Analýza bezpečnosti inteligentného elektronického zámku

Bc. Martin Sýkora
RNDr. Richard Ostertág, PhD.

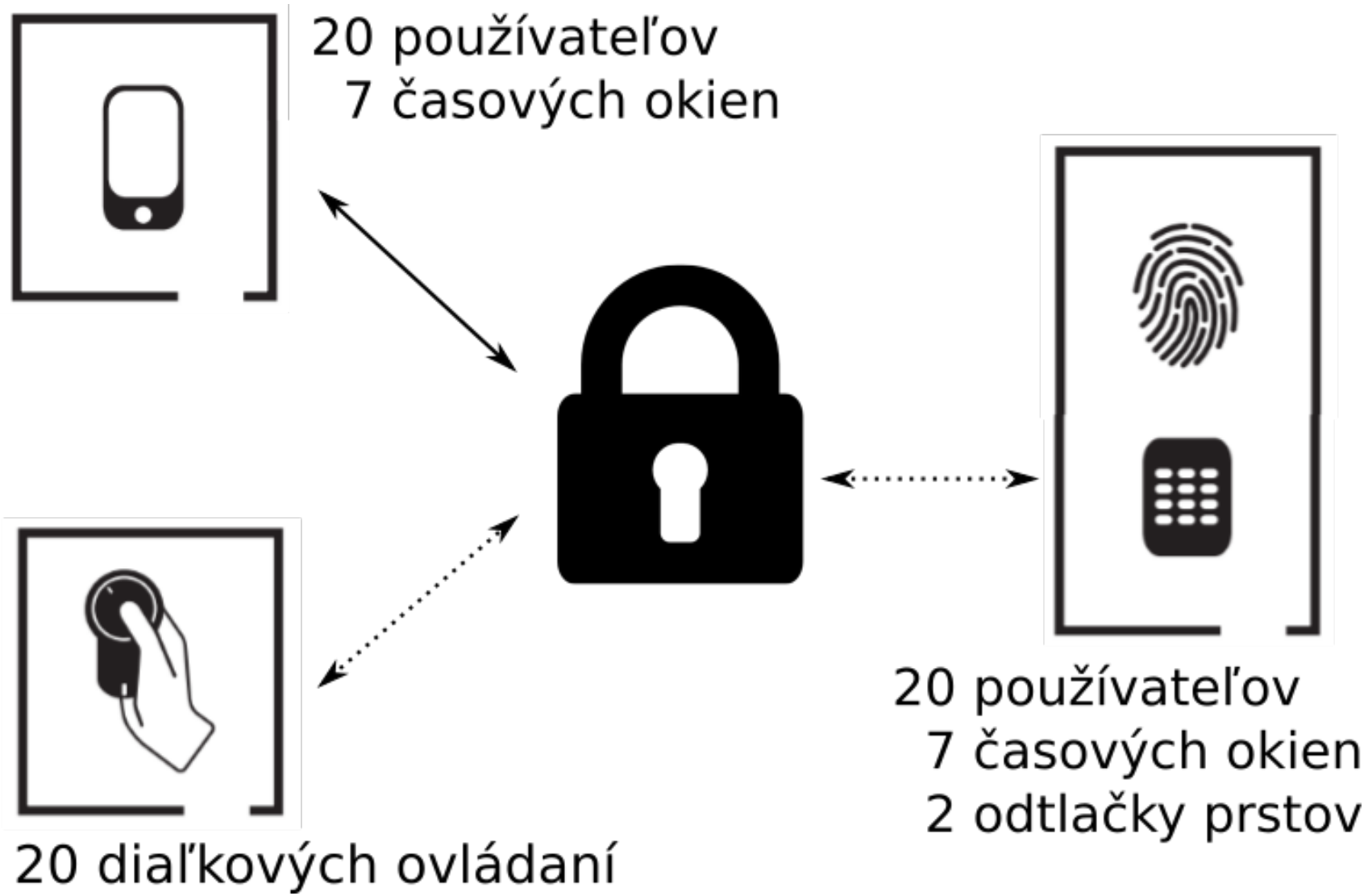
17. júna 2020

FAB Entr


FAB
ASSA ABLOY


1 2 ABC 3 DEF
4 GHI 5 JKL 6 MNO
7 PQRS 8 TUV 9 WXYZ
* 0 # OK
FAB


FAB
ASSA ABLOY


20 používateľov
7 časových okien
20 používateľov
7 časových okien
2 odtlačky prstov
20 diaľkových ovládaní

