

Analysis of a door locking system

Rémi Audebert Pierre Surply

2014-07-17

Analysis of a
door locking
system

Rémi
Audebert,
Pierre Surply

Introduction

Signals

Hardware

Software

In situ

Conclusion

Introduction

Analysis of a door locking system

Rémi Audebert, Pierre Surply

Introduction

Signals

Hardware

Software

In situ

Conclusion



- The door lock is broken: fix-it!
- Power is working, the door is always locked
- Control is not working

Analysis of a
door locking
system

Rémi
Audebert,
Pierre Surply

Introduction

Signals

Hardware

Software

In situ

Conclusion

- Part 1: Electrical reverse engineering
 - Power, signals, 9N1, . . .
- Part 2: Hardware reverse engineering
 - Microcontrollers, converters, PHY, . . .
- Part 3: Software reverse engineering
 - PIC16F87, architecture, banking, . . .
- Part 4: A practical use of this knowledge
 - The big picture, controlling a door ourself

Analysis of a
door locking
system

Rémi
Audebert,
Pierre Surply

Introduction

Signals

Hardware

Software

In situ

Conclusion

Signals

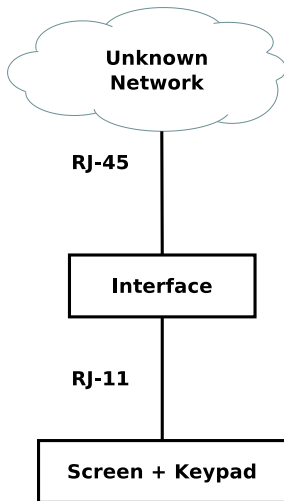


Figure 1: Probe points

Analysis of a
door locking
system

Rémi
Audebert,
Pierre Surply

Introduction

Signals

Hardware

Software

In situ

Conclusion

- Our goal: identify signals
- Possible signals:
 - Power
 - **Ground(s)**
 - Clock
 - Data
 - Differential data
 - Pull up

Tools

- Multimeters
- Digital Oscilloscope (ATTEN ADS1102CAL 100MHz)
- Logic analyser (Saleae Logic)

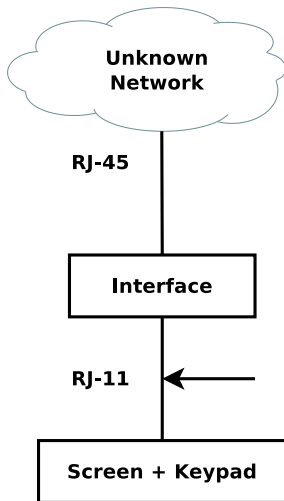


Figure 2: Probe points

Analysis of a
door locking
system

Rémi
Audebert,
Pierre Surply

Introduction

Signals

Hardware

Software

In situ

Conclusion

- 5V
- Ground
- ?
- ?
- ?
- ?

Analysis of a door locking system

Rémi Audebert, Pierre Surply

Introduction

Signals

Hardware

Software

In situ

Conclusion

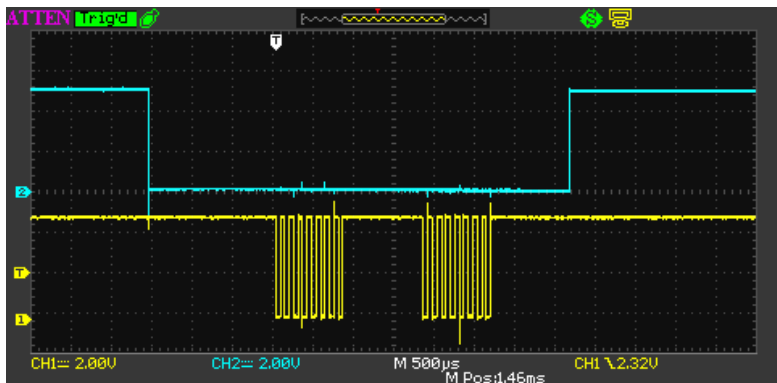


Figure 3: Frame

Analysis of a door locking system

Rémi Audebert, Pierre Surply

Introduction

Signals

Hardware

Software

In situ

Conclusion

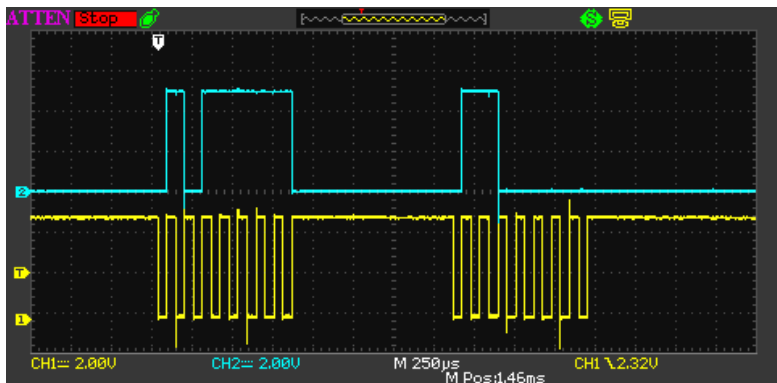


Figure 4: Frame

Analysis of a
door locking
system

Rémi
Audebert,
Pierre Surply

Introduction

Signals

Hardware

Software

In situ

Conclusion

- ~~UART-TTL~~
- I2C
- RS232
- **SPI**
- ...

