace. Vybrané způsoby ochrany budou vyhodnoceny z hlediska složitosti použití v praxi, vhodnosti v různých situacích a předpokládané úrovně bezpečnosti. Na základě získané informace bude vytvořeno schéma, které pomůže uživateli být co nejvíce opatrným a zároveň ochráněným.

3 Teoretická východiska

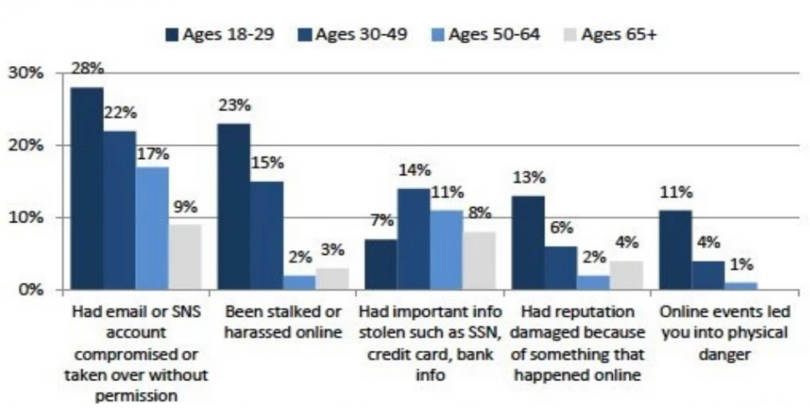
3.1 Anonymita

Anonymita na internetu lze charakterizovat jako formu jednání a komunikace, v rámci které není užíváno nebo explicitně prezentováno skutečné jméno nebo identita. Zahrnuje též praktiky, které mají za cíl ochranu před odhalením jména či identity, například využití falešného jména, jež není spojeno s legální nebo běžnou identitou.

Podle průzkumu provedeného Pew Research Center's Internet & American Life Project Survey v roce 2013 uplatňuje většina uživatelů internetu různá opatření k zajištění své anonymity online [1]:

- 86 % uživatelů internetu podniklo kroky k odstranění nebo maskování svých digitálních stop, od vymazání souborů cookie po šifrování e-mailů, přes vyhýbání se používání svého jména až po využívání virtuálních sítí, které zakrývají jejich internetovou adresu.
- 55 % uživatelů internetu přijímá opatření s cílem zabránit sledování konkrétními osobami, organizacemi nebo vládními institucemi.

Obr. 1 Statistika hrozby na internetu



Zdroj: Pew Research Center. *Anonymity, Privacy, and Security Online*. Pew Research Center [online]. 5.09.2013. Dostupné z: https://www.pewresearch.org/internet/2013/09/05/anonymity-privacy-and-security-online-2/

Nicméně mnoho uživatelů internetu zažilo komplikace (viz obr. 1) v důsledku nedostatečné bezpečnosti online. Mezi tyto komplikace patří krádež osobních údajů, únos e-mailových účtů, pronásledování, ztráta dobré pověsti nebo viktimizace podvodníky. Tato situace zdůrazňuje důležitost zvýšení povědomí o bezpečnosti online a implementaci vhodných opatření pro zachování anonymity a bezpečnosti uživatelů na internetu.

3.2 Kryptografie

3.2.1 Šifrování

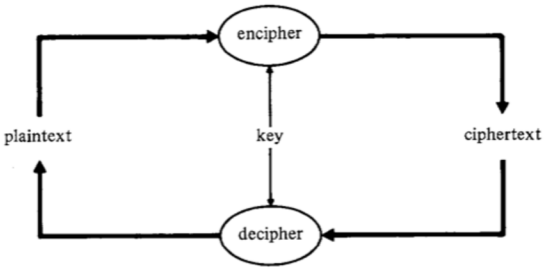
Šifrování představuje klíčový nástroj pro dosažení anonymity a zabezpečení online komunikace, "*je to matematický proces, který převádí zprávy, informace nebo data do formy, kterou je mimo zamýšleného příjemce nemožné přečíst*" [2]. Tímto způsobem se chrání důvěrnost a integrita obsahu před jakýmkoli neoprávněným přístupem či manipulací ze strany třetích stran. *„Pro provádění šifrování nezbytné tři hlavní komponenty: samotná data, matematický algoritmus a klíč, který slouží k zašifrování a dešifrování dat“* [3] (viz obr. 2).

Historie šifrování sahá hluboko do minulosti a rozděluje se do dvou klíčových období: klasické a moderní šifrování. Klasické šifrování, jako například tabulky záměn, stenografie a Vigenèrova šifra, má své místo v historii, ale trpí nedostatečnou odolností vůči moderním počítačovým útokům, zejména kvůli slabším algoritmům.

Moderní šifry se dělí do dvou hlavních typů: symetrických a asymetrických. Při implementaci šifrování je klíčové pečlivě vybrat správný algoritmus, určit optimální velikost klíče, zvolit spolehlivý šifrovací software a zajistit bezpečnost klíče.

Šifrování nachází uplatnění v různých oblastech zabezpečení dat, například při autentizaci pomocí protokolů SSL/TLS, šifrování síťového provozu pomocí IPsec VPN, zabezpečení webového provozu HTTPS, šifrování e-mailů, schvalování a autorizaci či zabezpečení paměťových zařízení USB. Podrobnější informace o aplikacích šifrování budou popsány v další části této práce (viz 3.3).

Obr. 2 Šifrování a dešifrování



Symetrické šifrování

Další označení pro klasické šifrování, které přesněji vystihuje jeho algoritmus, je metoda jednoho klíče. Tato šifrovací technika se skládá z pěti základních prvků: původní text, tajný klíč, šifrovaný text, šifrovací algoritmus a dešifrovací algoritmus.

1. Původní text představuje zprávu nebo data, která jsou vstupem do šifrovacího algoritmu. Toto je zpráva, kterou chceme šifrovat.
2. Tajný klíč je speciální hodnota, která slouží jako vstup do šifrovacího algoritmu. Klíč určuje transformace, které algoritmus provádí v závislosti na něm.
3. Šifrovaný text je výsledkem šifrování původního textu pomocí šifrovacího algoritmu a tajného klíče. To je zakódovaná zpráva, která vzniká jako výstup.
4. Kódovaná zpráva je vytvořena jako výsledek šifrování. Její podoba závisí na původním textu a tajném klíči; použití dvou různých klíčů vytváří dvě odlišné šifrované zprávy.
5. Dešifrovací algoritmus pracuje opačným směrem než šifrovací algoritmus. Používá šifrovaný text a tajný klíč k obnovení původního textu.

Asymetrické šifrování

V asymetrickém šifrování je klíčový rozdíl oproti symetrickému šifrování. Zde jsou potřeba dva odlišné klíče, z nichž jeden musí být veřejně dostupný. Hlavním požadavkem je, aby bylo prakticky *„nemožné vypočítat dešifrovací klíč pouze na základě znalosti kryptografického algoritmu a veřejného klíče“* [3].

Základní kroky asymetrického šifrování jsou následující [3]:

1. **Generování klíčů**: Každý uživatel vytvoří pár klíčů, které budou použity pro šifrování a dešifrování zpráv.
2. **Veřejný a soukromý klíč:** Každý uživatel umístí jeden z klíčů do veřejného rejstříku nebo jiného veřejně přístupného místa. Toto je veřejný klíč. Druhý klíč je soukromý a uchovává se utajeně. Uživatelé mají přístup k veřejným klíčům ostatních uživatelů.
3. **Šifrování zpráv**: Pokud uživatel B chce poslat důvěrnou zprávu uživateli A, B zašifruje zprávu veřejným klíčem uživatele A.
4. **Dešifrování zpráv**: Uživatel A může obdrženou zprávu dešifrovat pomocí svého soukromého klíče. Žádný jiný příjemce nemůže zprávu dešifrovat, protože pouze A zná svůj soukromý klíč.

V tomto systému mají všichni účastníci přístup k veřejným klíčům, zatímco soukromé klíče si každý uživatel generuje lokálně. Soukromé klíče zůstávají utajeny a bezpečné, a pokud je třeba, uživatel je může kdykoliv změnit a nahradit svůj veřejný klíč novým, který bude zveřejněn. Tímto způsobem zůstává příchozí komunikace bezpečná, pokud je soukromý klíč uživatele chráněn.

Symetrické a asymetrické šifrování poskytují základní poznatky o tom, jak data mohou být zabezpečena, přičemž symetrické šifrování využívá stejný klíč pro šifrování a dešifrování, zatímco asymetrické šifrování využívá páry veřejných a privátních klíčů.

3.2.2 Algoritmy

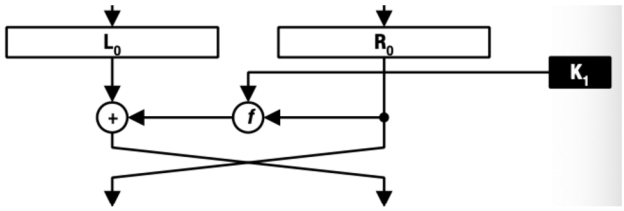
V této kapitole budou charakterizovány známé šifrovací algoritmy.

Feistelův algoritmus

Feistelova šifra je široce používaný algoritmus šifrování se symetrickým klíčem, který vychází z principu rozdělení původního textu na dvě poloviny. *„Tento algoritmus dělí proces šifrování do několika kol zpracování. Každé kolo se skládá ze dvou operací: substituce a permutace. Pravá polovina bloku prochází funkcí s aktuálním klíčem v daném*

kole, přičemž výsledek je kombinován s levou polovinou pomocí operace XOR. Tento proces se opakuje pro více kol, kde výstup z předchozího kola slouží jako vstup pro další kolo, dokud se nevytvoří konečný šifrovaný text" [16] (viz obr. 3).

Obr. 3 Postup šifru Feistelu



Zdroj: STEPHEN, Thomas, SPENCER, Marjorie, ed. SSL and TLS essentials. United States of America: John Wiley & Sons, 2000. ISBN 0-471-38354-6.

Síla Feistelovy šifry spočívá v její schopnosti reagovat na drobné změny ve vstupních datech nebo klíči, což vede k výrazným změnám ve výstupu díky permutacím a substitucím. Feistelova šifra je odolná vůči útokům, jako jsou diferenciální a lineární kryptoanalýza.

Některé populární šifrovací algoritmy využívají princip Feistelu, jako je DES (Standard šifrování dat) a 3DES (Triple DES). Feistelova šifra byla také použita jako stavební blok pro moderní šifrovací algoritmy, včetně AES a Blowfish algoritmu.

DES

Standard šifrování dat (DES) představuje Feistelovu šifru s dodatečnými počátečními a konečnými permutacemi, a byl široce používán pro bezpečnou komunikaci a ochranu dat, dokud nebyl nakonec nahrazen pokročilejším Advanced Encryption Standard (AES).

„DES pracuje na blocích dat o velikosti 64 bitů a využívá 56bitový klíč pro šifrování a dešifrování. Algoritmus se skládá ze 16 kol zpracování, přičemž každé kolo obsahuje krok substituce (s-box) a permutace (P-box). V každém kole je původní text rozdělen na levý a pravý 32bitový blok, a pravý blok je rozšířen na 48 bitů pomocí expanzní permutace. Tento rozšířený blok je následně kombinován s klíčem kola pomocí operace XOR. Výsledek prochází S-boxem, který provádí substituční operaci na 48bitovém bloku, následovanou

permutací pomocí P-boxu. Výstup P-boxu je pak kombinován s levým 32bitovým blokem pomocí operace XOR a celý proces se opakuje pro více kol" [3].

I když je DES poměrně bezpečný algoritmus, má několik omezení. Délka klíče 56 bitů je v dnešní době považována za příliš krátkou, a velikost bloku algoritmu 64 bitů zvyšuje zranitelnost vůči útokům, jako jsou útoky na šifrovaný text, útoky hrubou silou (brute-force) a další moderní kryptografické metody. Z tohoto důvodu není DES považován za bezpečný pro moderní kryptografické aplikace a byl nahrazen bezpečnějším algoritmem AES.

AES

AES představuje symetrický šifrovací algoritmus, který je široce uznávaný jako jeden z nejbezpečnějších šifrovacích standardů, které jsou v současné době k dispozici.

AES pracuje s datovými bloky o velikosti 128 bitů a využívá klíče o délkách 128, 192 nebo 256 bitů pro šifrování a dešifrování. Algoritmus se skládá z několika kol zpracování, přičemž počet kol závisí na délce klíče. *„Pro 128bitový klíč používá AES 10 kol, pro 192bitový klíč 12 kol a pro 256bitový klíč 14 kol"* [2]. V každém kole provádí AES čtyři hlavní operace na vstupním bloku: *„SubBytes, ShiftRows, MixColumns a AddRoundKey"* [3]:

1. SubBytes: Nahrazuje každý bajt vstupu odpovídajícím bajtem ze substituční tabulky zvané s-box.
2. ShiftRows: Posune bajty každého řádku vstupního bloku o určitý počet pozic.
3. MixColumns: Provádí násobení matice na sloupcích vstupního bloku.
4. AddRoundKey: Provádí operaci XOR mezi vstupním blokem a klíčem kola odvozeným od hlavního klíče.

