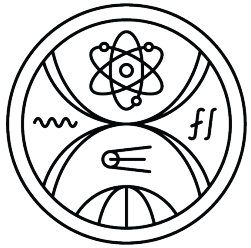
Útoky na hardvér pomocou indukovania chýb

Dennis Vita

školiteľ: RNDr. Richard Ostertág, PhD.

22. 06. 2023



FAKULTA MATEMATIKY,
FYZIKY A INFORMATIKY
Univerzita Komenského
v Bratislave

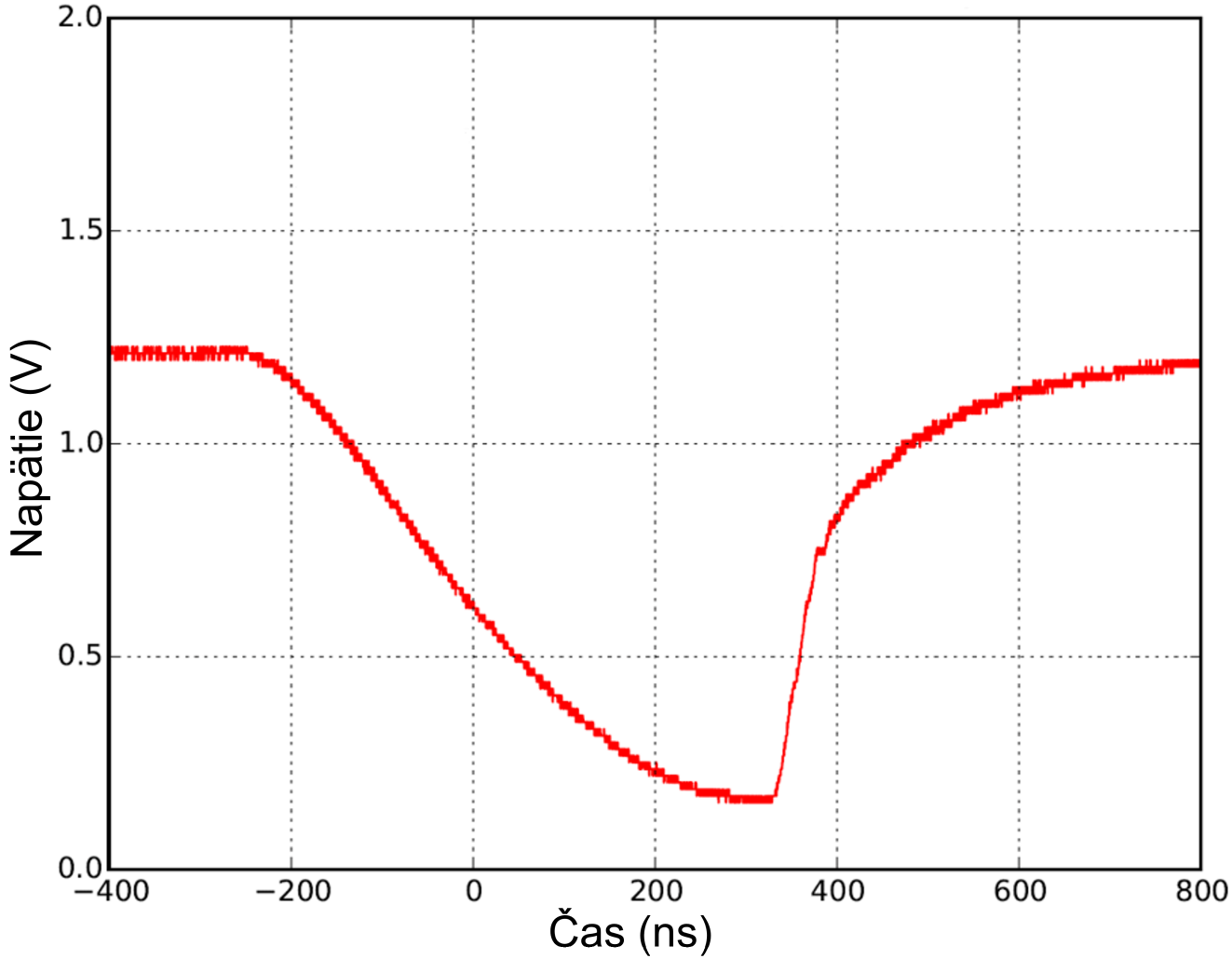
Útoky pomocou indukovania chýb

- externé faktory ovplyvňujú správanie hardvéru
- útok pomocou indukovania chýb (fault injection)
  - cielené ovplyvnenie správania
- vyžaduje fyzický prístup k zariadeniu
- rôzne techniky:
  - zmena napätia, manipulácia hodín, elektromagnetické rušenie, ...
- rôzne druhy chýb:
  - výsledok operácie, podmienený skok, vynechanie inštrukcie, prečítanie pamäte, ...