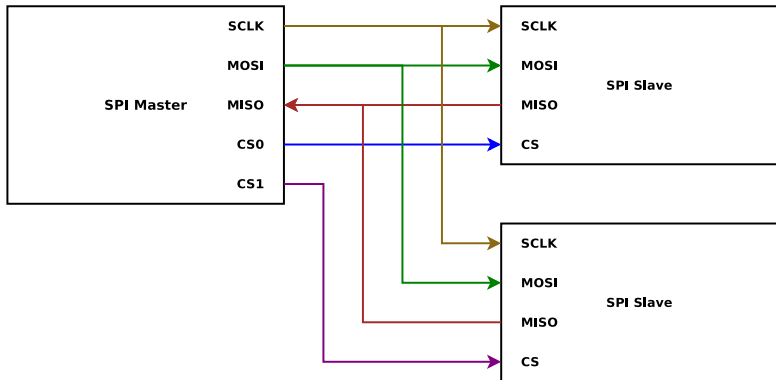


Figure 5: Frame

Analysis of a door locking system

Rémi Audebert, Pierre Surply

Introduction

Signals

Hardware

Software

In situ

Conclusion

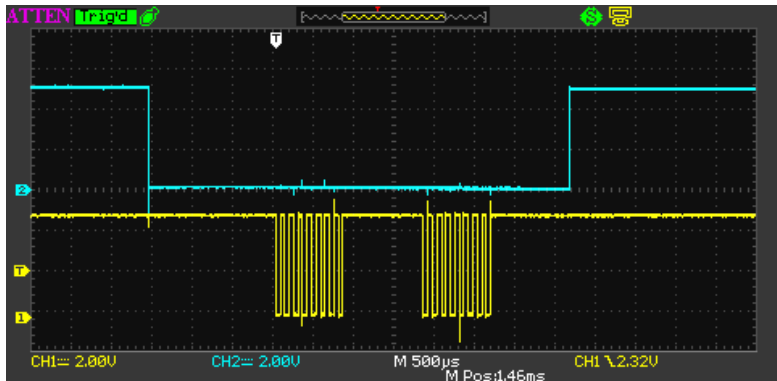


Figure 6: Frame

Analysis of a door locking system

Rémi Audebert, Pierre Surply

Introduction

Signals

Hardware

Software

In situ

Conclusion

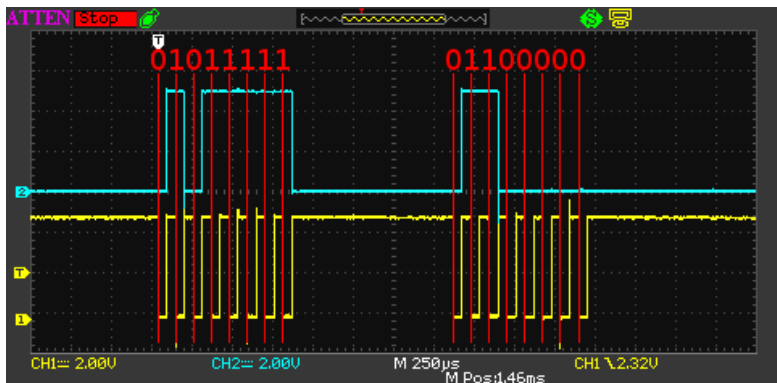


Figure 7: Frame

Analysis of a
door locking
system

Rémi
Audebert,
Pierre Surply

Introduction

Signals

Hardware

Software

In situ

Conclusion

- 5V
- Ground
- MOSI
- MISO
- SS
- SCK

Analysis of a door locking system

Rémi Audebert, Pierre Surply

Introduction

Signals

Hardware

Software

In situ

Conclusion

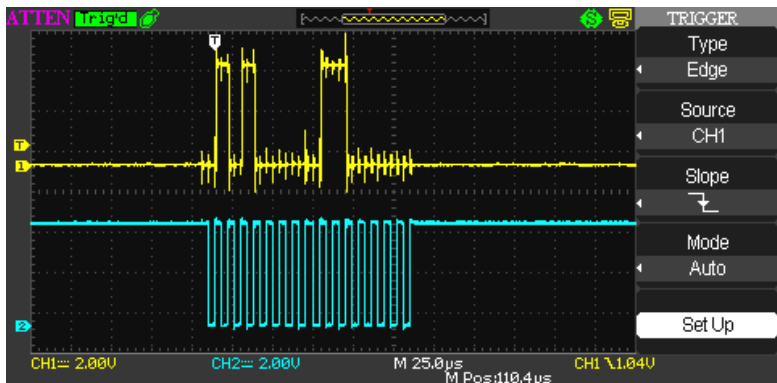


Figure 8: Frame

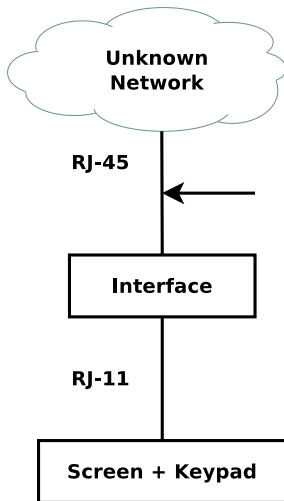


Figure 9: Probe points

Analysis of a
door locking
system

Rémi
Audebert,
Pierre Surply

Introduction

Signals

Hardware

Software

In situ

Conclusion

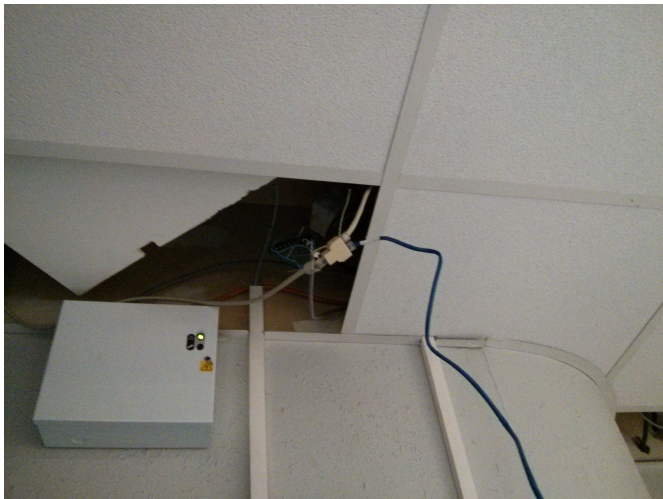


Figure 10: Ceiling cable