Zámok

- nikdy nezačína komunikáciu ako prvý
- odpovedá na párovanie a zamknutie/odomknutie

- reset do továrenských nastavení - údaje z bezdrôtovej klávesnice zostávajú uchované v nej, stačí ju len znova spárovať

Klávesnica s čítačkou odtlačkov prstov

- signál vysiela iba pri
  - párovaní
  - odomknutí/zamknutí (po zadaní správneho kódu/odtlačku)
- 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

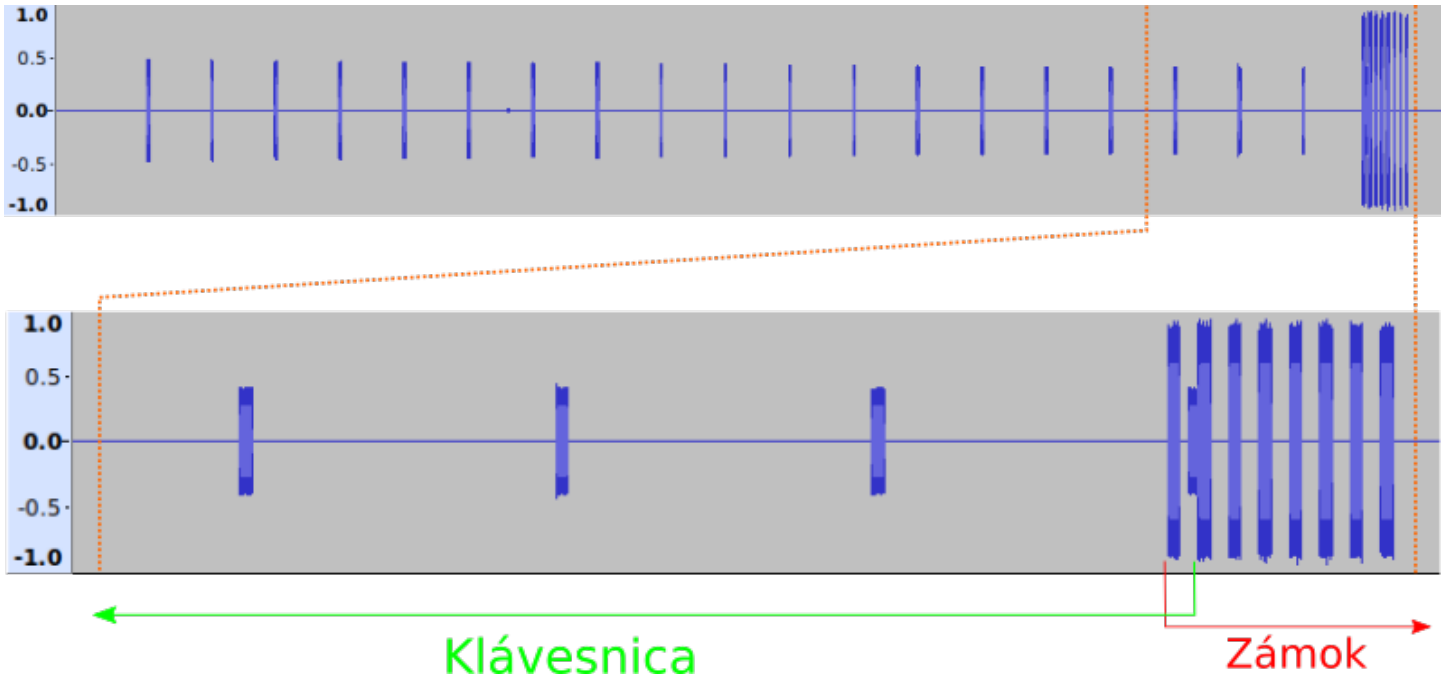
Diaľkové ovládanie

- signál vyšle vždy po stlačení tlačidla
- keď chceme odpojiť jedno diaľkové ovládanie, budú odstránené všetky diaľkové ovládania aj bezdrôtové klávesnice
- môže byť spárované len s jedným zámkom (na spárovanie s iným treba zásah autorizovaného servisu)

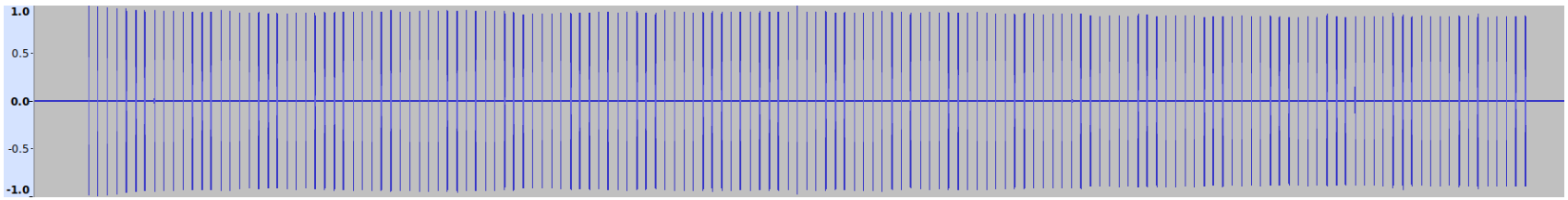
Plávajúci kód

- synchronizačné počítadlo C
- posledná valídna synchronizačná hodnota N
- akceptačné okno K
  - $0 < N - C < K + 1$
- resynchronizačné okno
  - $K < C - N < ResyncWindow$
- Rolljam

