

SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE
FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Evidenčné číslo: FEI-5382-91764

PASSWORD MANAGER
BAKALÁRSKA PRÁCA

2020

Peter Čuřík

SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE
FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Evidenčné číslo: FEI-5382-91764

PASSWORD MANAGER
BAKALÁRSKA PRÁCA

Študijný program: Aplikovaná informatika
Číslo študijného odboru: 2511
Názov študijného odboru: 9.2.9 Aplikovaná informatika
Školiace pracovisko: Ústav informatiky a matematiky
Vedúci záverečnej práce: prof. Ing. Pavol Zajac, PhD.
Konzultant: unknown

Bratislava 2020

Peter Čuřík

SÚHRN

SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE
FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Študijný program:	Aplikovaná informatika
Autor:	Peter Čuřík
Bakalárska práca:	Password manager
Vedúci záverečnej práce:	prof. Ing. Pavol Zajac, PhD.
Konzultant:	unknown
Miesto a rok predloženia práce:	Bratislava 2020

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean et est a dui semper facilisis. Pellentesque placerat elit a nunc. Nullam tortor odio, rutrum quis, egestas ut, posuere sed, felis. Vestibulum placerat feugiat nisl. Suspendisse lacinia, odio non feugiat vestibulum, sem erat blandit metus, ac nonummy magna odio pharetra felis. Vivamus vehicula velit non metus faucibus auctor. Nam sed augue. Donec orci. Cras eget diam et dolor dapibus sollicitudin. In lacinia, tellus vitae laoreet ultrices, lectus ligula dictum dui, eget condimentum velit dui vitae ante. Nulla nonummy augue nec pede. Pellentesque ut nulla. Donec at libero. Pellentesque at nisl ac nisi fermentum viverra. Praesent odio. Phasellus tincidunt diam ut ipsum. Donec eget est. A skúška mäččėňov a dlžnov.

Klíčové slová: tbd

ABSTRACT

SLOVAK UNIVERSITY OF TECHNOLOGY IN BRATISLAVA
FACULTY OF ELECTRICAL ENGINEERING AND INFORMATION TECHNOLOGY

Study Programme:	Applied Informatics
Author:	Peter Čuřík
Bachelor's thesis:	Password manager
Supervisor:	prof. Ing. Pavol Zajac, PhD.
Consultant:	unknown
Place and year of submission:	Bratislava 2020

On the other hand, we denounce with righteous indignation and dislike men who are so beguiled and demoralized by the charms of pleasure of the moment, so blinded by desire, that they cannot foresee the pain and trouble that are bound to ensue; and equal blame belongs to those who fail in their duty through weakness of will, which is the same as saying through shrinking from toil and pain. These cases are perfectly simple and easy to distinguish. In a free hour, when our power of choice is untrammelled and when nothing prevents our being able to do what we like best, every pleasure is to be welcomed and every pain avoided. But in certain circumstances and owing to the claims of duty or the obligations of business it will frequently occur that pleasures have to be repudiated and annoyances accepted. The wise man therefore always holds in these matters to this principle of selection: he rejects pleasures to secure other greater pleasures, or else he endures pains to avoid worse pains.

Keywords: tbd

Podakovanie

Rád by som sa poďakoval vedúcemu tejto práce, prof. Ing. Pavlovi Zajacovi, Phd., za všetky rady, pripomienky a vedenie. Vážim si jeho trpezlivosť, každú ochotu navyše a taktiež jeho priateľský a úctivý prístup.

Obsah

Úvod	1
1 Základné pojmy	2
1.1 Heslo	2
1.2 Autentizácia	2
1.3 Sila hesla	2
2 Problém password managerov	5
3 Recitácia	6
4 Možnosti anonymizácie	7
4.1 Súkromné prehliadanie	7
4.2 Anonymná sieť	7
4.3 Funkcionalita	7
4.3.1 Funkcionalita2	7
4.4 Vzhľad	7
Záver	11
Zoznam použitej literatúry	I
Prílohy	I
A Štruktúra elektronického nosiča	II
B Algoritmus	III
C Výpis sublime	IV

Zoznam obrázkov a tabuliek

Obrázok 1	Predpokladaný vzhľad rozšírenia.	9
Tabuľka 1	Zložitosť prelomenia hesiel pomocou útoku brute-force	3
Tabuľka 2	Moduly a ich funkcie pri anonymizácii	8