Analysis of a
door locking
system

Rémi
Audebert,
Pierre Surply

Introduction

Signals

Hardware

Software

In situ

Conclusion

- Our goal: identify signals
- Possible signals:
 - Power: 12V
 - Ground: Yes
 - Clock
 - Data
 - Differential data: On two wires

Analysis of a
door locking
system

Rémi
Audebert,
Pierre Surply

Introduction

Signals

Hardware

Software

In situ

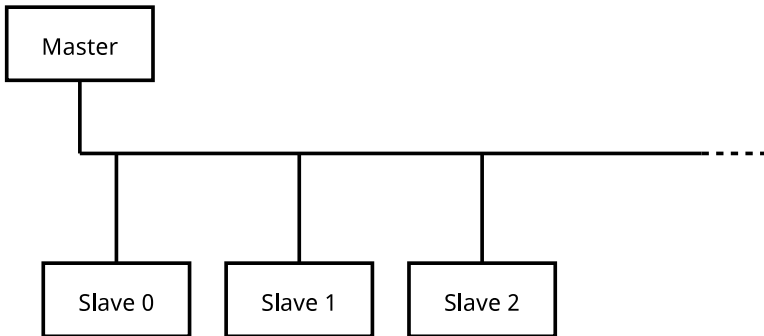
Conclusion

- ~~UART-TTL~~
- ~~SPI~~
- ~~I2C~~
- ~~RS232~~
- *Ethernet PHY*
- ~~CAN~~
- **RS485**

- ~~UART-TTL~~
- SPI
- I2C
- RS232
- *Ethernet PHY*
- CAN
- **RS485**

RS485 in short

- Two wires: A and B
- Differential signal:
 - $A - B < -200\text{mV}$ is 1
 - $A - B > +200\text{mV}$ is 0



- Same bus
- One master, many slaves
- Bidirectional communication:
 - Master polls slaves periodically
 - Slave answer when talked to

- No clock!

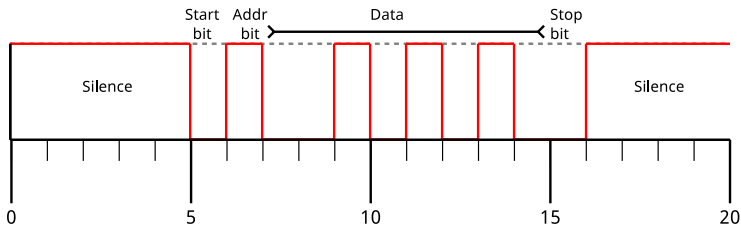


Figure 11: A word in this protocol

Principles of 9bit data mode

- 9th bit is used to signal an address
- The slave only listen when the address matches it's own

