Průzkum možností prolomení a zabezpečení správců hesel

-

Patrik Hajšo

Bakalářská práce
2022

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav informatiky a umělé inteligence

Akademický rok: 2021/2022

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Patrik Hajšo**
Osobní číslo:	**A19030**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Softwarové inženýrství**
Forma studia:	**Prezenční**
Téma práce:	**Průzkum možností prolomení a zabezpečení správců hesel**
Téma práce anglicky:	**Exploring the Security and Cracking Capabilities of Password Managers**

Zásady pro vypracování

1. Proveďte rešerši stávajících řešení správy hesel.
2. Rozeberte kryptografické algoritmy ve vazbě na správce hesel.
3. Popište aktuální i budoucí možnosti prolomení zabezpečení správců hesel.
4. Vyberte nejpoužívanější správce hesel a vyhodnoťte jejich zabezpečení.
5. Výsledky vhodně prezentujte.

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

Seznam doporučené literatury:

1. OULEHLA, Milan a Roman JAŠEK. Moderní kryptografie. [Praha]: IFP Publishing, 2017. ISBN 978-80-87383-67-4.
2. DAEMEN, Joan a Vincent RIJMEN. The design of Rijndael: AES – the Advanced Encryption Standard. Berlin: Springer, 2002. ISBN 3-540-42580-2.
3. STAMP, Mark a Richard M. LOW. Applied Cryptanalysis: Breaking Ciphers in the Real World. San Jose: Wiley-IEEE Press, 2007. ISBN 978-0470114865.
4. KLEIN, Ken S. Healthy Passwords: Learn to make strong passwords you can remember. Sustainable Alternatives, 2011. ISBN 978-0615456850.

Vedoucí bakalářské práce: **Ing. Petr Žáček, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání bakalářské práce: **3. prosince 2021**
Termín odevzdání bakalářské práce: **23. května 2022**

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. Mgr. Milan Adámek, Ph.D. v.r.
děkan

prof. Mgr. Roman Jašek, Ph.D., DBA v.r.
ředitel ústavu

Ve Zlíně dne 24. ledna 2022

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že 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;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že 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 totožné.

Ve Zlíně, dne 22.5.2022

Patrik Hajšo v. r.
podpis studenta

ABSTRAKT

Bakalárska práca sa zaoberá rozborom bezpečnosti správcov hesiel. V teoretickej časti sú popísané základné termíny spojené so správcami, kryptografické základy, teoretický rozbor kryptografických algoritmov používaných v náväznosti na správcov a teoretický rámec možností ich prelomenia. Ďalej sú v tejto časti popísané technológie používané pre ich zabezpečenie. Praktická časť obsahuje popis možných aplikácií daných útokov a vyhodnotenie zabezpečenia najpoužívanejších správcov.

Klíčová slova: správca hesla, zabezpečenie, možnosti prelomenia, zranitelnosti kryptografie, kryptoanalýza

ABSTRACT

This bachelor thesis deals with the security analysis of password managers. The theoretical part describes the basic terms associated with password managers, cryptographic bases, theoretical analysis of cryptographic algorithms in connection with password managers and theoretical framework of possibilities of breaking them. The technologies used to secure password managers are also described in this part. The practical part contains a description of possible applications of the attacks and security assessment of the most commonly used password managers.

Keywords: password manager, security, breaking possibilities, cryptography vulnerabilities, cryptoanalysis

Ďakujem vedúcemu mojej bakalárskej práce Ing. Petrovi Žáčkovi, Ph.D. za jeho ochotu, pomoc a odborné rady pri vedení práce.

Prehlasujem, že odovzdaná verzia bakalárskej práce a verzia elektronická nahraná do IS/STAG sú totožné.

OBSAH

ÚVOD

Heslá sú súčasťou počítačových systémov už od ranných začiatkov vývoja výpočtovej techniky. Od začiatku bolo ich úlohou overovať identity užívateľských účtov, aby sa predchádzalo neautorizovaným vstupom do systému alebo jeho časti. Neskôr sa heslá stali základným pilierom v autentifikačných systémoch, či už pri prihlasovaní do systému alebo do užívateľských účtov na rôznych webových stránkach.

Pretože heslá predstavujú hlavnú ochranu užívateľských účtov, sú na ne upriamené rôzne útoky s cieľom ich prelomiť. Preto boli vyvinuté postupy nielen na ich šifrovanie, ale aj pre ich bezpečné spravovanie a ukladanie. Tieto postupy boli nakoniec skombinované do programu, ktorý chráni a spravuje užívateľské heslá, preto sa mu hovorí správca hesla. Títo správcovia plnia základné úlohy práce s údajmi a zabezpečujú ich ochranu, integritu, ukladanie a dostupnosť.

Práca sa zaoberá predovšetkým bezpečnostným rozborom správcov. V teoretickej časti sú uvedené základné pojmy riešenia správcov, kryptografické základy, teoretický rozbor algoritmov používaných na šifrovanie dát a teoretické základy možných útokov, ako na samotné heslá tak aj na logiku správcov. Túto časť uzatvára popis jednotlivých technológií, ktoré správcovia používajú pre bezpečnosť ukladaných dát.

Praktická časť rozoberá možnosti dostupných pokusov o prelomenie a ich dopad na bezpečnosť správcov hesla, takisto skúma aj budúce vyhliadky bezpečnosti a ohrozenie správcov z pohľadu vývoja moderných a výkonných počítačových strojov. Na záver je práca zameraná na vyhodnocovanie bezpečnosti najpoužívanejších správcov a ich porovnávanie.

I. TEORETICKÁ ČASŤ

1 TEORETICKÝ RÁMEC

Heslo je v počítačovom systéme postupnosť určitých znakov, ktorá sa používa na dokázanie užívateľskej identity. Heslá by mali byť tvorené z niekoľkých rôznych znakov, ktoré by mali tvoriť kombináciu malých aj veľkých písmen, čísel, aj špeciálnych symbolov. [1]

Správca hesla je softvérový nástroj, ktorý umožňuje užívateľom alebo iným skupinám bezpečne ukladať a udržiavať všetky ich osobné údaje, ako sú heslá, alebo platobné údaje, v chránenom a šifrovanom úložnom priestore, ktorý sa nazýva trezor. Takisto sa používa na samotné generovanie týchto hesiel. Na základe potreby sa správcovia delia do niekoľkých skupín alebo plánov určených:

- Pre individuálov
- Pre tímy a rodiny
- Pre spoločnosti

Na základe potreby plnia správcovia nasledujúce funkcionality:

- Uchovávanie hesiel a údajov, automatické vyplňovanie uložených údajov, dodržiavanie pravidiel pre tvorenie veľmi silných hesiel.
- Bezpečné zdieľanie hesiel medzi členmi rodiny alebo tímu pre prístup k webovým účtom alebo iným aplikáciám.
- Zdieľanie užívateľských účtov v rámci podniku, udržovanie auditovaných záznamov alebo dôležitých správ. [2]

Na základe určitých znakov dokážeme rozlíšiť tieto typy správcov hesiel:

- **Online (Cloud-Based) správca hesla** ukladá heslá a údaje priamo na serveroch umiestených na internete, ktoré patria poskytovateľovi. Veľkou výhodou týchto správcov je, že užívateľ má prístup k svojim údajom z akéhokoľvek zariadenia s prístupom k internetu. Takýto správca je primárne dostupný ako rozšírenie internetového prehliadača, ale môže sa jednať aj o iný druh softvéru, napríklad desktopová alebo mobilná aplikácia.

- **Offline (Locally-Based) správca hesla** sa od online správcu hesla líši tým, že heslá sú ukladané lokálne na užívateľskom zariadení a uchovávané v chránenom úložisku. Prístup k tomuto úložisku a samotným heslám je možný len z tohoto zariadenia, to znamená stratu všetkých hesiel v prípade straty samotného zariadenia. Tento typ správcu svojím riešením poskytuje vyššiu ochranu a súkromie pre užívateľov, ktorí nechcú, aby ich údaje boli uložené a kontrolované niekým iným.

- **Single sign-on (SSO) správca hesla** umožňuje, na rozdiel od iných správcov, ktorí uchovávajú rôzne heslá pre rôzne typy aplikácií, používať jedno a to isté heslo pre všetky z nich. Užívateľ nemusí dokazovať svoju identitu pri využívaní SSO, namiesto toho je za to zodpovedný poskytovateľ tejto služby. Takýto systém ma hlavne vo svete biznisu niekoľko výhod, napríklad umožňuje zamestnancom jednoduchý prístup k aplikáciám a šetrí tým čas spojený s problémom zabudnutých hesiel. [3]

1.1 Vývoj autentifikácie v počítačových systémoch

Na počiatku 60. rokov 20. storočia vytvoril inštitút MIT systém pre autentifikáciu používateľov počítačových systémov pomocou hesla. Tieto heslá boli pre každého jedinečné a uchovávali sa priamo v systéme.

Približne v tom istom čase výskumník MIT Allan Scheer využíval počítačový systém pre výskum, ale jeho používanie bolo pre každého užívateľa časovo obmedzené. Aby obišiel toto obmedzenie, našiel spôsob, ako sa dostať k systémovým heslám ostatných užívateľov a vytlačiť si ich zoznam s cieľom využívať viac časového limitu. Tento akt je považovaný za jeden z prvých hackerských útokov na počítačový systém.

V 70. rokoch bola vyvinutá nová metóda pre jednoduché šifrovanie hesiel, ktorá dostala názov *hashing*. Pomocou hashovania sa heslo prevádzalo z pôvodnej textovej formy na numerickú hodnotu.

Neskôr roku 1979, boli k hashovaným heslám pridávané dodatočné znaky, označované ako *salt***.** Táto forma zabezpečenia hesla sa dnes často používa. [4] [5]

1.2 Kryptografické základy

1.2.1 Kryptografia

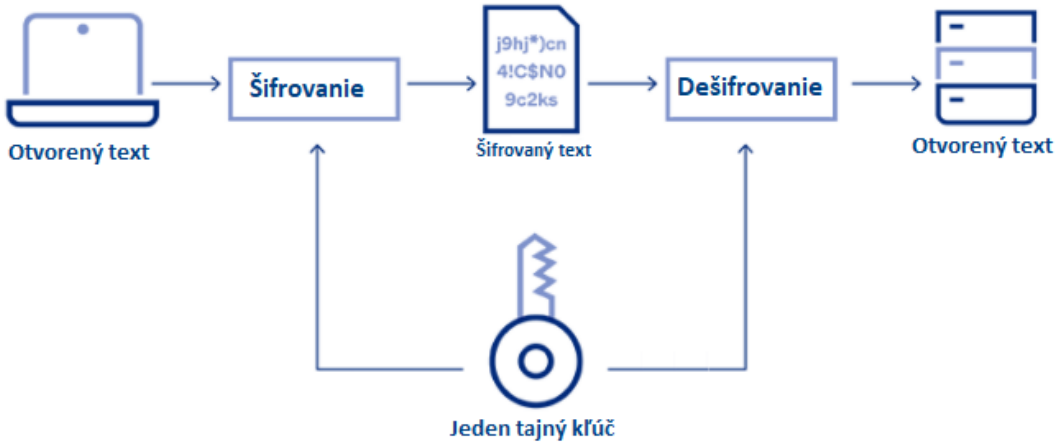
Kryptografia označuje postup, pri ktorom sa údaje prevádzajú z textovej podoby do nejasnej, šifrovanej formy, pričom cieľom je poskytnutie ochrany údajov. Dáta v textovej forme sa označujú ako otvorený text a po premene ako šifrovaný text. Proces premeny sa nazýva šifrovanie, opačný proces sa nazýva dešifrovanie. [6]

