



PASSWORD MANAGER

BAKALÁRSKA PRÁCA



Master password



Autofill



Password complexity





Základný problém

1

Použiteľnosť password manageru mimo “ekosystému”

Hrozby

- ⚠ Krádež telefónu útočníkom
- ⚠ Odfotenie obrazovky telefónu útočníkom
- ⚠ Opísanie hesla nakuknutím útočníka

Z hľadiska pohodlnosti (user-friendliness)
ide taktiež o nevýhodné riešenie.

Manuálny prepis hesla



Riešenie problému

2

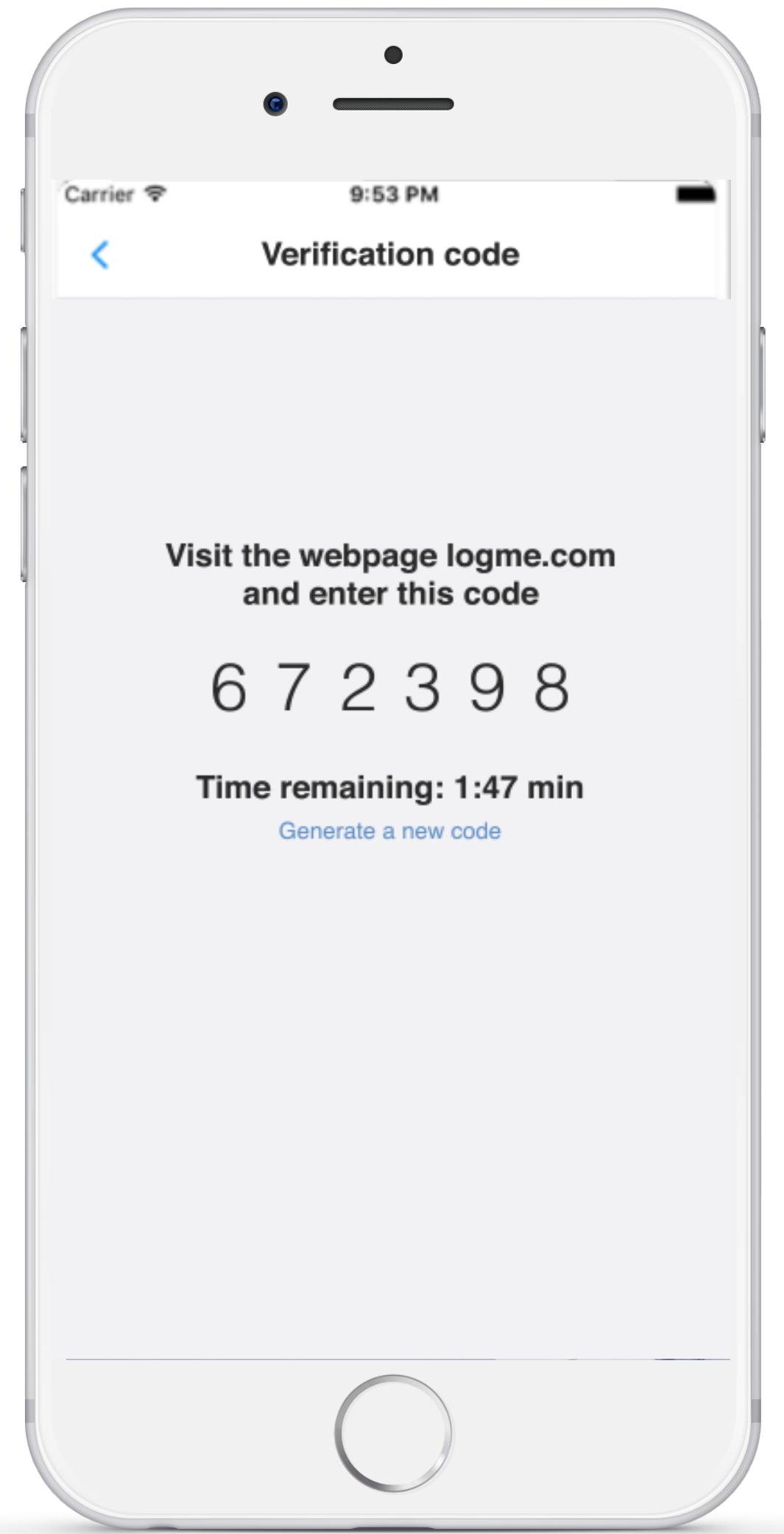
Výstup bakalárskej práce

Cieľom práce je vyvinúť password manager a nájsť bezpečný,
pohodlný a efektívny spôsob prístupu užívateľa k heslu password
managera na cudzom zariadení.