AES je odolný vůči mnoha kryptografickým útokům, včetně diferenciální a lineární kryptoanalýzy, a je považován za *„odolný proti útokům hrubou silou"* [4]. Algoritmus je také relativně rychlý a má nízkou paměťovou náročnost, což jej činí vhodným pro použití v prostředích s omezenými zdroji.

V dnešní době je AES nejpoužívanějším šifrovacím algoritmem. Důvody zahrnují rychlost, malou paměťovou náročnost, bezpečnost, jednoduchost a vhodnost pro implementaci jak v hardwaru, tak v softwaru, a také flexibilitu v délce klíčů.

Algoritmy hrají klíčovou roli v udržování bezpečnosti na internetu tím, že šifrují komunikace a data tak, aby byla nečitelná pro neoprávněné osoby. Tím pádem se vytváří prostředí důvěry a bezpečnosti pro uživatele i organizace, což je základní kámen digitální společnosti. Zároveň umožňují algoritmy uživatelům zachovat svou anonymitu, což je klíčové pro svobodu projevu a soukromí online.

3.3 Síťový model

Pro podrobnější zkoumání metod ochrany dat na internetu je nezbytné mít pochopení internetových modelů. Tato sekce se zaměří na rozbor těchto modelů a jejich význam v souvislosti s bezpečností dat na internetu.

3.3.1 TCP/IP model

„TCP (Protokol Transmission Control Protocol) je transportní protokol, který umožňuje aplikačním programům odesílání balíčků a doručování dat v síti“ [5]. TCP organizuje data tak, aby mohla být přenášena mezi serverem a klientem. To zaručuje integritu dat přenášených přes síť. Před přenosem dat TCP vytvoří spojení mezi zdrojem a jeho cílem, což zajišťuje jeho fungování před zahájením výměny dat. Poté rozdělí velké množství dat do menších segmentů a očísluje každý segment pro identifikaci. Pak tyto segmenty odešle po síti pomocí IP, která je zodpovědná za směrování paketů do správného cíle.

Internet Protokol (IP) je primární komunikační protokol pro *„adresování a směrování pro pakety dat mezi zařízeními na internetu“* [5]. Každé zařízení má svou jedinečnou IP adresu, která umožní sdílet data s jinými zařízeními připojenými k internetu. Jeho hlavním cílem je doručit datové pakety mezi původní a cílovou aplikací nebo zařízením pomocí informací o adresách, které jsou v datových balíčkách. IP je zodpovědný za formáty a pravidla pro výměnu dat a zpráv mezi počítači v jedné nebo více sítích připojených k

internetu a za rozdělení dat na menší pakety a určení nejúčinnějšího způsobu směrování těchto paketů z jednoho zařízení do druhého v síti.

Model TCP/IP určuje, jak musí zařízení mezi nimi přenášet data, a umožňuje komunikaci přes sítě a dlouhé vzdálenosti. Model představuje, jak jsou data vyměňována a uspořádána do sítí. Je rozdělena do čtyř úrovní, které stanovují standardy pro sdílení dat a určují, jak jsou data zpracovávána a balena při doručování. Datové pakety musí před přijetím cílovým zařízením projít čtyřmi vrstvami. Poté TCP/IP prochází vrstvami v opačném pořadí, aby se zpráva vrátila do původního formátu.

Vrstvy

- **Úroveň datového kanálu**

  Určuje způsob přenosu dat, zpracovává fyzickou akci odesílání a přijímání dat a odpovídá za přenos dat mezi aplikacemi nebo zařízeními v lokální síti a za vytáčené připojení. Zahrnuje definici toho, jak by měla být data přenášena hardwarem a dalšími přenosovými zařízeními v síti, například ovladačem zařízení počítače, ethernetovým kabelem nebo bezdrátovou sítí. Tato úroveň je kombinací fyzických a datových kanálů v rámci síťového modelu OSI, který standardizuje komunikační funkce v oblasti výpočetních a telekomunikačních systémů.

  Protokoly, které působí na této úrovni, zahrnují Ethernet, token bus, token ring, FDDI a další, jako jsou SLIP (Serial Line IP Protocol) a PPP (Point-to-Point Protocol). Později budou probírány zabezpečující protokoly L2TP a využívání VPN a firewallu (viz 3.3.2).

- **Síťová vrstva**

  Je zodpovědný za odesílání balíčků ze sítě a řízení jejich pohybu po síti, aby bylo zajištěno jejich doručení do cíle. *„Poskytuje funkce a postupy pro přenos datových sekvencí mezi aplikacemi a zařízeními přes sítě“* [6].

  Na této úrovni operuje protokol IP, a v této bakalářské práci budou rozebrány bezpečnostní protokoly této vrstvy, konkrétně IPsec a IKE (viz 3.3.3).

- **Transportní úroveň**

  Je odpovědná za zajištění spolehlivého spojení dat mezi původní aplikací nebo zařízením a jejím zamýšleným účelem. *„Tato úroveň je kritická, protože zde jsou data rozdělena do paketů a číslována tak, aby vytvořila sekvenci“* [6]. Transportní úroveň stanovuje, kolik dat má být odesláno, kam má být odesláno a jakou rychlostí. Zajistí odesílání datových paketů bez chyb a důsledně získá potvrzení, že cílové zařízení obdrželo datové pakety.

  Na této úrovni působí protokol TCP a zabezpečující protokol TLS. Je důležité zdůraznit, že jsou těsně spojeny s proxy a firewally, což bude probíráno v příslušné kapitole (viz 3.3.4).

- **Úroveň aplikace**

  Odkazuje na programy, které vyžadují TCP/IP pro zajištění své komunikace. To je úroveň, se kterou uživatelé komunikují. Například, e-mailové systémy a platformy pro posílání zpráv. Kombinuje relační, prezentační a aplikační vrstvy modelu OSI.

  Zabezpečujícím protokolem této vrstvy je HTTPS, což je rozšířením protokolu HTTP. Navíc zde najdeme technologii proxy, která přidává vyšší úroveň bezpečnosti pro firewally (viz 3.3.5).

Každá vrstva modelu TCP/IP má své vlastní zranitelnosti a vektory útoků, což komplikuje identifikaci jedné vrstvy jako nejzranitelnější. Některé vrstvy mohou být však častěji cílem útoků nebo mohou mít více potenciálních zranitelností. Například aplikační vrstva bývá často zasažena útoky, jako jsou XSS (cross-site scripting) a SQL injekce. Transportní vrstva může být zranitelná vůči útokům využívajícím slabiny v protokolech TCP nebo UDP. Internetová vrstva je ohrožena IP útoky pomocí manipulace zdrojových údajů (spoofing), které zahrnují vydávání se za jinou IP adresu, aby se obešla bezpečnostní opatření nebo zahájily útoky. Datová vrstva může být náchylná k útokům, jako je zaplavení MAC, což zahrnuje zahlcení přepínače falešnými MAC adresami, aby se přemohla síť. Dalším krokem v bakalářské práci bude detailní prozkoumání protokolů na každé vrstvě.

3.3.2 Úroveň datového kanálu

L2TP

Protokol tunelování na úrovni 2 (L2TP) je protokol, který *„vytváří se tunel mezi dvěma uzly v síti a umožní přenos různých síťových protokolů skrz tento tunel“* [7]. L2TP používá bezpečnostní mechanismy, jako jsou autentizace a šifrování, k ochraně přenášených dat. L2TP může být také použit pro připojení k internetu přes poskytovatele virtuální privátní sítí (VPN).

VPN

Používání virtuální privátní sítě může být efektivním způsobem, jak udržet webový provoz relativně anonymní a bezpečný. *„VPN vytváří šifrovaný tunel mezi zařízením uživatele a vzdáleným serverem, čímž umožňuje uživateli přístup k internetu prostřednictvím IP adresy serveru místo své vlastní“* [8]. Tato technologie VPN se skládá ze tří hlavních komponent: klienta, serveru a tunelu.

1. Klient je zařízení uživatele, jako je notebook nebo smartphone, které slouží k připojení k VPN. Klient používá tunel pro šifrovanou komunikaci se vzdáleným serverem.
2. Server je vzdálený počítač, ke kterému se klient připojuje. Tento server může být umístěn v jiné zemi nebo oblasti než klient. Je odpovědný za zpracování šifrovaných dat a jejich směrování na internet.
3. Tunel je šifrované spojení mezi klientem a serverem, které umožňuje bezpečný přenos dat. Všechny data, která procházejí tímto tunelem, jsou šifrována, což zajišťuje soukromí a bezpečnost uživatelských údajů.

Existují různé typy VPN, včetně [8]:

1. **VPN pro vzdálený přístup:** Tyto VPN jsou navrženy tak, aby umožnily vzdáleným pracovníkům bezpečný přístup k podnikové síti z libovolného místa.
2. **Sítě VPN typu Site-to-Site:** Tyto VPN propojují dvě nebo více sítí dohromady, což umožňuje uživatelům přístup ke zdrojům v různých sítích, jako by byly ve stejné lokální síti.

3. **VPN bez klientů:** Tyto VPN umožňují uživatelům bezpečný přístup k webovým aplikacím nebo službám bez nutnosti instalace klientské aplikace.
4. **SSL VPN:** Tyto VPN využívají protokol SSL pro zajištění bezpečného přístupu k webovým aplikacím.

Výhody VPN jsou zřejmé: uživatelé mohou udržet svou internetovou aktivitu anonymní a zabezpečenou před sledováním. VPN také umožňují překonání omezení vlády nebo cenzorů obsahu, což umožňuje přístup k blokovaným webovým stránkám nebo obsahu. Kromě toho VPN chrání soukromí uživatelů tím, že maskují jejich skutečnou IP adresu, což komplikuje sledování jejich online aktivit třetími stranami.

Je však třeba mít na paměti, že VPN mohou zpomalit rychlost internetového připojení kvůli šifrování dat. Navíc, při výběru poskytovatele VPN je důležité být opatrný a pečlivě zvážit bezpečnost a důvěryhodnost dané služby. Bezpečnost zdarma poskytovaných VPN může být diskutabilní, protože často není jasné, kdo službu financuje a jaký má k tomu zájem. *„Internetové zařízení, ke kterému se uživatel připojí, musí zachytit IP adresu, aby mohlo úspěšně směrovat data zpět. To znamená, že kdokoli, kdo má přístup k těmto záznamům, může odhalit informace o uživateli“* [9]. Je klíčové mít na paměti, že pouze používání VPN bez bezpečnostních opatření nemusí být dostatečné k zajištění bezpečnosti uživatelských dat. Udržení anonymity je zde závislé na důvěře k poskytovateli VPN, s výjimkou případů, kdy uživatel nastaví svůj vlastní VPN server nebo použije nesting VPNs.

Firewall

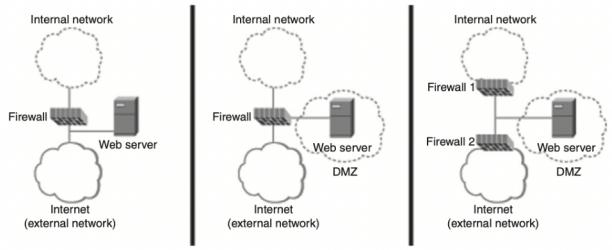
Firewally slouží jako obrana proti neoprávněnému přístupu a kybernetickým útokům. Firewall je zařízení mezi dvěma stranami pro zabezpečení sítě, které monitoruje příchozí a odchozí síťový provoz a rozhoduje, zda *„povolit nebo blokovat konkrétní provoz na základě sady předdefinovaných pravidel“* [5, 10].

Architektura firewallu obvykle zahrnuje tři hlavní komponenty: paketový filtr, stavový inspekční modul a bránu aplikační vrstvy. "*Filtr paketů je nejzákladnější komponentou, zkoumá každý paket dat, který prochází firewall, a určuje, zda by měl být povolen nebo*

blokován na základě předdefinovaných pravidel. Filtr paketů operuje na základě čísla protokolu, cílových a zdrojových IP adres a portů a TCP vlajek. Stavový inspekční modul jde o krok dále a sleduje stav každého síťového připojení, aby zajistil, že bude povolen pouze legitimní provoz. Na rozdíl od paketového filtru udržuje inspekční modul informace o předchozích IP paketech. Brána aplikační vrstvy je pokročilejší komponenta, která zkoumá obsah datových paketů za účelem identifikace a blokování konkrétních typů provozu, jako jsou malware nebo pokusy o phishing" [11]. To zvyšuje bezpečnost aplikací založených na TCP a aplikačních protokolů pro www.