1.2.2 Kryptoanalýza

Na rozdiel od kryptografie, kryptoanalýza je metóda, ktorá sa používa na zistenie otvoreného textu, rozborom a skúmaním šifrovaného textu, pričom nie je známy kľúč. Úlohou analytikov je analyzovať šifrovaný text a získať kľúč, ktorým sa dopracujú k pôvodnému otvorenému textu alebo nájsť iný spôsob, ako sa k nemu dopracovať, bez potreby znalosti šifrovacieho kľúča. Kryptoanalýza zvyčajne aplikuje znalosti z oblastí matematiky, kombinatoriky a analytického myslenia. [6]

1.2.3 Symetrická kryptografia

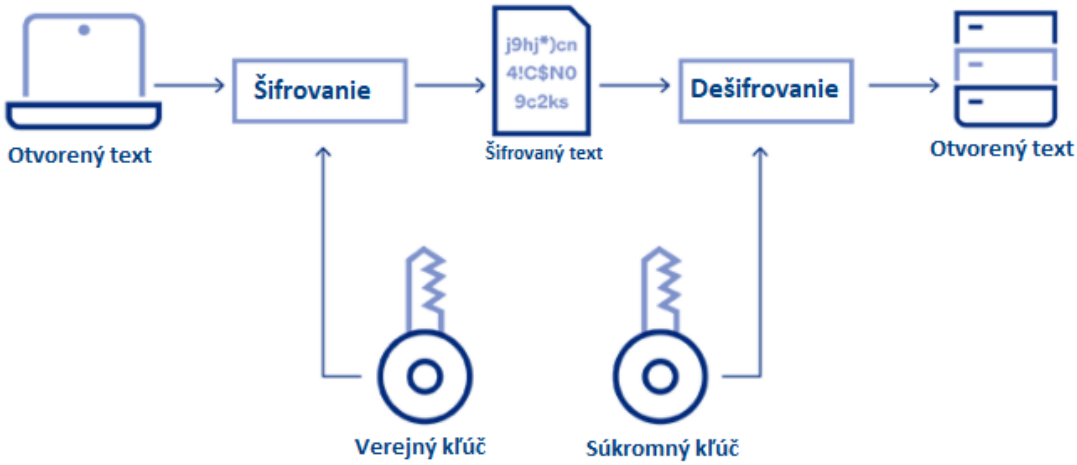
Symetrická kryptografia je jednou z metód šifrovania pomocou jedného kľúča, ktorý je rovnaký pre osobu, ktorá vykonáva šifrovanie ako aj pre osobu, ktorá vykonáva dešifrovanie. Najznámejšie symetrické algoritmy sú AES, DES a 3DES. [6]



Obr. 1 - Princíp symetrickej kryptografie [7]

1.2.4 Asymetrická kryptografia

V asymetrickej kryptografii sa na rozdiel od symetrickej používajú dva rozdielne kľúče – verejný a súkromný. Pre šifrovanie otvoreného textu sa používa verejný kľúč, ktorý vlastní príjemca šifrovaného textu. Tento kľúč je známy pre všetkých užívateľov. Pri dešifrovaní sa používa privátny kľúč, ktorý vlastní príjemca správy, no tento kľúč už nie je dostupný nikomu inému, len samotnému príjemcovi. Najznámejšie asymetrické algoritmy sú RSA a Diffie-Helmanov algoritmus. [6]



Obr. 2 - Princíp asymetrickej kryptografie [7]

1.2.5 Bloková šifra

Bloková šifra pracuje s blokmi dát s nemennou dĺžkou bloku, zvyčajne s bitovými blokmi o veľkosti 64 bitov a viac. Používa vždy rovnaký kľúč a šifruje blok dát do identického, šifrovaného bloku dát. Blokové šifry sa delia na prestavujúce alebo substitučné, kde patrí majorita používaných algoritmov. [8]

1.2.6 Prúdová šifra

Prúdová šifra operuje s prúdom bitov alebo niekoľko bitových slov textu. Pri každom kole šifrovania sa práve jeden bit zašifruje do iného bitu šifrovaného textu. Tieto operácie sú založené na generovaní pseudonáhodných postupností. Prúdové šifrovanie sa používa pri prenose prúdov informácii, kde prenos dát môže byť prerušený v určitej časovej chvíli, ako napríklad videohovor. [9]

1.2.7 Advanced Encryption Standard (AES)

V roku 1977 bol v USA oznámený podnet pre vytvorenie nového šifrovacieho štandardu, ktorý mal nahradiť už starnúci štandard DES. Nový štandard musel splňovať určité bezpečnostné špecifikácie a požiadavky. Do finálového kola sa dostalo päť kandidátov - MARS, RC6, Rijndael, Serpent a Twofish. V roku 2000 bol za víťaza vyhlásený Rijndael, ktorý sa stal štandardom AES. [10]

1.2.7.1 Šifrovanie

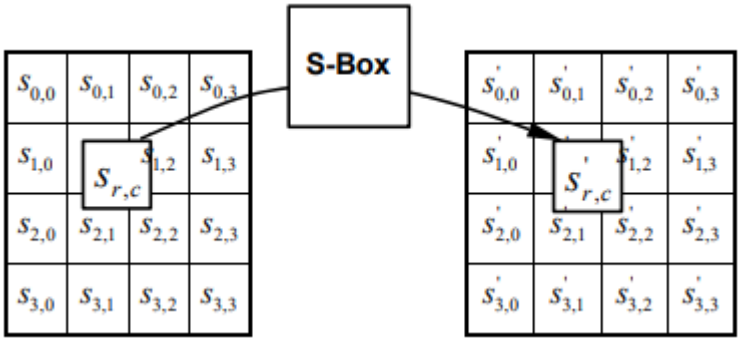
Rijndael je iteračná bloková šifra s nemennou dĺžkou bloku o veľkosti 128 bitov a premennou dĺžkou kľúča, ktoré môžu dosahovať 128, 192 alebo 256 bitov. Rijndael pracuje s poliami bajtov (stav) a pozostáva z aplikovania opakovanej kolovej funkcie. Počet kôl záleží na dĺžke kľúča. Každé jedno kolo pozostáva z aplikovania štyroch transformácií. Tieto transformácie sa nazývajú SubBytes(), ShiftRows(), MixColumns() a AddRoundKey(). [11]

	Key Length *(Nk words)*	Block Size *(Nb words)*	Number of Rounds *(Nr)*
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Obr. 3 - Počet kôl pre jednotlivé verzie AES na základe dĺžky kľúča [11]

1.2.7.2 SubBytes()

SubBytes() predstavuje nelineárnu substitúciu bajtov, ktorá používa substitučnú tabuľku (S- box), ktorá je uvedená v hexadecimálnom tvare. Táto substitúcia je vykonávaná na každom bajte. Inverzná operácia SubBytes() sa nazýva InvSubBytes(). [11]



Obr. 4 - SubBytes() aplikuje S-box na každý bajt stavu [11]

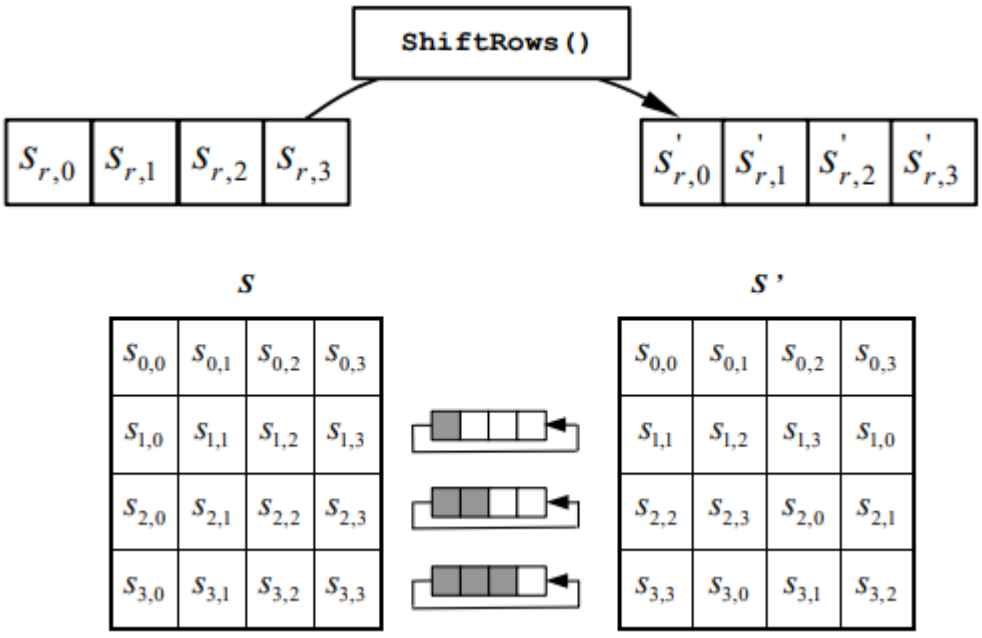
Substitučná hodnota bajtov je určená priesečníkom riadku a stĺpca v substitučnej tabuľke, kde prvá hodnota predstavuje index riadku a druhá hodnota index stĺpca. [11]

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Obr. 5 - S-box tabuľka v hexadecimálnej forme používaná v AES [11]

1.2.7.3 ShiftRows()

Pri transformácii ShiftRows() sú jednotlivé bajty v riadkoch stavu posunuté doľava o hodnoty, ktorým sa hovorí *offsety* (Obr.7). Prvý riadok s hodnotou offsetu 0 zostáva vždy nemenný. Inverzná operácia ShiftRows() sa nazýva InvShitRows(). [11]



Obr. 6 - Posúvanie posledných riadkov v stave [11]

N_b	C_0	C_1	C_2	C_3
4	0	1	2	3
5	0	1	2	3
6	0	1	2	3
7	0	1	2	4
8	0	1	3	4

Obr. 7 - Offsety pre rôzne blokové dĺžky N_b [11]

1.2.7.4 MixColumns()

Transformácia MixColumns() pracuje so stĺpcami v stave. Tieto stĺpce sú násobené pevným polynómom a(x) = $\{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$. [11]

$$s'_{0,c} = (\{02\} \bullet s_{0,c}) \oplus (\{03\} \bullet s_{1,c}) \oplus s_{2,c} \oplus s_{3,c}$$

$$s'_{1,c} = s_{0,c} \oplus (\{02\} \bullet s_{1,c}) \oplus (\{03\} \bullet s_{2,c}) \oplus s_{3,c}$$

$$s'_{2,c} = s_{0,c} \oplus s_{1,c} \oplus (\{02\} \bullet s_{2,c}) \oplus (\{03\} \bullet s_{3,c})$$

$$s'_{3,c} = (\{03\} \bullet s_{0,c}) \oplus s_{1,c} \oplus s_{2,c} \oplus (\{02\} \bullet s_{3,c}).$$

