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, consectetuer 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 mäkčeňov a dĺžnov.

Kľúčové 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

Poďakovanie

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

Zoznam obrázkov a tabuliek

Zoznam algoritmov

Zoznam výpisov

Úvod

V dnešnej dobe je svet každým dňom viac a viac 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 útokom. Preto každá aplikácia, či systém, ktorá pracuje s informáciami, používa účty. Používateľ si vytvorí ten svoj a dostane sa doň pomocou dvoch vecí: 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. 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 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 aplikáciou. Tou druhou možnosťou je použitie aplikácie typu password manager (po slovensky správca hesiel). Môžeme o ňom uvažovať ako o trezore. Doňho 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 managera 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 managera za dostatočne rozvinutú. Preto sme sa rozhodli venovať oblasti mimo neho. Cieľom práce je vyvinúť password manager a nájsť bezpečný, pohodlný a efektívny spôsob prístupu používateľa k heslu password managera 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 Úkážka glossaries

Verzia FEIstyle 1.5 používa glossary[1] balík. Code Division Multiple Access (CDMA) je dlhá skratka naopak GSM je skratka v krátkej forme.

[1] `https://www.ctan.org/pkg/glossaries?lang=en`

2 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.

3 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 možnosti anonymizácie.

3.1 Súkromné prehliadanie

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

3.2 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 ...

3.3 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 dispozícií len najnovšie údaje, ale aj údaje odoslané v nejakom časovom období. Nejaky listing z priloh C.1.

3.3.1 Funkcionalita2

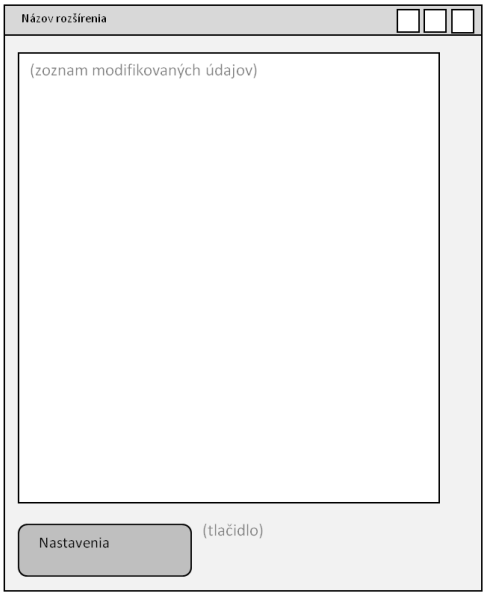
Samozrejmosťou bolo nastavenie zapnutia rozšírenia pri štarte, prípadne interval zmeny odosielaných údajov.

3.4 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 jednoduchej 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 1: Moduly a ich funkcie pri anonymizácii

	Funkcia													
						Modifikácia								
Modul	zobrazenie hlavičky	blokovanie skriptov	zmena IP	zmena lokalizácie	zmazanie/blokovanie cookies	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 jednoduchej a praktickej 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

/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 ⇐ 1
if n < 0 then
    X ⇐ 1/x
    N ⇐ −n
else
    X ⇐ x
    N ⇐ n
end if
while N ≠ 0 do
    if N is even then
        X ⇐ X × X
        N ⇐ N/2
    else {N is odd}
        y ⇐ y × X
        N ⇐ 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