Firewally lze rozdělit do dvou kategorií: hardware a software. *„Hardwarové firewally jsou samostatná zařízení umístěná mezi sítí a internetem. Softwarové firewally jsou instalovány na jednotlivých počítačích nebo serverech"* [12]. Oba typy firewallů fungují na stejných základních principech, ale hardwarové firewally jsou obvykle výkonnější a mohou chránit celou síť, zatímco softwarové firewally poskytují ochranu jednotlivým strojům. Mezi hlavní výhody hardwarové brány firewall patří zvýšená pásmo propustnosti a snížená latence. Stavové filtrování je snadnější pro softwarový firewall, který navíc v sobě zahrnuje automatické obnovování.

Obr. 4 Konfigurace DMZ



Zdroj: VACCA, John. Managing Information Security. ELSEVIER, 2009. ISBN 978-1-59749-533-2.

„Konfigurace firewallu může mít několik tvaru: demilitarizované zóny, obvodové sítě, konfigurace dvou routerů, konfigurace dual-homed. V porovnání s ostatními způsoby konfigurace, DMZs poskytuje vetší bezpečí tím, že zabraňuje uživatelům z externí sítě získání přímého přístupu k počítačům v interní síti" [13] (viz obr. 4).

Jednou z klíčových výhod firewallů je, že mohou pomoci zabránit neoprávněnému přístupu k síti. *„Zkoumáním příchozího a odchozího provozu a blokováním podezřelé aktivity mohou brány firewall zabránit útočníkům v získání přístupu k citlivým datům nebo zdrojům“* [13]. Firewally mohou také zabránit vírům, keyloggingu a útokům typu odmítnutí služby (DoS) blokováním provozu ze známých škodlivých zdrojů.
Mezi nevýhody firewallu patří potenciální ovlivnění výkonu sítě zavedením další latence a režie. Podle Glosáře internetové bezpečnosti je *"obtížnou částí definování kritérií, kterým paketům je odepřen průchod firewallem, protože firewall musí nejen udržovat neoprávněný provoz (tj., vetřelci), ale obvykle také musí nechat autorizovaný provoz projít dovnitř i ven"* [15]. Nedostatek firewallu se objevuje při používání standardních portů, jako je HTTP port 80. Útočníci je mohou obejít pomocí pokročilých technik, jako je fragmentace paketů nebo tunelování. *"Některé aplikace generují dynamické porty interně po uzavření řídicího kanálu, což ztěžuje firewallům určení portů, které budou použity pro přenos dat. V důsledku toho může být nutné trvale povolit celou řadu pomíjivých portů pro procházení firewallem. Zlepšení výkonu brány firewall lze dosáhnout minimalizací pravidel v zásadách (především pro softwarové brány firewall)"* [2].

Závěrem lze říci, že firewall poskytuji vrstvu obrany, kde dle potřeb lze nasadit komponenty v různých konfiguracích k ochraně před vnějšími a interními hrozbami. Nicméně používaná kombinace komponentů může mít svoje nedostatků. I když brány firewall zvyšují úroveň bezpečnosti, měly by být používány ve spojení s dalšími bezpečnostními opatřeními k zajištění komplexní ochrany, jako je TLS/SSL.

3.3.3 Síťová vrstva

Žádná záruka neexistuje, že přijatá data skutečně pocházejí od nárokovaných odesílatelů, jsou doručena správným adresátům, obsahují původní informace a nebyla odposlouchána, zatímco datové jednotky byly předány od odesílatelů k příjemcům. Nedostatek vnitřního zabezpečení platí zejména pro IP pakety. V důsledku toho bylo vynaloženo mnoho úsilí na zvýšení bezpečnosti přenosu dat.

Bezpečnostní protokoly zahrnují zapouzdření, což znamená, že data jsou uložena v datových jednotkách, a k datovým jednotkám jsou přidány záhlaví na různých vrstvách, které obsahují další informace. Zapouzdření dat přidává k datům informace o protokolu, aby mohl přenos dat probíhat správným způsobem, a je pohodlná a průhledná schéma přenosu informace, která obsahuje šifrovanou datu a nešifrované záhlaví, které je určeno pro směrování paketu.

IPsec architektura zahrnuje v sobě protokoly IPsec a IKE. *„Tato architektura poskytuje kryptografickou ochranu pro IP datagramy v síťových paketech IPv4 a IPv6“* [5]. Tato ochrana může zahrnovat důvěrnost, silnou integritu dat, ověřování dat a částečnou integritu sekvence. IKE a IPsec společně poskytují bezpečný a ověřený způsob komunikace po síti. *„IKE je zodpovědný za navázání zabezpečeného připojení, zatímco IPsec poskytuje šifrování a ověřování dat přenášených přes toto připojení“* [5]. IKE a IPsec se běžně používají v připojeních VPN (viz 3.3.2), která umožňují vzdáleným uživatelům bezpečně přistupovat ke zdrojům v privátní síti, jako by k ní byli přímo připojeni.

IPsec

IPsec je protokol používaný k *„zabezpečení IP komunikace šifrováním a ověřováním IP paketů mezi dvěma síťovými zařízeními“* [5], jako jsou směrovače nebo brány firewall. Na rozdíl od jiných kryptografických protokolů, jako je TLS nebo SSH, IPsec umožňuje chránit každou komunikaci založenou na IP. Zapouzdření na internetové vrstvě obsahuje proces převzetí segmentu a přidání mu záhlaví ověřování (AH) pro nastavení integrity a zapouzdření užitečného zatížení (ESP) pro důvěrnost s volitelnou integritou.

„Záhlaví ověřování poskytuje autentizaci dat, silnou integritu a ochranu proti přehrávání datagramů IP“ [8]. AH chrání větší část IP datagramu, ale přesto neposkytuje služby důvěrnosti dat. *„Zapouzdření je zodpovědné za důvěrnost dat a za částečnou důvěrnost tok dat“* [8].

Lokace AH a ESP záleží na režimu přenosu dat. *„Rozlišujeme transportní, kde je šifrována pouze datová část IP paketu, a tunelový řežím, kde je celý IP paket šifrován a zapouzdřen*

do jiného IP paketu" [5]. IPsec používá dva typy algoritmu: HMAC-MD5 a HMAC-SHA-1 pro autentizace a DES-CBC, AES-CBC a Blowfish pro šifrování.

Nicméně ani AH, ani ESP nemohou zachránit od analýzu trafiku. ESP může pomoct maximálně s částečným tok provozu, proto je důležité přistupovat ke komunikaci na síti s obezřetností a zvážit další bezpečnostní opatření k ochraně citlivých údajů.

IKE

Výměna klíčů (IKE) je protokol používaný k nastavení zabezpečeného a ověřeného komunikačního kanálu mezi dvěma stranami prostřednictvím VPN. *„IKE je zodpovědný za vyjednávání parametrů připojení, jako jsou metody šifrování a ověřování, a generování sdíleného tajného klíče používaného k šifrování a dešifrování dat"* [5]. Obvykle se používá ve spojení s protokolem IPsec.

„Protokol IKE je protokol typu požadavku a odpovědi s iniciátorem a odpovídačem" [5]. IKE definuje politiku v rámci ochranných sad s ohledem na zabezpečení komunikace. Každá sada ochrany musí definovat alespoň šifrovací algoritmus, hash algoritmus, skupinu Diffie-Hellman a metodu ověřování. IKE nejčastěji používá certifikáty x. 509 infrastrukturu veřejného klíče (PKI) pro autentizaci a protokol Diffie-Hellman pro výměnu klíčů k vytvoření sdílené tajné relace. Databáze zásad IKE je pak seznam všech ochranných sad vážených v pořadí podle preferencí.

Vytvoření IPsec SA pomocí IKE je dvoufázový proces [5]:

1. Proces vytvoření počátečního ověřeného klíčovacího materiálu mezi dvěma vrstevníky.
2. Proces vyjednávání dalších odvozených klíčů pro mnoho různých spojení založených na IP mezi těmito dvěma

Tyto protokoly jsou nezbytné pro ochranu citlivých informací přenášených po internetu. Použití IKE a IPsec je rozmanité, ať už jde o bezpečné připojení vzdálených síťových prvků, virtualizovaných prostředí nebo zabezpečení komunikace mezi koncovými zařízeními. Jejich význam spočívá v tom, že umožňují důvěrnou a bezpečnou výměnu dat mezi stranami, které nemusí být navzájem důvěřivé.

3.3.4 Transportní úroveň

SSL

Historie zabezpečení úrovně internetu se začala vyvíjet s vývojem protokolu SSL (Secure Socket Layer). SSL je součást bezpečnostní vrstvy mezi aplikační a transportní úrovní. SSL je vložen nad transportní vrstvu s TCP protokolem, protože *„nesplňují bezpečnostní požadavky pro UDP protokol“* [5]. *„SSL protokol poskytuje bezpečnost komunikaci s třemi vlastností: autentizace komunikujících stán pomocí šifrování veřejným klíčem, zabezpečení důvěryhodnosti data trafiku díky šifrování dat po handshaku a sjednáváni klice relaci, autenticitu a integritu data trafiku díky kontrole MAC“* [14].

Přesto SSL protokol nezachrání proti analýze provozu. Například zkoumáním nešifrovaných zdrojových IP adres a čísel portů TCP nebo zkoumáním objemu odeslaných dat je možné určit, jaké strany komunikují, jaké typy služeb se používají, a někdy získání informaci o pracovních nebo osobních vztazích. Dál bude řečeno o způsobu zvýšení úrovně bezpečností.

TLS

TLS (Transport Layer Security) představuje vylepšenou *“verzi SSL protokolu, využívající TCP k poskytování spolehlivých end-to-end zabezpečených služeb”* [2]. Na rozdíl od SSL je považován za bezpečnější a komplexnější. TLS je využíván k zvyšování úrovně zabezpečení a poskytuje bezpečnější prostředí pro komunikaci mezi klientem a serverem.

TLS protokol zahrnuje v sobě dvě hlavních částí: Record protokol a ostatní čtyři subprotokoly: Handshake, který je pro autentizaci klientu a serveru a pro výměnu session klíče, Change CipherSpec pro změnu šifrováni, Alert pro vysílání upozornění a data aplikaci, který je pro předávání dat přímo do Record protokolu. SSL získává data z vyšších subprotokolů a vnoří ji do kroků fragmentace, komprese a šifrování.

TLS staví na základech SSL, přináší vylepšení k zvýšení bezpečnosti. Adresuje zranitelnosti přítomné v SSL a přináší pokročilé kryptografické algoritmy. Kromě toho podporuje TLS širší škálu šifrovacích sad, což zajišťuje kompatibilitu s moderními bezpečnostními standardy

Průchod firewallem

SSL a TLS protokoly jsou založeny na end-to-end bázi, což může usnadnit kontrolu trafiku. Je šifrován HTTP provoz namísto přímého šifrování IP paketů. Proto se obvykle používá firewall. Brány firewall jsou navrženy tak, aby *„omezovaly přístup k síti nebo konkrétním službám a monitorovala aktivity v sítí“* [5]. Nicméně on může blokovat provoz v dosažení zamýšleného cíle nebo může zabránit úspěšnému dokončení SSL/TLS handshaku.

K překonání těchto problémů se obvykle používají proxy servery nebo tunelování jako man-in-the-middle. *„Tunelování zahrnuje zapouzdření provozu protokolu nebo aplikace v rámci jiného protokolu, který je povolen firewallem. Proxy zahrnuje odesílání provozu prostřednictvím proxy serveru, který může komunikovat s vnější sítí jménem protokolu nebo aplikace“* [5].

3.3.5 Úroveň aplikace

HTTPS

Bezpečnostní protokol HTTPS (Hypertext Transfer Protocol Secure over SSL) představuje zabezpečenou variantu běžného protokolu HTTP, který se používá k přenosu dat přes světový web. Oproti klasickému HTTP poskytuje HTTPs další vrstvu bezpečnosti pomocí šifrování dat mezi klientem a webovým serverem. Tento šifrovaný datový protokol, podporující různé kryptografické protokoly, vytváří bezpečný kanál komunikace mezi uživatelem a webovou stránkou.

Hlavním rozdílem, který uživatelé webových prohlížečů vidí, je začátek URL adresy. HTTP používá port 80, zatímco při použití HTTPS se využívá port 443, což vyvolává TLS. Po ověření pravosti webové stránky začíná výměna šifer, a to prostřednictvím symetrických a asymetrických klíčů. Při používání HTTPS jsou šifrovány klíčové části komunikace, včetně URL požadovaného dokumentu, obsahu hlavičky HTTP, obsahu formulářů vyplněných uživatelem, obsahu samotného dokumentu a cookies přenášené mezi prohlížečem a serverem.