Analysis of a door locking system

Rémi Audebert, Pierre Surply

Introduction

Signals

Hardware

Software

In situ

Conclusion

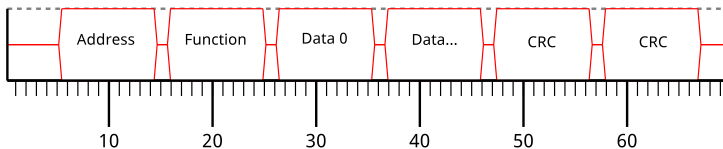


Figure 12: Message structure

Modbus RTU

- Another serial communication protocol

Similarities

- Same CRC polynom
- Message format

Differences with modbus RTU

- Not the same function
- Use an address bit
- Broadcast address is FF

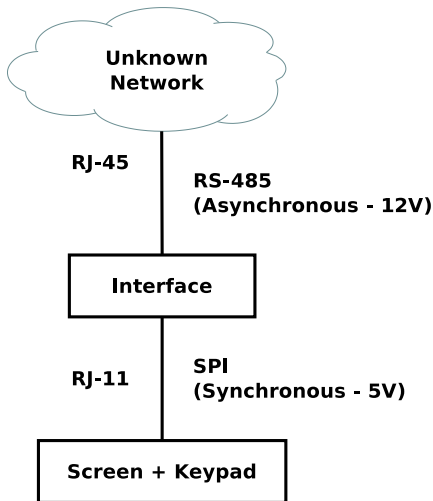


Figure 13: Probe points

Analysis of a
door locking
system

Rémi
Audebert,
Pierre Surply

Introduction

Signals

Hardware

Software

In situ

Conclusion

Hardware

Analysis of a door locking system

Rémi Audebert, Pierre Surply

Introduction

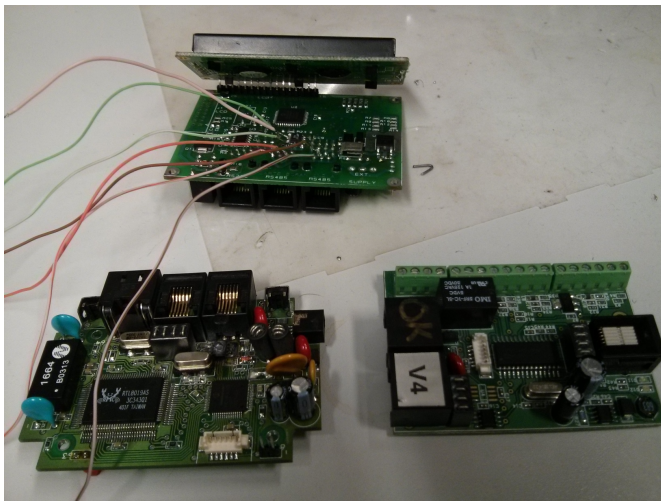
Signals

Hardware

Software

In situ

Conclusion



- Identify the parts
- Dump what you can

Analysis of a
door locking
system

Rémi
Audebert,
Pierre Surply

Introduction

Signals

Hardware

Software

In situ

Conclusion

- “Passive” components:
 - Resistors
 - Capacitors
 - Inductors
- “Active” components:
 - Microcontrollers
 - PHY, signal converters

Analysis of a
door locking
system

Rémi
Audebert,
Pierre Surply

Introduction

Signals

Hardware

Software

In situ

Conclusion

Screen Board

- UART to RS232
- PIC16F877

Secu Board

- UART to RS485
- Relay
- PIC18F6720

Unknown Board

- UART to RS485
- Ethernet PHY
- PIC18F2480

Analysis of a door locking system

Rémi Audebert, Pierre Surply

Introduction

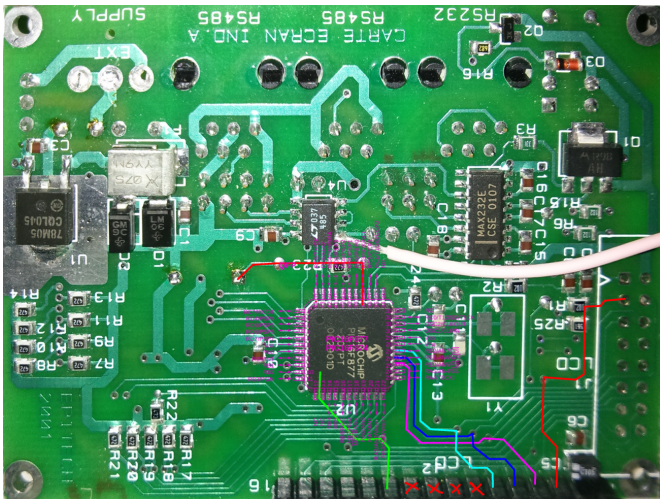
Signals

Hardware

Software

In situ

Conclusion



Analysis of a
door locking
system

Rémi
Audebert,
Pierre Surply

Introduction

Signals

Hardware

Software

In situ

Conclusion

Software

Analysis of a
door locking
system

Rémi
Audebert,
Pierre Surply

Introduction

Signals

Hardware

Software

In situ

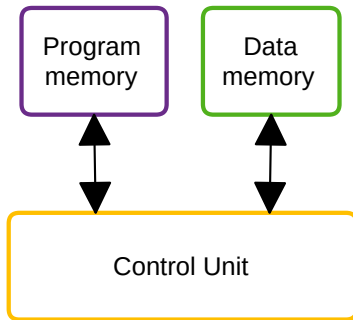
Conclusion

- A very common 8bit μ C.
- RISC: 35 instructions
- 8K Flash program memory
- 368 bytes of RAM
- 256 bytes of EEPROM
- Program instruction bus: 14bits
- Program counter: 13bits
- Data bus: 8bits

Dumping the flash

- Code protection: No!