Útoky pomocou indukovania chýb

- externé faktory ovplyvňujú správanie hardvéru
- útok pomocou indukovania chýb (fault injection)
  - cielené ovplyvnenie správania
- vyžaduje fyzický prístup k zariadeniu
- rôzne techniky:
  - zmena napätia, manipulácia hodín, elektromagnetické rušenie, ...
- rôzne druhy chýb:
  - výsledok operácie, podmienený skok, vynechanie inštrukcie, prečítanie pamäte, ...

Zmena napätia



Zdroj:
https://eprint.iacr.org/2016/810.pdf

Motivácia

- útočník môže dosiahnuť:
  - obídenie bezpečnostného mechanizmu
  - ovplyvnenie vykonania kryptografických algoritmov
- mnoho článkov a prác:
  - najčastejšie vnorené (embedded) systémy
  - obvykle stredné až veľmi vysoké náklady (stovky až desaťtisíce eur)
- známe útoky
  - prečítanie pamäte s firmvérom aj pri zapnutej ochrane (Colin O'Flynn, 2020)
  - útok na zavádzací softvér – štart z nepovoleného média (Jan Van den Herrewegen, et al., 2020)
  - faktorizácia verejného modulu inštancie RSA schémy (Alessandro Barenghi, et al., 2012)

Motivácia

- útočník môže dosiahnuť:
  - obídenie bezpečnostného mechanizmu
  - ovplyvnenie vykonania kryptografických algoritmov
- mnoho článkov a prác:
  - najčastejšie vnorené (embedded) systémy
  - obvykle stredné až veľmi vysoké náklady (stovky až desaťtisíce eur)

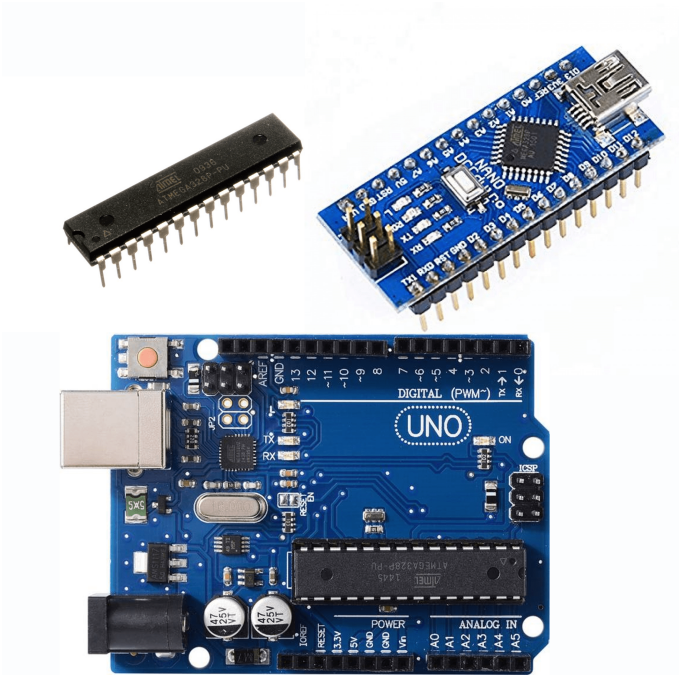
- známe útoky
  - prečítanie pamäte s firmvérom aj pri zapnutej ochrane (Colin O'Flynn, 2020)
  - útok na zavádzací softvér – štart z nepovoleného média (Jan Van den Herrewegen, et al., 2020)
  - faktorizácia verejného modulu inštancie RSA schémy (Alessandro Barenghi, et al., 2012)

Hlavné výsledky práce

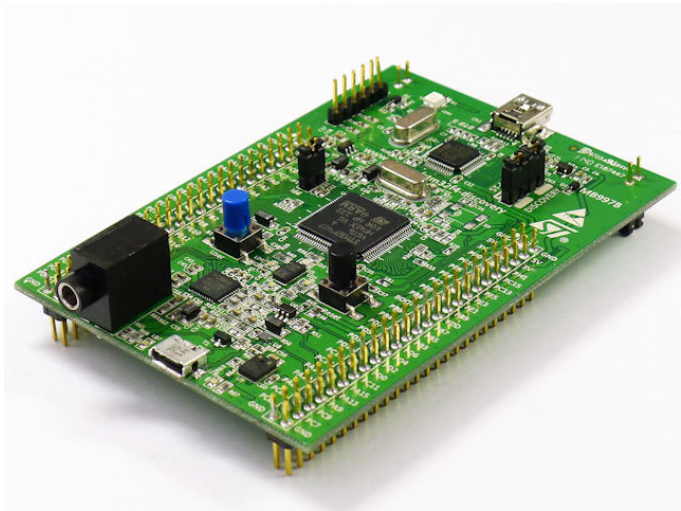
- útoky s využitím lacného hardvéru (desiatky eur)
- implementácia a analýza vybraných útokov
- technika zmeny napätia (dve konkrétne zapojenia)
- skúmali sme potrebnú presnosť načasovania
- demonštrácia výsledkov na jednoduchých programoch