Používání HTTPS má několik výhod:

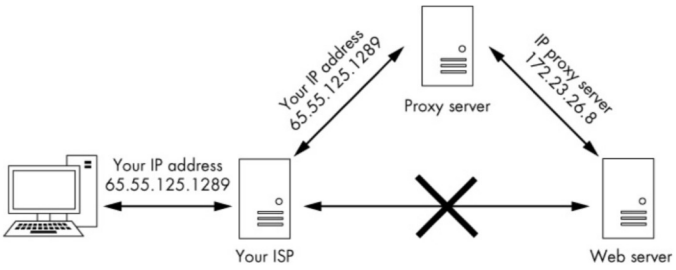
1. Důvěrnost dat: HTTPS zajišťuje, že data přenášená mezi klientem a serverem jsou šifrována a nemohou být zachycena třetími stranami.
2. Integrita dat: HTTPS zajišťuje, že data přenášená mezi klientem a serverem nebyla během přenosu upravena nebo manipulována.
3. Ověřování: HTTPS poskytuje klientovi způsob, jak ověřit identitu webového serveru, ke kterému se připojuje, a zajišťuje, že nekomunikuje s podvodníkem.
4. Vylepšené hodnocení vyhledávačů: Webové stránky používající HTTPS získávají vyšší hodnocení ve výsledcích vyhledávačů, což zvyšuje návštěvnost.

Používání HTTPS představuje klíčový krok k zajištění bezpečnosti dat na internetu. Tento protokol nejenom šifruje data, ale také zvyšuje důvěryhodnost webů a poskytuje bezpečný a spolehlivý zážitek uživatelů při prohlížení internetu. Jeho jednoduchá správa ze strany uživatele činí z HTTPS jedno z nejefektivnějších opatření pro zvýšení bezpečnosti při online komunikaci.

Proxy Server

Proxy server představuje sofistikovaný systém skládající se z hardwarových platforem a softwarových aplikací, který funguje jako prostředník v sítě, zprostředkovávající komunikaci mezi uživateli a cílovými servery. *„Když uživatel přistoupí k proxy serveru, jeho provoz je nejprve směrován na IP adresu proxy serveru. Proxy server přijímá požadavky od klienta, analyzuje je a dále je předává na cílový server, přičemž vystupuje jako klient. Když odpověď dorazí z cíle, proxy server ji přeposílá zpět ke zdroji“* [9] (viz obr. 5). Tímto způsobem je zdánlivě veškerý provoz pocházející z proxy, nikoli z původní IP adresy uživatele. Pro sledování provozu na vyšší úrovni bezpečnosti je možné použít více proxy serverů ve strategii známé jako "proxy řetězec".

Obr. 5 Komunikace při použití proxy serveru



Zdroj: OccupyTheWeb. Linux basics for hackers: getting started with networking, scripting and security in Kali. No Starch Press, Inc. 1, [2018]. ISBN 9781-593278557.

Používání proxy serveru přináší relativní jednoduchost pro uživatele, kteří si mohou službu zakoupit od poskytovatele a začít ji využívat pomocí pluginu do svého internetového prohlížeče. Další výhodou proxy serverů je možnost cachování, které uchovává informace o předchozích aktivitách, čímž zvyšuje efektivitu a rychlost přístupu.

Nicméně, proxy server se může stát nevýhodou v případě jeho kompromitace, a dodatečné posílání dat přes server může zpomalit internetový provoz. Proxy servery pracují na aplikační vrstvě pro analýzu příchozích požadavků, což jim přiděluje název "proxy aplikace". Tyto servery umožňují manipulaci s různými protokoly pomocí různých proxy serverů nebo serverů s více protokoly. Proxy servery jsou instalovány v počítačích pomocí firewall brány, která slouží jako brána pro zprostředkování sítě protokolu aplikace, a tím zvyšuje bezpečnost, jak bylo diskutováno v jedné z předchozích kapitol. Zajímavým jevem je, že proxy servery mohou být klíčovým prvkem při zajišťování bezpečnosti sítě, ale současně i potenciálním bodem zranitelnosti, který vyžaduje pečlivé řízení a monitorování. Jejich důležitost v současné době není možné podceňovat, neboť představují klíčový nástroj pro zajištění bezpečné a anonymní internetové komunikace.

3.4 Anonymní prohlížení

V této části bakalářské práci budou probrány způsoby anonymního prohlížení, které budou užitečné v další kapitole.

3.4.1 Směrovací řešení

HTTP proxy servery

HTTP proxy servery jsou servery, které fungují jako prostředníci mezi klienty a webovými servery. *„Když klient odešle požadavek na webový server, je tento požadavek nejprve odeslán na HTTP proxy server. Proxy server pak předává tento požadavek webovému serveru. Odpověď ze webového serveru je následně odeslána zpět na proxy server, který ji posílá zpět klientovi“* [9].

Používání HTTP proxy serveru nabízí několik výhod. Může například zlepšit výkon tím, že ukládá často přístupné obsahy do mezipaměti [9], čímž snižuje objem datového provozu v síti a zrychluje přístup k často navštěvovaným webům. Proxy server lze také použít k filtrování obsahu, například blokování přístupu na webové stránky, které jsou považovány za nevhodné nebo škodlivé. Při odesílání požadavků přes proxy server je IP adresa klienta skryta před webovým serverem, což může pomoci chránit soukromí a zabezpečení klienta.

Proxy servery HTTP lze nasadit v různých nastaveních, včetně podnikových sítí, veřejných hotspotů Wi-Fi a osobních zařízení. Tyto servery mohou být nakonfigurovány tak, aby poskytovaly různé úrovně zabezpečení a soukromí v závislosti na potřebách uživatele nebo organizace.

Crowds

Směrovaní Crowds představuje technologii, která slouží k posílení soukromí v rámci počítačových sítí, zajišťující anonymní komunikaci. Oproti tradiční metodě směrovaní Onion, která operuje s pevným počtem uzlů pro přenos dat, přináší směrovaní Crowds decentralizovaný přístup, který využívá široký počet náhodně vybraných uzlů. *„Každý uživatel je reprezentován procesem známým jako "jondo". Po spuštění kontaktuje tento proces server, označovaný jako "blender", a žádá o vstup do davu. Po akceptaci této žádosti informuje blender o jondově identitě, což mu umožňuje účastnit se systému. Uživatel dále nakonfiguruje jondo tak, aby fungoval jako proxy server, přičemž zadá jeho název hostitele a číslo portu do svého prohlížeče jako proxy pro všechny služby. Jakýkoli požadavek vycházející z prohlížeče je následně směrován přímo na jondo. Pro odeslání zprávy ji uživatel zašifruje a pošle do náhodné skupiny uzlů v síti. Jondo náhodně vybere*

dalšího jonda z davu (případně sám sebe) a předá mu žádost. Po obdržení žádosti jondo náhodně určí, zda ji předá dalšímu jondovi, nebo ji pošle webovému serveru, pro který byla původně určena" [5]. Každý požadavek tak putuje od prohlížeče uživatele přes řadu jondo až k webovému serveru. Další požadavky, které na stejném jondovi zahájí uživatel, budou následovat stejnou cestu, s výjimkou případu, kdy je změněn cílový webový server. Odpovědi serveru procházejí toutéž cestou jako zprávy požadavků, ale opačným směrem. Každý uzel v síti pak předá zprávu nové sadě náhodně vybraných uzlů, dokud zpráva nedosáhne svého cíle. Používání šifrování zaručuje důvěrnost obsahu zprávy.

Směrovaní Crowds nabízí několik výhod v porovnání s jinými technikami zvyšujícími soukromí. Jeho odolnost vůči určitým typům útoků, například analýze provozu, umožňuje bezpečnou komunikaci bez rizika zjištění původu zprávy, což je častý problém u jiných technik. Tento přístup je také flexibilní, protože se dokáže přizpůsobit různým síťovým nastavením a není závislý na pevném počtu uzlů, což přináší větší míru adaptability.

Onion

Směrovaní Onion představuje sofistikovanou techniku, která umožňuje uživatelům surfovat po internetu zcela anonymně. Princip fungování spočívá v tom, že *„aplikace, (tzv. iniciátor), vytváří anonymní připojení pomocí sekvence speciálních směrovačů zvaných "onion routers" namísto běžného přímého TCP připojení"* [5]. Proces spočívá v zabalení dat do více vrstev šifrování, podobně jako vrstvy cibule. Každá vrstva šifrování je odstraněna jedním z uzlů v síti, odhalující tak další vrstvu dat, dokud zpráva nedorazí ke svému původnímu cíli.

Pro využití směrovaní Onion se uživatelé připojují k síti Tor. *„Data uživatele jsou opakovaně šifrována, přičemž každá vrstva šifrování nese informace o dalším uzlu v síti, který má tuto vrstvu odstranit. Data jsou pak posílána po síti, přeskočující z uzlu na uzel, kde každý uzel odstraňuje jednu vrstvu šifrování, dokud data nedosáhnou svého cíle"* [9]. Tímto způsobem je prakticky nemožné vysledovat původ dat, protože každý uzel má informace pouze o předchozích a následujících uzlech v řetězci.

Směrovaní Onion poskytuje uživatelům řadu výhod při anonymním procházení internetem. Chrání uživatele před sledováním a cenzurou ze strany vlád a jiných subjektů. Zároveň

zabezpečuje uživatelskou identitu, protože skutečná IP adresa je skryta za vrstvami šifrování.

Prohlížeč Tor je postaven na platformě Firefox a zahrnuje dodatečné bezpečnostní prvky, jako je implicitní blokování souborů cookie a sledovačů třetích stran. Jeho významná výhoda spočívá v možnosti anonymního procházení internetem bez ohrožení soukromí uživatele.

3.4.2 Prohlížeče

Tor Browser

TOR (The Onion Router) představuje nejvýznamnější a nejoblíbenější nástroj pro dosažení anonymity na internetu. Jedná se o svobodný a otevřený software, který pracuje na principu tzv. „cibulového směrování". To znamená, že *„všechna data, která vstupují do sítě Tor, procházejí třemi náhodně vybranými uzly sítě a jsou postupně šifrována klíči těchto uzlů před odesláním"* [18]. Když první uzel obdrží balíček, dešifruje jeho horní vrstvu a zjišťuje, kam má balíček dále poslat. Stejný postup následují i druhý a třetí server. Nejzranitelnějšími místy v takovémto řetězci jsou výstupní uzly, kde je provoz konečně dešifrován a směrován ke svému cílovému zdroji. Na výstupních uzlech by mohl být provoz odposloucháván, což je důležité vzít v úvahu při připojování se k zdrojům pomocí nezabezpečených protokolů, například při návštěvě webových stránek, které nepodporují HTTPS.

Webové stránky a do nich vložená reklama jsou často využívány sledovači, kteří shromažďují různé informace o prohlížeči, jako jsou nainstalovaná písma, velikost obrazovky, operační systém, verze nebo pluginy, což umožňuje identifikaci uživatelů na webových stránkách. Tato technika je známá jako „otisky prstů". Tor Browser se snaží maskovat jedinečné informace o uživateli, například pomocí standardní sady písem, standardní velikosti okna, předstírání informací o platformě a konzistentní sady pluginů. Zatímco sledovači nemohou rozpoznat, že je používán prohlížeč Tor, uživatel se bude jevit jako kterýkoli jiný uživatel tohoto prohlížeče.

Veškerý síťový provoz je směrován přes síť Tor, anonymní síť určenou k zakrytí polohy a IP adresy. Požadavky na webové stránky, které podporují protokol HTTPS, jsou automaticky převedeny na bezpečnější protokol. Prohlížeč Tor šifruje veškerý internetový provoz pomocí protokolu HTTPS, což pomáhá zabránit odposlechu a zachycení uživatelských dat. Síť Tor poskytuje end-to-end šifrování a zajišťuje, že data jsou šifrována na každém bodě sítě.

Tor šifruje veškerá uložená data pomocí *„algoritmů AES a Diffie-Hellman. Prohlížeč nabízí připojení k internetu pomocí různých protokolů, včetně HTTP (HTTPS-proxy), SOCKS (Proxy Socks5 a Socks4), SSH (použití tunelů SSH) a samotné sítě Tor*“ [18]. Tor maskuje IP adresu, což dává dojem, že internetový provoz pochází z jiné lokality. To pomáhá chránit soukromí a komplikuje sledování online aktivity webovými stránkami a dalšími službami.

Prohlížeč Tor uplatňuje přísné *„zásady no-logging, což znamená, že neuchovává záznamy o aktivitě uživatele ani osobních informacích, neuchovává přihlašovací údaje k webovým stránkám nebo historii mezi relacemi“* [18]. To pomáhá chránit soukromí uživatelů a brání třetím stranám v přístupu k uživatelským datům.

Prohlížeč Tor zahrnuje *„doplněk NoScript, který blokuje spouštění Javascriptu a dalších potenciálně škodlivých skriptů na navštívených webových stránkách“* [18]. To pomáhá zabránit otiskům prstů prohlížeče, což je technika používaná některými webovými stránkami k identifikaci a sledování jednotlivých uživatelů na základě jejich konfigurace prohlížeče.

Kromě toho prohlížeč Tor umožňuje uživatelům posílit bezpečnost pomocí nastavení. Uživatelé s nejvyššími povolenými bezpečnostními nastaveními budou varováni při návštěvě některých webových stránek, zejména těch, které silně závisí na Javascriptu, a možná budou muset čelit omezené funkčnosti. Je pravděpodobné, že některé stránky a streamovací služby, jako je Netflix, nebudou fungovat. Interaktivní funkce, které webové stránky využívají, mohou být zakázány, aby zabránily odhalení příliš mnoho informací o uživateli.

