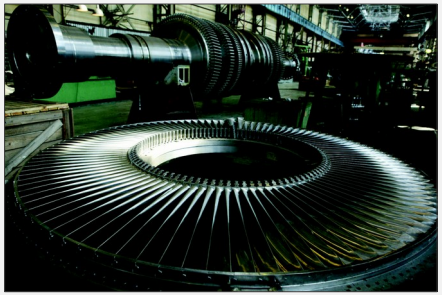
FoxGuard Solutions®

FoxGuard Solutions

Hacking firmware where you least expect it: in your tools



Monta Elkins

Security Architect
for FoxGuard Solutions

melkins@FoxGuardSolutions.com

FoxGuard Solutions

- Security Research
- New Attacks
- Training Classes
- Conference Talks
- New Product Creation
- Industry Requirements

FoxGuard Solutions

Operation and Disassembly

Processing Power

Drill:

- 8 Mhz clock
- 8 channel 10-bit ADC
- 6 PWM channels
- Multiply 2 cycles

Calculator:

- 6 Mhz clock

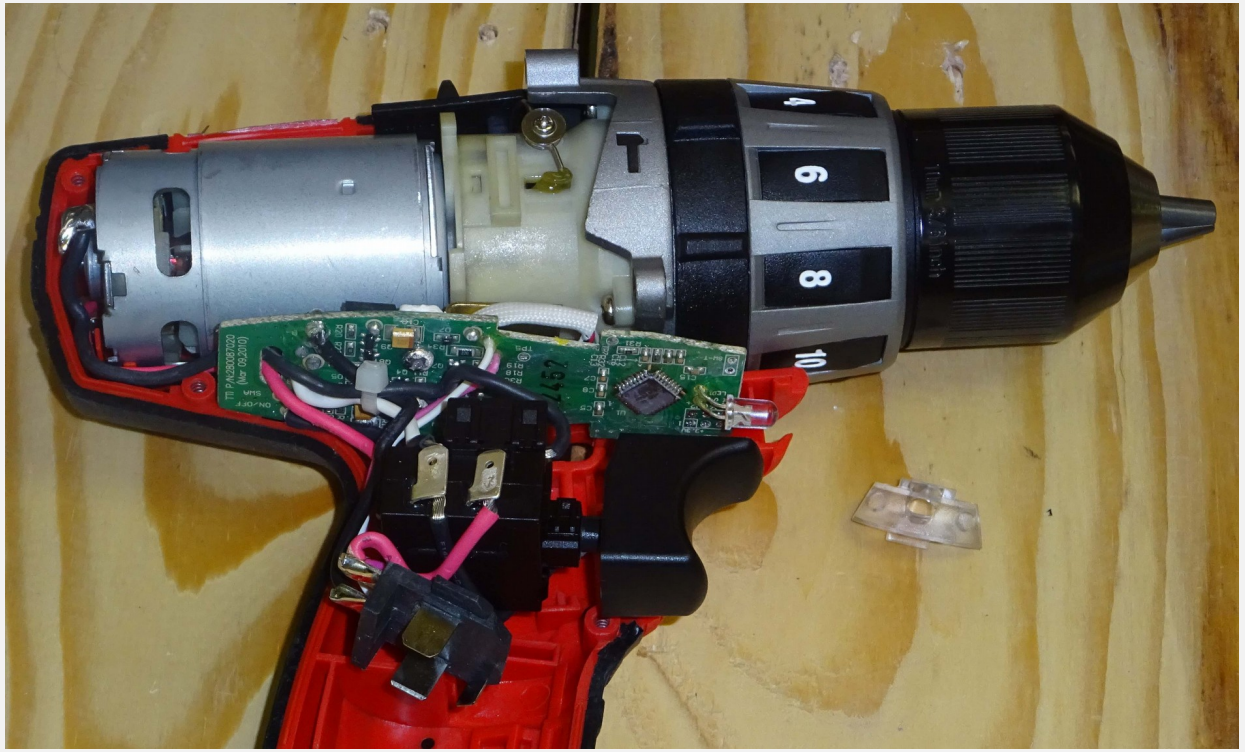
Here is a list of how many clockcycles the z80 instructions take.