Hardvér

- ATMega328P
- 16MHz

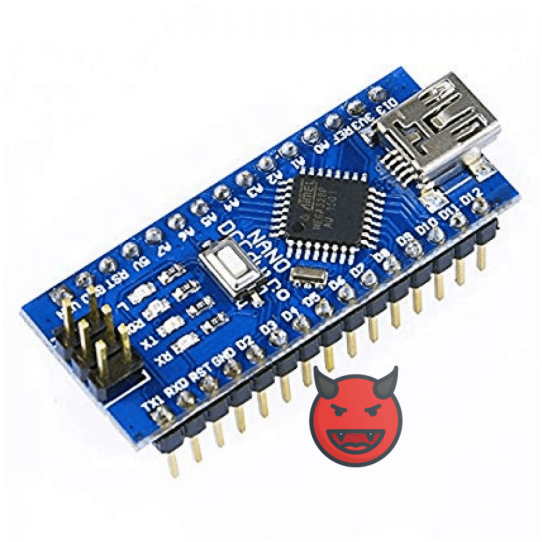


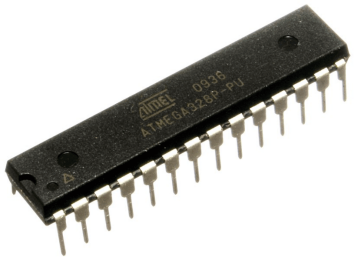
- STM32F4
- 168MHz

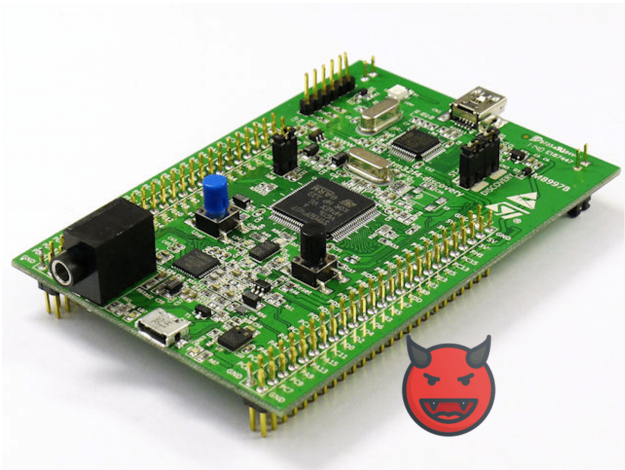


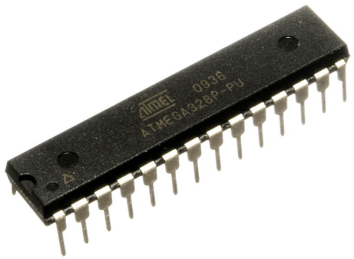
Zdroje:
https://en.wikipedia.org/wiki/ATmega328
https://nanopowerbd.com/index.php?route=product/product&product_id=114
https://www.twinschip.com/Arduino_Nano_V3.0
http://nicot31.fr/en/stm32f4-discovery-presentation/