- Code and data are stored in different memories



Harvard

Analysis of a
door locking
system

Rémi
Audebert,
Pierre Surply

Introduction

Signals

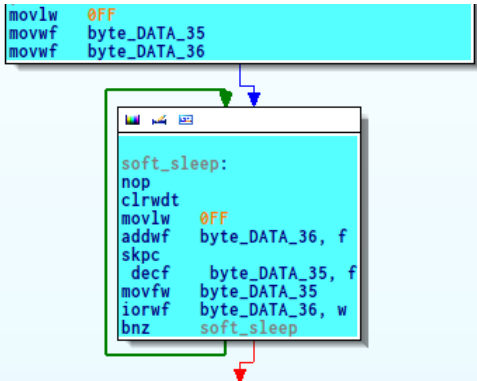
Hardware

Software

In situ

Conclusion

- Software sleeps
- Banking systems
- Indirect read/writes
- PIC's version of progmem/progspace



PIC16F87: Memory Banks

Analysis of a door locking system

Rémi Audebert, Pierre Surply

Introduction

Signals

Hardware

Software

In situ

Conclusion

File Address	File Address	File Address	File Address
Indirect addr. ⁽¹⁾ 00h	Indirect addr. ⁽¹⁾ 80h	Indirect addr. ⁽¹⁾ 100h	Indirect addr. ⁽¹⁾ 180h
TMR0 01h	OPTION_REG 81h	TMR0 101h	OPTION_REG 181h
PCL 02h	PCL 82h	PCL 102h	PCL 182h
STATUS 03h	STATUS 83h	STATUS 103h	STATUS 183h
FSR 04h	FSR 84h	FSR 104h	FSR 184h
PORTA 05h	TRISA 85h	105h	185h
PORTB 06h	TRISB 86h	PORTB 106h	TRISB 186h
PORTC 07h	TRISC 87h	107h	187h
PORTD ⁽²⁾ 08h	TRISD ⁽²⁾ 88h	108h	188h
PORTE ⁽²⁾ 09h	TRISE ⁽²⁾ 89h	109h	189h
PCLATH 0Ah	PCLATH 8Ah	PCLATH 10Ah	PCLATH 18Ah
INTCON 0Bh	INTCON 8Bh	INTCON 10Bh	INTCON 18Bh
PIR1 0Ch	PIE1 8Ch	EEDATA 10Ch	EECON1 18Ch
PIR2 0Dh	PIE2 8Dh	EEADR 10Dh	EECON2 18Dh
YMR1L 0Eh	PCON 8Eh	EEDATH 10Eh	Reserved ⁽³⁾ 18Eh
YMR1H 0Fh	8Fh	EEADRH 10Fh	Reserved ⁽³⁾ 18Fh
Y1CON 10h	90h	110h	190h
YMR2 11h	SSPCON2 91h	111h	191h
Y2CON 12h	PR2 92h	112h	192h
SSPBUF 13h	SSPADD 93h	113h	193h
SSPCON 14h	SSPSTAT 94h	114h	194h
CCPR1L 15h	95h	115h	195h
CCPR1H 16h	96h	116h	196h
CCP1CON 17h	97h	General Purpose Register 117h	General Purpose Register 197h
RCSTA 18h	TXSTA 98h	16 Bytes 118h	198h
TXREG 19h	SPBRG 99h	119h	199h
RCREG 1Ah	9Ah	11Ah	19Ah
CCPR2L 1Bh	9Bh	11Bh	19Bh
CCPR2H 1Ch	9Ch	11Ch	19Ch
CCP2CON 1Dh	9Dh	11Dh	19Dh
ADRESH 1Eh	ADRESL 9Eh	11Eh	19Eh
ADCON0 1Fh	ADCON1 9Fh	11Fh	19Fh
20h	A0h	120h	1A0h
General Purpose Register 96 Bytes	General Purpose Register 80 Bytes	General Purpose Register 80 Bytes	General Purpose Register 80 Bytes
Bank 0 7Fh	Bank 1 Fh	Bank 2 17Fh	Bank 3 1FFh
	EFh	16Fh	1EFh
	F0h	170h	1F0h
	accesses 70h-7Fh	accesses 70h-7Fh	accesses 70h-7Fh