Mnemonic	**Clock**	Siz	OP-Code
ADC A,(HL)	7	1	8E
ADC A,(IX+N)	19	3	DD 8E XX
ADC A,(IY+N)	19	3	FD 8E XX
ADC A,r	4	1	88+rb
ADC A,N	7	2	CE XX
ADC HL,BC	15	2	ED 4A
ADC HL,DE	15	2	ED 5A
ADC HL,HL	15	2	ED 6A
ADC HL,SP	15	2	ED 7A
ADD A,(HL)	7	1	86
ADD A,(IX+N)	19	3	DD 86 XX
ADD A,(IY+N)	19	3	FD 86 XX

…

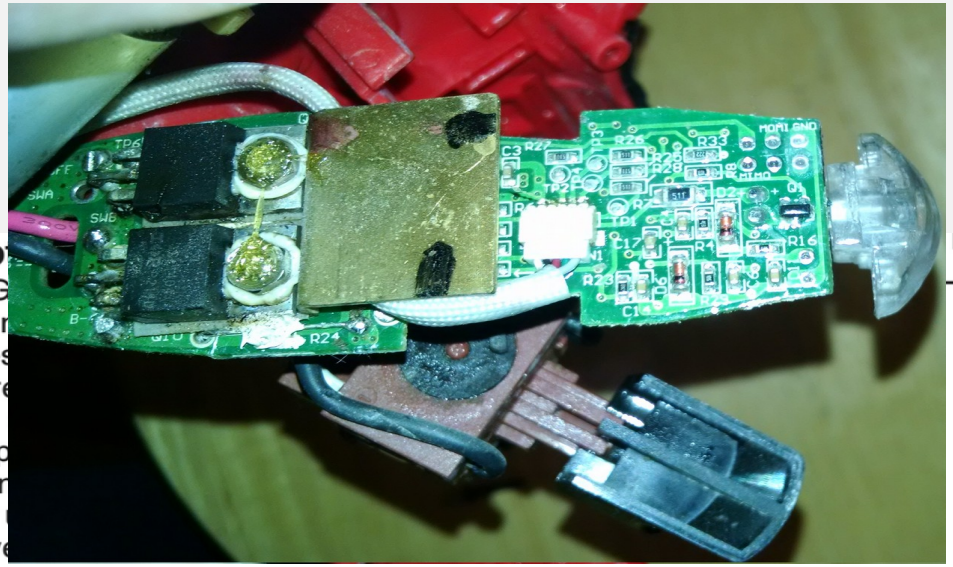
http://www.z80.info/z80time.txt

Drill Anatomy Overview



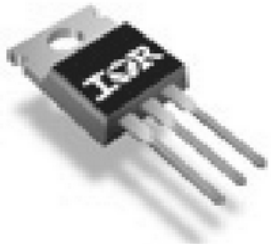
- Milwaukee 2411-20 M12
- 12V Li-Ion 3/8" Cordless Hammer Drill

Mosfets with Heatsink



Descrip
Seventh G
Internatio
techniques
silicon ar
switching
HEXFET p
the desig
device for
automotiv

The TO-220 package is universally preferred for all automotive-commercial-industrial applications at power dissipation levels to approximately 50 watts. The low thermal resistance and low package cost of the TO-220 contribute to its wide acceptance throughout the industry.