Hardvér

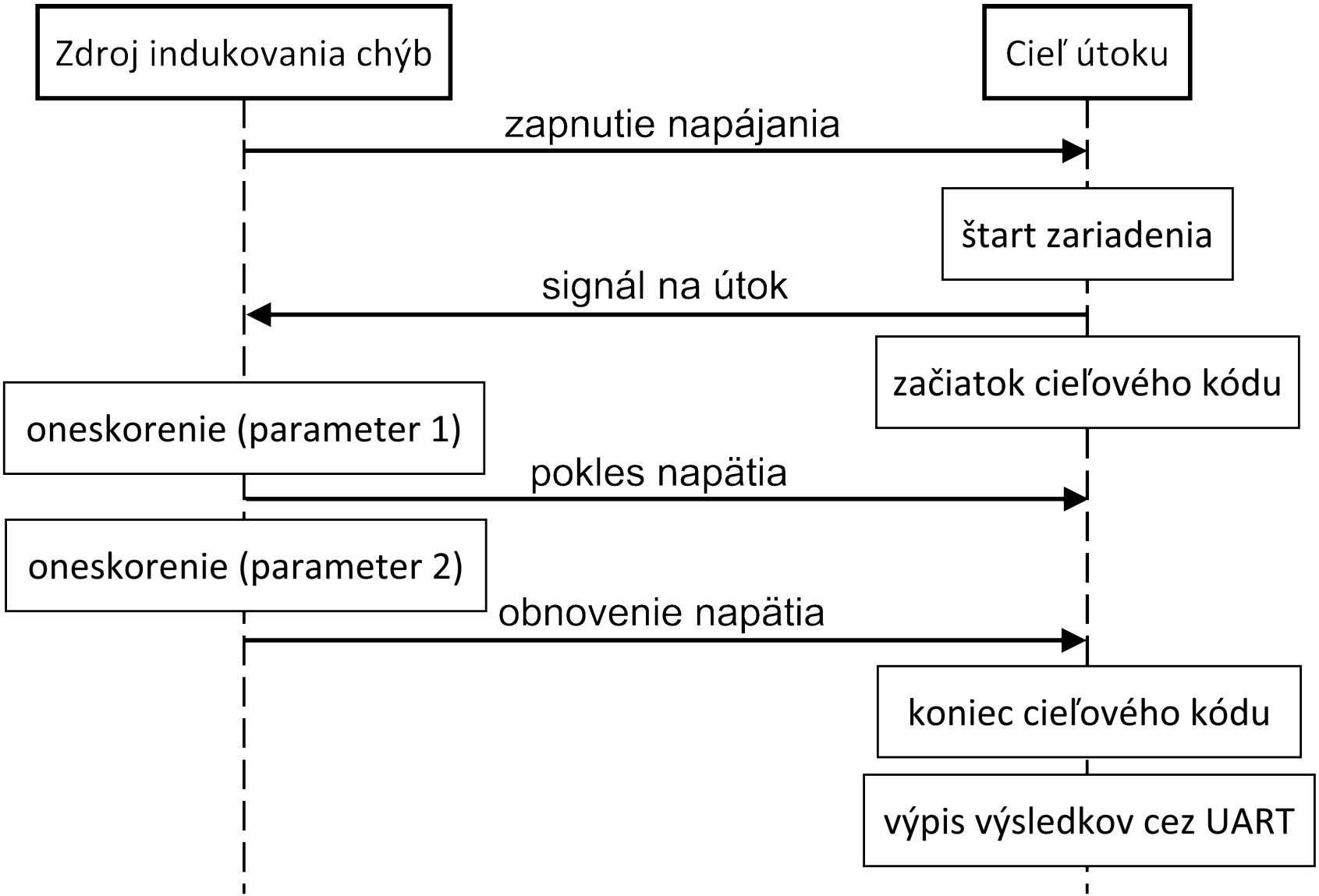




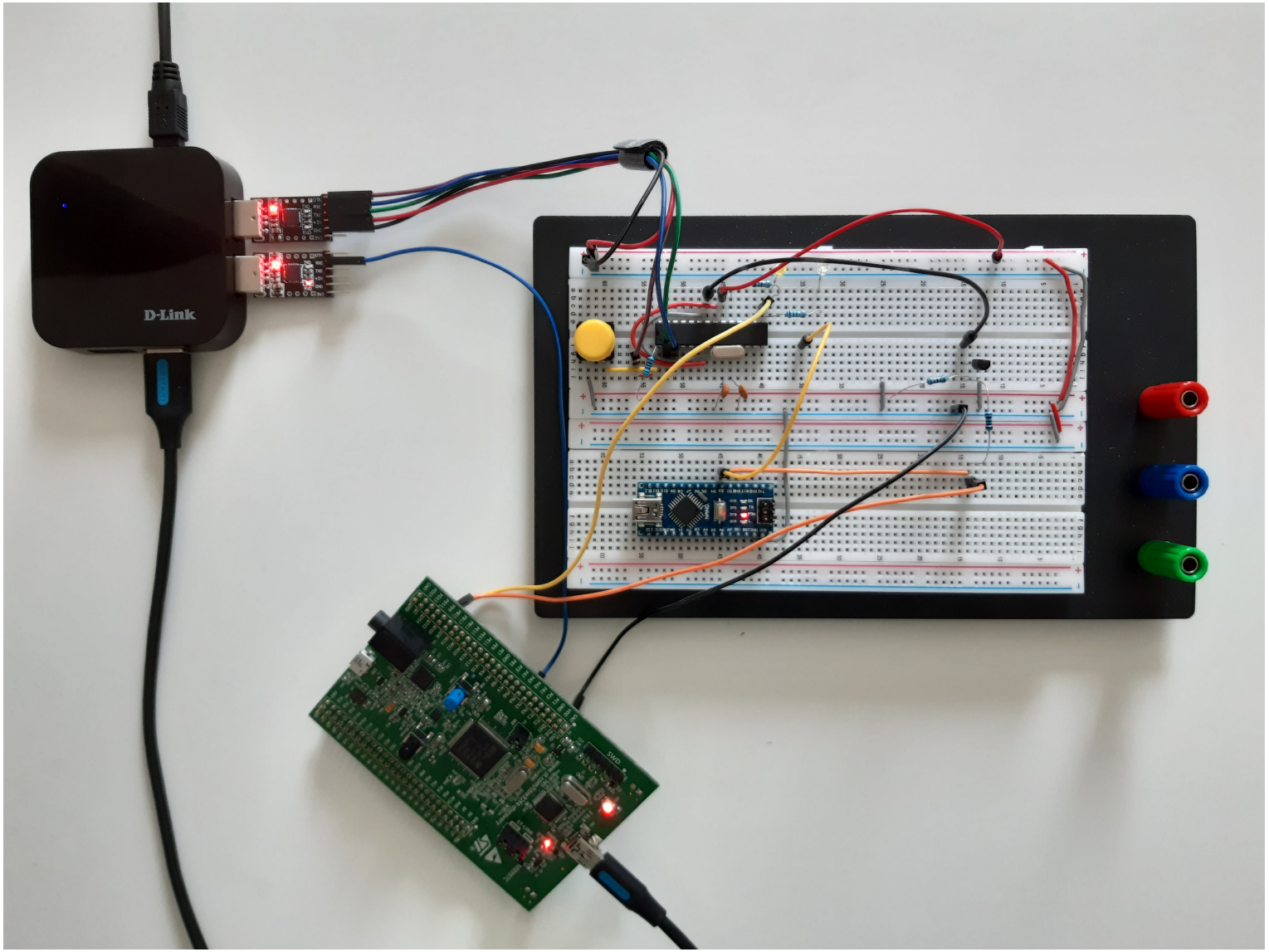




Experimenty



Experimenty



Príklady experimentov – vynechanie inštrukcie

Prepísanie hodnoty registra:

```
ldi r16, 0x00
ldi r16, 0x55
```