Odomykanie/zamykanie



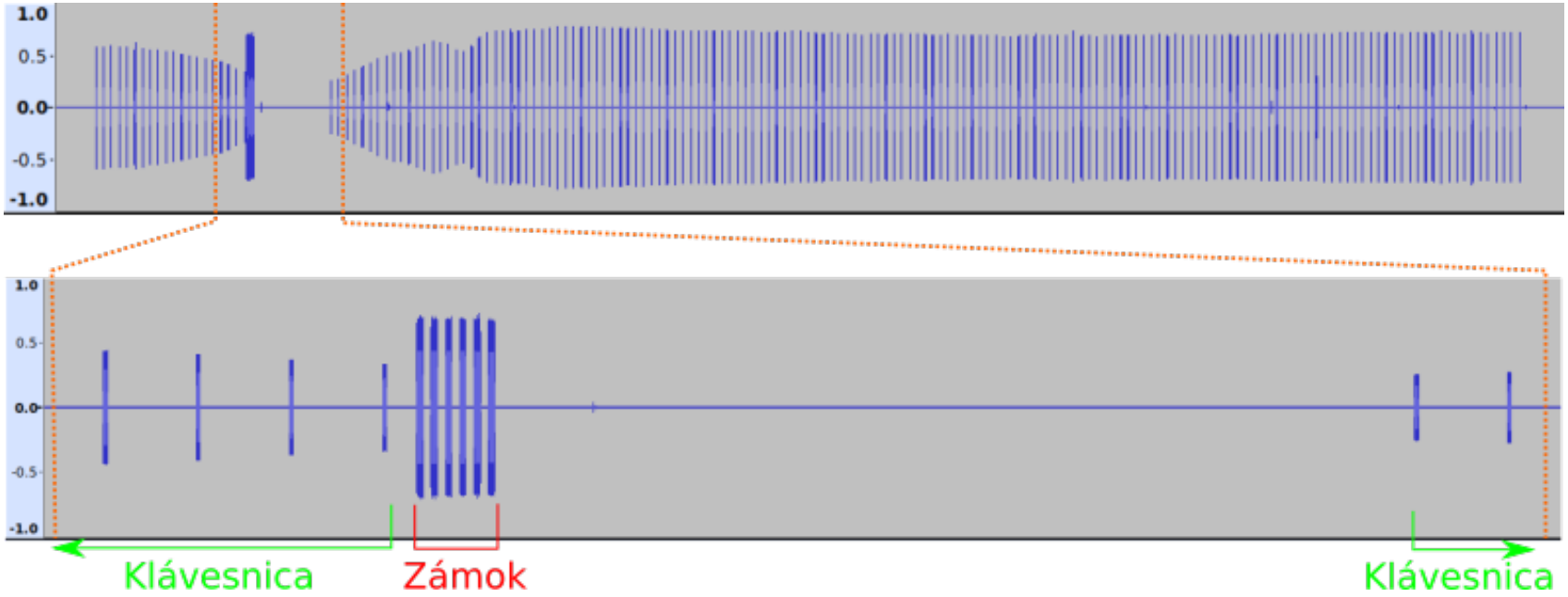
(a) V dosahu zámku



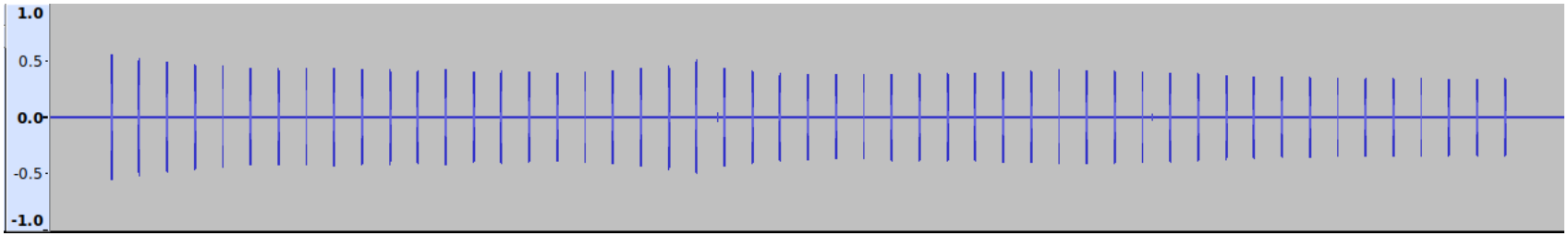
(b) Mimo dosahu zámku

Obr.: Signál pri odomykaní z klávesnice

Párovanie



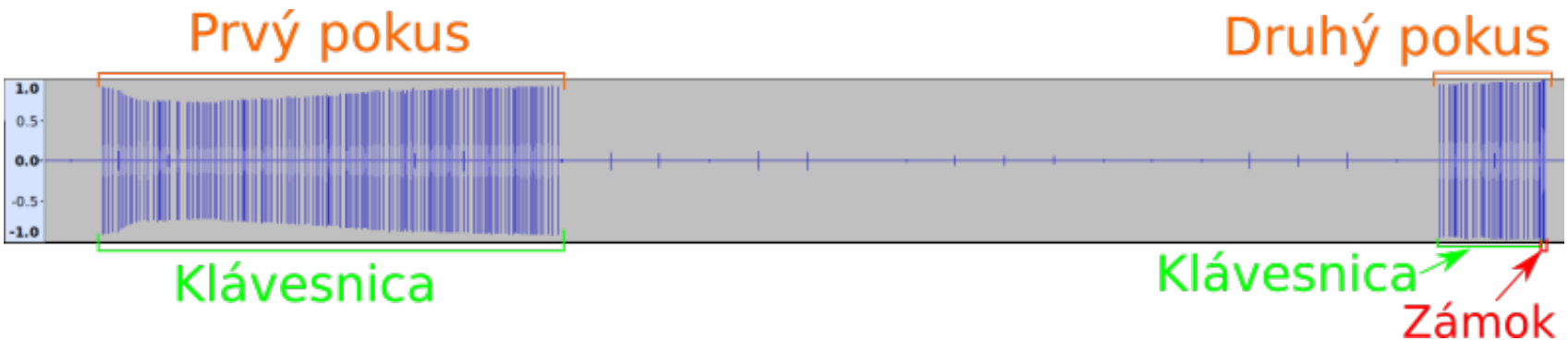
(a) Klávesnica



(b) Diaľkové ovládanie