Jednorázový kód

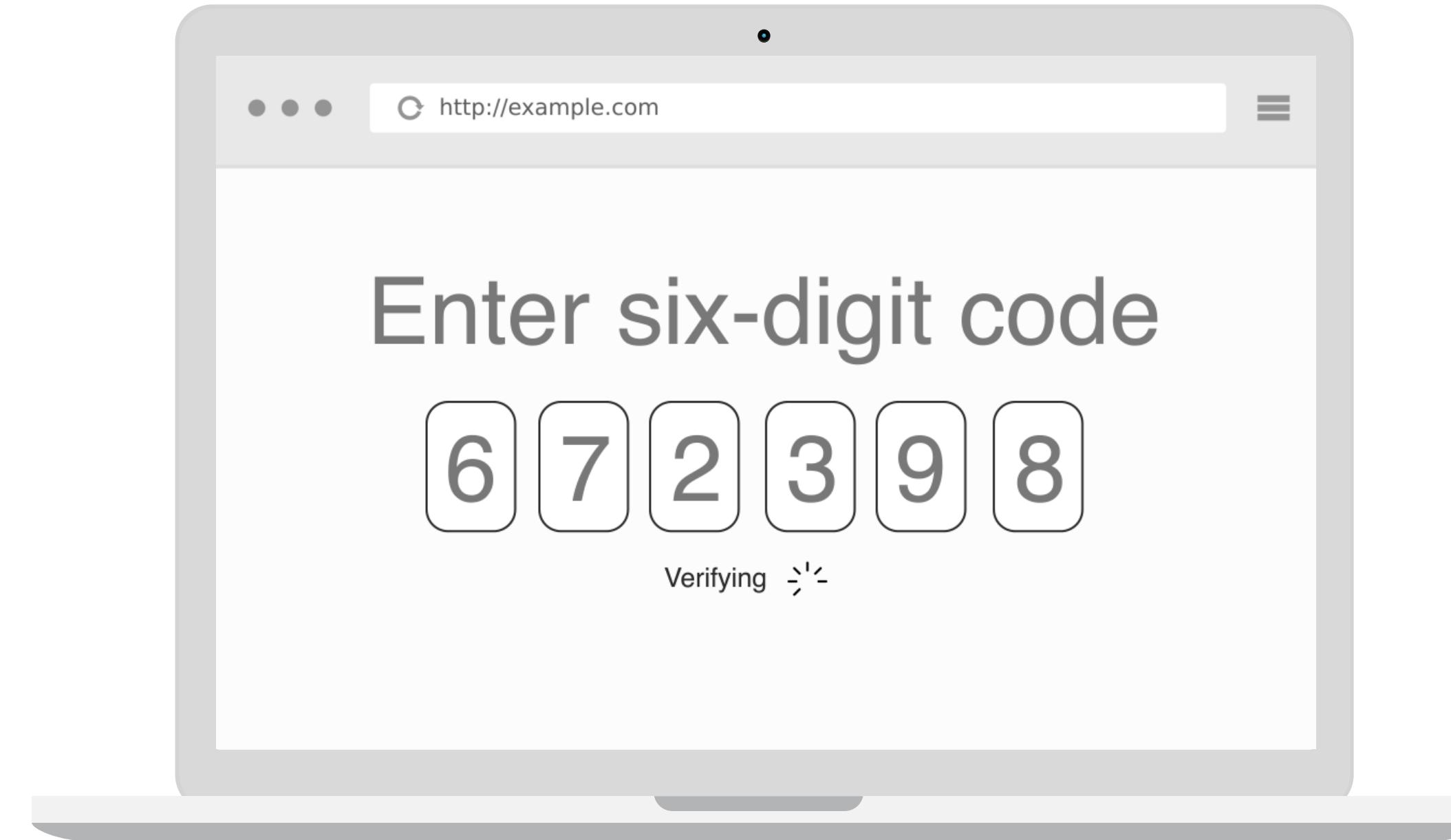
Potenciálne riešenie problému





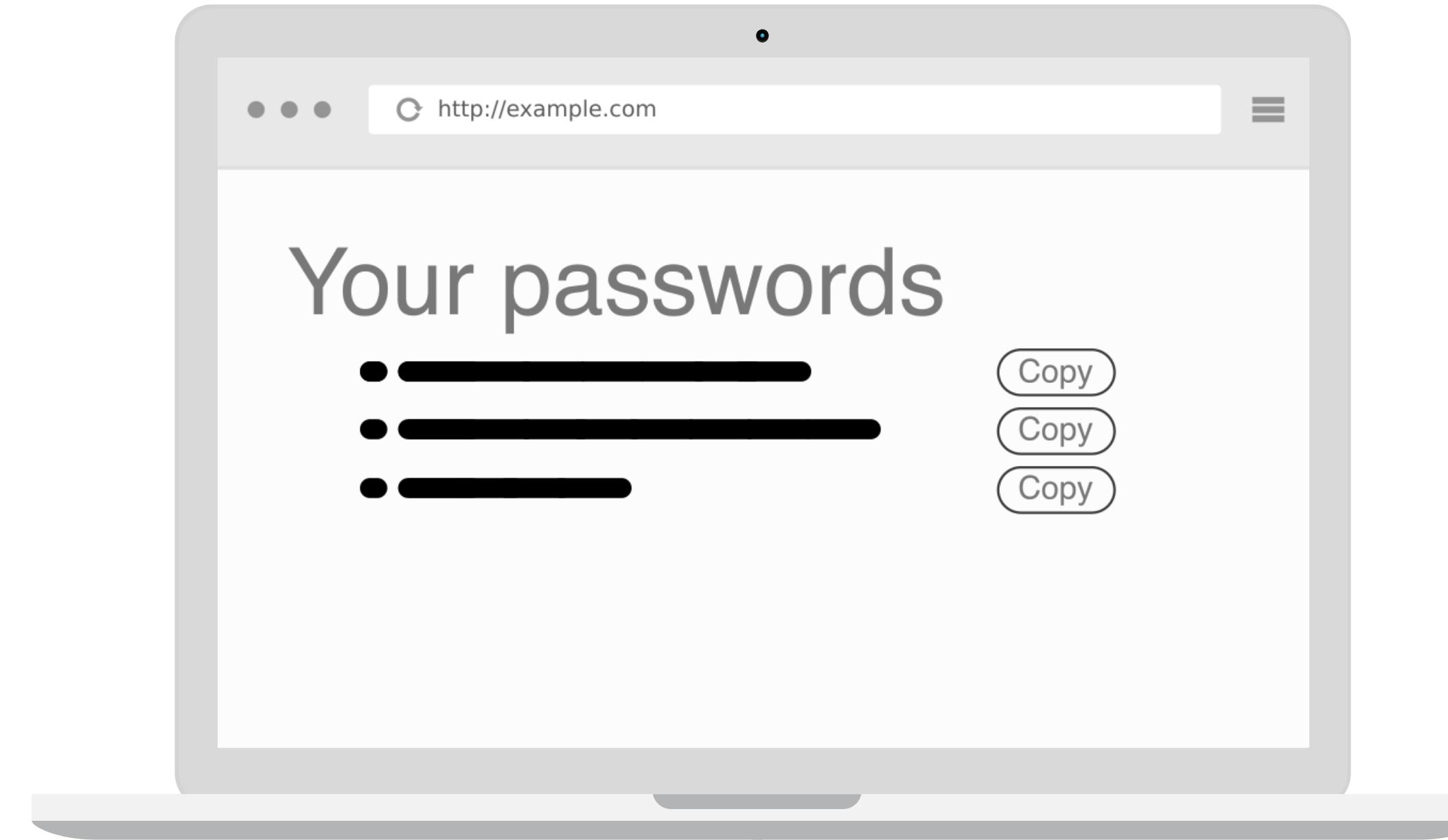
iOS aplikácia

Užívateľ si v aplikácii nechá vygenerovať jednorázový kód s platnosťou dvoch minút