PIC16F87: Memory Banking

Analysis of a door locking system

Rémi Audebert, Pierre Surply

Introduction

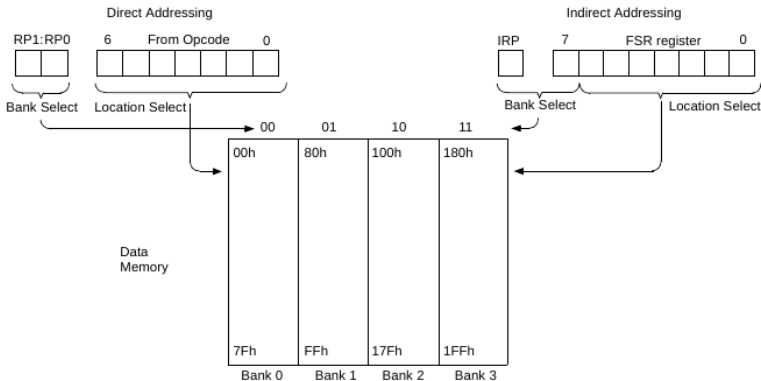
Signals

Hardware

Software

In situ

Conclusion



```
store_indf_7E_to_7C:
bcf    BANK0:STATUS, RP1
bcf    BANK0:STATUS, RP0
btfsc  byte_DATA_7C, 2
b      write_eeprom_addr7A_data7E
```

```
btfss  byte_DATA_7C, 4
return
bcf    BANK0:STATUS, RP1
bcf    BANK0:STATUS, RP0
movwf  byte_DATA_7A
movwf  BANK0:FSR
movwf  byte_DATA_7E
btfss  byte_DATA_7B, 3
b      loc_CODE_31A
```

```
Set IRP accordingly to byte_DATA_7B
```

```
loc_CODE_323:
movwf  BANK0:INDF
return
; End of function store_indf_7E_to_7C
```

```

CODE:1598 s_access_opened:
CODE:1598          retlw  41 ; 'A'
CODE:1599          ; -----
CODE:1599          retlw  63 ; 'c'
CODE:159A          ; -----
CODE:159A          retlw  63 ; 'c'
CODE:159B          ; -----
CODE:159B          retlw  65 ; 'e'
CODE:159C          ; -----
CODE:159C          retlw  73 ; 's'
CODE:159D          ; -----
CODE:159D          retlw  73 ; 's'
CODE:159E          ; -----
CODE:159E          retlw  20 ; ' '
CODE:159F          ; -----
CODE:159F          retlw  4F ; 'O'
CODE:15A0          ; -----
CODE:15A0          retlw  70 ; 'p'
CODE:15A1          ; -----
CODE:15A1          retlw  65 ; 'e'
CODE:15A2          ; -----
CODE:15A2          retlw  6E ; 'n'
CODE:15A3          ; -----
CODE:15A3          retlw  65 ; 'e'
CODE:15A4          ; -----
CODE:15A4          retlw  64 ; 'd'
CODE:15A5          ; -----
CODE:15A5          retlw  64 ; 'd'
CODE:15A6          ; -----
CODE:15A6          retlw  64 ; 'd'
CODE:15A7          ; -----
CODE:15A7          retlw  64 ; 'd'
CODE:15A8          ; -----
CODE:15A8          retlw  64 ; 'd'
CODE:15A9          ; -----
CODE:15A9          retlw  64 ; 'd'
CODE:15AA          ; -----
CODE:15AA          retlw  64 ; 'd'
CODE:15AB          ; -----
CODE:15AB          retlw  64 ; 'd'
CODE:15AC          ; -----
CODE:15AC          retlw  64 ; 'd'
CODE:15AD          ; -----
CODE:15AD          retlw  64 ; 'd'
CODE:15AE          ; -----
CODE:15AE          retlw  64 ; 'd'
CODE:15AF          ; -----
CODE:15AF          retlw  64 ; 'd'
CODE:15B0          ; -----
CODE:15B0          retlw  64 ; 'd'
CODE:15B1          ; -----
CODE:15B1          retlw  64 ; 'd'
CODE:15B2          ; -----
CODE:15B2          retlw  64 ; 'd'
CODE:15B3          ; -----
CODE:15B3          retlw  64 ; 'd'
CODE:15B4          ; -----
CODE:15B4          retlw  64 ; 'd'
CODE:15B5          ; -----
CODE:15B5          retlw  64 ; 'd'
CODE:15B6          ; -----
CODE:15B6          retlw  64 ; 'd'
CODE:15B7          ; -----
CODE:15B7          retlw  64 ; 'd'
CODE:15B8          ; -----
CODE:15B8          retlw  64 ; 'd'
CODE:15B9          ; -----
CODE:15B9          retlw  64 ; 'd'
CODE:15BA          ; -----
CODE:15BA          retlw  64 ; 'd'
CODE:15BB          ; -----
CODE:15BB          retlw  64 ; 'd'
CODE:15BC          ; -----
CODE:15BC          retlw  64 ; 'd'
CODE:15BD          ; -----
CODE:15BD          retlw  64 ; 'd'
CODE:15BE          ; -----
CODE:15BE          retlw  64 ; 'd'
CODE:15BF          ; -----
CODE:15BF          retlw  64 ; 'd'
CODE:15C0          ; -----
CODE:15C0          retlw  64 ; 'd'
CODE:15C1          ; -----
CODE:15C1          retlw  64 ; 'd'
CODE:15C2          ; -----
CODE:15C2          retlw  64 ; 'd'
CODE:15C3          ; -----
CODE:15C3          retlw  64 ; 'd'
CODE:15C4          ; -----
CODE:15C4          retlw  64 ; 'd'
CODE:15C5          ; -----
CODE:15C5          retlw  64 ; 'd'
CODE:15C6          ; -----