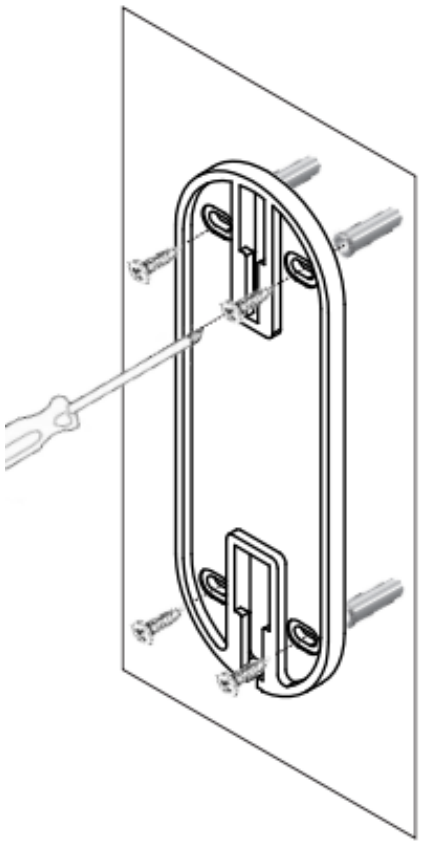
Obr.: Signál pri párovaní

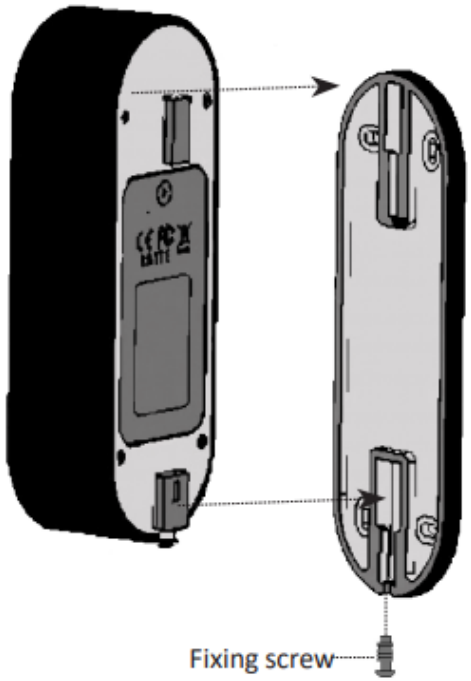
Synchronizácia



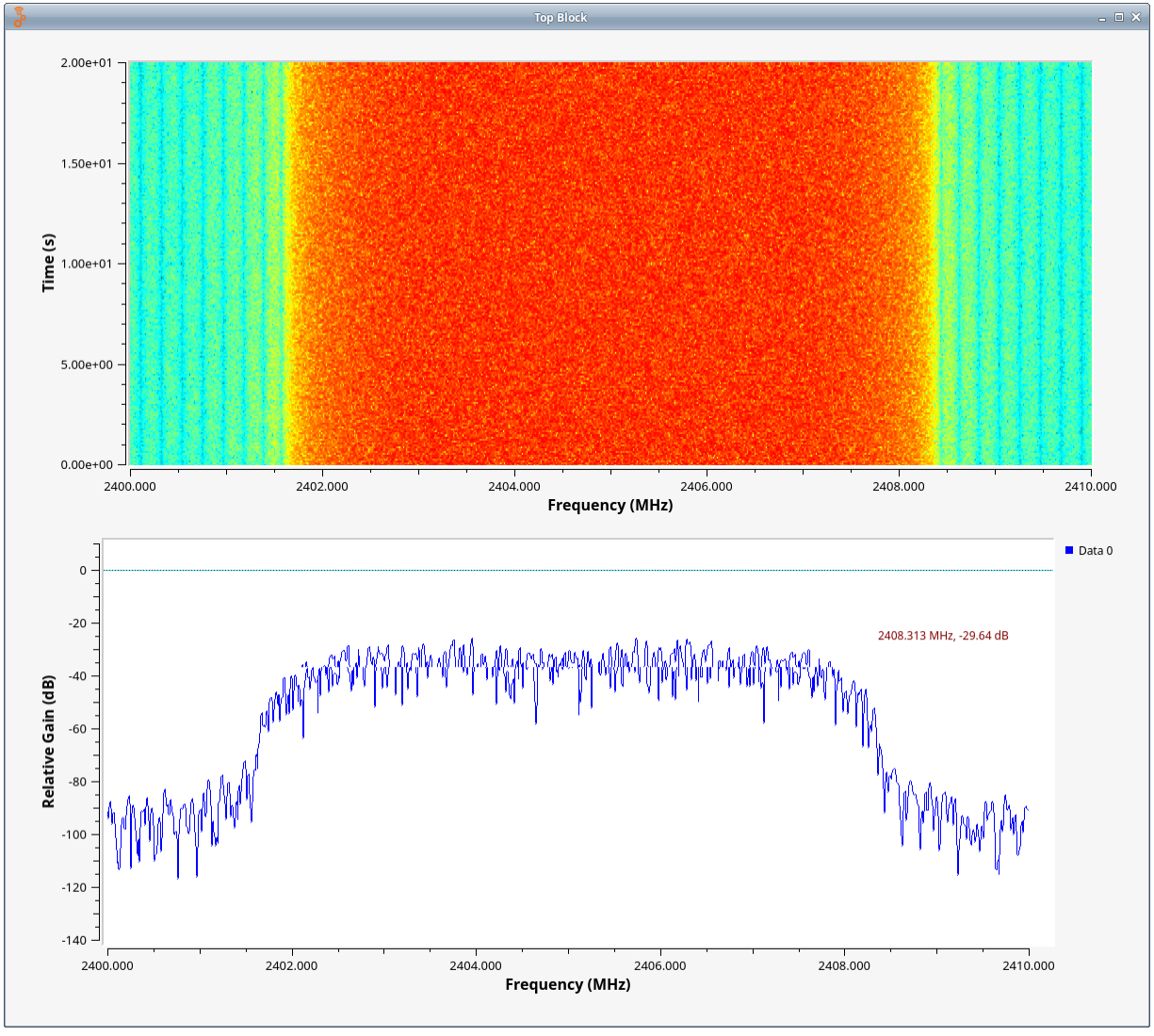
Obr.: Synchronizácia klávesnice pri odomykaní

Útok skrutkovačom





Zahltenie komunikačného pásma



Zistenie vlastností prístupového kódu

- dĺžka prístupového kódu
- zadané čísla podľa časového rozostupu
- „stlačené“ čísla podľa odtlačkov na klávesnici

Naivný útok hrubou silou

- prístupový kód: [0-9]{4,10}
- 3x zlý prístupový kód $\Rightarrow$ blokované 1 minútu
- vyskúšanie 1 prístupového kódu – 3 sekundy

- $\approx 11,1 \cdot 10^9$ možných kódov
- 8098 rokov

- štvormiestne prístupové kódy $\Rightarrow$ 10 000 možností

$$\left.\begin{array}{rl} 10000 & \text{kódov} \\ 3 & \text{nové kódy v slote} \\ 69 & \text{sekúnd na slot} \end{array}\right\} \approx 3333 \text{ slotov} \cdot 69 \text{ sekúnd}$$

