Analýza bezpečnosti inteligentného elektronického zámku

Martin Sýkora
RNDr. Richard Ostertág PhD.

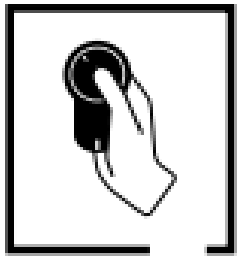
21. februára 2020

Ciele

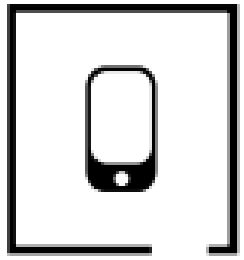
- popísať útoky na inteligentné zámky
- ak je to možné, tak ich aj aplikovať
- nájsť útoky na konkrétny inteligentný zámok
- návrhy, ako sa útokom vyhnúť

FAB Entr

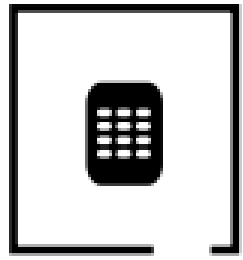
Otlačok prstu



Diaľkové ovládanie



Inteligentný telefón



Bezdrôtová klávesnica

zvětšit

470,38 € **Na dopyt**

zvětšit

52,90 € Viac ako 3 Ks

zvětšit

229,01 € Viac ako 3 Ks

- maximálne 20 používateľov bezdrôtovej klávesnice
  - maximálne 7 časových okien pre jedného používateľa
  - 2 otlačky prstov
- maximálne 20 diaľkových ovládačov
- maximálne 20 používateľov aplikácie
  - maximálne 7 časových okien pre jedného používateľa

Branding

- Tessa
- Mul-T-Lock
- Assa Abloy
- Fab
- Yale
- Keso

FCC ID

- 2AHH8
- MUL-T-LOCK

- Modulácia
- Fotky rozobratého zariadenia
- Návod pre používateľa

Dverná jednotka

- PIN: [1-5]{4,10} (nie 12345)
- reset do továrenských nastavení - údaje z bezdrôtovej klávesnice zostávajú uchované v nej, stačí ju len znova spárovať

Bezdrôtová klávesnica s čítačkou otlačkov prstov

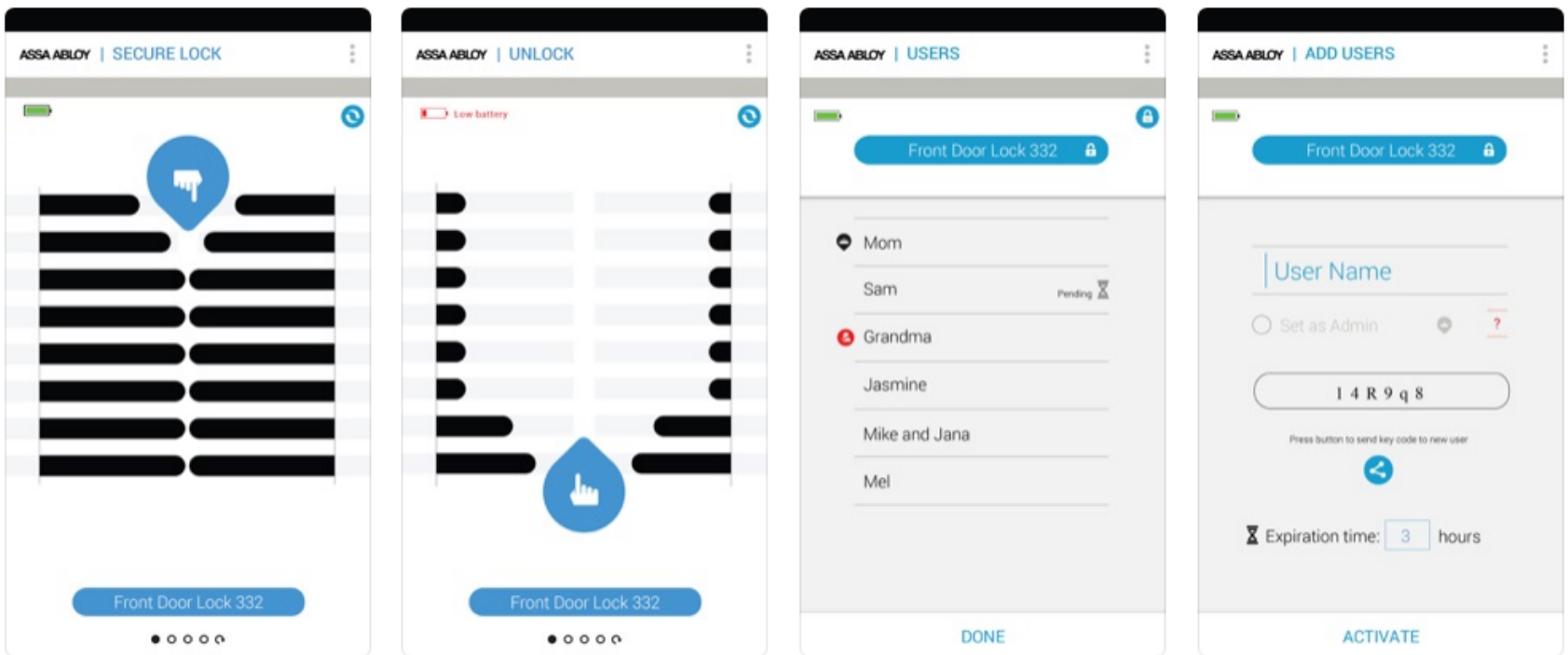
- prichytené jednou skrutkou
- po 3 zlých PINoch sa uzamkne na 1 minútu
- PIN: [0-9]{4,10}
- výmena batérií - používateľské dáta zostávajú uchované v pamäti, resetované sú iba dátum a čas
- reset do továrenských nastavení - zmaže všetky informácie uložené v pamäti, zahŕňajúc používateľov a spárované zámky
- AES-128
- 2.405 GHz
- zvuky nejdú vypnúť, ak používam PIN, viem jeho dĺžku