Obr. 8 - Operácia MixColumns() [11]

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix}$$

Obr. 9 - Maticový tvar operácie MixColumns() [11]

1.2.7.5 AddRoundKey()

Transformácia AddRoundKey() označuje prídavok kľúča, ktorý sa pridá do stavu bitovou operáciou XOR. Tento kľúč sa získava pomocou expanzie kľúča (Key Expansion). Tento proces expandovania kľúčov je popísaný v sekcii 6.2. AddRoundKey() nemá inverznú operáciu, nakoľko využíva iba bitovú operáciu XOR. [11]

$$\begin{bmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \end{bmatrix} + \begin{bmatrix} k_{0,0} & k_{0,1} & k_{0,2} & k_{0,3} \\ k_{1,0} & k_{1,1} & k_{1,2} & k_{1,3} \\ k_{2,0} & k_{2,1} & k_{2,2} & k_{2,3} \\ k_{3,0} & k_{3,1} & k_{3,2} & k_{3,3} \end{bmatrix} = \begin{bmatrix} b_{0,0} & b_{0,1} & b_{0,2} & b_{0,3} \\ b_{1,0} & b_{1,1} & b_{1,2} & b_{1,3} \\ b_{2,0} & b_{2,1} & b_{2,2} & b_{2,3} \\ b_{3,0} & b_{3,1} & b_{3,2} & b_{3,3} \end{bmatrix}$$

Obr. 10 - Pridávanie kľúča do stavu pomocou bitovej operácie XOR [10]

1.2.7.6 Expanzia kľúča (Key Expansion)

Expanzia kľúča určuje pravidlá odvodenia kľúčov (round keys) zo šifrovacieho kľúča. Táto operácia pozostáva z dvoch častí - prvá časť pozostáva z pridávania bitov zo šifrovacieho do rozšíreného kľúča a druhá časť pozostáva z výberu niekoľko bitových kľúčov z rozšíreného kľúča. [10]

1.2.7.7 Dešifrovanie

Dešifrovanie pozostáva z aplikovania krokov, ktoré sú inverznými k pôvodným krokom, použitých pri šifrovaní. Cieľom je získať inverznú šifru k pôvodnej šifre. V dešifrovacom algoritme sa môže líšiť aj poradie, v ktorom kroky nastávajú. [11]

1.2.8 ChaCha20

Salsa20 je skupina prúdových šifier používajúca kľúč o veľkosti 256-bitov, vytvorených pre projekt prúdových šifier nazývaný eSTREAM, kde postúpila do tretieho kola súťaže bez akýchkoľvek zmien. Verzia Salsa20/20, ktorá pozostáva z 20 kôl, je v porovnaní s AES rýchlejšia. Prúdové šifry z tejto skupiny sú považované za tie najrýchlejšie a odporúčané pre aplikácie, ktoré uprednostňujú rýchlosť. [12]

1.2.8.1 Šifrovanie

ChaCha je prúdová šifra s veľkosťou kľúča 256-bitov, ktorej prvá verzia pochádza zo šifry Salsa20/8. Jedná sa o vylepšená verziu, vytvorenú pre zvýšenie odolnosti voči kryptoanalýze, pričom zlepšuje časovú náročnosť jedného kola šifrovania. Jedno kolo, podobne ako kolo u šifry Salsa20, má 16 prídavkov a rovnaký počet XORovaní a rotácii 32-bitových slov. [13]

1.2.8.2 Štvrťkolo (quarter-round)

Pre zmenu štyroch 32-bitových slov v stave sa využívajú 4 pridania, 4 XORovania a 4 rotácie v každom kole štvrťkola. Na rozdiel od Salsa20, ChaCha vykonáva tento proces v inom poradí, pričom dovoľuje reformovať každé slovo dvakrát. [13]

```
a += b; d ^= a; d <<<= 16;
c += d; b ^= c; b <<<= 12;
a += b; d ^= a; d <<<= 8;
c += d; b ^= c; b <<<= 7;
```

Obr. 11 - Operácia štvrťkola v ChaCha20 – Add, Xor, Rotate [13]

Podobne ako Salsa20, ChaCha má k dispozícii 16 slov, ale v jednom časovom úseku pracuje iba so 4 slovami. Takáto operácia umožňuje všetkým vstupným slovám ovplyvniť všetky výstupné slová a takisto dokáže rýchlejšie šíriť zmeny pomocou bitov. [13]

1.2.8.3 Matica

Salsa20 používa maticu o veľkosti 4x4 pre uloženie 4 vstupných slov, skladajúcich sa z nonce a blokového počítadla, 8 kľúčových a 4 konštantných slov. Následne pomocou kôl premieňa maticu a získaný výsledok je pridávaný do matice, z ktorej sa získa 16- slovný, teda 64-bitový blok. [13]

constant	constant	constant	constant
key	input	key	key
input	key	key	input
key	key	input	key

Obr. 12 - Inicializačná matica Salsa20 [13]

ChaCha rovnako ako Salsa20 vytvára podobne veľkostnú maticu, z ktorej takisto dostáva 64-bitový výsledný blok. [13]

constant	constant	constant	constant
key	key	key	key
key	key	key	key
input	input	input	input

Obr. 13 - Inicializačná matica ChaCha [13]

V porovnaní so Salsa20, ChaCha ukladá vstupné slová na spodok matice, no konštanty zostávajú stále rovnaké. V inicializačnom kole sú kľúčové slová pridávané medzi konštanty, následne sú XORované a nakoniec prebieha ich rotácia, pričom výsledky sú pridávané do kľúčových slov. [13]

```
QUARTERROUND( x0, x4, x8,x12)
QUARTERROUND( x1, x5, x9,x13)
QUARTERROUND( x2, x6,x10,x14)
QUARTERROUND( x3, x7,x11,x15)
```

Obr. 14 - Štvrťkolá aplikované na stĺpce matice [13]

```
QUARTERROUND( x0, x5,x10,x15)
QUARTERROUND( x1, x6,x11,x12)
QUARTERROUND( x2, x7, x8,x13)
QUARTERROUND( x3, x4, x9,x14)
```

Obr. 15 - Štvrťkolá aplikované na uhlopriečky matice [13]

1.2.8.4 Dešifrovanie

ChaCha, rovnako ako Salsa20, používa pri dešifrovaní rovnaký algoritmus, ako ten používaný pri šifrovaní. Výstup procesu je následne XORovaný s 64-bitovým blokom šifrovaného textu, čím sa produkuje rovnako veľký blok otvoreného textu. [14]

1.3 Útoky na heslá

1.3.1 Dictionary Attack (Slovníkový útok)

Slovníkový útok je jeden z najpoužívanejších útokov. Hlavným cieľom je zostaviť zoznam, nazývaný slovník. Ten obsahuje užívateľské heslá, typické pre ľudské uvažovanie. Následne sa s pomocou tohto slovníka snaží útočník uhádnuť heslo. Heslá v tomto slovníku môžu mať ďalej určenú prioritu a byť testované s vyššou pravdepodobnosťou úspechu, čo môže znížiť časovú náročnosť útoku. Pretože užívatelia si vyberajú heslá, ktoré možno predvídať, účinnosť takéhoto útoku môže byť vysoká. [15]

1.3.2 Brute-Force Attack (Útok hrubou silou)

Útok hrubou silou je veľmi podobný slovníkovému útoku s tým rozdielom, že pri útoku sa skúša každá možná kombinácia hesla. Takisto môžu byť kombinácie týchto hesiel uprednostňované v poradí na základe určitej pravdepodobnosti. S dostatočným výpočtovým výkonom a časom je možné nájsť požadovanú zhodu, no čím väčší je heslový priestor, tým sa šanca prehľadať ho znižuje. [15]

1.3.3 Malware

Malware, skratka pre zlomyseľný softvér, je označenie pre rôzny typ softvéru, ktorý je do zariadenia pridaný bez vedomia a súhlasu jeho majiteľa. Malware často obsahuje rôzne vírusové programy. Hlavným cieľom takéhoto softvéru je tajne zhromažďovať užívateľské dáta zo zariadenia a následne zabezpečiť, aby ich útočník získal. [15]

1.3.3.1 Keylogger

Keylogger je typ malvéru, ktorý je primárne určený pre zaznamenávanie stlačenia klávesov na klávesnici. Môže sa dostať do zariadenia rôznymi spôsobmi. Keylogger, keďže je považovaný za malvér, je schopný prakticky vykonávať rôznu špionáž v zariadení. Existujú keyloggery, ktoré dokážu zaznamenávať iba stlačenia klávesov, ale aj dokonalejšie verzie, ktoré dokážu napríklad zaznamenávať prihlasovacie dáta, ktoré boli zadané, bez použitia stlačení jednotlivých klávesov na klávesnici alebo dáta, ktoré boli kopírované. [16]

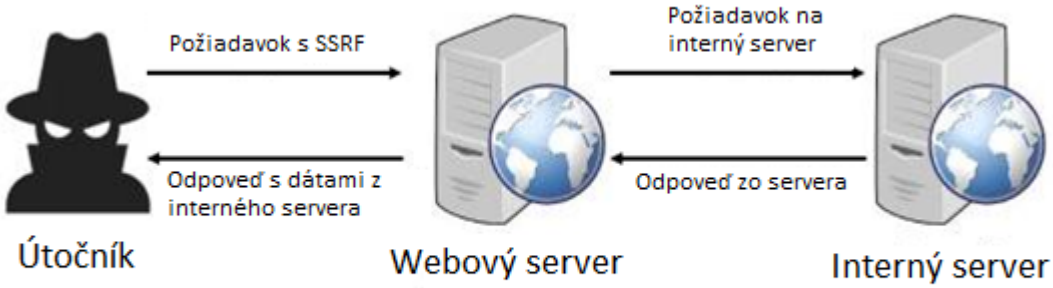
1.3.4 Man-in-the-middle-attack

Man in the middle attack je typ útoku, kde sa útočník nachádza v strede medzi klientom a serverom a tým dokáže vidieť komunikáciu, ktorá medzi nimi prebieha. Bez zabezpečeného spojenia môže útočník bez námahy vidieť a zaznamenať celý prenos dát, stačí mu, ak sa dokáže dostať medzi klienta a server, napríklad predstieraním, že je súčasťou siete. Pre eliminovanie tejto hrozby boli vyvinuté protokoly, z ktorých najnovší je TLS (Transport Layer Security), ktoré zabezpečujú šifrovanú komunikáciu pomocou rôznych kľúčov, ku ktorým útočník nemá prístup. [17]

1.4 Útoky na aplikačnú logiku

1.4.1 SSRF (Server Side Request Forgery)

SSRF je typ útoku, pri ktorom je funkcionalita servera použitá pre prístup alebo úpravu vnútorných údajov. Útok prebieha tak, že je serveru dodaná upravená adresa URL, ktorú server dokáže prečítať. Ak útočník dokáže vybrať tie správne URL adresy, dokáže vidieť do vnútra servera, získať prístup k databázovým a iným službám a vykonávať rôzne požiadavky. Týmto spôsobom je možné získať skryté informácie v systéme, ako napríklad zdrojový kód alebo autentifikačné údaje. [18]



Obr. 16 - Schéma SSRF útoku [19]