Prohlížeč Tor také izoluje procesy v rámci prohlížeče, aby zmírnil dopad zranitelností. Každý samostatný web, který uživatel navštíví, je izolován od ostatních, takže sledovací soubory cookie nemohou sledovat uživatele při procházení, což omezuje možnost vytvořit si profil uživatele. Tyto cookies třetích stran jsou nastavovány, když provozovatel webové stránky využívá externí službu k poskytování dalších funkcí, obvykle reklam nebo analýz.

Tor je považován za relativně spolehlivý nástroj pro anonymizaci, avšak případy odhalení identity uživatelů se opakovaně vyskytly. Deanonimizace není vždy spojena se zranitelnostmi samotného Tor, často jsou využívány metody sociálního inženýrství a uživatelé sami mohou dělat chyby, o čemž bude řečeno později (viz 4.2.4).

Linken Sphere

Linken Sphere představuje webový prohlížeč, který může efektivně chránit online soukromí a anonymitu. Vývojáři využili zdrojový kód Chromia, avšak odstranili všechny funkce sledování, které jsou povolené ve standardním prohlížeči Google Chrome.

Prohlížeč pracuje v *„režimu Off-the-Record Messaging“* [19], což znamená, že na počítači nejsou ukládány žádné stopy akcí. Toto je dosaženo díky místnímu, netrvalému úložišti relací prohlížeče, což zabrání nežádoucímu přístupu k informacím a potenciálním škodlivým programům.

Linken Sphere disponuje pokročilou technologií proti detekci, která umožňuje obejít bloky webových stránek a vyhnout se detekci systémy proti podvodům a dalšími bezpečnostními opatřeními. Funkce anti-detekce pravidelně aktualizuje konfiguraci uživatele, jazyky, geolokaci a mnoho dalších parametrů, které mohou být měněny v reálném čase.

Prohlížeč obsahuje integrovanou VPN, která chrání online aktivitu šifrováním internetového připojení a směrováním přes zabezpečený server. Toto je užitečné při potřebě přístupu k webům nebo službám, které mohou být v dané oblasti blokovány, a zároveň chrání před odposlechem a dalšími formami dohledu.

Linken Sphere šifruje veškerá uložená data pomocí algoritmu AES-256, přičemž všechna data uložená na serveru jsou šifrována hashi. Prohlížeč podporuje připojení k internetu

prostřednictvím různých protokolů, včetně „*HTTP (HTTPS proxy), SOCKS (Proxy Socks5), SSH (použití tunelů SSH), TOR (použití sítě Tor), TOR + SSH (Tor + tunel) a DYNAMIC SOCKS (dynamický proxy)*“ [19].

Uživatelé mají možnost přizpůsobit každou otevřenou kartu podle svých potřeb. Linken Sphere umožňuje spravovat více online účtů a profilů z jednoho prohlížeče, což je užitečné pro přihlášení k různým účtům, jako jsou sociální média nebo e-mail, aniž by bylo nutné používat více virtuálních strojů.

Je důležité zdůraznit, že Linken Sphere byl vytvořen pro právně legitimní účely, jako jsou penetrační testy, průzkum trhu sociálních médií, výzkum klíčových slov a pro soukromé uživatele, kteří spravují více účtů najednou. Nicméně, jak již bylo uvedeno dříve, bezpečnost má dvě stránky. Historicky se kybernetičtí zločinci snažili obcházet digitální otisky prstů pomocí technologií, jako jsou virtuální stroje, proxy a servery VPN. Systémy proti podvodům se však staly dostatečně sofistikovanými, aby identifikovaly podezřelé IP adresy, i když jsou používány tyto taktiky. Proto kybernetičtí zločinci začali využívat prohlížeč Linken Sphere pro nelegitimní aktivity. Linken Sphere dynamicky mění konfigurace webového prohlížeče a generuje neomezené množství konfigurací, což jim umožňuje napodobit činnost legitimních uživatelů.

Pro uživatele představuje Linken Sphere jedno z nejbezpečnějších řešení „vše v jednom“, které značně usnadňuje mnoho každodenních úkolů. Nicméně je důležité si být vědomi toho, že ačkoliv Linken Sphere nabízí několik výhod pro ochranu soukromí a zabezpečení online, žádný prohlížeč nemůže zaručit úplnou anonymitu nebo ochranu před všemi online hrozbami. Je vždy vhodné používat vícevrstvé opatření pro zabezpečení a ochranu osobních údajů, jako jsou silná hesla, vyhýbání se veřejným Wi-Fi sítím a udržování aktuálního softwaru a operačního systému. Při sdílení osobních údajů online je rovněž důležité postupovat obezřetně a být si vědom zásad ochrany osobních údajů a postupů shromažďování údajů na webových stránkách a službách.

4 Vlastní práce

4.1 Porovnání algoritmů

Pro srovnání šifrovacích algoritmů se budou využívat znalosti o jejich základních charakteristikách, jako jsou délka klíče, algoritmická složitost, počet kroků a čas nutný pro úspěšný útok.

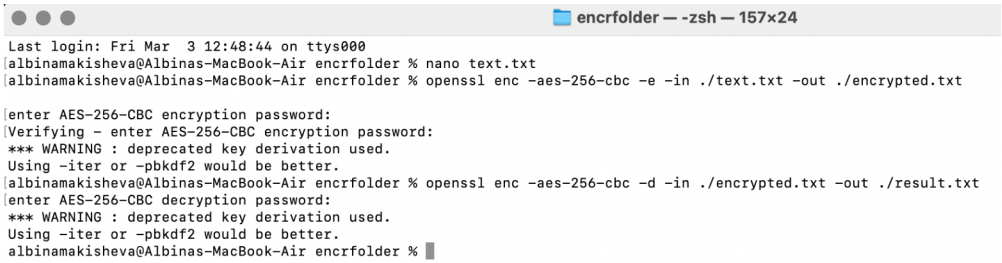
Získávání informací

1. **Implementace**

   Uživatel má na výběr z několika způsobů šifrování na MacOS a Windows OS, z nichž v této bakalářské práci budou testovány dva: pomocí terminálu a Disk Utility, případně nastavení souboru.

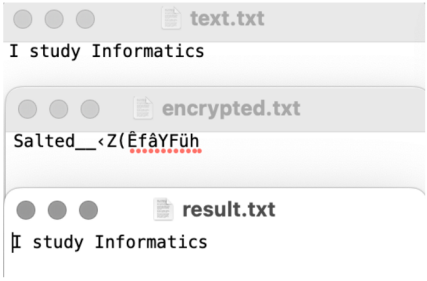
   Terminál: Tento způsob je přístupný pro každého uživatele a umožňuje nastavení cílové složky, výběr použitého šifrovacího algoritmu a určení umístění budoucího zašifrovaného souboru (viz obr. 6, 7). Nicméně je třeba poznamenat, že ovládání terminálu může být obtížné pro uživatele s omezenými technickými znalostmi.

Obr. 6 Postup šifrování a dešifrování

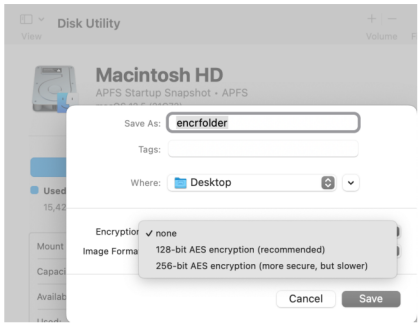


Disk Utility MacOS: Volba šifrování pomocí Disk Utility nabízí omezené možnosti, zahrnující algoritmy AES s dvěma různými délkami klíče (viz obr. 8). I přesto uživatel dostává možnost výběru mezi nejsilnějšími algoritmy šifrování.

Obr. 7 Výsledek šifrování a dešifrování DES

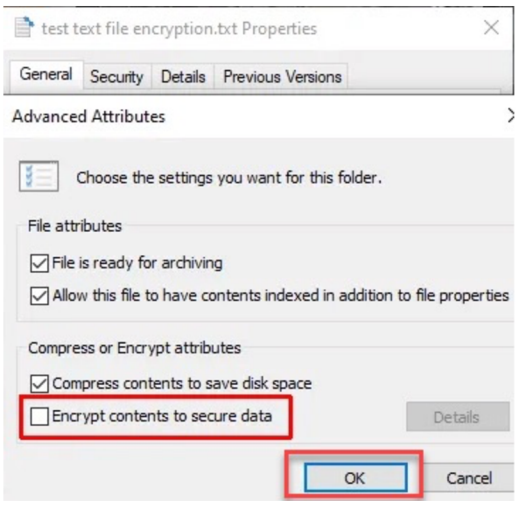


Obr. 8 Šifrování pomocí disk utilitu



Nastavení souboru v operačním systému Windows: V tomto případě je šifrování souboru relativně snadné. Stačí otevřít vlastnosti souboru a vybrat možnost šifrování (viz obr. 9). Nicméně defaultně se používá AES256 algoritmus, což je bezpečné, ale uživatel nemá možnost výběru šifrovacího algoritmu.

Obr. 9 Šifrování ve Windows OS



Na základě dostupných možností šifrování je DES hodnocen 1 bodem, DES3 získává 1 bod, zatímco AES128 a AES256 obdržely 2 body. Toto hodnocení zohledňuje dostupnost silnějších algoritmů uživatelům, kteří preferují používání Disk Utility, ačkoliv s omezeným počtem možností.

2. Složitost

DES:

Délka klíče: 56 bitů

Délka bloku: 64 bitů

Počet kol: 16

Počet alternativních klíčů: 2^56=7.2 * 10^16

Čas pro dešifrování hrubou silou [17]:

(7.2 * 10^16) / [(10.51 * 10^12) * 31536000) = (0.685 * 10^4) / 31536000 = 0.2172 roky

"Čas potřebný na 10^13 dešifrování moderním počítačem roven 1 hodině" [4].

3DES:

Délka klíče: 168 bitů (3 klíče x 56 bitů)

Délka bloku: 64 bitů

Počet kol: 48

Počet alternativních klíčů: 2^168 = 3.4 * 10^38

Čas pro dešifrování hrubou silou [17]:

(3.4 * 10^38) / ((10.51 * 10^12) * 31536000) = (0.323 * 10^26) /31536000= 1.02 * 10^18 let

AES128:

Délka klíče: 128/192/256 bitů

Délka bloku: 128/192/256 bitů

Počet kol: 10/12/14

Počet alternativních klíčů: 2^128=3.4 * 10^38

Čas pro dešifrování hrubou silou [17]:

(3.4 * 10^38) / [(10.51 * 10^12) * 31536000) = (0.323 * 10^26) / 31536000=1.02 * 10^18

"Čas potřebný na 10^13 dešifrování moderním počítačem roven 5.3 10^17 let"* [4].

AES256:

Délka klíče: 128/192/256 bitů

Délka bloku: 128/192/256 bitů

Počet kol: 10/12/14

Počet alternativních klíčů: 2^256=1.18 * 10^77

Čas pro dešifrování útokem brute-force [17]:
(1.18 * 10^77) / [(10.51 * 10^12) * 31536000) = (1.18 * 10^77) / 31536000=3.56 * 10^56

Na základě složitosti dešifrování útokem hrubou silou jsou DES ohodnocen 1 bodem, DES3 2 body, AES128 3 body a AES256 4 body. AES má mnohem vyšší odolnost vůči útokům hrubou silou díky své delší délce klíče a většímu počtu možných kombinací, což ho činí bezpečnějším pro moderní kryptografické aplikace.

3. Čas

V případě testování na konkrétním hardwaru bych použil MacBook Pro s procesorem M2, 32 GB pamětí RAM a operačním systémem Ventura OS na disku o kapacitě 994 GB. Tento konkrétní hardware poskytuje solidní výkon a dostatečný výpočetní potenciál.

Pro lepší vizualizaci rozdílu byla vytvořena složka obsahující 7 MB, a byla provedena testování rychlosti šifrování. Z výsledků (viz obr. 10) je patrné, že AES algoritmus je výrazně rychlejší. Je však důležité vzít v úvahu, že tento rozdíl v rychlosti nemusí mít zásadní vliv na celkový výkon, pokud uživatel šifruje pouze jednu malou složku. Avšak, v případě většího systému je třeba na toto dbát.

Je také důležité poznamenat, že šifrování pomocí DES nebylo možné provést úspěšně. Při pokusu o DES šifrování byla zaznamenána chyba, což ukazuje na omezení a nedostatečnou podporu tohoto algoritmu. Tento fakt podtrhuje důležitost používání

modernějších a bezpečnějších šifrovacích algoritmů, jako je AES, který byl úspěšně implementován a vykazoval výrazně lepší výsledky v testech rychlosti šifrování.