Príklady experimentov – vynechanie inštrukcie

Prepísanie hodnoty registra:

```
nop
...
nop
ldi r16, 0x00
ldi r16, 0x55
```

Príklady experimentov – vynechanie inštrukcie

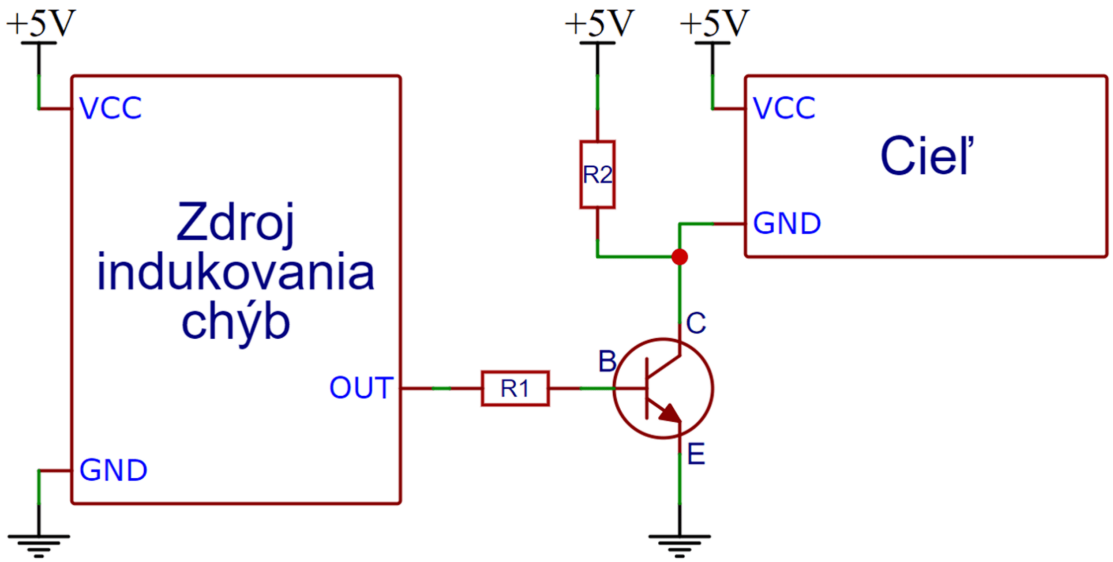
Prepísanie hodnoty registra:

