Prezentácia doterajších výsledkov v zimnom semestri

1

- Dobrý deň prajem, moje meno je Peter Čuřík a vítam vás na prezentácii mojej bakalárskej práce - Password manager.
- Dnes sa bližšie pozrieme na túto tému, aké má ciele, úlohy a na čom sa ešte bude pracovať v letnom semestri.

2

- Sme v dobe, kde existuje stále viac služieb a produktov, ktoré denne využívame. Tieto veci vyžadujú prístup, login, heslo. Aby sme mali tieto heslá mali bezpečné a na jednom mieste, vznikli password managere. Tie zhromažďujú všetky heslá a uzatvoria ich do trezoru pod jedným master heslom. Vďaka tomu môžeme používať rôzne, zložitejšie a bezpečnejšie heslá, lebo si ich už nemusíme pamätať. Navyše, tie pokročilejšie password managere si automaticky nové loginy ukladajú a pomocou autofillu ich automaticky za usera doplnia do vstupov vo fáze prihlasovania

3

- Základný problém password managerov je jeho použiteľnosť mimo jeho dosah
- Modelový príklad: letisko
    - potrebujem sa na letiskovom počítači prihlásiť na stránku leteckej spoločnosti, z ktorej si následne vytlačím letenku
    - čo ak mám do účtu zložité heslo generované password managerom? —> musím si otvoriť aplikáciu na smrtfóne a prepísať heslo manuálne

4

- Toto ale predstavuje nasledovné hrozby ako:
    - krádež telefónu
    - odfotenie obrazovky telefónu
    - opísanie hesla nakuknutím
- Toto riešenie je nevýhodné z hľadiska jednoduchosti pre užívateľa. Pri komplexnom a dlhšom hesle musí pracne po jednom prepisovať znaky
- Táto skutočnosť môže byť jeden z dôvodov, prečo ľudia nechcú používať password managery. Úspešné riešenie tohto problému a jeho integrácia do password managera by mohla byť ďalším z argumentov prečo používať tieto technológie.

5

- Táto práca sa bude snažiť riešiť jeho problém

6

- Teda cieľom práce je vyvinúť password manager a nájsť bezpečný, pohodlný a efektívny spôsob prístupu užívateľa k heslu password managera na cudzom zariadení.
- Výsledkom ale môže byť aj ukážka, ako sa to nedá, alebo ako to nie je výhodné. Zatiaľ nevieme, či potenciálne alternatívne spôsoby sú skutočne dostatočne bezpečné a komfortné pre užívateľa
- Jeden z nich je:

7

- Jednorázový kód
- myšlienka je nasledovná:

8

- v aplikácii na operačný systém iOS by existovala funkcionalita na generovanie 6 miestneho číselného kódu
- ten by sa dočasne umiestnil na server a bol by v zozname správnych kľúčov

9

- užívateľ pôjde na webovú stránku, špeciálne vyhradenú na tento účel a kód zadá.
- server overí validitu z poľa správnych kľúčov
- po správnom overení respektíve po dvoch minútach od pridania do poľa server kód z poľa odstráni

10

- užívateľ je vpustený do zoznamu jeho hesiel, ktoré smie len kopírovať. nemôže ich ani zobraziť, ani meniť, ani odstraňovať.

11

- tu vidíme nejakú predstavu o zložitosti z pohľadu užívateľa

12

- môže sa to javiť ako dvojfaktorová autorizácia, ale v tomto procese ide o iba jedno overenie
- two factor spočíva v následnej autorizácii po prihlásení

13

- doterajšie výsledky

1 4

- Prieskum trhu:
    - predtým, než začneme s implementáciou nejakej funkcionality, musíme sa uistiť že pracujeme na niečom, čo tu ešte nebolo
    - urobili sme analýzu mnohých password managerov ako LastPass, 1Password a podobne
    - niektoré ponúkali browser extension, iné zase desktop aplikáciu —> oboje spôsoby sú príliš zložité a zdĺhavé na jednorázové použitie
    - nenašli sme aplikáciu, ktorá by korektne a efektívne riešila problém, ktorým sa zaoberá táto práca

- Návrhy, prototypy