Zoznam algoritmov

1	Ukážka príkazov pre algorithmic	10
B.1	Vypočítaj $y = x^n$	III

Zoznam výpisov

1	Ukážka algoritmu	9
C.1	Ukážka sublime-project	IV

Úvod

V dnešnej dobe je svet každým dňom stále väčšími digitalizovaný. Neustále vznikajú nové produkty a služby. Systémy, ktoré nám pomáhajú mať všetko na jednom mieste. Bezpečnosť týchto systémov je rovnako dôležitá, ako jej funkčnosť. Keďže uchovávajú citlivé informácie používateľov, je absolútne kľúčové ich chrániť pred útokmi. Preto veľká väčšina aplikácií a systémov, ktoré pracujú s informáciami, používa účty. Používateľ si vytvorí svoj účet a dostane sa doň pomocou dvoch vstupov: používateľského mena a hesla. Heslo jeho účet chráni, keďže používateľské meno je verejné.

Na začiatku som uvádzal, že neustále vznikajú nové produkty, služby, či systémy. Môžeme teda očakávať, že bežný človek ich bude využívať viacero na dennej báze. Po-vedzme, že používa email, má účty v niekoľkých sociálnych sieťach, používa aplikáciu na elektronické bankovníctvo, je zaregistrovaný v niekoľkých internetových obchodoch, pravidelne pristupuje k svojim dátam na cloude (online úložisko) a podobne. Každá z týchto položiek pracuje s nejakým heslom, ktorá autentifikuje osobu, ktorá heslo zadala.

Ak hovoríme o hesle ako o reťazci, teda postupnosti znakov, používateľ si tento reťazec musí pamätať, aby mohol vstúpiť do systému. Tu vzniká problém. Problém pamätania si každého hesla pre každú aplikáciu. Existujú dve riešenia. Prvou možnosťou je nastavenie ľahko zapamätateľného, prípadne rovnakého hesla do všetkých účtov. Týmto sa dramaticky znižuje úroveň bezpečnosti. Zároveň sa ale zvyšuje level komfortu pri interakcii s aplikáciami.

Tou druhou možnosťou je použitie aplikácie typu password manager (správca hesiel). Môžeme o ňom uvažovať ako o trezore. Dovnútra môžeme uložiť všetky naše heslá a zamknúť ich pod jedným kľúčom. Situácia sa odrazu mení. Zrazu si nemusíme pamätať niekoľko hesiel, ale iba jedno. Úroveň komfortu pri interakcii s aplikáciami ostáva zachovaná, avšak rovnako je dosiahnutá vysoká úroveň bezpečnosti.

V praxi vytvára implementácia tohto manažera určitý ekosystém. Teda, password manager dokáže poskytovať svoje služby len zariadeniu, na ktorom je nainštalovaný. Mimo tohto prostredia používateľ stráca znalosť o svojich údajoch. V súčasnosti považujeme oblasť ekosystému password manažera za dostatočne rozvinutú. Preto sme sa rozhodli venovať oblasti mimo neho.

Cieľom práce je vyvinúť aplikáciu password manager a nájsť bezpečný, pohodlný a efektívny spôsob prístupu používateľa k heslám na cudzom zariadení. Teda na takom zariadení, kde password manager s citlivými údajmi používateľa nie je prítomný (mimo ekosystému). Snahou bude vymyslieť riešenie (riešenia), ktoré by toto umožňovali.

1 Základné pojmy

Pred samotným uvedením do problému, ktorým sa zaoberá táto práca je dôležité vysvetliť a definovať základné pojmy, ktoré sú spojené s danou problematikou a využívané v texte.

1.1 Heslo

Heslo je prostriedok, pomocou ktorého je overená totožnosť používateľa. [1] Pomocou neho vieme získať prístup k informáciám, dátam atď. ktoré sú pod ním uzamknuté. Teda iba ten, kto heslo pozná, môže pristupovať k týmto materiálom. Z tohto môžeme usúdiť, že heslo by malo byť dostatočne silné. Musí byť ťažko uhádnuteľné a komplexné. Jeho vlastník by ho mal ukryť pred odhalením alebo uhádnutím útočníka. Týmto nám vznikajú rôzne otázky: *Aké miesto je bezpečné na ukrytie hesla? Kedy môžeme prehlásiť, že heslo je "silné"?*

1.2 Autentizácia

[2] Proces, pri ktorej je overená totožnosť osoby, sa nazýva autentizácia. Predchádza ju proces identifikácie, kedy sa osoba "predstaví a povie, kto je. Systém ho ďalej v procese autentizácie "vyzve", aby dokázal, že dotyčná osoba je naozaj tou, za ktorú sa prehlásil. Tým dôkazom myslíme vyššie spomínané heslo.