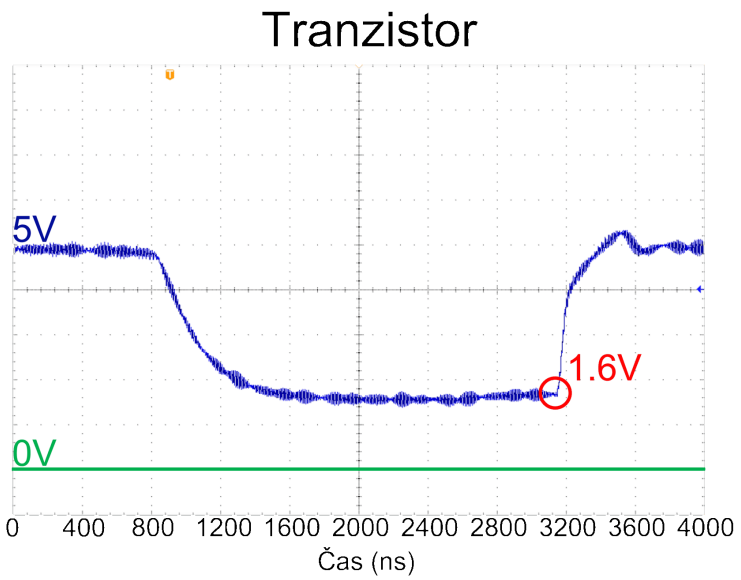
```
nop
...
nop
ldi r16, 0x00
ldi r16, 0x55
```

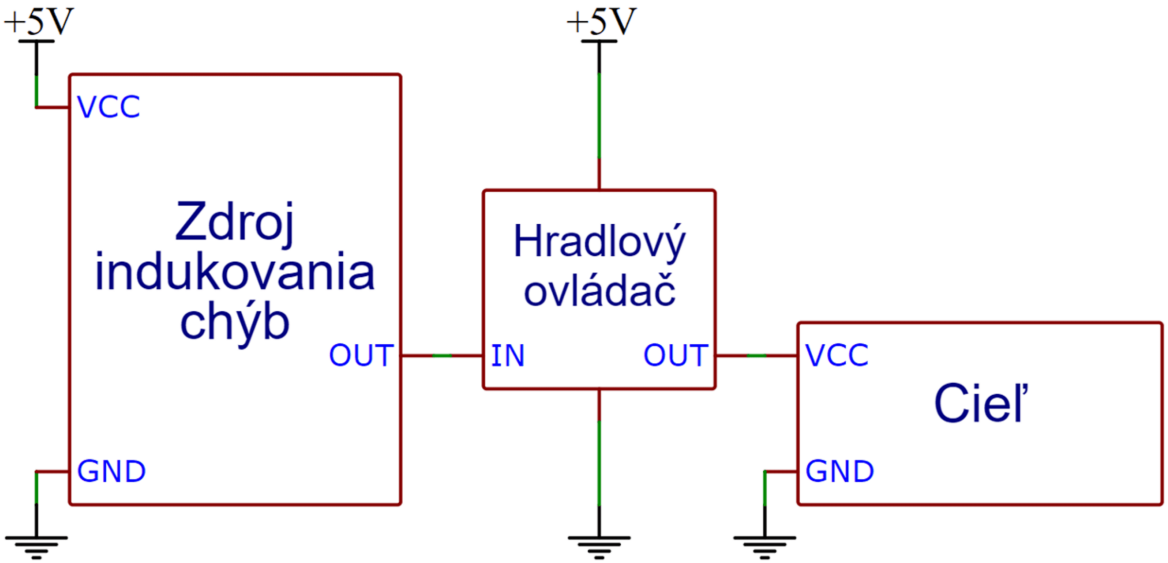
Séria inkrementov:

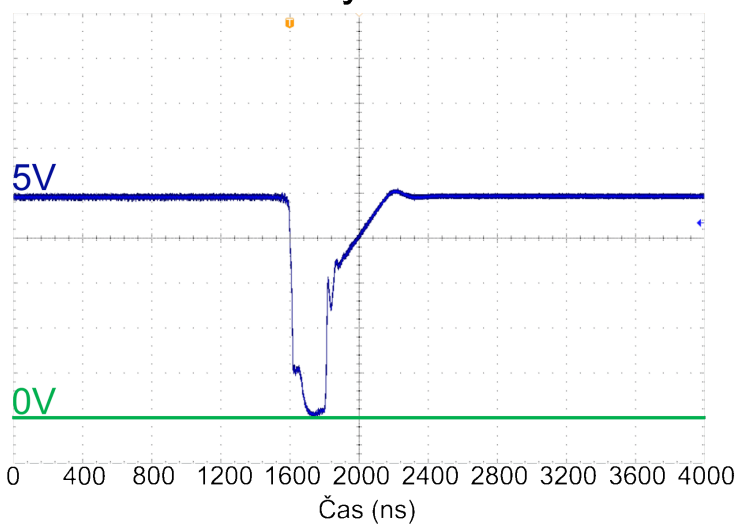
```
ldi r16, 0x00
inc r16
inc r16
...
inc r16
```

Porovnanie zapojení









Príklad útoku – čítačka RFID kariet

- demonštrácia vynechania inštrukcie
- jednoduchý program:
  - udeľuje prístup na základe hodnoty UID prečítanej karty
  - prístup má len karta s fixnou („zadrôtovanou“) hodnotou UID
  - vynechanie konkrétnej inštrukcie spôsobí udelenie prístupu aj neoprávnenej karte