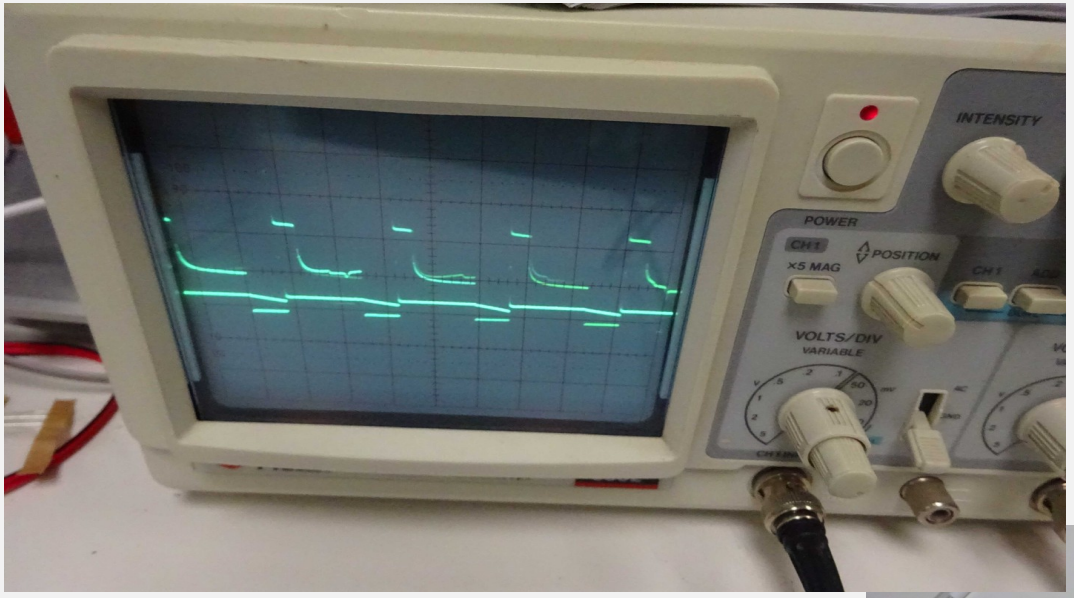


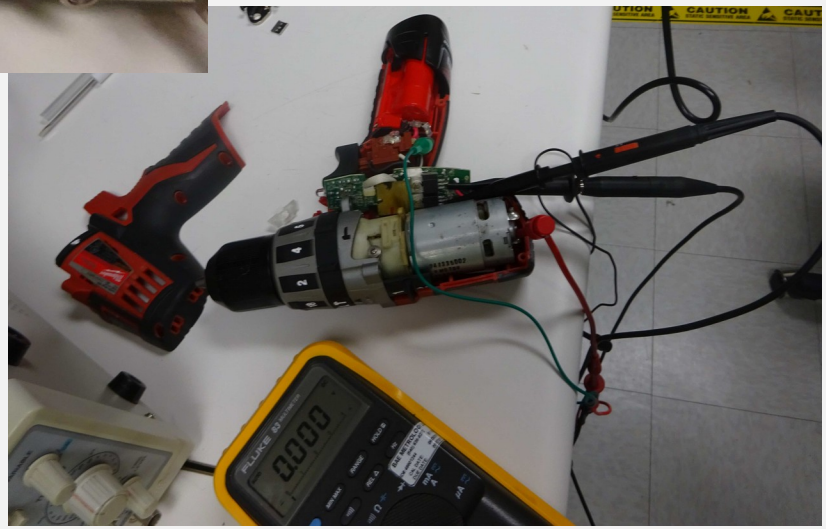
TO-220AB

Absolute Maximum Ratings

	Parameter	Max.	Units
I_D @ T_C = 25°C	Continuous Drain Current, V_{GS} @ 10V	202⑥	A
I_D @ T_C = 100°C	Continuous Drain Current, V_{GS} @ 10V	143⑥	
I_{DM}	Pulsed Drain Current ①	808	
P_D @T_C = 25°C	Power Dissipation	333	W
	Linear Derating Factor	2.2	W/°C