CODE:15C6          retlw  64 ; 'd'
CODE:15C7          ; -----
CODE:15C7          retlw  64 ; 'd'
CODE:15C8          ; -----
CODE:15C8          retlw  64 ; 'd'
CODE:15C9          ; -----
CODE:15C9          retlw  64 ; 'd'
CODE:15CA          ; -----
CODE:15CA          retlw  64 ; 'd'
CODE:15CB          ; -----
CODE:15CB          retlw  64 ; 'd'
CODE:15CC          ; -----
CODE:15CC          retlw  64 ; 'd'
CODE:15CD          ; -----
CODE:15CD          retlw  64 ; 'd'
CODE:15CE          ; -----
CODE:15CE          retlw  64 ; 'd'
CODE:15CF          ; -----
CODE:15CF          retlw  64 ; 'd'
CODE:15D0          ; -----
CODE:15D0          retlw  64 ; 'd'
CODE:15D1          ; -----
CODE:15D1          retlw  64 ; 'd'
CODE:15D2          ; -----
CODE:15D2          retlw  64 ; 'd'
CODE:15D3          ; -----
CODE:15D3          retlw  64 ; 'd'
CODE:15D4          ; -----
CODE:15D4          retlw  64 ; 'd'
CODE:15D5          ; -----
CODE:15D5          retlw  64 ; 'd'
CODE:15D6          ; -----
CODE:15D6          retlw  64 ; 'd'
CODE:15D7          ; -----
CODE:15D7          retlw  64 ; 'd'
CODE:15D8          ; -----
CODE:15D8          retlw  64 ; 'd'
CODE:15D9          ; -----
CODE:15D9          retlw  64 ; 'd'
CODE:15DA          ; -----
CODE:15DA          retlw  64 ; 'd'
CODE:15DB          ; -----
CODE:15DB          retlw  64 ; 'd'
CODE:15DC          ; -----
CODE:15DC          retlw  64 ; 'd'
CODE:15DD          ; -----
CODE:15DD          retlw  64 ; 'd'
CODE:15DE          ; -----
CODE:15DE          retlw  64 ; 'd'
CODE:15DF          ; -----
CODE:15DF          retlw  64 ; 'd'
CODE:15E0          ; -----
CODE:15E0          retlw  64 ; 'd'
CODE:15E1          ; -----
CODE:15E1          retlw  64 ; 'd'
CODE:15E2          ; -----
CODE:15E2          retlw  64 ; 'd'
CODE:15E3          ; -----
CODE:15E3          retlw  64 ; 'd'
CODE:15E4          ; -----
CODE:15E4          retlw  64 ; 'd'
CODE:15E5          ; -----
CODE:15E5          retlw  64 ; 'd'
CODE:15E6          ; -----
CODE:15E6          retlw  64 ; 'd'
CODE:15E7          ; -----
CODE:15E7          retlw  64 ; 'd'
CODE:15E8          ; -----
CODE:15E8          retlw  64 ; 'd'
CODE:15E9          ; -----
CODE:15E9          retlw  64 ; 'd'
CODE:15EA          ; -----
CODE:15EA          retlw  64 ; 'd'
CODE:15EB          ; -----
CODE:15EB          retlw  64 ; 'd'
CODE:15EC          ; -----
CODE:15EC          retlw  64 ; 'd'
CODE:15ED          ; -----
CODE:15ED          retlw  64 ; 'd'
CODE:15EE          ; -----
CODE:15EE          retlw  64 ; 'd'
CODE:15EF          ; -----
CODE:15EF          retlw  64 ; 'd'
CODE:15F0          ; -----
CODE:15F0          retlw  64 ; 'd'
CODE:15F1          ; -----
CODE:15F1          retlw  64 ; 'd'
CODE:15F2          ; -----
CODE:15F2          retlw  64 ; 'd'
CODE:15F3          ; -----
CODE:15F3          retlw  64 ; 'd'
CODE:15F4          ; -----
CODE:15F4          retlw  64 ; 'd'
CODE:15F5          ; -----
CODE:15F5          retlw  64 ; 'd'
CODE:15F6          ; -----
CODE:15F6          retlw  64 ; 'd'
CODE:15F7          ; -----
CODE:15F7          retlw  64 ; 'd'
CODE:15F8          ; -----
CODE:15F8          retlw  64 ; 'd'
CODE:15F9          ; -----
CODE:15F9          retlw  64 ; 'd'
CODE:15FA          ; -----
CODE:15FA          retlw  64 ; 'd'
CODE:15FB          ; -----
CODE:15FB          retlw  64 ; 'd'
CODE:15FC          ; -----
CODE:15FC          retlw  64 ; 'd'
CODE:15FD          ; -----
CODE:15FD          retlw  64 ; 'd'
CODE:15FE          ; -----
CODE:15FE          retlw  64 ; 'd'
CODE:15FF          ; -----
CODE:15FF          retlw  64 ; 'd'