230000 sekúnd $\approx$ 3833 minút $\approx$ 64 hodín $\approx$ 2.7 dní

Útok hrubou silou s využitím batérií

- po vybratí batérií si klávesnica nepamätá, že má byť blokovaná
- vybratie batérií a naštartovanie – cca 15-17 sekúnd

$$\left.\begin{array}{rl} 10000 & \text{kódov} \\ 3 & \text{nové kódy v slote} \\ 26 & \text{sekúnd na slot} \end{array}\right\} \approx 3333 \text{ slotov} \cdot 26 \text{ sekúnd}$$

$$\approx 86667 \text{ sekúnd} \approx 1444 \text{ minút} \approx 24 \text{ hodín} \approx 1 \text{ deň}$$

Útok hrubou silou s využitím časového okna

- používateľ má povolený vstup len v určitom časovom okne
- po zadaní platného prístupového kódu mimo časového okna sa počet neúspešných pokusov vynuluje

$$\left.\begin{array}{rl} 10000 & \text{kódov} \\ 2 & \text{nové kódy v slote} \\ 9 & \text{sekúnd na slot} \end{array}\right\} 5000 \text{ slotov} \cdot 9 \text{ sekúnd}$$

$$45000 \text{ sekúnd} \approx 750 \text{ minút} \approx 12.5 \text{ hodín} \approx 0.52 \text{ dňa}$$

Útok hrubou silou s využitím administrátorského rozhrania

- hádanie administrátorského kódu, len 1 kliknutie navyše
- žiadna ochrana

$$\left.\begin{array}{rl} 10000 & \text{kódov} \\ 1 & \text{nový kód v slote} \\ 3 & \text{sekundy na slot} \end{array}\right\} 10000 \text{ slotov} \cdot 3 \text{ sekundy}$$

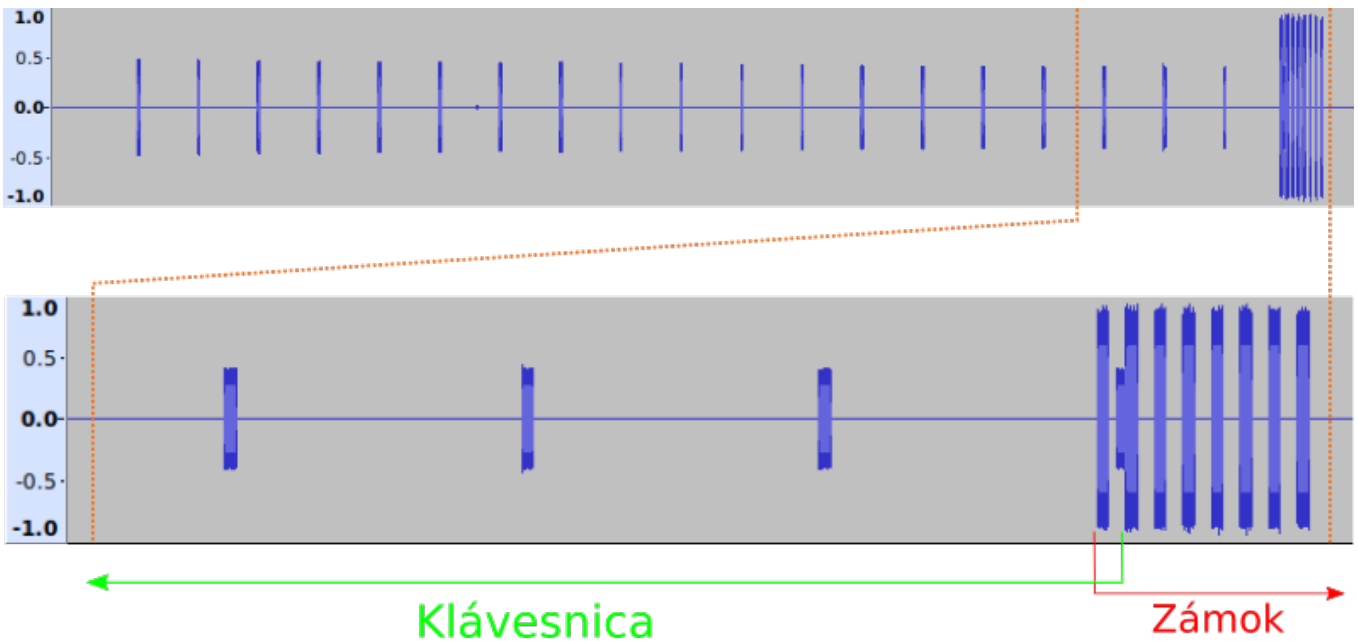
$$30000 \text{ sekúnd} \approx 500 \text{ minút} \approx 8.3 \text{ hodín} \approx 0.35 \text{ dňa}$$