V praktickej rovine sú spôsoby autentizácie rôzne, ako napríklad: biometrický odtlačok, fráza vo forme hlasu, textového reťazca, číselný PIN a podobne [3].

1.3 Sila hesla

Uvažujme heslo ako textový reťazec. Sila hesla označuje stupeň obtiažnosti s akou ho neautorizovaná osoba dokáže uhádnuť [4]. Heslo môže byť silné alebo slabé, v závislosti od toho, ako ťažké ho je uhádnuť [4]. Slabé heslo je napríklad používanie iba malých písmen alebo iba číslíc. Dôvod, prečo to tak je, je príliš malý priestor výberu znaku. Pri číselnom hesle hovoríme o priestore desiatich znakov. Uvažujme štandardnú telegrafnú abecedu s 26 písmenami. Potom je priestor pri použití hesla iba z malých písmen veľký 26 znakov. Útočník môže predpokladať, že používateľ má heslo zložené iba z číslíc alebo iba z malých písmen¹.

Preto na druhej strane hovoríme, že silné heslo je také heslo, ktoré obsahuje kombináciu veľkých a malých písmen a číslíc. Už len kombináciou veľkých a malých písmen sa nám

¹Možnosť použitia hesla iba z veľkých písmen nespomíname, pretože z matematického hľadiska náročnosti prelomenia hesla ide o rovnaký prípad ako pri malých písmenách.

priestor zdvojnásobí. Abeceda veľkých písmen aj malých písmen má 26 znakov, čo je spolu 52 znakov. Zrazu je pre útočníka pri každom písmene nutné uvažovať, či sa použilo ako veľké, alebo ako malé. Z matematického hľadiska, teda z hľadiska permutácií sa celkový počet možných usporiadaní exponenciálne zvýši. Permutácia znamená usporiadanie.

Tabuľka 1: Zložitosť prelomenia hesiel pomocou útoku brute-force

Typ Hesla	Heslo	Priestor	Počet možností
Číslice (ďalej len C)	01234	10	$1, 11 * 10^5$
Malé písmená (ďalej MP)	heslo	26	$1, 24 * 10^7$
MP + veľké písmená (VP)	hEsLo	52	$3, 88 * 10^8$
MP + VP + C	h3sL0	62	$9, 31 * 10^8$
MP + VP + C	h3sL0jeSiLn3	62	$3, 28 * 10^{21}$
MP + VP + C + špec. znaky	h3sL0=%SiLn3	95	$5, 46 * 10^{23}$

Čas (online útok)	Čas (offline útok)
pri 1000 pokusoch/s	pri miliarde pokusoch/s
1,85 min	0,00000111 s
3,43 hod	0,000124 s
4,49 dní	0,00388 s
1,54 týždňov	0,00931 s
104 miliárd rokov	1043 rokov
17,4 biliónov rokov	1740 rokov

Z tabuľky sme pozorovaním zistili, že rovnako ako bohatý priestor znakov je dôležitá aj dĺžka hesla. S použitím veľkých aj malých písmen pri dĺžke hesla 5 by bol útočník schopný zistiť naše heslo za veľmi krátky čas. Môžeme si z časových výsledkov všimnúť, že z praktického hľadiska skoro ani nezáleží, či použijeme C, MP, MP + VP alebo MP + VP + C, pokiaľ je heslo krátke. Najmä pri offline útoku zjavne vidieť, že vo všetkých prípadoch by stroj uhádol heslo doslova do sekundy.

Silu exponenciálneho rastu si všimame pri zmene dĺžky hesla na 12 znakov. Celá situácia sa dramaticky zmenila a kombinácie C, MP a VP už dávajú zmysel. Ďalší veľký skok spôsobilo pridanie špeciálnych znakov. Keďže zväčšili priestor rôznych znakov o viac ako polovicu, významná zmena je vidieť aj vo výsledkoch.

[5] Predpokladajme, že útočník má informáciu, že používateľ vlastní heslo zložené iba z MP. Potom platí, že ak by používateľ zväčšil dĺžku hesla o jeden znak, útočník musí

vykonať v priemere o 26 viac pokusov pri každej permutácii.