```

```

; assume pclath = 0

; goto $7b$7a

lookup_table_get:
bcf    BANK0:STATUS, RP1 ; reset bank
bcf    BANK0:STATUS, RP0 ; reset bank
movwf  byte_DATA_7B     ; bank0:7b == 16
movwf  BANK0:PCLATH     ; pclath <- 16
movwf  byte_DATA_7A     ; bank0:7a == 18
movwf  BANK0:PCL        ; pcl <- 18
; End of function lookup_table_get ; GOTO 0x1618
    
```

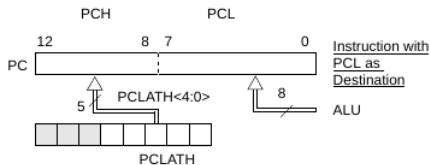


Figure 14: PIC paging

Analysis of a
door locking
system

Rémi
Audebert,
Pierre Surply

Introduction

Signals

Hardware

Software

In situ

Conclusion

In situ

Analysis of a
door locking
system

Rémi
Audebert,
Pierre Surply

Introduction

Signals

Hardware

Software

In situ

Conclusion

- The door lock is broken: fix-it!
- Power is working, the door is always locked
- Control is not working

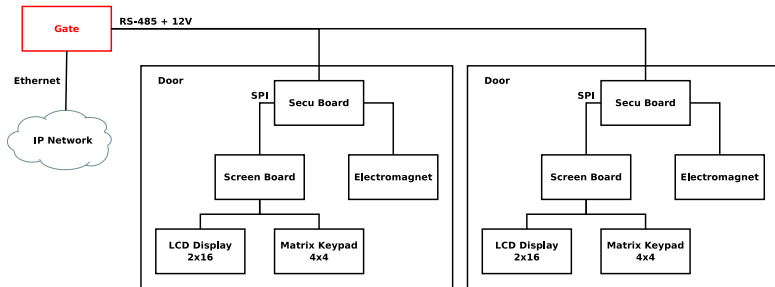


Figure 15: Topology

Analysis of a
door locking
system

Rémi
Audebert,
Pierre Surply

Introduction

Signals

Hardware

Software

In situ

Conclusion

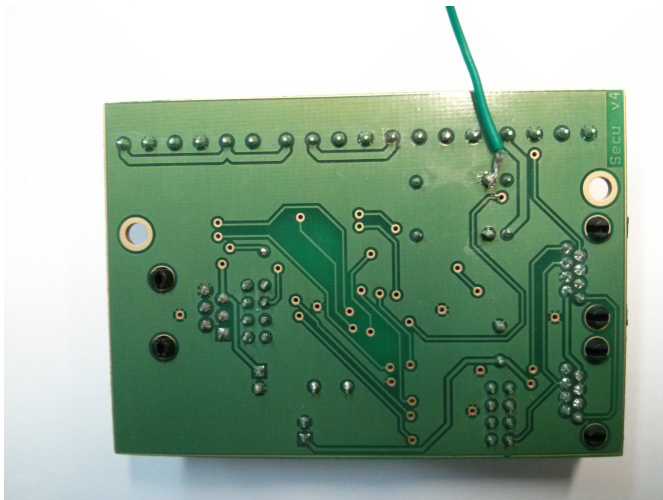


Figure 16: Our wire

Analysis of a door locking system

Rémi Audebert, Pierre Surply

Introduction

Signals

Hardware

Software

In situ

Conclusion

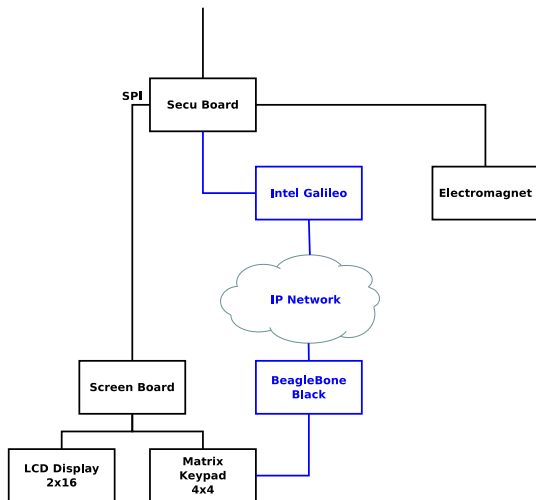


Figure 17: Topology

Analysis of a
door locking
system

Rémi
Audebert,
Pierre Surply

Introduction

Signals

Hardware

Software

In situ

Conclusion

Conclusion

Analysis of a
door locking
system

Rémi
Audebert,
Pierre Surply

Introduction

Signals

Hardware

Software

In situ

Conclusion

- This system is too rigid: custom hardware, half-duplex
- Not resilient too power failure: every thing is online, multiple SPOF
- No security: clear text communication

Analysis of a
door locking
system

Rémi
Audebert,
Pierre Surply

Introduction

Signals

Hardware

Software

In situ

Conclusion

Misc. good reads

- <http://www.bunniestudios.com>
- <http://www.spritesmods.com>
- <http://www.devtty0.com>

Hardware hacking exercices

- <http://blog.scrt.ch/2013/03/26/insomnihack-2013-life-is-hardware/>
- <http://www.balda.ch/posts/2014/Apr/01/ins14-life-is-even-harder/>
- <https://microcorruption.com>

Analysis of a
door locking
system

Rémi
Audebert,
Pierre Surply

Introduction

Signals

Hardware

Software

In situ

Conclusion

- Pierre Bourdon
- Théo
- Christian Dujardin
- Evolutek<<
- Prologin

Analysis of a
door locking
system

Rémi
Audebert,
Pierre Surply

Introduction

Signals

Hardware

Software

In situ

Conclusion

Contact

- Rémi 'halfr' Audebert
 - IRC: `halfr@irc.rezosup.org`
 - Mail: `halfr@lse.epita.fr`
 - Twitter: `@halfr`
- Pierre 'Ptishell' Surply
 - IRC: `Ptishell@irc.rezosup.org`
 - Mail: `surply@lse.epita.fr`
 - Twitter: `@Ptishell`