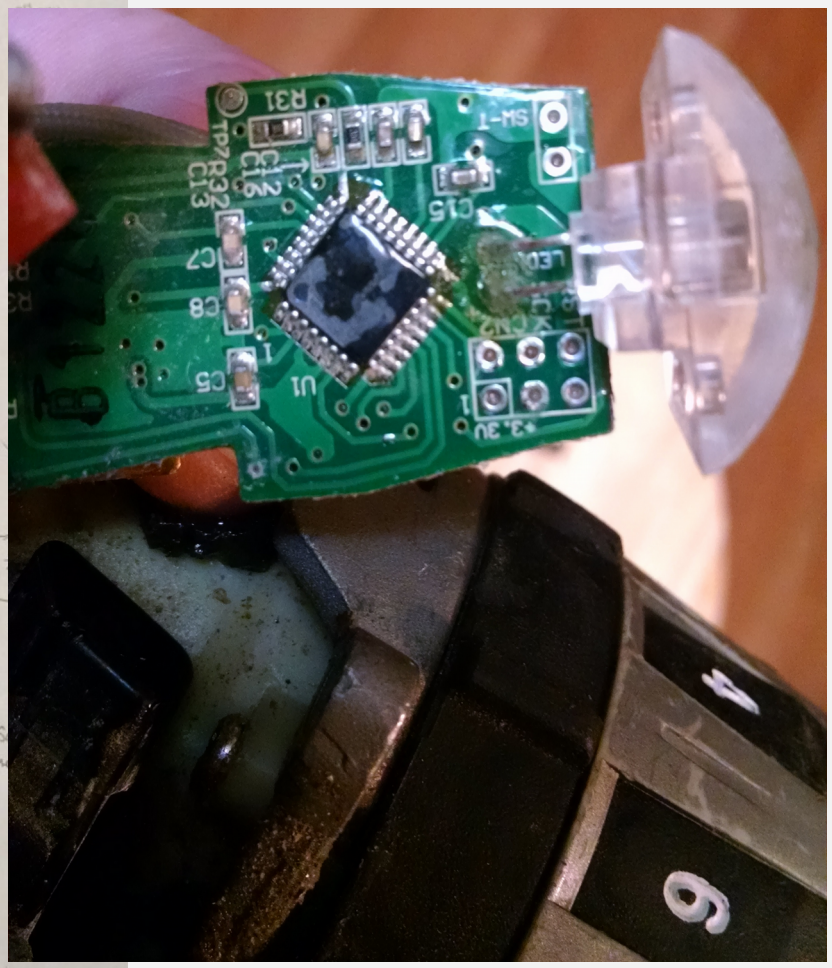
Reverse Engineering Hardware





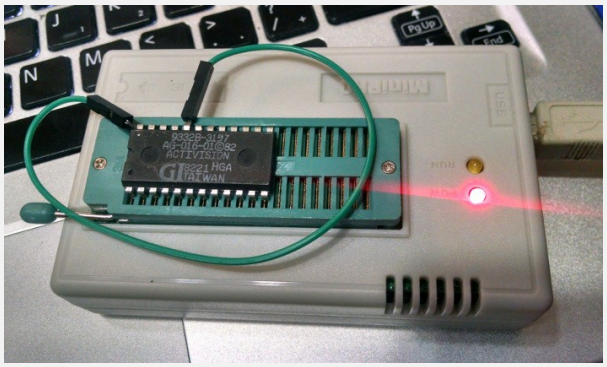
Microcontroller

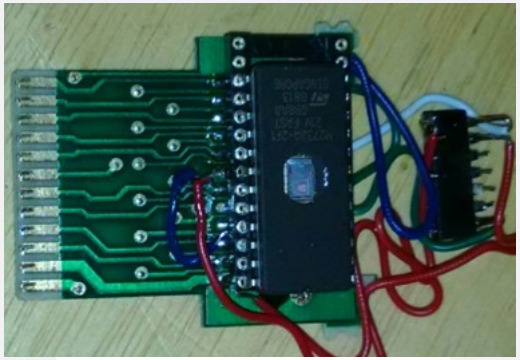
- ATMega88P
- 32 pin
  - Front LED
  - 4 Power LEDs
  - 2 Mosfets
  - Mosfet Temp
  - Battery Temp
  - Battery Voltage
  - Trigger Pot
  - 4 Comm port
  - “enable” pins