Diaľkové ovládanie

- AES-128
- 2.405 GHz
- keď chcem odpojiť jedno diaľkové ovládanie, budú odstránené všetky diaľkové ovládania aj bezdrôtové klávesnice
- môže byť spárovaný len s jedným zámkom (na spárovanie s iným treba zásah autorizovaného servisu)

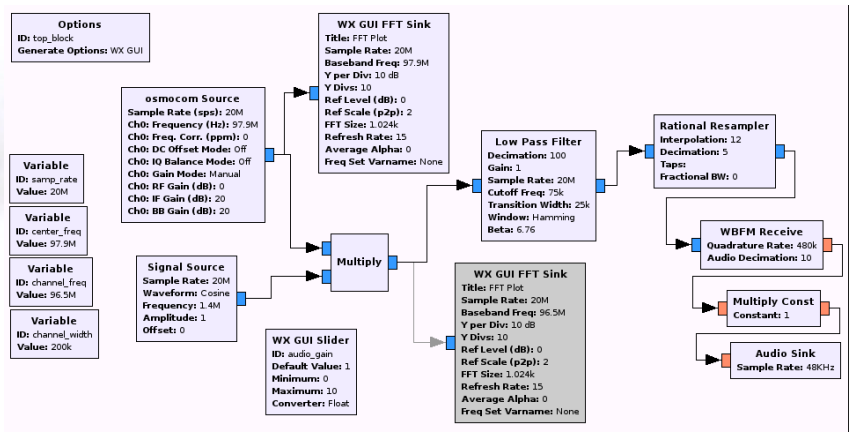
Aplikácia

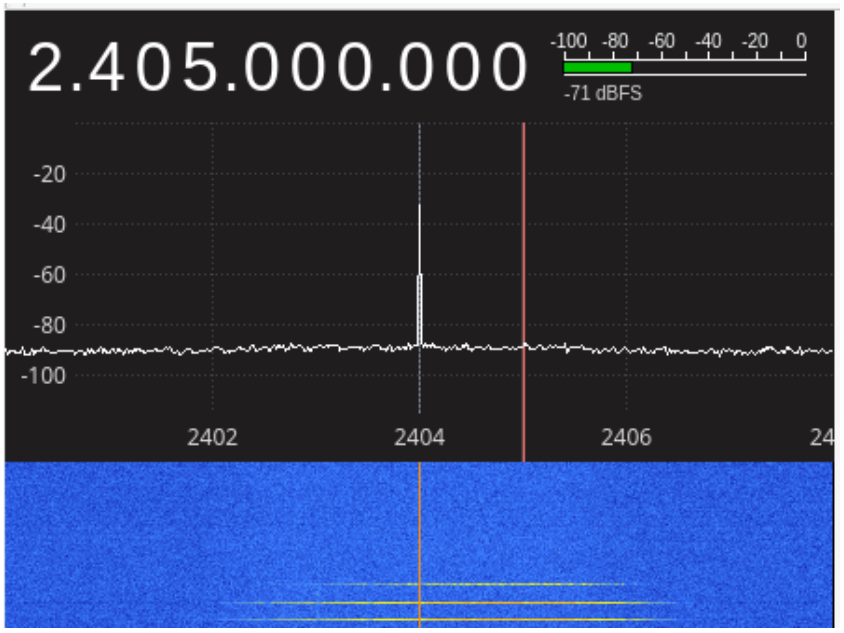
- Android
  - 4.4+
  - 10,000+ inštalácií
  - 2.5 hviezdičky
- Apple
  - iOS 7.0+
  - 2 hviezdičky