1.4.2 XSS (Cross-Site Scripting)

Cross-site scripting je založený na vložení určitých škodlivých skriptov alebo kódu do webových stránok. Webový prehliadač iného užívateľa nemá ako overiť dôveryhodnosť takéhoto kódu, a teda ho spustí. Dôsledkom toho môže skript získať prístup k veciam, ktoré prehliadač uchováva a využíva pre interakciu s webovou stránkou alebo aj jednoducho prepísať kód stránky. Takýto typ útoku možno využiť všade tam, kde sa neošetrujú a nijak zvlášť nezakódujú vstupy od užívateľa. [20]

1.5 Kvantová výpočetná technika

1.5.1 Post-kvantová kryptografia

Post-kvantová kryptografia označuje vývoj algoritmov, schopných používať pre klasické počítače a odolných voči kvantovým počítačom. Cieľom je navrhnutie alebo vylepšenie zložitých funkcií, ktoré bude náročné prelomiť pomocou kvantových počítačov. [21]

1.5.2 Kvantový počítač

Kvantový počítač je počítačový stroj určený pre ukladanie a spracovanie dát, ktorý využíva funkcie a princípy kvantovej fyziky. Zatiaľ čo dnešné počítače používajú jednotku bit, ktorá nadobúda hodnotu 0 alebo 1, kvantový bit používajú kvantové počítače. Tieto kvantové bity môžu reprezentovať niekoľko vecí v rovnakom čase. Štruktúra kvantového počítača prináša benefity pre riešenie niektorých úloh, kde môže výkonovo hravo prekonať dnešné superpočítače. [22]

1.5.2.1 Shorov algoritmus

Shorov algoritmus, pomenovaný podľa jeho objaviteľa Petra Shora, je kvantová metóda pre faktorizáciu čísla N s časovou náročnosťou O((log N)*3) a priestorovou náročnosťou O(log N). Táto technika spolu s výkonným kvantovým počítačom dokáže prelomiť algoritmy asymetrickej kryptografie, napríklad RSA, v polynomiálnom čase, čo nedokáže žiadny klasický algoritmus. Dodáva správne výsledky s vysokou, no nie úplne istou pravdepodobnosťou, no čím viac sa algoritmus vykoná, tým sa zníži šanca, že nájdená odpoveď nebude správna. [23]

1.5.2.2 Groverov algoritmus

Groverov algoritmus, pomenovaný podľa objaviteľa Lova Grovera, je kvantová vyhľadávacia technika pre neusporiadané N záznamy s časovou náročnosťou O(N 1/2) a priestorovou náročnosťou O(log N). Považuje sa za najrýchlejší vyhľadávací algoritmus pre neusporiadané prvky. Takisto dokáže spracovať a riešiť rôzne NP problémy . Keďže sa jedná o kvantový algoritmus, podobne ako v prípade Shorovho algoritmu, dáva vysoko pravdepodobnostné výsledky a každým opakovaním sa približuje k správnemu výsledku. [24]

1.6 Bezpečnostné technológie správcov hesiel

1.6.1 Multi-faktorová autentifikácia (MFA)

Multi-faktorová autentifikácia (MFA) je mechanizmus autentifikácie, ktorému je potreba dať dodatočné overovacie informácie, aby mohol vykonať prihlásenie. MFA popri bežných prihlasovacích údajoch potrebuje minimálne jednu informáciu, aby bola schopná garantovať zvýšenú odolnosť voči útokom. Väčšinou sa metódy používané v MFA spoliehajú na tri typy dodatočných informácií:

1. **Znalosť** určitých vecí – niečo, čo vie iba užívateľ.
2. **Vlastníctvo** určitých vecí – niečo, čo vlastní iba užívateľ.
3. **Charakteristickosť** samotných ľudí – niečo, čo biologicky charakterizuje užívateľa. [25]

1.6.2 Zero-knowledge

Zero-knowledge architektúra alebo ZK protokol, je metóda, prebiehajúca medzi osobou, ktorá niečo dokazuje a osobou, ktorá to overuje. Táto osoba, označovaná aj ako dokazovateľ, vie dokázať osobe, označovanej ako overovateľ, že vie o niečom, no neodhalí skutočnú informáciu. Táto architektúra sa zvyčajne využíva v aplikáciách, ktoré vyžadujú súkromie a zabezpečenie. V systémoch, ktoré vyžadujú prihlásenie, sa architektúra používa na overenie prihlasovacích údajov bez toho, aby bolo potrebné ich odhaliť. [26]

1.6.3 Virtuálna privátna sieť (VPN)

Virtuálna privátna sieť (VPN) umožňuje IP adrese, ktorá sa presunie cez server hostiteľa takejto siete, jej skrytie. To znamená, že zdrojom, z ktorého budú pochádzať užívateľove dáta, bude práve VPN server. Takýmto riešením sa zabezpečuje ochrana dát a súkromia, keďže nežiadúce strany nezaznamenajú, akú časť internetu užívateľ navštevuje ani tok dát v danej sieti. [27]

1.6.4 Biometrická autentifikácia

Biometrická autentifikácia je technika overenia, ktorá záleží na potvrdení identity užívateľa pomocou jeho biologických znakov. Po získaní týchto údajov sa porovnávajú s predošlými údajmi, ktoré patria užívateľovi. Ak sú obe vzorky týchto údajov identické, systém môže vykonať prihlásenie. Pri autentifikácii sa často používajú rôzne formy systémov:

1. Sietnicové skenery
2. Skenery dúhovky
3. Skenery odtlačkov prstov
4. Skenery geometrie rúk
5. Skenery pre rozpoznávanie tváre
6. Skenery pre rozpoznávanie žíl

[28]

1.6.5 Funkcie pre odvodenie kľúča

Password-Based Key Derivation Function 2 (PBKDF2) je funkcia odvodenia kľúča. Je navrhnutá tak, aby pre procesor vytvárala náročné výpočtové operácie a tým zvýšila odolnosť systému proti útokom. Zahŕňa to opakované použitie pseudonáhodnej funkcie, ktorá vytvára kľúčový materiál z vstupných hodnôt funkcie, ako sú vstupné heslo, dodatok - salt, počet iterácii a požadovaná dĺžka výsledného kľúča. [29]

Argon2 je pamäťovo náročná, viacúčelová funkcia, ktorá primárne slúži ako hashovacia funkcia alebo funkcia pre odvodenie kľúča. Existujú dve verzie funkcie, ktorými sú Argon2d a Argon2i. Argon2d je rýchlejšia verzia ako verzia Argon2i. Argon2 používa funkciu kompresie a hashovaciu funkciu. Funkcia má dva primárne vstupy – správu a nonce, teda heslo a dodatok (salt), ktoré sa použijú pre hashovanie hesla. Ostatné vstupy sú sekundárne, ako napríklad paralelizmus. Ak nie je použitý stupeň paralelizmu ako vstupný parameter, funkcia G je jednoducho iterovaná zvoleným počtom opakovaní. [30]

II. PRAKTICKÁ ČASŤ

2 APLIKAČNÉ MOŽNOSTI ÚTOKOV

2.1 Kryptografické algoritmy

2.1.1 Kryptoanalýza AES-256

AES-256 predstavuje najbezpečnejší šifrovací algoritmus. Potencionálny útočník by pre nájdenie správneho kľúča potreboval prejsť 2^{256} možností, čo predstavuje neskutočné obrovské číslo. Platí, že AES-256 je plne odolný voči útoku hrubou silou, pretože s dnešnou výpočtovou technikou by jeho prelomenie trvalo prinajmenšom miliardy rokov.

V roku 2009 bola objavená možnosť útoku s názvom related-key attack. Táto metóda pomocou rozdielnych kľúčov skúma, ako samotná šifra pracuje, no dá sa využiť iba pri nesprávnej konfigurácii systému, ktorý využíva AES.

Najväčšia hrozba prichádza v podobe útoku postrannými kanálmi. Zmyslom takéhoto útoku je zber informácii, ktoré zo systému unikajú, ako napríklad rôzne zvukové a elektromagnetické signály. Je teda nutné tieto riziká eliminovať či už odstránením takýchto únikov alebo ich maskovaním (vytváranie ďalších signálov a zvukov). Opäť platí, že pri správnej realizácii AES, bude systém odolný aj proti takýmto typom útoku. [31]

2.1.2 Kryptoanalýza ChaCha20

ChaCha sa stáva stále populárnejšou šifrou, dokonca aj medzi správcami hesiel. Napriek niekoľkým pokusom o prelomenie slabších verzií z rodiny ChaCha, žiadne slabiny neboli objavené alebo potvrdené v plnej verzii tejto šifry. Podobne ako v prípade AES, útok hrubou silou tu nie je prakticky možný, pretože ChaCha takisto využíva 256-bitový kľúč. Šifra takisto vykazuje odolnosť voči rôznym praktikám kryptoanalýzy.

V teoretickej rovine je možné vykonať isté útoky zamerané na pamäť a dáta, no časová náročnosť týchto útokov nevychádza menej ako 2^{256}.

ChaCha, podobne ako AES, pri nesprávnej konfigurácii môže čeliť útokom postrannými kanálmi, ničmenej správne nastavenie systému a aplikovanie známych opatrení dokáže predísť tomuto riziku. [32]

2.1.3 Použitie kryptoanalýzy

Vzhľadom k tomu, že na AES-256 a ChaCha20 bolo vykonaných niekoľko pokusov o prelomenie, nebol zaznamenaný žiadny významnejší úspech narušenia ich konštrukcie a integrity. Oba šifrovacie algoritmy sú plne odolné voči bežne známym, ale aj sofistikovanejším útokom. V súčasnosti a ani v blízkej budúcnosti, keďže sa predpokladá, že oba algoritmy budú odolné voči kvantovým počítačom, zrejme nebudú objavené žiadne významnejšie slabiny, ktoré by mohli narušiť ich bezpečnosť. Správcovia sa v tomto ohľade nemusia obávať o kryptoanalytické útoky na algoritmy, ktoré používajú pre šifrovanie a dešifrovanie ukladaných dát.

2.2 Prelomenie hlavného hesla

Hlavné heslo používajú správcovia pre šifrovanie a dešifrovanie ukladaných údajov. Predstavuje kľúč, vďaka ktorému má užívateľ prístup ku svojej databáze.

V prípade online aj offline správcu platí, že ak sa útočník bude chcieť zmocniť údajov uložených v databáze, nebude ju schopný bez hlavného hesla dešifrovať, preto je odporúčané zvoliť si dostatočne bezpečné a dlhé heslo, aby bola eliminovaná hrozba vykonania slovníkového útoku (1.3.1) alebo útoku hrubou silou (1.3.2).

2.2.1 Náročnosť útoku hrubou silou

Rovnica vykonania útoku hrubou silou sa udáva nasledovne :

$$Možné\ kombinácie\ hesiel = \ počet\ možných\ znakov^{\ dĺžka\ hesla}$$

Výsledkom sú možné kombinácie všetkých hesiel. Tento výsledok je nakoniec delený počtom možných vykonaní takýchto pokusov za sekundu, ktorý sa môže líšiť v závislosti od výkonu použitého hardvéru. Finálny výsledok je časová náročnosť útoku uvedená v sekundách. [33]

Čím komplikovanejšie heslo, tvorené rozličnými znakmi z klávesnice, malými aj veľkými písmenami a číslami, tým sa náročnosť jeho prelomenia rapídne zvyšuje. V prípade komplexného a dostatočne dlhého hesla je prakticky nemožné nájsť zhodu.