Obr. 10 Test rychlosti šifrování DES a AES

```
albinamakisheva@MacBook-Pro-2 encrfolder % time openssl enc -des -e -in ./text.txt -out ./encDES.txt

enter DES-CBC encryption password:
Verifying - enter DES-CBC encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
Error setting cipher DES-CBC
80A07DE901000000:error:0308010C:digital envelope routines:inner_evp_generic_fetch:unsupported:crypto/evp/evp_fetch
.c:341:Global default library context, Algorithm (DES-CBC : 13), Properties ()
openssl enc -des -e -in ./text.txt -out ./encDES.txt  0.01s user 0.01s system 0% cpu 9.598 total
albinamakisheva@MacBook-Pro-2 encrfolder % time openssl enc -des-ede3-cbc -e -in ./text.txt -out ./encDES3.txt
enter DES-EDE3-CBC encryption password:
Verifying - enter DES-EDE3-CBC encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
openssl enc -des-ede3-cbc -e -in ./text.txt -out ./encDES3.txt  0.25s user 0.02s system 3% cpu 6.771 total
albinamakisheva@MacBook-Pro-2 encrfolder % time openssl enc -aes-128-cbc -e -in ./text.txt -out ./encAES128.txt
enter AES-128-CBC encryption password:
Verifying - enter AES-128-CBC encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
openssl enc -aes-128-cbc -e -in ./text.txt -out ./encAES128.txt  0.01s user 0.02s system 0% cpu 6.248 total
albinamakisheva@MacBook-Pro-2 encrfolder % time openssl enc -aes-256-cbc -e -in ./text.txt -out ./encAES256.txt
enter AES-256-CBC encryption password:
Verifying - enter AES-256-CBC encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
openssl enc -aes-256-cbc -e -in ./text.txt -out ./encAES256.txt  0.02s user 0.02s system 0% cpu 4.857 total
```

Na základě rychlosti šifrování byl DES ohodnocen 0 body, DES3 získal 2 body, AES128 získal 4 body a AES256 obdržel 3 body.

4. **Odolnost vůči útokům**:

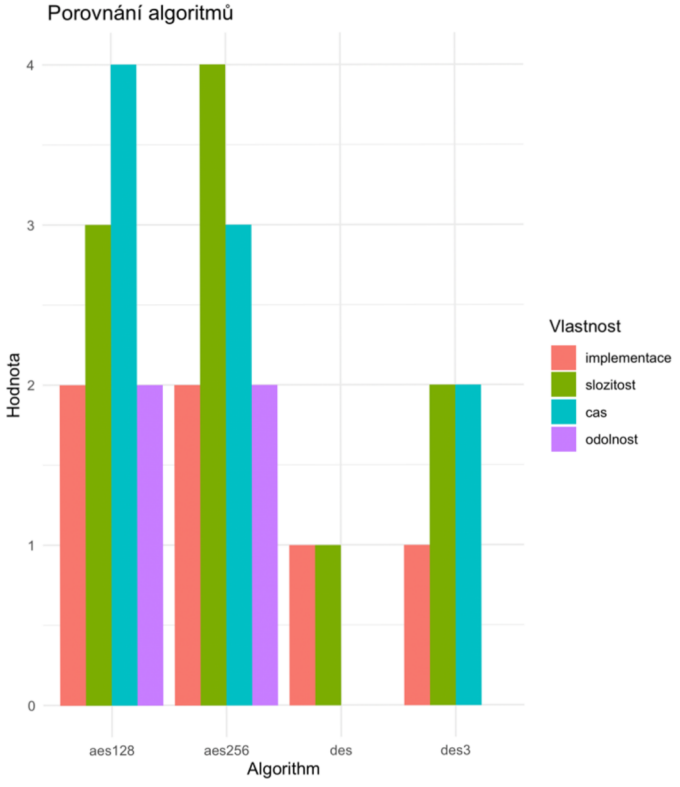
DES byl kdysi široce používaný šifrovací algoritmus, avšak kvůli své omezené délce klíče (56 bitů) se stal náchylným k moderním útokům a není dnes považován za bezpečný. Na rozdíl od DES byl AES navržen tak, aby byl odolnější proti různým útokům. *„AES používá delší klíče (128, 192 nebo 256 bitů), což zvyšuje jeho odolnost proti hrubou silou útokům a dalším kryptografickým hrozbám“* [17]. Útoky, které mohou ohrozit DES, zahrnují útoky hrubou silou, kdy útočník systematicky vyzkouší všechny možné kombinace klíčů. AES, s delšími klíči a sofistikovanějším návrhem, je mnohem odolnější vůči těmto druhům útoků. Rozdíly ve struktuře a délce klíčů mezi DES a AES přispívají k tomu, že AES je dnes považován za bezpečnější a modernější šifrovací standard pro ochranu citlivých informací.

Na základě odolnosti vůči útokům jsou DES a DES3 ohodnoceny 0 body, zatímco AES128 a AES256 obdržely 2 body.

Grafické znázornění výsledků

Pro znázornění výsledků bude použit software Rstudio (viz obr. 11).

```
> my_dataframe <- data.frame(
  alg = c("des", "des3", "aes128", "aes256"),
  implementace = c(1, 1, 2, 2),
  slozitost = c(1, 2, 3, 4),
  cas = c(0, 2, 4, 3),
 odolnost = c(0, 0, 2, 2))
> long_data <- reshape2::melt(my_dataframe, id.vars = "alg")
> ggplot(long_data, aes(x = alg, y = value, fill = variable)) +
  geom_bar(stat = "identity", position = "dodge") +
  labs(title = " Porovnání algoritmů",
       x = "Algorithm",
       y = "Hodnota",
       fill = "Vlastnost",
       color = "Vlastnost") +
  theme_minimal()
```



Obr. 11 Porovnání algoritmů

4.2 Porovnání Linken Sphere a Tor

Při srovnání bezpečnosti webových prohlížečů budou měřeny různé aspekty, včetně rychlosti, technického přístupu, bezpečnostních technologií a bezpečnostních politik. V rámci tohoto výzkumu bude použit BeEF framework ve spojení s prohlížečem Safari pro dosažení přesnějších a relevantnějších výsledků.

4.2.1 BeEF

BeEF framework je nástroj pro penetrační testování, navržený k zneužívání zranitelností webových prohlížečů. BeEF umožňuje testovači spustit řízené příkazové moduly a útoky přímo z prostředí prohlížeče. Tímto způsobem může tester provádět útoky a hodnotit bezpečnostní pozici systému z pohledu prohlížeče. BeEF se zaměřuje na zranitelnosti v běžných prohlížečích a využívá techniky sociálního inženýrství k obejití síťových bezpečnostních zařízení a antivirových aplikací hostitele. Tento framework umožňuje provádět útoky na straně klienta a hodnotit bezpečnostní slabiny v reálném prostředí prohlížeče.

4.2.2 Sběr dat

Po stažení balíčku BeEF frameworku je nutné provést jeho instalaci a spuštění. Po úspěšném spuštění frameworku jsou dostupné odkazy na různé stránky. Jedna z těchto stránek může být poslána cílovému jednotlivci, zatímco druhá slouží jako ovládací panel pro testera. Po otevření odeslaného odkazu bude uživatel informován prostřednictvím terminálu (viz obr. 12). Následně lze přistoupit k získání informací o cíli a pokračování v provádění útoků.

Tímto postupem se vytváří efektivní a komplexní prostředí pro penetrační testování. Tester má možnost vytvářet sociálně inženýrské útoky pomocí přesvědčivých odkazů, které mohou být nasměrovány na cílové osoby. Jakmile cílová osoba otevře odkaz, testovatel obdrží upozornění a může začít shromažďovat informace o cíli. Tento krok je zásadní pro pochopení zabezpečení a odhalení slabých míst v bezpečnosti systému. Získané informace mohou být dále využity k provedení dalších útoků a hodnocení bezpečnosti ze strany testera.

Obr. 12 Spuštění BeEF

```
albinamakisheva@Albinas-MacBook-Air beef % ./beef
[11:11:33][!] Warning: System language $LANG '' does not appear to be UTF-8 compatible.
[11:11:33][*] Browser Exploitation Framework (BeEF) 0.5.4.0
[11:11:33]    |   Twit: @beefproject
[11:11:33]    |   Site: https://beefproject.com
[11:11:33]    |   Blog: http://blog.beefproject.com
[11:11:33]    |_  Wiki: https://github.com/beefproject/beef/wiki
[11:11:33][*] Project Creator: Wade Alcorn (@WadeAlcorn)
-- migration_context()
   -> 0.0075s
[11:11:33][*] BeEF is loading. Wait a few seconds...
[11:11:34][*] 8 extensions enabled:
[11:11:34]    |   XSSRays
[11:11:34]    |   Social Engineering
[11:11:34]    |   Requester
[11:11:34]    |   Proxy
[11:11:34]    |   Network
[11:11:34]    |   Events
[11:11:34]    |   Demos
[11:11:34]    |_  Admin UI
[11:11:34][*] 309 modules enabled.
[11:11:34][*] 2 network interfaces were detected.
[11:11:34][*] running on network interface: 127.0.0.1
[11:11:34]    |   Hook URL: http://127.0.0.1:3000/hook.js
[11:11:34]    |_  UI URL:   http://127.0.0.1:3000/ui/panel
[11:11:34][*] running on network interface: 172.20.10.7
[11:11:34]    |   Hook URL: http://172.20.10.7:3000/hook.js
[11:11:34]    |_  UI URL:   http://172.20.10.7:3000/ui/panel
[11:11:34][*] Public:
[11:11:34]    |   Hook URL: https://b642-78-80-123-131.eu.ngrok.io:443/hook.js
[11:11:34]    |_  UI URL:   https://b642-78-80-123-131.eu.ngrok.io:443/ui/panel
[11:11:34][*] RESTful API key: 2214f3ca8631692337c9c87ba70749b83ddb74b6
[11:11:34][!] [GeoIP] Could not find MaxMind GeoIP database: '/usr/share/GeoIP/GeoLite2-City.mmdb'
[11:11:34][*] HTTP Proxy: http://127.0.0.1:6789
[11:11:34][*] BeEF server started (press control+c to stop)
[11:17:06][!] [Browser Details] Invalid browser name returned from the hook browser's initial connection.
[11:17:06][*] New Hooked Browser [id:2, ip:2a0b:f4c2:1::1, browser:UNKNOWN-102.0, os:OSX-], hooked domain [b642-78-80-123-131.eu.ngrok.io:443]
[11:19:27][*] New Hooked Browser [id:3, ip:78.80.123.131, browser:S-6, os:OSX-], hooked domain [b642-78-80-123-131.eu.ngrok.io:443]
```

4.2.3 Safari

Safari, jakožto webový prohlížeč od renomované společnosti Apple, přináší rozsáhlé spektrum funkcí zajišťujících plynulý a bezpečný online zážitek. Tyto funkce zahrnují nejen rychlé procházení webovými stránkami, ale také optimalizovanou energetickou účinnost, schopnost blokování reklam, podporu pro více záložek, možnosti ukládání hesel a automatické dokončování formulářů. Safari dále disponuje integrovanou čtečkou, možností sdílení obsahu a rozšiřitelností prostřednictvím rozšíření, jež umožňují uživatelům plné přizpůsobení prohlížeče jejich individuálním potřebám. V oblasti

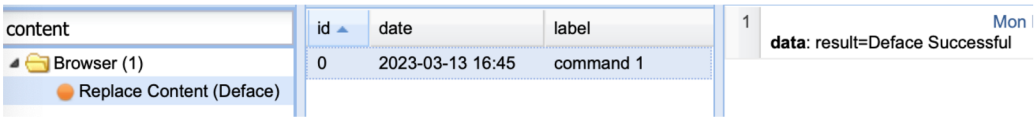
bezpečnosti Safari poskytuje podporu HTTPS, efektivní prevenci sledování a upozornění na potenciálně podvodné webové stránky.

Obr. 13 Informace uživatele Safari

browser.date.datestamp	Mon Mar 13 2023 15:33:52 GMT+0100 (CET)
browser.engine	WebKit
browser.language	en-GB
browser.name	S
browser.name.friendly	Safari
browser.name.reported	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.6 Safari/605.1.15
browser.platform	MacIntel
browser.plugins	WebKit built-in PDF
browser.version	6
browser.window.cookies	BEEFHOOK=Ql5bpodQo4ISucspd3Kj5OGCbkOYQyU0qZnekETmBCz4hKYJ… abuse_interstitial=51ce-2a02-8308-4004-d700-d446-a99d-28f1-4292.eu.ngrok.io
browser.window.hostname	51ce-2a02-8308-4004-d700-d446-a99d-28f1-4292.eu.ngrok.io
browser.window.hostport	443
browser.window.origin	https://51ce-2a02-8308-4004-d700-d446-a99d-28f1-4292.eu.ngrok.io
browser.window.referrer	Unknown
browser.window.size.height	820
browser.window.size.width	1185
browser.window.title	The Butcher
browser.window.uri	https://51ce-2a02-8308-4004-d700-d446-a99d-28f1-4292.eu.ngrok.io/demos/butcher/index.html
hardware.battery.level	unknown
hardware.cpu.arch	UNKNOWN
hardware.cpu.cores	8
hardware.gpu	Apple GPU
hardware.gpu.vendor	Apple Inc.
hardware.memory	unknown
hardware.screen.colordepth	24
hardware.screen.size.height	900
hardware.screen.size.width	1440
hardware.screen.touchenabled	No
hardware.type	Unknown
host.os.arch	32

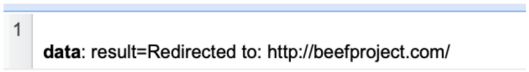
Je třeba však zdůraznit, že i přes tyto pokročilé bezpečnostní opatření může Safari být zranitelným místem, pokud cílený uživatel navštíví nebezpečné webové stránky. Útočník může s minimálním úsilím získat základní informace o oběti (viz obr. 13), což může sloužit jako základ pro další sofistikované útoky. Skrze odeslání žádosti může zločinec vyvolat dialogová okénka, jež mu umožní získat podrobnější informace o prohlížeči, síťových parametrech, otisku zařízení a geolokaci uživatele (viz obr. 14, 15).