Príklad útoku – čítačka RFID kariet

```
; inicializácia – vynulovanie registrov
clr r16
eor r0, r0

; porovnanie prvého bajtu
cpi r17, 0x04
breq skip_1
inc r0

; porovnanie druhého bajtu
skip_1:
cpi r18, 0xA3
breq skip_2
inc r0

; porovnanie tretieho bajtu
skip_2:
; ...
; ...
breq skip_5
inc r0

skip_5:
tst r0 ; test na 0 kontrolného súčtu

; podmienený skok ak kontrolný súčet ≠ 0
brne fail

ldi r16, 0x01 ; uloženie 1 do výstupu
fail:
nop

; nasleduje návrat z funkcie
```

Príklad útoku – čítačka RFID kariet

```
; inicializácia – vynulovanie registrov
clr r16
eor r0, r0

; porovnanie prvého bajtu
cpi r17, 0x04
breq skip_1
inc r0

; porovnanie druhého bajtu
skip_1:
cpi r18, 0xA3
breq skip_2
inc r0

; porovnanie tretieho bajtu
skip_2:
; ...
; ...
breq skip_5
inc r0

skip_5:
tst r0 ; test na 0 kontrolného súčtu

; podmienený skok ak kontrolný súčet ≠ 0
brne fail

ldi r16, 0x01 ; uloženie 1 do výstupu
fail:
nop

; nasleduje návrat z funkcie
```

Príklad útoku – čítačka RFID kariet

```
; inicializácia – vynulovanie registrov
clr r16
eor r0, r0

; porovnanie prvého bajtu
cpi r17, 0x04
breq skip_1
inc r0

; porovnanie druhého bajtu
skip_1:
cpi r18, 0xA3
breq skip_2
inc r0

; porovnanie tretieho bajtu
skip_2:
; ...
; ...
breq skip_5
inc r0

skip_5:
tst r0 ; test na 0 kontrolného súčtu

; podmienený skok ak kontrolný súčet ≠ 0
brne fail

ldi r16, 0x01 ; uloženie 1 do výstupu
fail:
nop

; nasleduje návrat z funkcie
```

Príklad útoku – čítačka RFID kariet

```
; inicializácia – vynulovanie registrov
clr r16
eor r0, r0

; porovnanie prvého bajtu
cpi r17, 0x04
breq skip_1
inc r0

; porovnanie druhého bajtu
skip_1:
cpi r18, 0xA3
breq skip_2
inc r0

; porovnanie tretieho bajtu
skip_2:
; ...
```

```
; ...
breq skip_5
inc r0

skip_5:
tst r0 ; test na 0 kontrolného súčtu

; podmienený skok ak kontrolný súčet ≠ 0
brne fail

ldi r16, 0x01 ; uloženie 1 do výstupu
fail:
nop

; nasleduje návrat z funkcie
```

Príklad útoku – čítačka RFID kariet

```
; inicializácia – vynulovanie registrov
clr r16
eor r0, r0

; porovnanie prvého bajtu
cpi r17, 0x04
breq skip_1
inc r0

; porovnanie druhého bajtu
skip_1:
cpi r18, 0xA3
breq skip_2
inc r0

; porovnanie tretieho bajtu
skip_2:
; ...
```

```
; ...
breq skip_5
inc r0

skip_5:
tst r0 ; test na 0 kontrolného súčtu

; podmienený skok ak kontrolný súčet ≠ 0
brne fail

ldi r16, 0x01 ; uloženie 1 do výstupu
fail:
nop

; nasleduje návrat z funkcie
```

Príklad útoku – čítačka RFID kariet

```
; inicializácia – vynulovanie registrov
clr r16
eor r0, r0

; porovnanie prvého bajtu
cpi r17, 0x04
breq skip_1
inc r0

; porovnanie druhého bajtu
skip_1:
cpi r18, 0xA3
breq skip_2
inc r0

; porovnanie tretieho bajtu
skip_2:
; ...
```

```
; ...
breq skip_5
inc r0

skip_5:
tst r0 ; test na 0 kontrolného súčtu

; podmienený skok ak kontrolný súčet ≠ 0
brne fail

ldi r16, 0x01 ; uloženie 1 do výstupu
fail:
nop

; nasleduje návrat z funkcie
```

Príklad útoku – čítačka RFID kariet

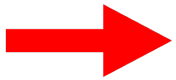
```
; inicializácia – vynulovanie registrov
clr r16
eor r0, r0

; porovnanie prvého bajtu
cpi r17, 0x04
breq skip_1
inc r0

; porovnanie druhého bajtu
skip_1:
cpi r18, 0xA3
breq skip_2
inc r0

; porovnanie tretieho bajtu
skip_2:
; ...
```

na túto inštrukciu cielime



```
; ...
breq skip_5
inc r0

skip_5:
tst r0 ; test na 0 kontrolného súčtu

; podmienený skok ak kontrolný súčet ≠ 0
brne fail

ldi r16, 0x01 ; uloženie 1 do výstupu
fail:
nop

; nasleduje návrat z funkcie
```