2.2.2 Infikovanie keyloggerom

Závažná situácia nastáva v prípade prítomnosti malvéru v zariadení. Ak je zariadenie infikované, špeciálne keyloggerom (1.3.3.1), napriek tomu, že užívateľ používa správcu hesla, útočník môže získať prístup nielen k hlavnému heslu od jeho trezoru ale aj k všetkým údajom a heslám, ktoré užívateľ použije. Žiadny správca nie je úplne schopný ochrániť údaje pred sofistikovaným keyloggerom, alebo iným druhom malvéru. [16]

2.3 Prenos dát v online správcoch hesla

V prípade online správcov je dôležité zaistiť nie len samotnú bezpečnosť dát, ale aj ich bezpečný prenos zo servera a na server. Preto správcovia zabezpečujú samotný kanál, cez ktorý komunikuje klient a server, pomocou protokolov, ktoré dohliadajú na to, aby odosielané dáta boli vo forme šifrovaného a nie otvoreného textu. [34]

Šifrovaním komunikácie sa predchádza útoku Man-in-the-middle-attack (1.3.4), nakoľko útočník nachádzajúci sa medzi serverom a klientom, bude zaznamenávať iba šifrované texty dát, ktoré nebude schopný dešifrovať.

V prípade, že komunikačný kanál nie je nijak zabezpečený šifrovaním, dáta sú prenášané v bežnej textovej podobe a nechránené voči možným pokusom o ich získanie.

2.4 Aplikovanie útokov na webové aplikácie

2.4.1 Aplikovanie XSS

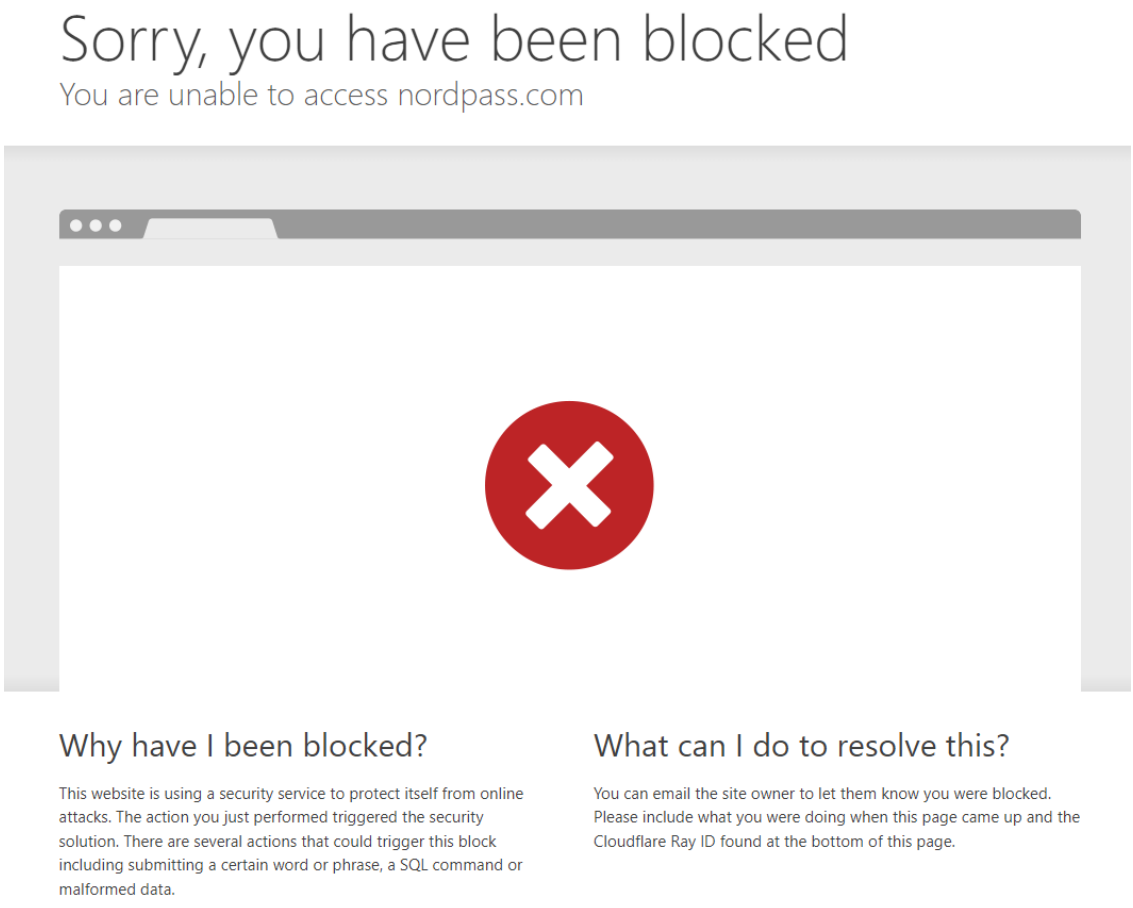
Nesprávne ošetrené vstupy webových stránok a aplikácií dávajú šancu aplikovať rôzne útoky založené na báze vloženia škodlivého skriptu alebo kódu.

Samotný správcovia svojím aktuálnym riešením neposkytujú modely, možné pre aplikovanie XSS útoku priamo v ich webových aplikáciách. Problém však môže nastať, ak je nejaká iná webová stránka zraniteľná voči XSS. V tom prípade je teoreticky možné nájsť spôsoby ako sa pokúsiť zmocniť uživateľských údajov.

2.4.2 Aplikovanie SSRF

Pri aplikácii SSRF útoku (1.4.1) sa útočník nesnaží vsunúť skript alebo kód, ale upravenú URL adresu. Týmto spôsobom sa snaží odoslať požiadavok za účelom získania informácií zo servera.

V prípade aplikovania akokoľvek upravenej URL adresy, správcovia vykonávajú automatické odhlásenie. V prípade NordPassu vybehlo okno oznamujúce zablokovanie prístupu (Obr. 17). To znamená, že správcovia určitým spôsobom ošetrujú užívateľské vstupy, alebo inak kontrolujú odosielané požiadavky.



Obr. 17 - Oznámenie o zablokovaní prístupu k NordPass

3 BUDÚCE MOŽNOSTI PRELOMENIA

3.1 Využitie kvantových počítačov

3.1.1 Prelomenie šifrovacích algoritmov kvantovým počítačom

Mnoho kryptografických riešení je ohrozených s príchodom kvantových počítačov, hlavne algoritmy využívajúce šifrovanie verejným kľúčom, založené na faktorizácii alebo diskrétnych logaritmoch a to použitím Shorovho algoritmu (1.5.2.1). Takýmto algoritmom je napríklad RSA. Rozdielna situácia nastáva pri algoritmoch využívajúcich symetrické šifrovanie, u ktorých sa predpokladá odolnosť voči kvantovým počítačom, a to dvojnásobným zvýšením dĺžky šifrovacieho kľúča kvôli eliminovaniu rizika Groverovho algoritmu (1.5.2.2). [35]

3.1.2 Protokol TLS a kvantové počítače

Protokol TLS (Transport Layer Security), ktorý bol vyvinutý za účelom šifrovania komunikácie, je kvôli používaným asymetrickým algoritmom nedostatočne bezpečný voči kvantovým počítačom. Má hlavne dve slabiny :

- Pomocou asymetrickej kryptografie dochádza k výmene kľúčov, z ktorej sa získava symetrický kľúč, pomocou ktorého sa šifruje komunikácia. U symetrických algoritmoch, narozdiel od asymetrických, stačí zvýšiť dĺžku ich kľúča, aby boli plne odolné voči kvantovým počítačom.
- V komunikácii si pomocou verejného kľúča server s klientom overujú identity pomocou asymetrických algoritmov určených na podpisovanie – RSA a elektronický podpis.

V budúcnosti bude potrebné nahradiť aktuálne asymetrické algoritmy za algoritmy, ktoré budú vykazovať odolnosť voči klasickým aj kvantovým počítačom. [36]

3.2 Vplyv kvantových počítačov na správcov

Zo zistených poznatkov o kvantových počítačoch boli vyhodnotené nasledujúce závery:

1. Kvantové počítače nepredstavujú riziko pre aktuálne postupy symetrického šifrovania dát. Správcovia používajú silné symetrické šifrovacie algoritmy, považované za kvantovo odolné.
2. V prípade online správcov zrejme nastanú zmeny v komunikácii medzi klientom a serverom, nakoľko bude potrebné nahradiť asymetrické šifrovacie postupy, aby nedošlo k narušeniu prenosu dát.
3. Výkonný kvantový počítač dokáže znížiť časovú náročnosť potrebnú na hádanie hesiel, no zvýšením komplexnosti a dĺžky používaných hesiel, ideálne na dvojnásobok, by sa malo predísť riziku ich prelomenia.

4 NAJPOUŽÍVANEJŠÍ SPRÁVCOVIA A ICH ZABEZPEČENIE

Existuje mnoho nástrojov pre správu hesiel. V tejto časti je vyhodnotených a popísaných 6 z tých najpopulárnejších a najznámejších správcov – NordPass, Dashlane, LastPass, BitWarden, Sticky Password a 1Password, ktorí sa nachádzajú aj v rebríčku najlepších správcov pre rok 2022, vytvoreným populárnym časopisom zo sveta počítačov – PCMag. [37]

4.1 NordPass

NordPass je jeden z aktuálne najpopulárnejších správcov hesiel, vytvorený spoločnosťou Nord Security. Je dostupný v bezplatnej a v prémiových verziách. Disponuje rozšíreniami pre všetky známe prehliadače pre pohodlnejšie narábanie a využívanie uložených hesiel.

NordPass má podobu desktopovej aplikácie alebo mobilnej aplikácie s využitím hlavného hesla. Dokáže generovať veľmi silné a komplikované heslá a ukladá ich do svojho šifrovacieho trezoru. Dáta sú šifrované lokálne priamo v zariadení. Vďaka automatickému vyplňovaniu prihlasovacích údajov, je možné tvoriť veľmi dlhé heslá a nie je nutné sa obťažovať s ich vypĺňaním. Vo svojom balíku služieb ponúka aj vlastnú VPN sieť. [38]

4.1.1 Zhodnotenie

4.1.1.1 Šifrovanie

NordPass je inovatívny správca hesla. Snaží sa využívať najnovšie technológie v oblasti šifrovania a derivačných funkcii, dôkazom toho je uprednostnenie rozšírenej verzie ChaCha20, ktorá je rýchlejšia ako AES- 256 a derivačnej funkcie Argon2. Ako správny online správca je postavený na architektúre Zero-knowledge, čím nedrží hlavné heslo ani šifrovacie kľúče v databáze, pretože šifrovanie prebieha na úrovni zariadenia a následne sa šifrované dáta posielajú na server. [39]

4.1.1.2 Autentifikácia

NordPass podporuje multi-faktorovú autentifikáciu pomocou autentifikačných aplikácií alebo fyzických kľúčov, napríklad USB. Zvyšuje tak ochranu proti neautorizovaným vstupom do trezoru. V mobilnej aplikácii je možnosť nastavenia biometrickej autentifikácie ako pokročilej metódy overovania namiesto používania hlavného hesla.