[5] Ďalej predpokladajme, že používateľ vlastní heslo zložené z MP, VP a C. Takáto kombinácia je dnes pri registrácii vo veľkej miere povinnosťou na rôznych webových stránkach. Potom platí, že pri zväčšení dĺžky hesla o jeden znak by sa zložitosť hesla nezvýšila iba 26, ale až 62-násobne. Z toho vyplýva, že útočník by musel mať 62-násobne väčší výkon, aby mohol za rovnaký čas zlomiť heslo z pôvodnou dĺžkou. Ten sa zvyšuje každé dva roky dvojnásobne, podľa Moorovho zákona.

Táto úvaha spolu s ďalšími typmi útokov a ochranov pred nimi je hlbšie obsiahnutá v práci [5].

2 Problém password managerov

Password manager ponúka používateľovi mnohé výhody.

3 Recitácia

Citujem všetky zdroje v `bibliography.bib`, [`t00`, `t01`, `t02`, `t03`, `kniha`, `kniha2`, `kniha3`, `small`, `big`, `cs`, `koll`, `kap`, `tug`, `knuth`, `zbornik`, `prispevok`].

Good luck.

4 Možnosti anonymizácie

Anonymizácia znamená zmena alebo úprava údajov tak, aby sa podľa nich nedala jednoznačne určiť osoba, ktorej tieto údaje patria [t01]. Existuje niekoľko spôsobov, ktorými môžeme dosiahnuť rôznu úroveň anonymizácie na internete: od mazania cookies súborov po ukončení prehliadania webových stránok až po používanie operačných systémov, ktoré sú na anonymite založené; od bezplatných možností až po komerčné verzie.

Nasleduje priblíženie niektorých možností anonymizácie.

4.1 Súkromné prehliadanie

Najpoužívanjšie internetové prehliadače súčasnosti majú v sebe zabudovanú funkcionality, ktorá dokáže čiastočne anonymizovať prístup na internet. Táto funkcionality blokuje ukladanie navštívených stránok do histórie a nezaznamenáva súbory, ktoré sa stiahnu z internetu. SW a Halo Wars sú skratky.

4.2 Anonymná sieť

Anonymná sieť je sieť serverov, medzi ktorými dáta prechádzajú šifrované. V anonymných sieťach dáta prechádzajú z počítača používateľa, odkiaľ bola požiadavka poslaná, cez viaceré proxy smerovače, z ktorých každý správu doplní o smerovanie a zašifruje vlastným kľúčom. Cesta od ...

4.3 Funkcionalita

Rozšírenie tiež okrem splnenia špecifikácie malo pre prehľadnosť a overenie funkčnosti zobrazovať údaje, ktoré boli na server odoslané. Zoznam údajov odoslaných na server, sa mal ukladať do krátkodobej histórie, aby nemal používateľ k dispozícii len najnovšie údaje, ale aj údaje odoslané v nejakom časovom období. Nejaký listing z príloh C.1.

4.3.1 Funkcionalita2

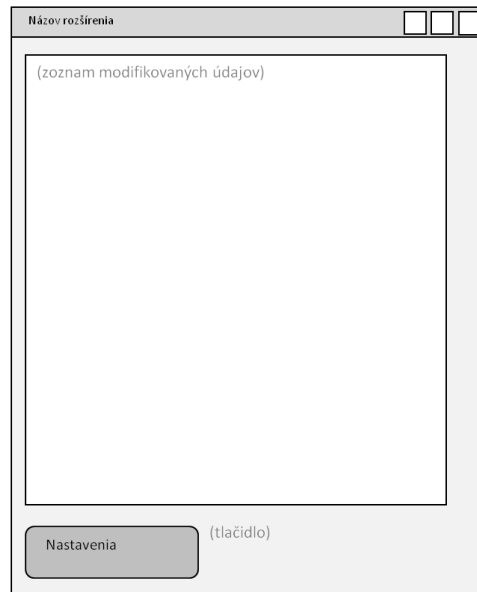
Samozrejmosťou bolo nastavenie zapnutia rozšírenia pri štarte, prípadne interval zmeny odosielaných údajov.