Cudzie zariadenie

Vloženie kódu a jeho následná verifikácia



Cudzie
zariadenie po
verifikácii

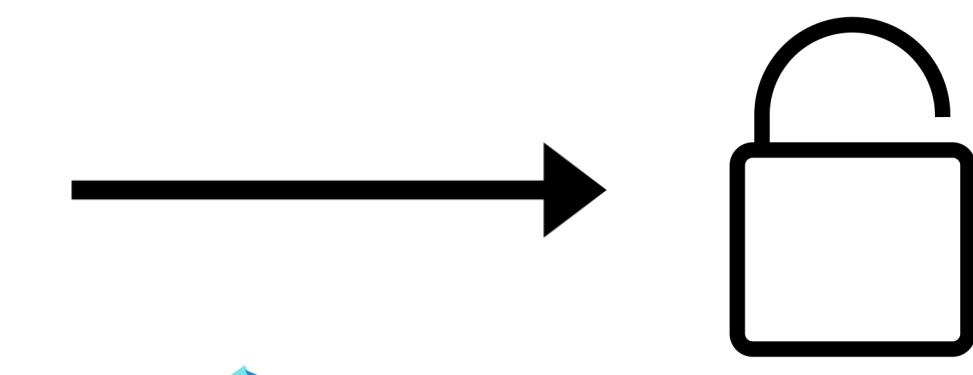
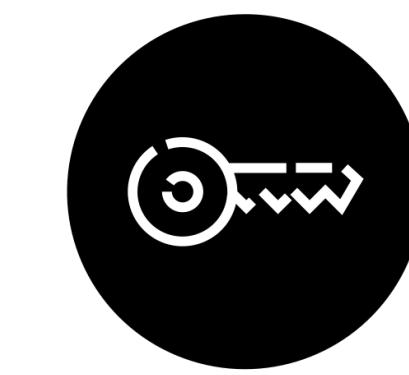
User-friendly zložitosť

-
- 01 Otvorenie iOS aplikácie
 - 02 Vyžiadanie jednorázového kódu
 - 03 Otvorenie webstránky na cudzom zariadení
 - 04 Manuálny prepis 6 znakového jednorázového kódu

Toto nie je dvojfaktorová autorizácia

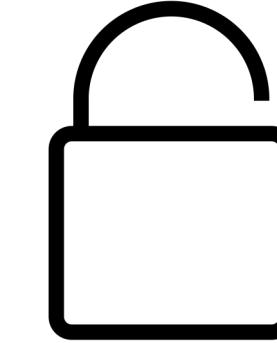
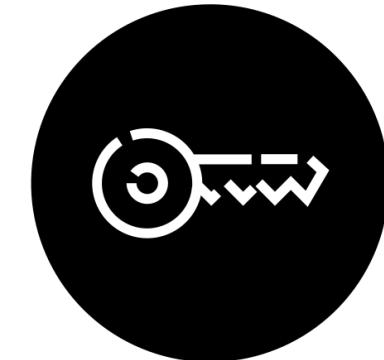
Two-factor

Dodatočné overenie po prihlásení



Jednorázový kód

Jediný prostriedok na overenie





Doterajšie výsledky

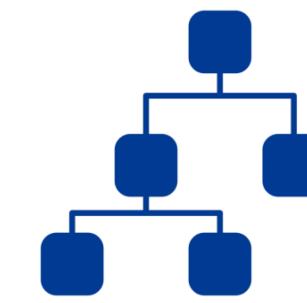
3

Úvodná analýza a modelovanie



Prieskum trhu

Analýza existujúcich password managerov.
Chceme sa uistíť, že sa nesnažíme znova ”vynájsť koleso”.



Návrhy, prototypy

Diagramy a nákresy, ako by systém mohol fungovať.
Surová kostra iOS aplikácie a webstránky.



Bezpečnosť

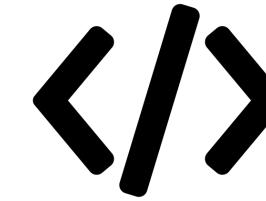
Analýza existujúcich šifier a metód používaných na bezpečnosť údajov. Využitie keystore-u, štúdium moderných šifier, hashing.



Ďalší postup

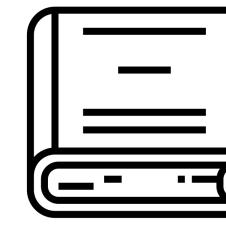
4

Ciele do letného semestra



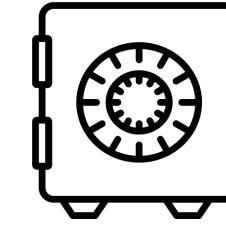
Aplikácia a web

Vývoj aplikácie password manager na platformu iOS a webstránky slúžiacej na prístup k heslám na cudzích zariadeniach