4.1.1.3 Zabezpečenie komunikácie

Šifrovanie procesu zdieľania dát je dôležité pre dosiahnutie zabezpečeného spojenia. NordPass pri tejto komunikácii zabezpečuje prenos dát pomocou protokolu TLS a princípov asymetrickej kryptografie – súkromného a verejného kľúča. [39]

4.1.1.4 Audity a záznamy

NordPass prešiel aj niekoľkými nezávislými rozbormi a auditmi. [39]

Z výskumu technickej univerzity v Ontáriu vyplýva, že doteraz nebola nájdená výrazná slabina alebo nedostatok v zabezpečení systému. [48]

4.2 Dashlane

Dashlane je jedným z popredných správcov hesiel, vyvinutý spoločnosťou Dashlane. Je dostupný v bezplatnej verzii Free a taktiež ponúka plány Business, Individual a Family. Disponuje množstvom funkcii a poskytuje užívateľom bezproblémové ukladanie hesiel a jednoduché narábanie.

Dashlane je správca, ktorý sa správa ako rozšírenie v prehliadači, webová aplikácia alebo mobilná aplikácia. Pre prístup k obsahu trezoru využíva hlavné heslo, pomocou ktorého sa dáta lokálne šifrujú a ukladajú do zariadenia. Obsahuje generátor komplikovaných reťazcov znakov, ktorý je možné si podľa potrieb nastaviť a disponuje funkciou automatického vyplňovania údajov. Vo svojom balíku ponúka VPN sieť pre bezpečnejšie prehliadanie internetu. [40]

4.2.1 Zhodnotenie

4.2.1.1 Šifrovanie

Dashlane pre šifrovanie dát využíva najznámejší a najpoužívanejší šifrovací štandard AES- 256**.** Dashlane dokáže pracovať s oboma funkciami pre odvodenie kľúča, ktorými sú Argon2 a PBKDF2 a je na samotnom užívateľovi, ktorú z nich si vyberie alebo bude preferovať. Jeho architektúra je založená na modeli Zero-knowledge, takže nikto okrem užívateľa nemôže mať prístup k dátam, nakoľko iba on pozná hlavné heslo. [34]

4.2.1.2 Autentifikácia

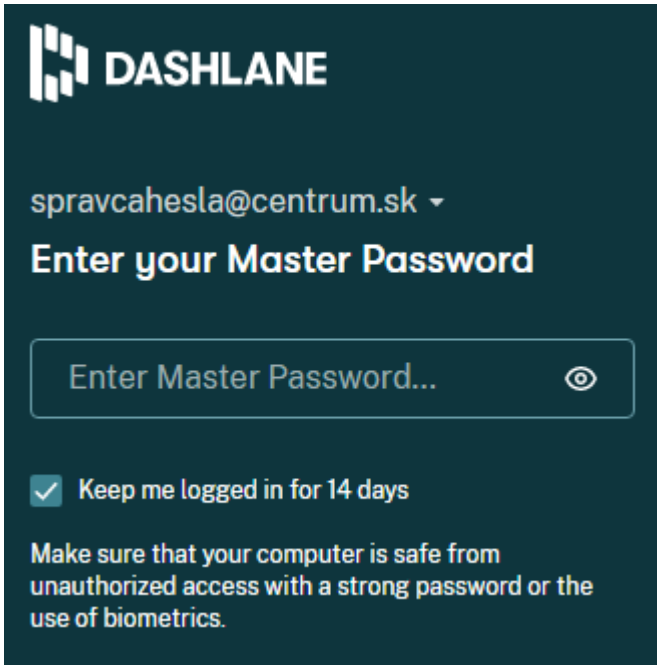
Dashlane podporuje dodatočné zabezpečenie pomocou aplikácií určených pre viacvrstvové zabezpečenie. V mobilnej aplikácii je možné zvoliť biometrický systém pre prístup k trezoru.

4.2.1.3 Zabezpečenie komunikácie

Veškerú komunikáciu medzi klientom a serverom Dashlane zabezpečuje cez HTTPS, ktorý využíva protokol TLS. Ten zabezpečuje šifrovanú komunikáciu pomocou certifikátov a šifrovacích kľúčov. [34]

4.2.1.4 Zistené nedostatky

Zjavným nedostatkom sa javí možnosť zapamätania prihlásenia vo webovej aplikácii po dobu 14 dní, ktorá súvisí s tým, že po vypnutí prehliadača sa správca automaticky odhlási a je nutné opäť zadávať hlavné heslo. Ak je povolené takéto automatické prihlásenie, vytvára to obrovské riziko v prípade straty alebo odcudzenia zariadenia, takisto aj v prípade nepovoleného prístupu do zariadenia.



Obr. 18 - Možnosť zapamätania prihlásenia - Dashlane

4.2.1.5 Audity a záznamy

Systém CVE, ktorý udržiava záznamy o zistených slabinách a hrozbách v systémoch, tu má jeden záznam o potvrdenom nedostatku z minulých čias, kedy ešte Dashlane využíval desktopovú aplikáciu. [49]

4.3 LastPass

LastPass je jedným z najstarších nástrojov pre správu hesiel. Je dostupný vo verzii Free a vo verzii Premium. Ponúka celú radu bohatých nástrojov a taktiež podporuje rôzne platformy a disponuje rozšíreniami pre mnohé prehliadače.

LastPass je typ správcu hesla, ktorý je navrhnutý ako webové rozhranie s možnosťou rozšírenia v akomkoľvek známom prehliadači, na rôznych operačných systémoch. Jeho súčasťou je podobne ako u ostatných moderných správcov aj efektívny generátor na heslá. Samozrejmosťou je aj funkcia pre automatické vyplňovanie údajov. Drží krok s modernými správcami, generuje komplikované heslá a pre zabezpečenie dát používa veľmi bezpečné algoritmy a funkcie. LastPass nemá vlastnú VPN ani neponúka túto technológiu vo svojom balíku. [41]

4.3.1 Zhodnotenie

4.3.1.1 Šifrovanie

Heslá a údaje sú v LastPass šifrované a dešifrované lokálne na úrovni zariadenia – táto technika sa nazýva Zero-knowledge. Pre šifrovanie dát využíva známy symetrický šifrovací štandard AES-256 spolu s funkciou pre odvodenie kľúča PBKDF2 pre maximálnu ochranu údajov. [42]

4.3.1.2 Autentifikácia

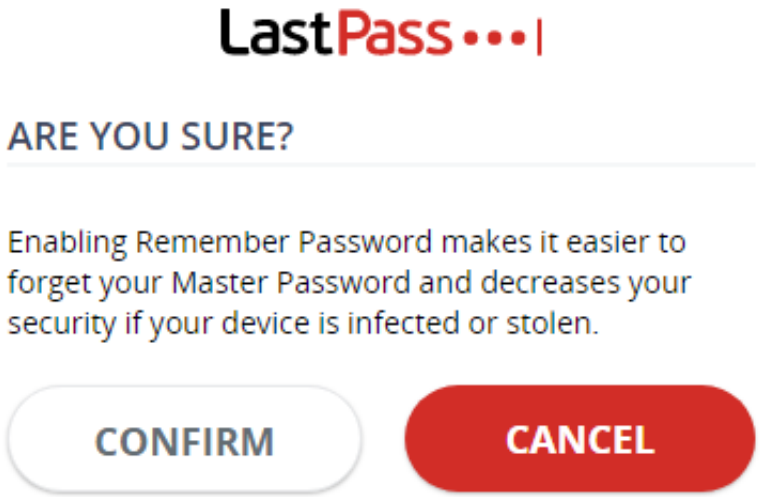
LastPass využíva autentifikáciu na základe hlavného hesla. Je možné aktivovať multi-faktorovú autentifikáciu pomocou rôznych aplikácií, disponuje aj vlastnou aplikáciou s názvom LastPass MFA. V mobilných zariadeniach umožňuje aktivovanie biometrickej autentifikácie.

4.3.1.3 Zabezpečenie komunikácie

Pre bezpečné zdieľanie dát LastPass zabezpečuje komunikačný kanál pomocou protokolu TLS, aby sa zabránilo odpočúvaniu komunikácie a zaistila ochrana pri prenose šifrovaných dát. [42]

4.3.1.4 Zistené nedostatky

Podobne ako v prípade Dashlane, LastPass má možnosť zapamätania prihlásenia (Obr.19), čo zvyšuje riziko neautorizovaného prístupu ku všetkým heslám a údajom v trezore. Aj keď pred týmto krokom samotný správca užívateľov varuje, táto možnosť by nemala byť v správcovi dostupná.



Obr. 19 - Možnosť zapamätania prihlásenia – LastPass

4.3.1.5 Audity a záznamy

Systém CVE má u LastPassu zaznamenaných 6 záznamov o zistených nedostatkoch v systéme. Tieto nedostatky sa týkajú možností obídenia niektorých autentifikačných krokov a závažných chybách v implementácii, hlavne v mobilnej verzii aplikácie. [51]

4.4 BitWarden

BitWarden je multiplatformový správca hesiel od spoločnosti Bitwarden. Poskytuje plány Business a Personal. Dokáže pracovať s takmer každým zariadením a známym prehliadačom.

BitWarden je jedným z open-source správcov hesiel, vďaka čomu sa môže ďalej rozvíjať a zvyšovať tak svoju bezpečnosť na základe odporúčaní a zistených nedostatkov zo strany užívateľov. Je dostupný v podobe desktopovej aplikácie, webového rozhrania, klasického rozšírenia v prehliadači s automatickým vypĺňaním údajov a generátorom pre tvorbu hesiel, alebo ako mobilnej aplikácie. Pre prístup k trezoru používa podobne ako ostatní správcovia hlavné heslo. [43]

4.4.1 Zhodnotenie

4.4.1.1 Šifrovanie

BitWarden nezaostáva za ostatnými správcami a pre šifrovanie dát využíva symetrický šifrovací štandard AES-256 s funkciou pre odvodenie kľúča PBKDF2 pre šifrovanie a dešifrovanie údajov. BitWarden je založený na modeli Zero-knowledge, nakoľko sa jedná o online správcu. [44]

4.4.1.2 Autentifikácia

BitWarden podporuje autentifikáciu zabezpečenú viacerými vrstvami pomocou rôznych aplikácií. V mobilnej verzii správcu podporuje nastavenie biometrickej autentifikácie namiesto používania hlavného hesla.

4.4.1.3 Zabezpečenie komunikácie

Spojenie medzi serverom BitWardenu a klientskym zariadením je zabezpečené pomocou protokolu TLS, ktorý zabezpečuje komunikáciu pomocou certifikátov a asymetrických princípov výmeny kľúčov. [44]

4.4.1.4 Open-source

BitWarden je open-source systém, čo znamená výhodu v tom, že samotná komunita je zapojená do vývoja a aktualizácie správcu, čo spôsobuje užívateľskú odozvu a pomoc pri riešení problémov, ale aj nevýhodu v zmysle, že samotné riešenie a kód je verejne dostupný a človek so zlými úmyslami môže nájsť chybu v implementácii a zneužiť ju vo svoj prospech.