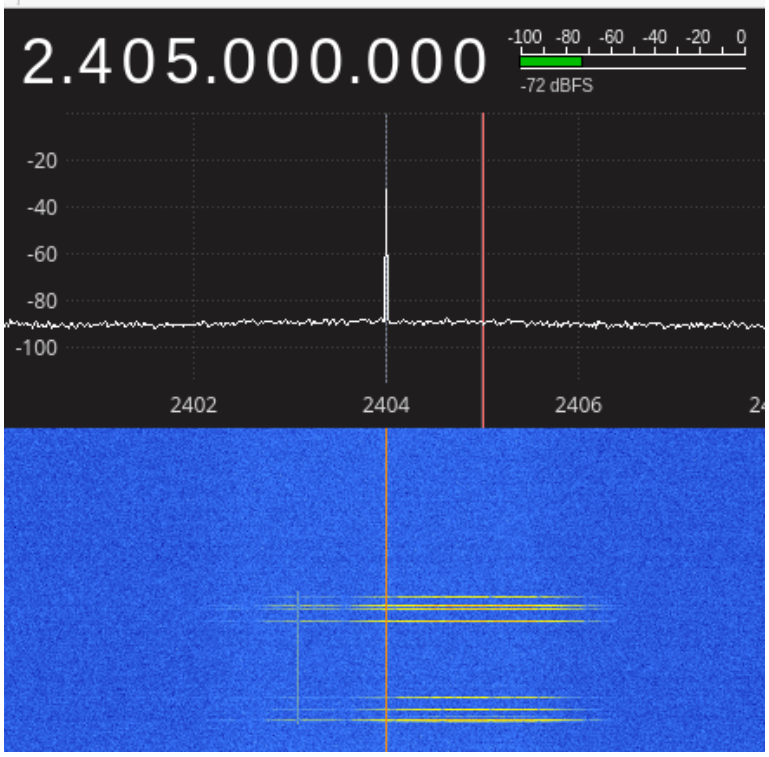


HackRF One

- frekvencie 1 MHz - 6 GHz
- half-duplex
- maximálna vzorkovacia frekvencia 20 MHz
- kompatibilné s GNU Radio, SDR#, GQRX




2.405.000.000
-100 -80 -60 -40 -20 0
-71 dBFS
-20
-40
-60
-80
-100
2402
2404
2406


2.405.000.000
-100 -80 -60 -40 -20 0
-72 dBFS
-20
-40
-60
-80
-100
2402
2404
2406

Primitívne DoS útoky

- rušenie signálu (jamming)
- odcudzenie bezdrôtovej klávesnice

Útok hrubou silou

- 3x zlý PIN $\Rightarrow$ blokované 1 minútu
- PIN: [0-9]{4,10}
- nech vyskúšanie jedného PINu trvá 3 sekundy
- berme len štvormiestne PINy $\Rightarrow$ 10 000 možností

- $3333 \cdot 69 = 229\ 977$ sekúnd $\Rightarrow$ 3 833 minút $\Rightarrow$ 64 hodín

Útok hrubou silou (2)

- po vybratí batérií si zámok nepamätá, že má byť blokovaný
- vybratie batérií a naštartovanie - cca 15-17 sekúnd
- $3333 \cdot 26 = 86\ 658$ sekúnd $\Rightarrow$ 1 444 minút $\Rightarrow$ 24 hodín

Útok hrubou silou (3)

- používateľ má povolený vstup len v určitom časovom okne
- po zadaní PINu mimo časového okna sa počet neúspešných pokusov vynuluje
- $5000 \cdot 9 = 45\ 000$ sekúnd $\Rightarrow$ 750 minút $\Rightarrow$ 12.5 hodiny

Útok hrubou silou (4)

- hádanie master PINu, len 1 kliknutie navyše
- žiadna ochrana
- $10000 \cdot 3 = 30\ 000$ sekúnd $\Rightarrow$ 500 minút $\Rightarrow$ 8.3 hodiny