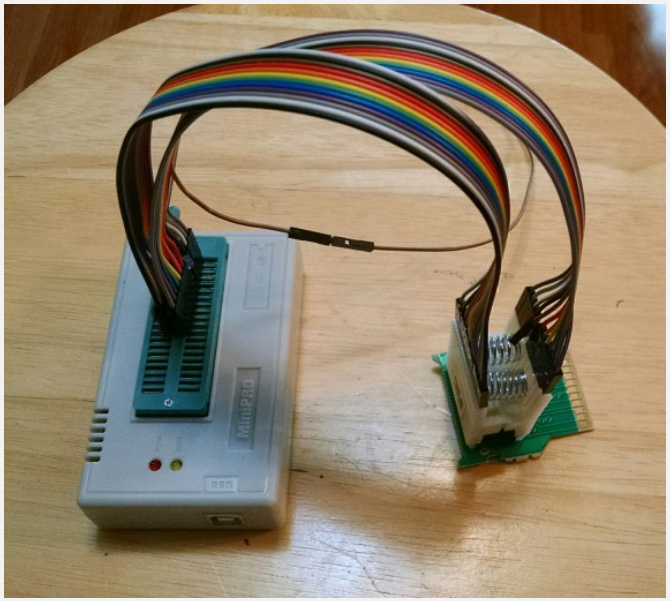


Memory Review

- RAM (rw, volatile)
- Masked ROM
- PROM (otp)
- (uv)-EPROM
- EEPROM
- FLASH



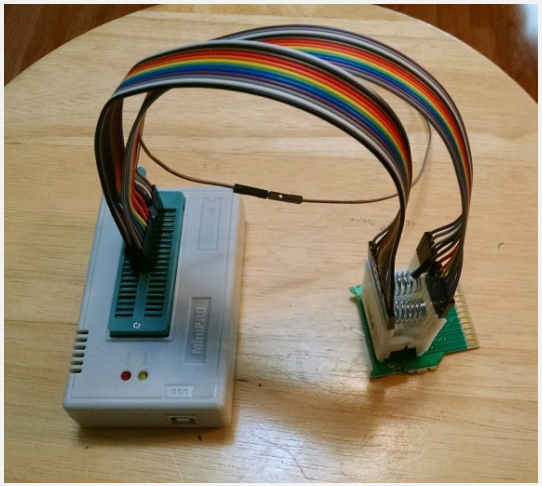




ATMega88P Memory

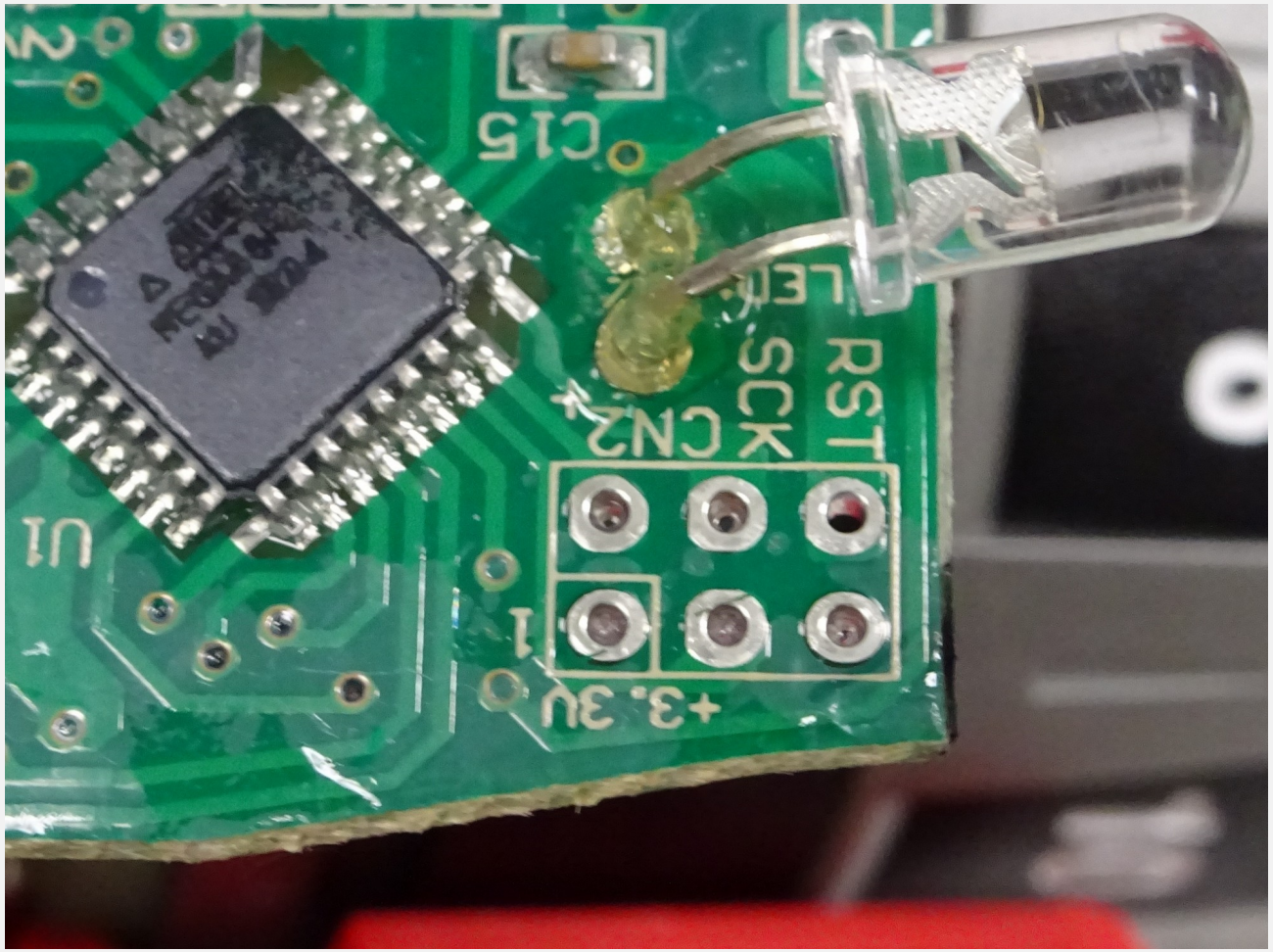
- EEPROM
  - 512 Bytes
- RAM
  - 1024 Bytes
- FLASH
  - 8096 Bytes
- FUSE
  - 2-3 Bytes