Obr. 14 Výsledek vyvolání výměna obsahu



Během hloubkové analýzy bylo identifikováno, že jednou z klíčových výhod Safari je jeho výjimečná rychlost prohlížení (viz obr. 16), která bezpochyby předčí rychlosti

Obr. 15 Výsledek vyvolání přesměrování



konkurenčních produktů. Tato vlastnost zvyšuje efektivitu a pohodlí uživatelského prožitku při procházení internetem. Nicméně je zásadní si být vědom možných bezpečnostních hrozeb a udržovat prohlížeč aktuální a chráněný před novými hrozbami.

Obr. 16 Rychlost prohlížeče Safari

4.2.4 Tor

Konfigurace Tor prohlížeče je překvapivě jednoduchá a dostupná pro jakéhokoli uživatele internetu. Po spuštění aplikace se zobrazí okno s otázkou, zda chce uživatel používat Tor síť. Pro uživatele, kteří chtějí zlepšit úroveň bezpečnosti, nabízí prohlížeč několik režimů: standardní, bezpečnější, nebo nejbezpečnější, které kontroly Javascript, HTTPS, audio a

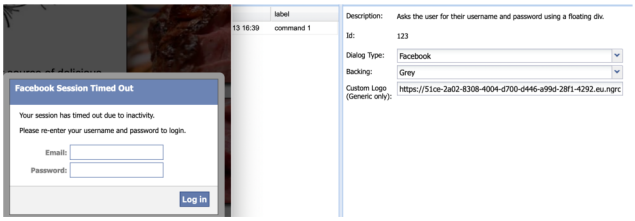
Obr. 17 Informace uživatele Tor

browser.date.datestamp	Mon Mar 13 2023 15:30:49 GMT+0000 (Coordinated Universal Time)
browser.engine	Gecko
browser.language	en-US
browser.name.reported	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:102.0) Gecko/20100101 Firefox/102.0
browser.platform	MacIntel
browser.plugins	PDF Viewer,Chrome PDF Viewer,Chromium PDF Viewer,Microsoft Edge PDF Viewer,WebKit built-in PDF
browser.version	102.0
browser.window.cookies	abuse_interstitial=51ce-2a02-8308-4004-d700-d446-a99d-28f1-4292.eu.ngrok.io; BEEFHOOK=8U76H5JJCZhCVo169To57YgHtn0ztFrvWx2WbLbhtP5GpCZePiJA2LgGnU11G4tCO0z4Y5zGusG47Kwe
browser.window.hostname	51ce-2a02-8308-4004-d700-d446-a99d-28f1-4292.eu.ngrok.io
browser.window.hostport	443
browser.window.origin	https://51ce-2a02-8308-4004-d700-d446-a99d-28f1-4292.eu.ngrok.io
browser.window.referrer	Unknown
browser.window.size.height	700
browser.window.size.width	1000
browser.window.title	The Butcher
browser.window.uri	https://51ce-2a02-8308-4004-d700-d446-a99d-28f1-4292.eu.ngrok.io/demos/butcher/index.html
hardware.battery.level	unknown
hardware.cpu.arch	UNKNOWN
hardware.cpu.cores	2
hardware.gpu	unknown
hardware.gpu.vendor	unknown
hardware.memory	unknown
hardware.screen.colordepth	24
hardware.screen.size.height	700
hardware.screen.size.width	1000
hardware.screen.touchenabled	No
hardware.type	Unknown
host.os.arch	32
host.os.family	OS X
host.os.name	OSX
host.os.version	
host.software.defaultbrowser	Unknown

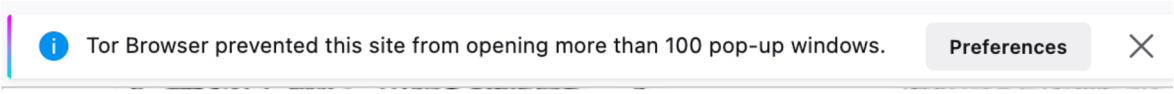
video. V případě potřeby může uživatel provádět manuální konfigurace proxy, mostů, cookies, HTTPS a povolení multimédií.

Během testování jsme zapnuli režim bezpečnější režim a přistoupili k útokům. Již v úvodním okně prohlížeče se zobrazilo několik základních informací, které lze získat při otevření odkazu (viz obr. 17). Po několika pokusech odesílání požadavků prohlížeč prokázal svoji zranitelnost vůči útokům, jako jsou nahrazování obsahu, vyvolávání falešných promptů a dialogových oken, přesměrování a další (viz obr. 18). Avšak prohlížeč byl účinný při blokování vyskakovacích oken, což významně zvýšilo úroveň bezpečnosti uživatele (viz obr. 19).

Obr. 18 Falešné okénko Facebooku



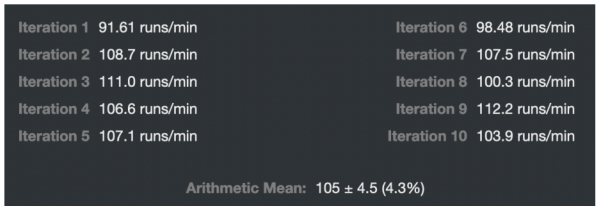
Obr. 19 Bezpečnostní upozornění Tor



Při aktivaci nejvyšší úrovně bezpečnosti, nejbezpečnějšího režimu, se stránka nedokázala vůbec načíst. To lze připsat skutečnosti, že tato nejvyšší úroveň zabezpečení může omezit určité funkce BeEF, zejména pokud jde o detekci prohlížeče a zneužívání zranitelností. I v případě, že by se stránka otevřela, žádná její funkcionalita by nefungovala, a BeEF by nebyl schopen posílat falešné požadavky prohlížeči. Nejbezpečnější režim prohlížeče Tor zakazuje JavaScript a mnoho dalších funkcí, aby poskytl vyšší úroveň soukromí a bezpečnosti. To však může komplikovat detekci prohlížeče ze strany frameworku a provádění určitých typů útoků. Některé funkce BeEF navíc vyžadují JavaScript, který je ve výchozím nastavení zakázán v nejbezpečnějším režimu Tor, pokud je protokol stránky HTTP.

Během testování rychlosti prohlížeče Tor jsme zjistili, že se rychlost výrazně zpomalila (viz obr. 20). Tento jev je způsoben směrováním přes několik vrstev šifrování. Nicméně, zvýšená bezpečnost, kterou Tor poskytuje, jasně převáží nad tímto omezením v rychlosti.

Obr. 20 Rychlost Tor prohlížeče

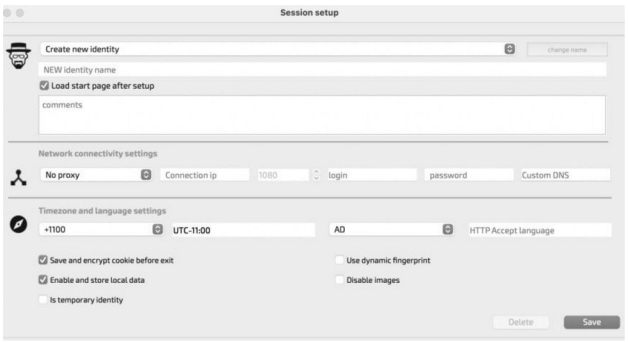


4.2.5 Linken Sphere

Po stažení prohlížeče je uživatelem vyžadováno zadání hesla, což od samého počátku zvyšuje jeho soukromí. Tato vrstva bezpečnosti má však i své negativní stránky, zejména v případě zapomenutí hesla, které nelze jednoduše resetovat.

Oproti Tor prohlížeči uvítá Linken Sphere uživatele pokročilými funkcemi a nastaveními. Uživatel má možnost nastavit proxy, VPN, Tor směrovaní, dynamické otisky, SSH tunel, změnu jazyka a časového pásma a šifrování cookies. Pro začínajícího uživatele mohou být tato nastavení matoucí a složitá, zejména pokud se snaží postupně dbát na svou bezpečnost a anonymitu při prohlížení internetu (viz obr. 21).

Obr. 21 Interface Linken Sphere



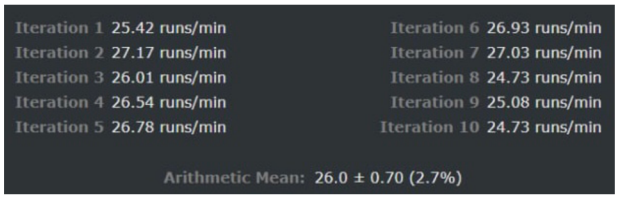
Předpokládá se, že uživatel začne s nejzákladnějšími bezpečnostními funkcemi, jako jsou Tor směrovaní, dynamické otisky a změna jazyka a časového pásma, a pokračuje v

prohlížení. Po spuštění falešného odkazu prohlížeč upozorní na nedůvěryhodnost stránky a nedovolí uživateli pokračovat dál.

Při zkoumání nastavení Linken Sphere lze pozorovat, že při otevření nové stránky se uživateli ptá, kterou identitu má použít. Tato funkce může být mimořádně užitečná, zejména pokud uživatel používá internetové služby, které vyžadují registraci a odhalení identity. V takovém případě může vytvořit jednu identitu pro tyto účely a druhou pro běžné prohlížení internetu, čímž oddělí své soukromé a veřejné aktivity.

Pokud jde o rychlost, z analýzy prohlížeče Sphere je zřejmé, že nemůže konkurovat ostatním kvůli své velmi pomalé rychlosti (viz obr. 22). Tato pomalost je nepochybně nevýhodou, kterou uživatelé musí brát v úvahu při výběru prohlížeče pro své online aktivity.

Obr. 22 Rychlost prohlížení Sphere



4.2.6 Porovnání Linken Sphere a Tor

Výběr metodiky pro porovnání

Pro porovnání prohlížeči používam metodu párového porovnání.

Porovnání

Pro porovnání dvou prohlížečů budeme věnovat pozornost takovým vlastnostem jako jsou rychlost, technický přístup a možnosti zabezpečení soukromích dat (viz t. 1), které se byli zmíněny v předcházející kapitole.

Vlastnost	Tor	Linken Sphere
Technický přístup	Síť serverů, podpora proxy serveru	VPN, dynamické otisky, podpora proxy serveru, Tor
Rychlost	105 procesů/min	26 procesů/min
TLS/SSL	Ano	Ano
Podpora proxy	Ano	Ano
Javascript	Povolen, lze deaktivovat	Povolen
Cookies	Blokovány	Přizpůsobitelné ovládání
Aktualizace	Automatické	Manuální

Tabulka č. 1 Porovnání prohlížeče

Interpretace výsledku

Při srovnání dvou prohlížečů bylo zjištěno, že prohlížeč Linken Sphere může být bezstarostnější volbou pro procházení sítí, ačkoliv jeho rychlost může být nižší a uživatel musí provádět manuální aktualizace. Jeho výhodou spočívá v tom, že má i ty vlastnosti, které má prohlížeč TOR, ale uživatel je může samostatně regulovat.