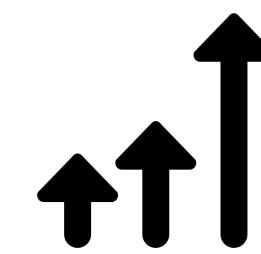
Písomná forma

Dokončenie písomného dokumentu bakalárskej práce, so všetkými formálno-obsahovými náležitostami



Bezpečnosť

Šifrovanie a bezpečné ukladanie hesiel (Keystore, AES), šifrované cestovanie jednorázového kľúča po sieti

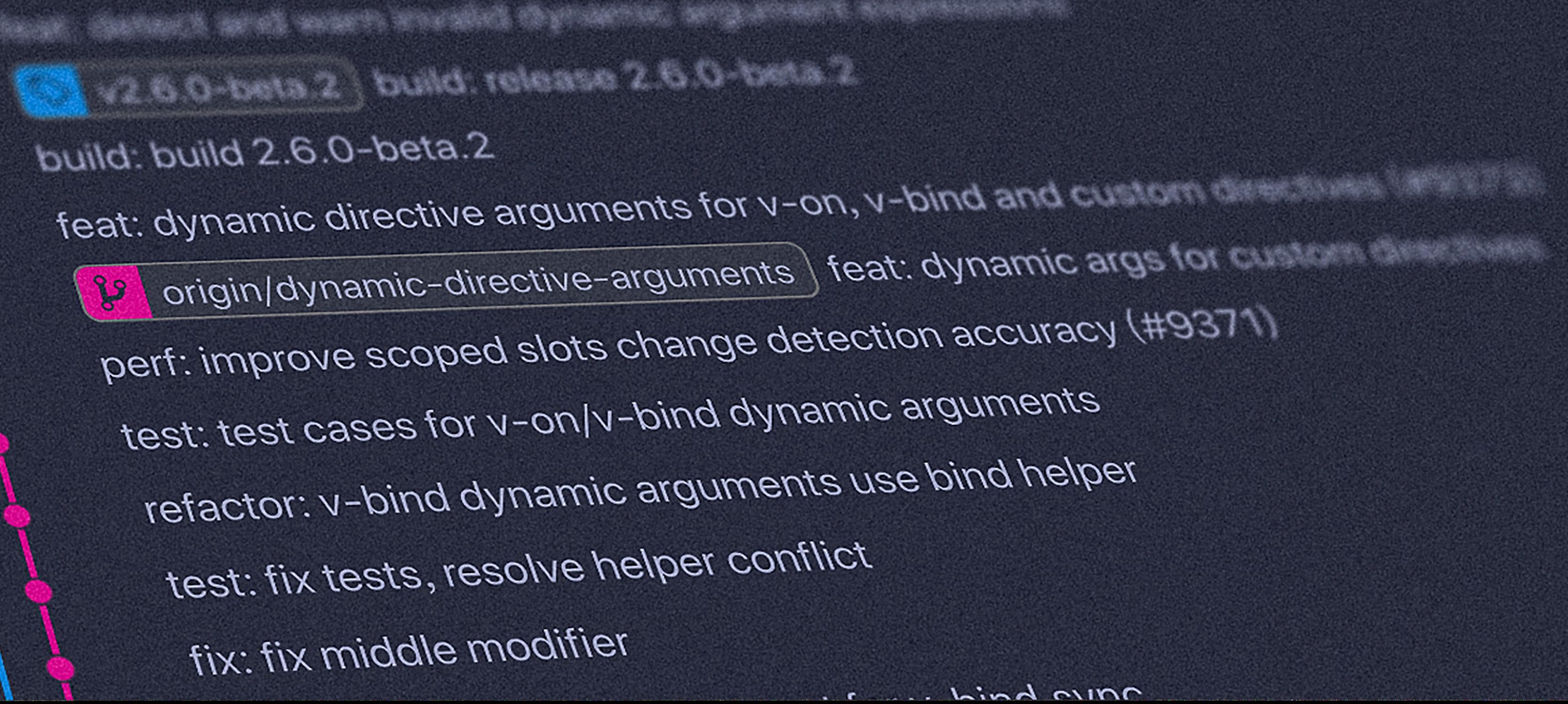


Meranie

Porovnanie novej metódy na získanie hesla na cudzom zariadení s existujúcimi (počet operácií zo strany užívateľa, časová náročnosť..)

- ▶ now
- ▶ packages
- ▶ scripts
- ▶ src
- ▶ test
- ▶ types

▶ tasks in progress



Ďakujem za pozornosť
Peter Čuřík, 2020