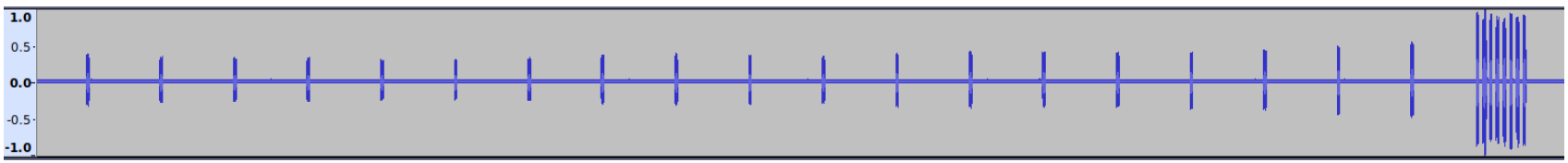
Útok resetovaním času

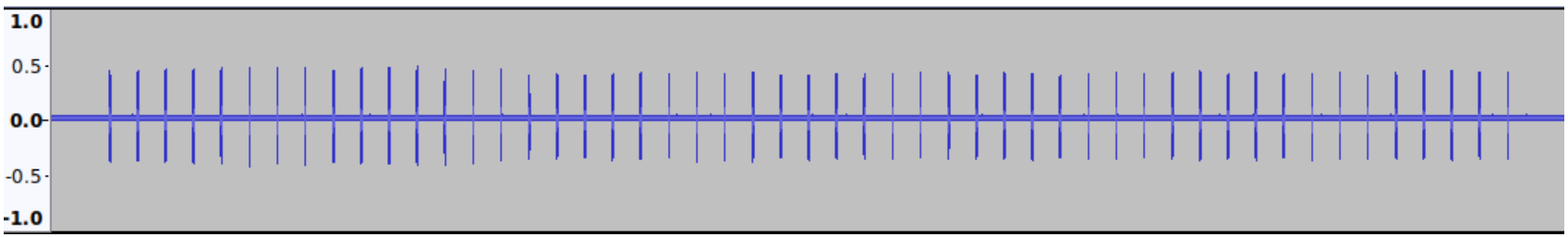
- vybratím batérií sa resetuje čas
- používateľ, ktorý má prístup v tomto časovom okne $\Rightarrow$ neobmedzený prístup
- formát HH:mm DD/MM/YY
- 00:00 01/01/13 (utorok)
- 00:00 01/01/00 (sobota)
- nefunguje

Útoky na komunikáciu

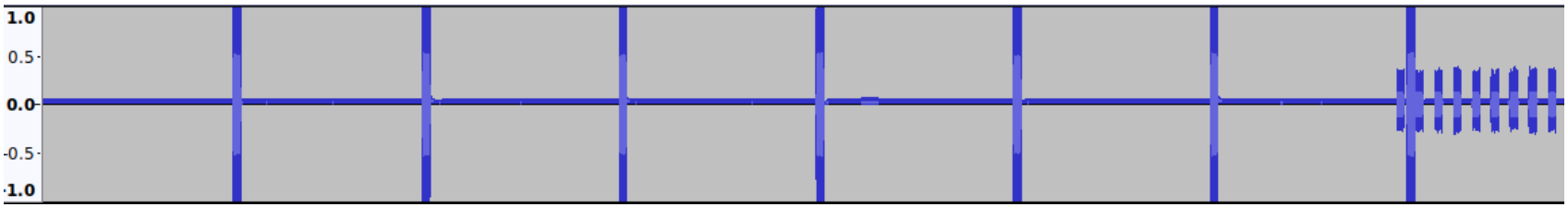
- pevný kód (fixed code)
- plávajúci kód (rolling code)
- obojsmerná komunikácia

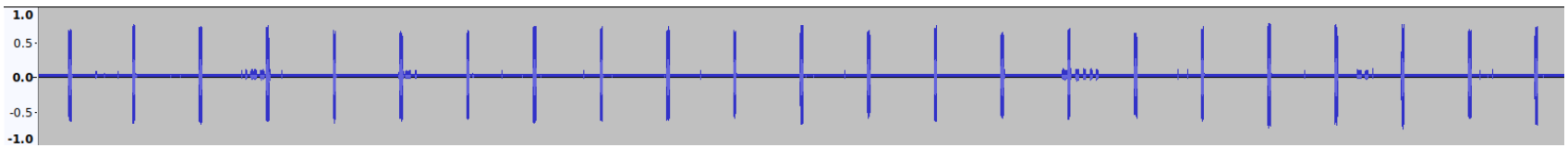
Diaľkové ovládanie





Bezdrôtová klávesnica





TODO

- demodulácia
- replay attack
- párovanie diaľkového ovládania a bezdrôtovej klávesnice
- čítačka odtlačkov prstov

Práca do budúcna

- analýza na úrovni firmvéru
- analýza mobilnej aplikácie