4.4.1.5 Audity a záznamy

Bitwarden má za sebou niekoľko bezpečnostných auditov vykonaných rôznymi testovacími skupinami. [44]

Systém CVE tu uchováva 2 záznamy o zistených nedostatkoch spojených s nedostatočným počtom iterácií derivačnej funkcie a nedostatočnej implementácie funkcie servera, ktorá nekontrolovala požiadavky prijímané z určitých druhov IP adries, čo mohlo spôsobiť aplikovanie SSRF útoku. [52]

4.5 Sticky Password

Sticky Password je jeden zo správcov hesiel, vytvorený spoločnosťou Lamantine Software. Je dostupný vo verzii Free a v platenej verzii Premium. Disponuje celým radom nástrojov s podporou pre všetky známe zariadenia a prehliadače.

Sticky Password prichádza v podobe desktopovej aplikácie, webového rozhrania, rozšírenia v prehliadači alebo mobilnej aplikácie. Dokáže synchronizovať dáta medzi jednotlivými zariadeniami a navzájom ich bezpečne zdieľať. Automatické vypĺňanie údajov a generátor hesiel je nevyhnutnou súčasťou správcu. Takisto disponuje možnosťou uloženia správcu na zariadenia USB alebo iné pamäťové úložiská a vďaka tomu mať prístup k heslám na ktoromkoľvek zariadení. Pri zadávaní hlavného hesla je možnosť použitia virtuálnej klávesnice, poskytujúcej ochranu voči možným pokusom o sledovanie aktivity v zariadení. Sticky Password neponúka žiadnu VPN vo svojom balíku. [45]

4.5.1 Zhodnotenie

4.5.1.1 Šifrovanie

Sticky Password šifruje a dešifruje dáta lokálne pomocou šifrovacieho štandardu AES-256 a v kombinácii s funkciou pre odvodenie kľúča PBKDF2 sú šifrované dáta ukladané do trezoru. Sticky Password je založený na architektúre Zero-knowledge, teda hlavné heslo nie je ukladané ani odosielané na servery správcu, čo poskytuje ochranu v prípade úniku dát zo servera. [46]

4.5.1.2 Autentifikácia

Pre zvýšenie bezpečnosti v oblasti autentifikácie správca podporuje multi-faktorovú autentifikáciu, pomocou autentifikačných aplikácií. V mobilných zariadeniach je možné používať biometrickú autentifikáciu, napríklad odtlačky prstov.

4.5.1.3 Zabezpečenie komunikácie

Sticky Password zabezpečuje komunikáciu pomocou HTTPS, ktorý využíva protokol TLS. Protokol TLS pracuje so serverovými certifikátmi a zaisťuje šifrovaný prenos dát medzi klientom a serverom, čím predchádza pokusom o infiltrovanie komunikácie. [46]

4.5.1.4 Audity a záznamy

O tomto správcovi nie sú vedené žiadne vykonané audity alebo rozbory, takisto nemá zaznamenané žiadne záznamy v systéme CVE, preto nie je možné potvrdiť žiadne slabiny alebo chyby v zabezpečení.

4.6 1Password

1Password je multiplatformový správca hesla. Je dostupný v plánoch Personal, Families a Business, ale nie vo verzii Free. Podobne ako ostatní správcovia ponúka množstvo nástrojov na zabezpečenie a jednoduché narábanie s dátami.

1Password je správca hesla, ktorý je dostupný ako desktopová aplikácia, rozšírenie v prehliadači alebo mobilná aplikácia. Má v sebe zabudovaný generátor hesiel a taktiež dokáže automaticky vyplňovať údaje naprieč webovými stránkami. Synchronizuje dáta medzi všetkými zariadeniami. Pre prístup k obsahu svojho trezoru vyžaduje hlavné heslo, ktorým sa šifrujú a dešifrujú ukladané údaje [47]

4.6.1 Zhodnotenie

4.6.1.1 Šifrovanie

1Password pre šifrovanie používa symetrický šifrovací štandard AES-256 a funkciou pre odvodenie kľúča PBKDF2 pre maximálnu bezpečnosť dát. 1Password je založený na modeli Zero-knowledge, čím sa svojou kvalitou zaraďuje medzi najlepších a najbezpečnejších správcov. [48]

4.6.1.2 Autentifikácia

1Password v nastaveniach podporuje povolenie multi-faktorovej autentifikácie pomocou autentifikačných aplikácií, ktoré generujú jednorazové kódy. V mobilnej aplikácii je možnosť používania inovatívnej biometrickej metódy prihlasovania.

4.6.1.3 Zabezpečenie komunikácie

Medzi serverom a klientom 1Password zabezpečuje komunikáciu pomocou protokolu TLS, ktorý je súčasťou HTTPS. Tento protokol poskytuje zabezpečenie prenášaným údajom a chráni ich pred neoprávneným získaním. [48]

4.6.1.4 Audity a záznamy

S ohľadom na bezpečnosť, systém CVE má pri tomto správcovi zaznamenaných 9 objavených nedostatkov a slabín, čo je najviac spomedzi hodnotených správcov. Tieto záznamy sa týkajú hlavne nedostatkov v konštrukcii mobilnej a webovej verzie správcu a prasklinám v zabezpečení na strane jeho servera. [53]

4.7 Tabuľka hodnotených správcov

Na základe zistených informácií bola z hodnotených správcov zostavená tabuľka (Tab.1), ktorá ich porovnáva na základe faktorov kvality. Určené faktory odrážajú technológie, ktoré správcovia používajú pre zabezpečenie údajov, doplnkové služby ponúkajúce vo svojom balíku (VPN) , dostupnosť a záznamy o zistených nedostatkoch.

	NordPass	Dashlane	LastPass	BitWarden	Sticky Password	1Password
Šifrovanie	XChaCha20	AES-256	AES-256	AES-256	AES-256	AES-256
Funkcia pre odvodenie kľúča	Argon2	Argon2 / PBKDF2	PBKDF2	PBKDF2	PBKDF2	PBKDF2
Podpora MFA	✓	✓	✓	✓	✓	✓
Pokročilé autentifikačné metódy	✓	✓	✓	✓	✓	✓
Zero-knowledge	✓	✓	✓	✓	✓	✓
Bezpečné zdielanie dát	✓	✓	✓	✓	✓	✓
Doplňujúce služby v baliku	✓	✓	✗	✗	✗	✗
Free verzia	✓	✓	✓	✓	✓	✗
Zistené nedostatky a slabiny	✗	✓	✓	✓	---	✓

Tab. 1 - Tabuľka hodnotených správcov na základe faktorov kvality

Z tabuľky vyplývajú nasledujúce výsledky:

1. Všetci hodnotení správcovia dodržujú bezpečnostné normy a na zabezpečenie používajú špičkové šifrovacie algoritmy a moderné technológie. Najviac inovatívny správca je NordPass, ktorý používa novší šifrovací štandard aj derivačnú funkciu v porovnaní s ostatnými správcami.
2. V oblasti autentifikácie zabezpečujú správcovia viacvrstvové overovanie identity pomocou MFA, v mobilných aplikáciách aj pomocou biometrického systému. Takisto dokážu bezpečne zdieľať dáta medzi užívateľmi.
3. Doplnkové služby v prémiovom balíku, napríklad VPN, ponúkajú iba NordPass a Dashlane.
4. Dostupnosťou bezplatnej verzie nedisponuje iba 1Password, ktorý je dostupný iba v prémiových plánoch.
5. U NordPassu, ako jediného správcu, neboli zistené žiadne výrazné nedostatky a chyby v zabezpečení systému. Sticky Password doteraz nebol dôkladnejšie hodnotený, nie sú o ňom vedené žiadne záznamy ani audity a teda nie je možné určiť jeho nedostatky. U zvyšných správcov je vedený minimálne jeden záznam o nájdenej slabine v zabezpečení systému.

ZÁVER

Práca je orientovaná na rozbor správcov hesla z pohľadu ich bezpečnostného aspektu a technológiám používaným pri ich zabezpečení, cieľom práce bolo poskytnúť prehľad o bezpečnosti správcov pri ochrane prihlasovacích alebo iných osobných údajov používaných na internete a poukázať na ich silné stránky, no zároveň aj hrozby, ktoré aktuálne alebo v neskorších dobách môžu ohroziť ich ochranu.

V prvej časti práce boli popísané základné teoretické pojmy spojené so správcami, ich členenie a zmysel používania. Malá časť sa venovala aj historickému vývoju samotnej autentifikácie. K základným teoretickým pojmom z oblasti kryptografie bol pridaný rozbor kryptografických algoritmov AES a ChaCha20, ktoré sú priamo spojené s používaním správcov. Rozbor sa venoval jednotlivým krokom a procesom, ktoré zabezpečujú šifrovanie a dešifrovanie dát. Nasledoval popis najznámejších útokov, nie len na heslá samotné, ale aj na logiku webových aplikácií. V spojení s budúcimi hrozbami nechýbala teória kvantových počítačov a kvantových algoritmov. Prvú časť uzatváral prehľad o bezpečnostných technológiách používaných v náväznosti na správcov hesiel, ktoré tvorili aj derivačné funkcie pre odvodenie kľúčov.

V druhej časti boli popísané aplikačné možnosti spomínaných útokov, uvedené boli informácie o kryptoanalytických pokusoch na šifrovacie algoritmy, hrozbách spojených s útokmi na heslá alebo webové aplikácie, bezpečnosti prenášaných dát medzi užívateľským zariadením a servorom správcu a vplyve kvantových počítačov na budúcnosť správcov. Záver práce sa zameral na rozbor šiestich najpopulárnejších správcov, ktorý vyhodnocoval bezpečnosť a používané technológie a následne pomocou vytvorenej tabuľky porovnával správcov medzi sebou na základe vybraných vlastností.