Zhrnutie útokov hrubou silou

	základ	batéria	okno	admin
nové kódy v slote	3	3	2	1
# slotov	≈ 3333	≈ 3333	5000	10000
dĺžka slotu (sek)	69	26	9	3
hodín	≈ 64	≈ 24	12.5	≈ 8.3
dní	≈ 2.7	≈ 1	≈ 0.52	≈ 0.35
percento času	100%	$\approx 37\%$	$\approx 20\%$	$\approx 13\%$

Replay attack

- signál nahraný mimo dosahu zámku
- nahrané signály
  - stlačenie diaľkového ovládania
  - odomknutie z klávesnice
  - zamknutie z klávesnice
- vyslané prvýkrát
- vyslané druhýkrát



Útok na párovanie

- návod odporúča pri problémoch s odomknutím zopakovať párovanie
- race condition – párovanie úspešné pri zariadení, ktoré začalo skôr

Útok na párovanie

- návod odporúča pri problémoch s odomknutím zopakovať párovanie
- race condition – párovanie úspešné pri zariadení, ktoré začalo skôr

1. zahltenie komunikačného pásma
2. párovanie
3. útočníkovi sa podarí pripojiť ďalšie diaľkové ovládanie
4. používateľove diaľkové ovládanie stále funguje

Útok vynulovaním času

- vybratím batérií sa vynuluje čas
- používateľ s prístupom časovom okne blízko vynulovaného času získava „neobmedzený prístup“

Útok vynulovaním času

- vybratím batérií sa vynuluje čas
- používateľ s prístupom časovom okne blízko vynulovaného času získava „neobmedzený prístup“
- 00:00 01/01/1970 (štvrtok)

Útok vynulovaním času

- vybratím batérií sa vynuluje čas
- používateľ s prístupom časovom okne blízko vynulovaného času získava „neobmedzený prístup“
- 00:00 01/01/1970 (štvrtok)
- 00:00 01/01/00 (sobota)

Útok vynulovaním času

- vybratím batérií sa vynuluje čas
- používateľ s prístupom časovom okne blízko vynulovaného času získava „neobmedzený prístup“
- 00:00 01/01/1970 (štvrtok)
- 00:00 01/01/00 (sobota)
- zvyšné dni

Rovnaký prístupový kód

- používatelia by nemali mať rovnaký prístupový kód
- popísané v návode

Rovnaký prístupový kód

- používatelia by nemali mať rovnaký prístupový kód
- popísané v návode
- neimplementované

Prerušenie počas zmeny kódu

- prechod do stavu spánku
  - podržaním "*"
  - nečinnosťou

Prerušenie počas zmeny kódu

- prechod do stavu spánku
  - podržaním "*"
  - nečinnosťou
- vymazanie používateľa
- eskalácia privilégií
- nepredvídateľné správanie

Práca do budúcna

- analýza firmvéru zariadení
- aplikovanie útokov, na ktoré sme nemali materiálne vybavenie
- demodulovanie – analýza posielaných dát

- analýza mobilnej aplikácie
- aplikovanie známych útokov pri komunikácii zámku s aplikáciou

Ďakujem za pozornosť

Otázky od oponenta

- Bolo rozhodnutie sústrediť sa výhradne na black-box analýzu spravené na začiatku práce, alebo vzniklo až v priebehu práce v dôsledku časových obmedzení?
  - v priebehu práce