4.4 Vzhľad

Dôležitou požiadavkou kladenou na rozšírenie bolo príjemné používateľské rozhranie. Z tohto dôvodu malo rozšírenie obsahovať zoznam modifikovaných vlastností a tlačidlo pre prístup k nastaveniam rozšírenia v jednoduchšej a praktickej forme. Predpokladaný vzhľad je zobrazený na obrázku č. 1. Dôležitou požiadavkou kladenou na rozšírenie bolo príjemné používateľské rozhranie.[t00] Z tohto dôvodu malo rozšírenie obsahovať zoznam

Tabuľka 2: Moduly a ich funkcie pri anonymizácii

Modul	Funkcia													
	zobrazenie hlavičky	blokovanie skriptov	zmena IP	zmena lokalizácie	zmazanie/blokovanie cookies	Modifikácia								
						blokovanie trackerov	popis	používateľský agent	kódové označenie prehliadača	názov prehliadača	verzia prehliadača	platforma	výrobca prehliadača	označenie výrobcu prehliadača
User agent switcher							X	X	X	X	X	X	X	X
Ghostery					X	X								
Better privacy					X									
Anonymox			X	X	X		X	X						
Modify headers					X			X						
Request policy						X								
Live HTTP headers	X													
User agent awitcher for chrome							X	X						
Header hacker							X	X	X	X	X	X	X	X
Mod header							X	X	X	X	X	X	X	X
Script no		X												
No script		X												
Proxify it			X	X										
I'm not here				X										
Get anonymous personal edition		X	X	X	X	X								
Anonymous browsing toolbar			X	X										
Easy hide your IP and surf anonymously			X	X				X	X	X	X			



Obr. 1: Predpokladaný vzhľad rozšírenia.

modifikovaných vlastností a tlačidlo pre prístup k nastaveniam rozšírenia v jednoduchéj a praktickéj forme. Predpokladaný vzhľad je zobrazený na obrázku č. 1.

```
/* Hello World program */  
  
#include<stdio.h>  
  
struct cpu_info {  
    long unsigned utime, ntime, stime, itime;  
    long unsigned iowtime, irqtime, sirqtime;  
};  
  
main()  
{  
    printf("Hello World");  
}
```

Listing 1: Ukážka algoritmu

Algorithm 1 Ukážka príkazov pre algorithmic

```
<text>
if <condition> then
  <text>
else
  <text>
end if
if <condition> then
  <text>
else if <condition> then
  <text>
end if
for <condition> do
  <text>
end for
for <condition> to <condition> do
  <text>
end for
for all <condition> do
  <text>
end for
while <condition> do
  <text>
end while
repeat
  <text>
until <condition>
loop
  <text>
end loop
Require: <text>
Ensure: <text>
return <text>
print <text> {<text>} and , or , xor , not , to , true, false
```

Záver

Conclusion is going to be where?

Here.

Prílohy

A	Štruktúra elektronického nosiča	II
B	Algoritmus	III
C	Výpis subline	IV

A Štruktúra elektronického nosiča

/CHANGELOG.md

- file describing changes made to FEIstyle

/example.tex

- main example *.tex* file for diploma thesis

/example_paper.tex

- example *.tex* file for seminar paper

/Makefile

- simply Makefile – build system

/fei.sublime-project

- is project file with build in Build System for Sublime Text 3

/img

- folder with images

/includes

- files with content

/bibliography.bib

- bibliography file

/attachmentA.tex

- this very file

B Algoritmus

Algorithm B.1 Vypočítaj $y = x^n$

Require: $n \geq 0 \vee x \neq 0$

Ensure: $y = x^n$

$y \leftarrow 1$

if $n < 0$ **then**

$X \leftarrow 1/x$

$N \leftarrow -n$

else

$X \leftarrow x$

$N \leftarrow n$

end if

while $N \neq 0$ **do**

if N is even **then**

$X \leftarrow X \times X$

$N \leftarrow N/2$

else $\{N$ is odd $\}$

$y \leftarrow y \times X$

$N \leftarrow N - 1$

end if

end while

C Výpis sublime

```
{
  "folders":
  [
    {
      "path": ".",
      "folder_exclude_patterns": [".build", ".aux"],
      "follow_symlinks": true
    }
  ],
  "settings" : {
    "TEXroot": "example.tex",
    "tex_file_exts": [".tex"],
    "use_biblatex": true,
    "glossary_auto_trigger": true,
    "aux_directory": "./.aux",
    "output_directory": "./.build",
    "builder_settings": {
      "program": "pdflatex",
      "options": "--shell-escape"
    }
  },
  "build_systems":
  [
    {
      "name": "FEI – LaTeX",
      "working_dir": "${folder}",
      "shell_cmd": "make",
      "variants": [
        {
          "name": "clean",
          "shell_cmd": "make clean",
        }
      ]
    }
  ]
}
```

Listing C.1: Ukážka sublime-project