Zhrnutie

Zhrnutie

- aj lacným hardvérom možno útočiť
- obmedzená presnosť
- vynechanie inštrukcie
  - iný druh chyby sa nepodarilo indukovať
- nadviazanie na prácu:
  - vyskúšanie analyzovaných útokov na produkčných zariadeniach
  - analýza ďalších zapojení, techník indukovania chýb
  - indukovanie iných druhov chýb

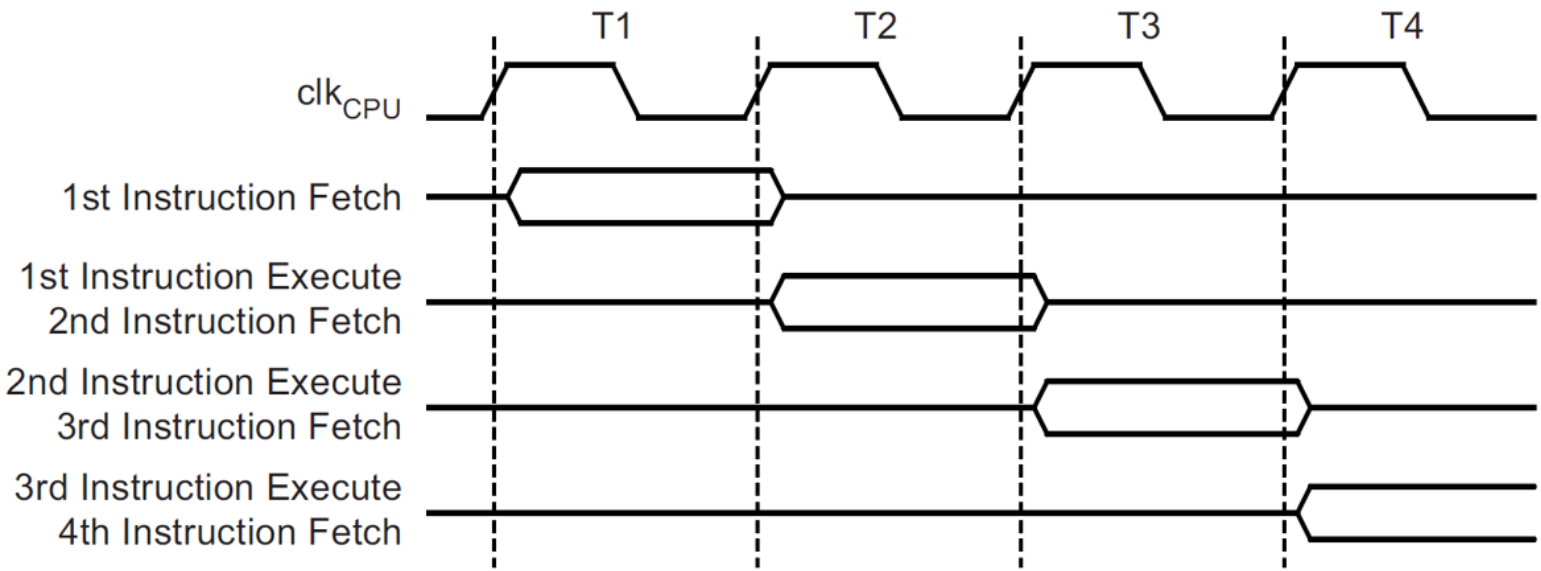
Zhrnutie

- aj lacným hardvérom možno útočiť
- obmedzená presnosť
- vynechanie inštrukcie
  - iný druh chyby sa nepodarilo indukovať
- nadviazanie na prácu:
  - vyskúšanie analyzovaných útokov na produkčných zariadeniach
  - analýza ďalších zapojení, techník indukovania chýb
  - indukovanie iných druhov chýb

Otázky

„Aký vnútorný mechanizmus spôsobuje, že pri krátkodobom znížení napájacieho napätia procesor jednu inštrukciu nevykoná (vynechá) a po obnovení úrovne napájania pokračuje vo vykonávanom programe ďalej?“

The Parallel Instruction Fetches and Instruction Executions



Zdroj:
https://ww1.microchip.com/downloads/en/DeviceDoc/Atmel-7810-Automotive-Microcontrollers-ATmega328P_Datasheet.pdf

Otázky

„Aké sú možné protiopatrenia na úrovni HW a SW voči opisovaným útokom?“

- HW:
  - pridanie kondenzátora
- SW:
  - náhodné oneskorenia
  - bezpečnejšie kompilovanie kódu