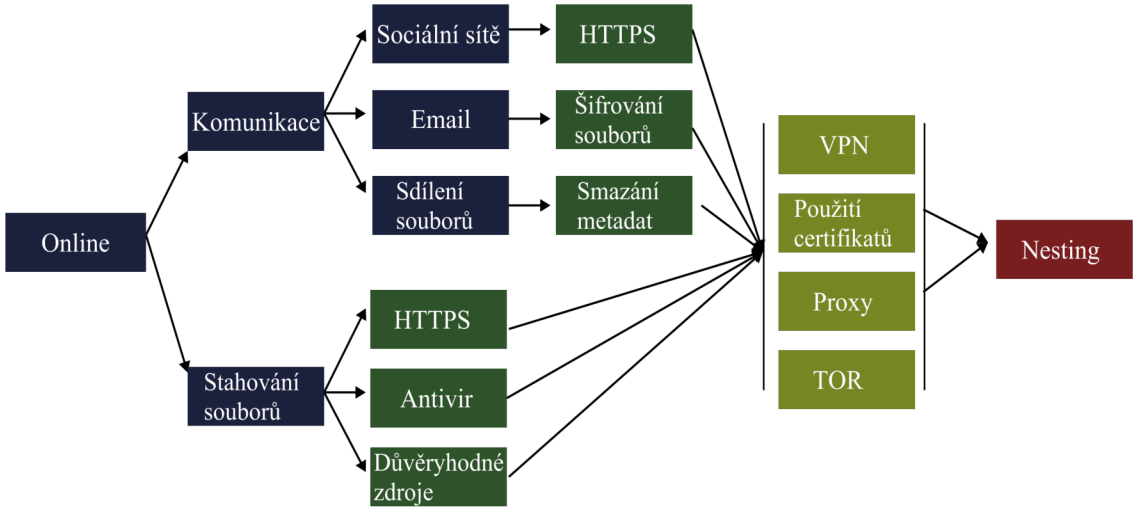
4.3 Schéma kroků

Dalším krokem po dokončení bakalářské práce je vytvoření schématu kroků (viz obr. 23, 24), které mají za cíl pomoci uživatelům zvýšit svou bezpečnost na internetu. Různé aktivity na internetu byly systematicky rozděleny do čtyř hlavních skupin: komunikace, stahování souborů, nákupy a prohlížení webových stránek. Následující kroky jsou

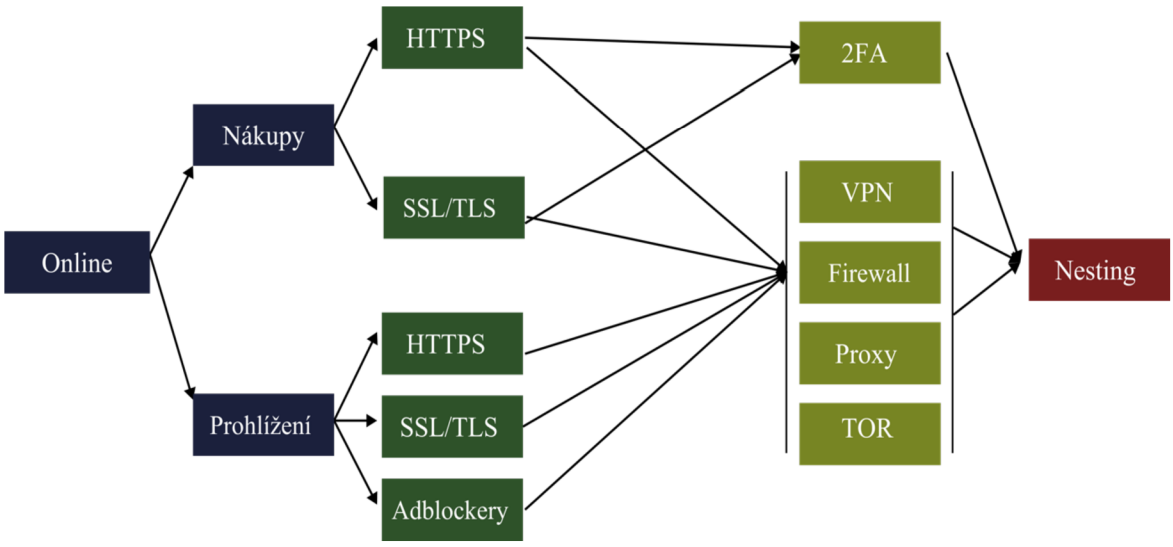
uspořádány podle složitosti používání v reálných situacích a zároveň podle úrovně bezpečnosti.

To znamená, že pokud začínající uživatel začíná postupně dbát na svou bezpečnost, měl by zvážit instalaci antivirového programu, šifrování svých souborů a pečlivou kontrolu, zda webová stránka používá protokol HTTPS. Pro uživatele s mírně pokročilými znalostmi je doporučeno využívání VPN, proxy serverů a prohlížečů s vhodnými směrovacími řešeními. Pro pokročilé uživatele existují sofistikovanější možnosti, jako je kombinace VPN a TOR nebo vícevrstvá VPN spojení, která mohou výrazně zlepšit úroveň anonymity a bezpečnosti. Toto schéma slouží jako praktický průvodce, který pomáhá uživatelům porozumět konkrétním krokům, které mohou podniknout ke zlepšení své bezpečnosti online. Je klíčové si uvědomit, že bezpečnost na internetu není univerzální a mění se v závislosti na konkrétní aktivitě, kterou vykonáváme. Důsledným dodržováním správných postupů v každém scénáři můžeme minimalizovat rizika a ochránit naši online identitu.

Obr. 23 Schéma kroků část 1



Obr. 24 Schéma kroků část 2



4.4 Závěr

Pro dosažení nejvyšší úrovně bezpečnosti by měli uživatelé upřednostňovat šifrovací algoritmy, jako je AES, pro šifrování svých souborů. Na základě výsledků lze konstatovat, že AES je bezpečnější a efektivnější šifrovací algoritmus než DES a je doporučován pro použití ve většině moderních šifrovacích aplikací. DES se stále využívá v některých starších systémech, ale pro nové aplikace není doporučován kvůli svým zranitelnostem.

Při porovnání různých prohlížečů bylo zjištěno, že optimální volbou je prohlížeč LinkenSphere, i když má nedostatky. Linken Sphere a Tor jsou oba webové prohlížeče vytvořené s cílem zabezpečit online soukromí a anonymitu. Avšak mezi těmito dvěma existují klíčové rozdíly, které by měli uživatelé zvážit při volbě pro své online aktivity. Tyto rozdíly zahrnují technický přístup, rychlost a povolení cookies a Javascriptu. Pro začínajícího uživatele může Tor prohlížeč působit jako jednodušší a pohodlnější volba. Nicméně, pokud má uživatel zájem o vyšší úroveň soukromí a bezpečnosti, měl by zvážit použití Linken Sphere. Rozdíly ve funkcích a bezpečnostních aspektech obou prohlížečů mohou ovlivnit individuální potřeby a preference uživatele při procházení online světem.

Hlavním přínosem této bakalářské práce je vytvořené schéma, které může pomoci uživatelům zlepšit svou vlastní bezpečnost a soukromí na internetu. Důležité je také dbát na pravidelné aktualizace prohlížečů, vyhledávat certifikované šifrovací protokoly a využívat spolehlivé bezpečnostní nástroje, jako jsou antivirové programy, VPN služby a firewall. Výzkum rovněž zdůraznil důležitost kombinací technických opatření s povědomím o bezpečnostních rizicích, aby uživatelé aktivně přispěli k zajištění kybernetické bezpečnosti.

5 Seznam zdrojů

Publikace:

1. Pew Research Center. *Anonymity, Privacy, and Security Online*. Pew Research Center [online]. 5.09.2013 [cit.15.08.2022]. Dostupné z: https://www.pewresearch.org/internet/2013/09/05/anonymity-privacy-and-security-online-2/
2. STALLINGS, William a Abhijit BAROI, JOHNSON, Tracy, ed. *Cryptography and Network Security: Principles and Practice*. 7th ed. United States of America: Pearson Education, 2017. ISBN 978-0-13-444428-4
3. PAAR, Christof, PELZL, Jan, *Understanding Cryptography*. Springer-Verlag Berlin Heidelberg, 2010. ISBN 978-3-642-04100-6
4. P. Sri Ram Chandra, G.Venkateswara Rao, M. S. Chakravarthy, T.V. Prasad. *Analysis of Brute-Force Attack in UES over DES*. International Journal of Innovative Technology and Exploring Engineering (IJITEE) 8, no. 6S3 (2019). ISSN: 2278-3075.
5. OPPLIGER, Rolf. *Security Technologies for the World Wide Web*. Artech House 2, 2003. ISBN 1-58053-348-5
6. HUNT, Craig. *TCP/IP Network Administartion*. O'reilly, 2002 (3). ISBN 978-0-596-00297-8
7. SHISH, Ahmad, JAMEEL, Ahmad, NABARUN, Barua, Mohd. Rizwan beg. *Meet In The Middle Attack: A Cryptanalysis Approach*. International Journal of Computer Applications 1, no. 25 (2010): 1–7. DOI 10.5120/467-772
8. HAMMADI, Abdallah, ROUBHI, Hamza. *Vpn (Virtual Private Network)*. Annee University, 2019. IGE 40
9. OccupyTheWeb. *Linux basics for hackers: getting started with networking, scripting and security in Kali.* No Starch Press, Inc. 1, [2018]. ISBN 978159327-8557.
10. SANTOSO, Budi, ASRUL, Sani, T. Husain, NEDI Hendri. "*Vpn site to site implementation using protocol l2tp and ipsec.*" TEKNOKOM 4, no. 1 (n.d.): 30–36. doi:10.31943/TEKNOKOM.V4I1.59.

11. CHOPRA, Aakanksha. *Security Issues of Firewall*. International Journal of P2P Network Trends and Technology (IJPTT) 22, no. 1 (2016). DOI 10.14445/22492615/IJPTT-V22P402.
12. ALLCOCK, William. *Firewall issues overview*. Open Grid Forum. 2006. GFD-I.083
13. VACCA, John. *Managing Information Security*. Elsevier, 2009. ISBN 978-1-59749-533-2
14. STEPHEN, Thomas, SPENCER, Marjorie, ed. *SSL and TLS essentials*. United States of America: John Wiley & Sons, 2000. ISBN 0-471-38354-6.

Normy:

15. [RFC4949] Shirey, R., *Internet Security Glossary*, Version 2, FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007. Dostupné z: https://www.rfc-editor.org/info/rfc4949

Webové stránky:

16. YOUNG, Bill. *Introduction to Computer Security* [online]. 25.10.2019 [cit. 13.03.2023] Dostupné z: https://www.cs.utexas.edu/~byoung/cs361/slides6-cryptography2-4up.pdf
17. MOHIT Arora. *How Secure is AES against brute-force attacks.* EETimes[online]. 05.07.2012 [cit. 15.03.2023]. Dostupné z: https://www.eetimes.com/document.asp?doc_id=1279619
18. *Tor Browser Manual* [online]. 6.03.2023 [cit. 10.03.2023] Dostupné z: https://tb-manual.torproject.org/
19. *Linken Sphere* [online]. 6.03.2023 [cit. 17.03.2023] Dostupné z: https://ls.tenebris.cc/documentation/introduction

6 Přílohy

Seznam obrázků

1. Statistika hrozby na internetu (s. 12)
2. Šifrování a dešifrování (s. 14)
3. Postup šifru Feistelu (s. 16)
4. Konfigurace DMZ (s. 23)
5. Komunikace při použití proxy serveru (s. 30)
6. Postup šifrování a dešifrování (s. 37)
7. Výsledek šifrování a dešifrování DES (s. 38)
8. Šifrování pomocí disk utilitu (s. 38)
9. Šifrovaní ve Windows OS (s. 38)
10. Test rychlosti šifrování DES a AES (s. 41)
11. Porovnání algoritmů (s. 42)
12. Spuštění BeEF (s. 44)
13. Informace uživatele Safari (s. 45)
14. Výsledek vyvolání výměna obsahu (s. 45)
15. Výsledek vyvolání přesměrování (s. 46)
16. Rychlost prohlížeče Safari (s. 46)
17. Informace uživatele Tor (s. 46)
18. Falešné okénko Facebooku (s. 47)
19. Bezpečnostní upozornění Tor (s. 47)
20. Rychlost Tor prohlížeče (s. 48)
21. Interface Linken Sphere (s. 48)
22. Rychlost prohlížení Sphere (s. 49)
23. Schéma kroků část 1 (s. 51)
24. Schéma kroků část 2 (s. 52)

Seznam tabulek

1. Porovnání prohlížeče (s. 12)

Použité zkratky

DES	Data Encryption Standard
AES	Advanced Encryption Standard
VPN	Virtual Private Network
TCP	Transmission Control Protocol
IP	Internet Protocol
HTTPS	HyperText Transfer Protocol Secure
HTTP	HyperText Transfer Protocol
SSL	Secure Socket Layer
TLS	Transport Layer Security
IPsec	IP Security
USB	Universal Serial Bus
3DES	Triple Data Encryption Standard
S-box	Substitution box
P-box	Permutation box
XOR	Exklusive OR
SLIP	Seriál Line Internet Protocol
PPP	Point-to-Point Protocol
L2TP	Layer 2 Tunneling Protocol
OSI	Open Systéms Interconnection
IKE	Internet Key Exchange
SQL	Structured Query Language
XSS	Cross-Site Scripting

UDP	User Datagram Protocol
MAC	Medium Access Control
DMZ	Demilitarized Zone
DoS	Denial of Service
ESP	Encapsulationg Security Payload
AH	Authentication Header
SSH	Secure Socket Shell
HMAC	Hash-based message authentication code
PKI	Public key infrastructure
SOCKS	Socket Secure
MB	MegaByte