All ISP (in system programming capable)

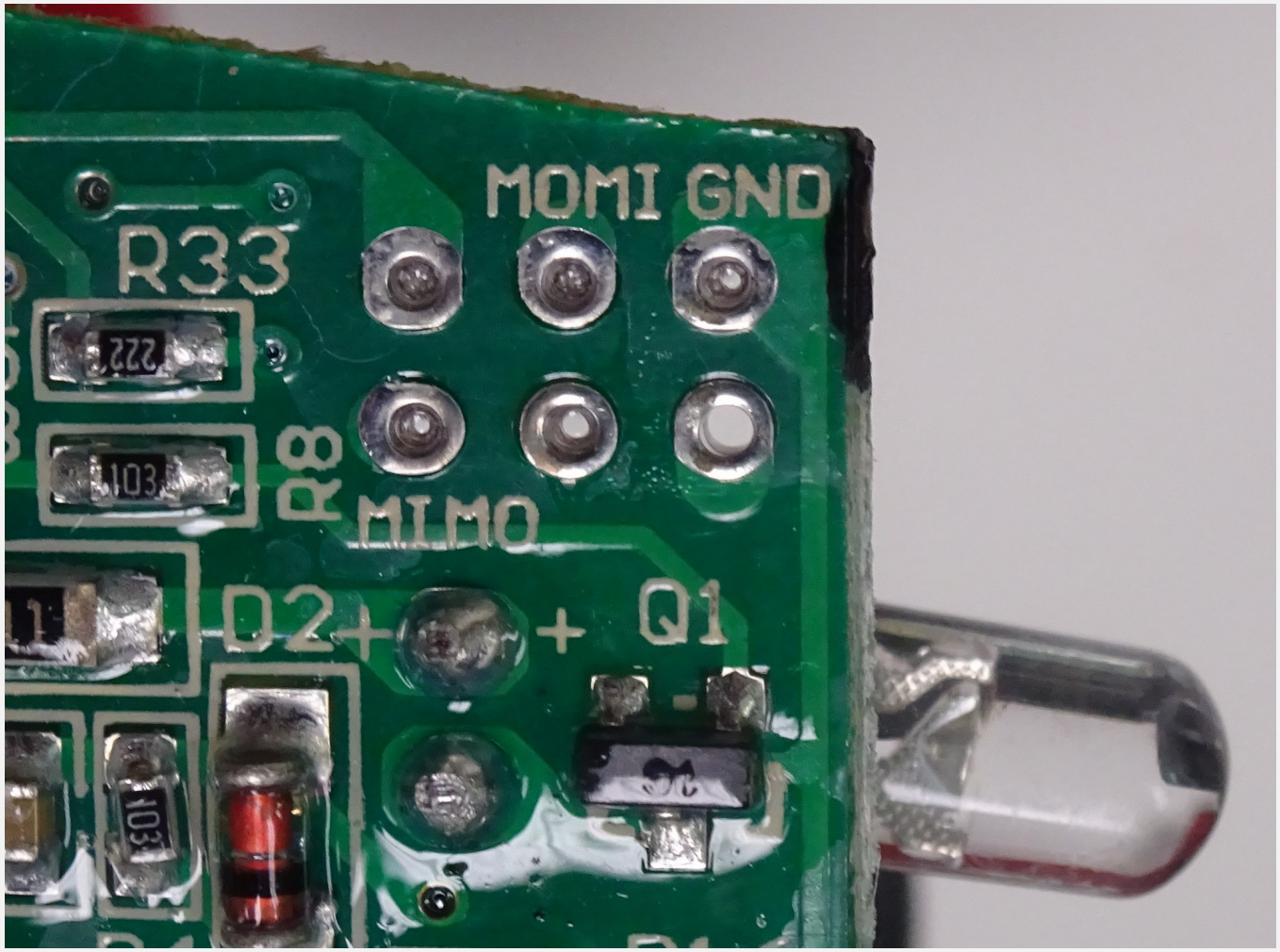


SPI port?