ZOZNAM POUŽITEJ LITERATÚRY

[1] Password. *TechTerms* [online]. 2006 [cit. 2022-05-09]. Dostupné z: https://techterms.com/definition/password

[2] Password Manager. *Zoho* [online]. c2022 [cit. 2022-05-09]. Dostupné z: https://www.zoho.com/vault/educational-content/what-is-a-password-manager.html

[3] Password manager. *Malwarebytes* [online]. c2022 [cit. 2022-05-09]. Dostupné z: https://www.malwarebytes.com/what-is-password-manager

[4] A short history of passwords. *SplashID* [online]. 2016 [cit. 2022-05-11]. Dostupné z: https://blog.splashid.com/a-short-history-of-passwords/

[5] The History And Future Of Passwords (And What's Next) - infographic. *DIGITAL INFORMATION WORLD* [online]. 2020 [cit. 2022-05-11]. Dostupné z: https://www.digitalinformationworld.com/2020/05/what-comes-after-passwords-infographic.html

[6] SHALLAL, Qahtan M. a Mohammad Ubaidullah BOKHARI. A Review on Symmetric Key Encryption Techniques in Cryptography. In: *International Journal of Computer Applications* [online]. 2016, s. 43-48 [cit. 2022-05-16]. ISSN 0975-8887. Dostupné z: https://www.researchgate.net/publication/333118027_A_Review_on_Symmetric_Key_Encryption_Techniques_in_Cryptography

[7] Asymmetric Encryption: Definition, Architecture, Usage. *Okta* [online]. c2022 [cit. 2022-05-16]. Dostupné z: https://www.okta.com/identity-101/asymmetric-encryption/

[8] AMIROVÁ, Kamilla. Blokové šifry. *Úvod do kryptografie* [online]. c2007 [cit. 2022-05-16]. Dostupné z: https://sifrovani.fd.cvut.cz/blok_sifr.html

[9] AMIROVÁ, Kamilla. Proudové šifry. *Úvod do kryptografie* [online]. c2007 [cit. 2022-05-16]. Dostupné z: https://sifrovani.fd.cvut.cz/prou_sifr.html

[10] DAEMEN, Joan a Vincent RIJMEN. *The Design of Rijndael: The Advanced Encryption Standard (AES)* [online]. 2nd edition. Springer, c2002-2020 [cit. 2022-05-16]. ISBN 978-3-662-60769-5. Dostupné z: https://www.academia.edu/44353417/The_Design_of_Rijndael_The_Advanced_Encryption_Standard_AES_Second_Edition

[11] FIPS Publication 197 : ADVANCED ENCRYPTION STANDARD (AES). In: *Federal Information Processing Standards Publications (FIPS PUBS)* [online]. November 26, 2001 [cit. 2022-05-16]. Dostupné z: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

[12] BERNSTEIN, Daniel J. *The Salsa20 family of stream ciphers* [online]. The University of Illinois at Chicago, 2005 [cit. 2022-05-16]. Dostupné z: https://cr.yp.to/snuffle/salsafamily-20071225.pdf

[13] BERNSTEIN, Daniel J. *ChaCha, a variant of Salsa20* [online]. The University of Illinois at Chicago, 2008 [cit. 2022-05-16]. Dostupné z: http://cr.yp.to/chacha/chacha-20080128.pdf

[14] Salsa20. *CRYPTO-IT* [online]. c2022 [cit. 2022-05-16]. Dostupné z: http://www.crypto-it.net/eng/symmetric/salsa20.html

[15] PRASAD, Ch. Krishna a A. Ramesh BABU. Evolution of Authentication Mechanisms. In: *International Journal of Computer Science and Mobile Computing (IJCSMC)* [online]. 11 November 2013, s. 166-174 [cit. 2022-05-16]. ISSN 2320–088X. Dostupné z: https://ijcsmc.com/docs/papers/November2013/V2I11201351.pdf

[16] NOTENBOOM, Leo. Will Using a Password Vault Thwart a Keylogger? | Ask Leo!. *YouTube* [online]. 2021 [cit. 2022-05-16]. Dostupné z: https://www.youtube.com/watch?v=J0kCzHNasZ4

[17] Man in the middle attack. *Multi Agent Systems on the University of Groningen* [online]. c2011 [cit. 2022-05-16]. Dostupné z: https://www.ai.rug.nl/mas/finishedprojects/2011/TLS/hermsencomputerservices.nl/mas/mitm.html

[18] DEMIR, Busra. A Pentester's Guide to Server Side Request Forgery (SSRF). *Cobalt* [online]. 2020 [cit. 2022-05-16]. Dostupné z: https://www.cobalt.io/blog/a-pentesters-guide-to-server-side-request-forgery-ssrf

[19] BOUKAR, A. Server-Side Request Forgery (SSRF) Explained. *Patch The Net* [online]. 2022 [cit. 2022-05-16]. Dostupné z: https://patchthenet.com/articles/web-application-security/server-side-request-forgery-ssrf-explained/

[20] S., Kirsten. Cross Site Scripting (XSS). *OWASP* [online]. c2022 [cit. 2022-05-16]. Dostupné z: https://owasp.org/www-community/attacks/xss/

[21] GILES, Martin. Explainer: What is post-quantum cryptography?. *Technology Review* [online]. 2019 [cit. 2022-05-16]. Dostupné z: https://www.technologyreview.com/2019/07/12/134211/explainer-what-is-post-quantum-cryptography/

[22] DONNA, Lu. What is a quantum computer?. *New Scientist* [online]. [cit. 2022-05-16]. Dostupné z: https://www.newscientist.com/question/what-is-a-quantum-computer/

[23] Shor's factoring algorithm. *Quantiki* [online]. 2015 [cit. 2022-05-16]. Dostupné z: https://www.quantiki.org/wiki/shors-factoring-algorithm

[24] Grover's search algorithm. *Quantiki* [online]. 2015 [cit. 2022-05-16]. Dostupné z: https://www.quantiki.org/wiki/grovers-search-algorithm

[25] What is Multi-Factor Authentication (MFA) and How Does it Work?. *Onelogin* [online]. c2022 [cit. 2022-05-16]. Dostupné z: https://www.onelogin.com/learn/what-is-mfa

[26] Zero-Knowledge Proofs. *Binance Academy* [online]. c2022 [cit. 2022-05-16]. Dostupné z: https://academy.binance.com/en/glossary/zero-knowledge-proofs

[27] What is VPN? How It Works, Types of VPN. *Kaspersky* [online]. c2022 [cit. 2022-05-16]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn

[28] Biometric authentication systems for identification, authentication and verification. *Boon Edam* [online]. [cit. 2022-05-16]. Dostupné z: https://www.boonedam.com/accessories-and-additions/biometric-authentication-systems

[29] VISCONTI, Andrea, Ondrej MOSNÁČEK, Milan BROŽ a Vashek MATYÁŠ. Examining PBKDF2 security margin --- case study of LUKS. In: *Journal of Information Security and Applications* [online]. 2019 [cit. 2022-05-16]. ISSN 2214-2126. Dostupné z: https://www.researchgate.net/publication/332428424_Examining_PBKDF2_security_margin_---_case_study_of_LUKS

[30] BIRYUKOV, Alex, Daniel DINU a Dmitry KHOVRATOVICH. *Argon2: the memory-hard function for password hashing and other applications* [online]. University of Luxembourg, 2015 [cit. 2022-05-16]. Dostupné z: https://www.password-hashing.net/argon2-specs.pdf

[31] Understanding AES 256 Encryption. *N-able* [online]. 2019 [cit. 2022-05-16]. Dostupné z: https://www.n-able.com/blog/aes-256-encryption-algorithm

[32] *Security Analysis of ChaCha20-Poly1305 AEAD* [online]. KDDI Research, 2017 [cit. 2022-05-16]. Dostupné z: https://www.cryptrec.go.jp/exreport/cryptrec-ex-2601-2016.pdf

[33] Brute-force attacks. *Passwrod Depot* [online]. c1998-2022 [cit. 2022-05-16]. Dostupné z: https://www.password-depot.de/en/know-how/brute-force-attacks.htm

[34] Security White Paper. *Dashlane* [online]. 2021[cit.2022-05-16]. Dostupné z: https://www.dashlane.com/download/Dashlane_SecurityWhitePaper_March2021.pdf

[35] DURMUTH, Markus, Maximilian GOLLA, Philipp MARKERT, Alexander MAY a Lars SCHLIEPER. *Towards Quantum Large-Scale Password Guessing on Real-World Distributions* [online]. Ruhr University Bochum [cit. 2022-05-16]. Dostupné z: https://eprint.iacr.org/2021/1299.pdf

[36] Post-Quantum TLS. *Microsoft* [online]. c2022 [cit. 2022-05-16]. Dostupné z: https://www.microsoft.com/en-us/research/project/post-quantum-tls/

[37] KEY, Kim a Ben MOORE. The Best Password Managers for 2022. *PCMag* [online]. 2022 [cit. 2022-05-16]. Dostupné z: https://www.pcmag.com/picks/the-best-password-managers

[38] Full-featured password manager. *NordPass* [online]. c2022 [cit. 2022-05-16]. Dostupné z: https://nordpass.com/features/

[39] NordPass Business Whitepaper. *NordPass* [online]. 2021 [cit. 2022-05-18]. Dostupné z: https://nordpass.com/business-whitepaper/

[40] THE APP THAT MAKES THE INTERNET EASIER. *Dashlane* [online]. c2022 [cit. 2022-05-22]. Dostupné z: https://www.dashlane.com/features

[41] The best way to manage passwords. *LastPass* [online]. c2022 [cit. 2022-05-16]. Dostupné z: https://www.lastpass.com/how-lastpass-works

[42] LastPass Technical WhitePaper. *LastPass* [online]. [cit. 2022-05-19]. Dostupné z: https://assets.cdngetgo.com/da/ce/d211c1074dea84e06cad6f2c8b8e/lastpass-technical-whitepaper.pdf

[43] The Bitwarden Password Manager. *BitWarden* [online]. c2022 [cit. 2022-05-16]. Dostupné z: https://bitwarden.com/products/

[44] BitWarden Security Paper. *BitWarden* [online]. 2020 [cit. 2022-05-19]. Dostupné z: https://bitwarden.com/images/resources/security-white-paper-download.pdf

[45] A bulletproof vest for your private data. *Sticky Password* [online]. c2001-2022 [cit. 2022-05-16]. Dostupné z: https://www.stickypassword.com/security

[46] The Security Behind Sticky Password: Technical White Paper. *Sticky Passowrd* [online]. 2015 [cit. 2022-05-19]. Dostupné z: https://www.stickypassword.com/downloads/Sticky_Password_Security_WhitePaper.pdf?v=3

[47] Security is not just a feature. It's our foundation. *1Password* [online]. c2022 [cit. 2022-05-16]. Dostupné z: https://1password.com/security/

[48] 1Password Security Design. *1Password* [online]. 2021 [cit. 2022-05-19]. Dostupné z: https://1passwordstatic.com/files/security/1password-white-paper.pdf

[49] GRANT, Matthew, Jamie KENNEDY, Jiechen ZHU a Jayden TAN. Security Concerns in Password Managers. *Research Gate* [online]. Ontario Tech University, 2021 [cit. 2022-05-19]. Dostupné z: https://www.researchgate.net/publication/350818744_Security_Concerns_in_Password_Managers

[50] Dashlane Search Results. *CVE* [online]. c1999-2022 [cit. 2022-05-16]. Dostupné z: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=Dashlane

[51] LastPass Search Results. *CVE* [online]. c1999-2022 [cit. 2022-05-16]. Dostupné z: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=LastPass

[52] BitWarden Search Results. *CVE* [online]. c1999-2022 [cit. 2022-05-16]. Dostupné z: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=Bitwarden

[53] 1Password Search Results. *CVE* [online]. c1999-2022 [cit. 2022-05-16]. Dostupné z: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=1Password

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

AES	Advanced Encryption Standard
CVE	Common Vulnerabilioties and Exposures
DES	Data Encryption Standard
HTTPS	HyperText Transfer Protocol Secure
IP	Internet Protocol
MIT	Massachusetts Institute of Technology
MFA	Multi-Factor Authentification
PBKDF	Password Based Key Derivation Function
RSA	Rivest Shamir Adleman
SSRF	Server Side Request Forgery
TLS	Transport Layer Security
VPN	Virtual Private Network
XOR	Exclusive OR
XSS	Cros-Site Scripting

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

ZOZNAM PRÍLOH

P I: CD s elektronickou verziou práce

PRÍLOHA P I: CD S ELEKTRONICKOU VERZIOU PRÁCE

Publikácia bakalárskej práce v PDF : fulltext.pdf