- 3 of 6 pins labeled

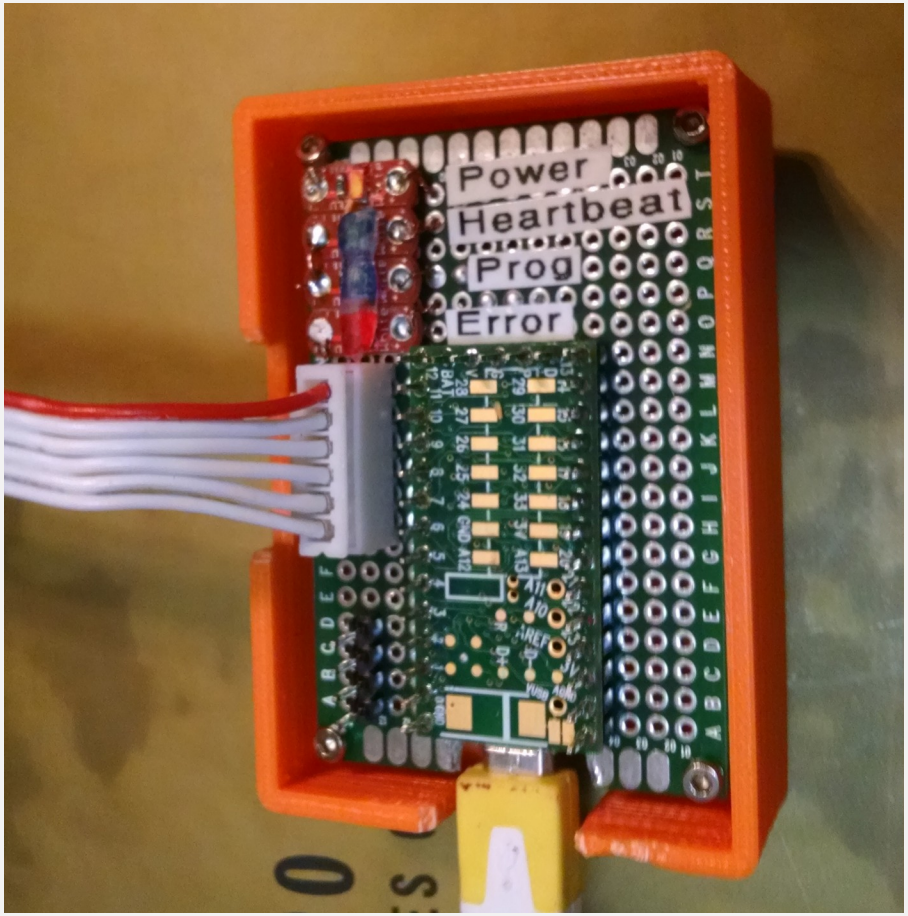


SPI port backside



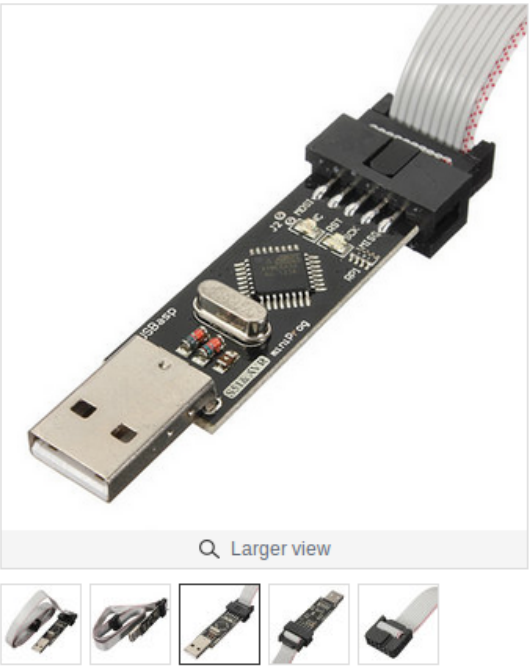
Build Programmer

- Teensy
- avrisp
- 3d printed case
- avrdude



Buy Programmer

Home › Electronics › Arduino SCM & 3D Printer Acc › Programmer & Logic Analyzer



USBASP USBISP 3.3 5V AVR Downloader Programmer With ATMEGA8 ATMEGA128

4.9 (125 Reviews) | Ask a question Product ID: 934425

In stock, usually dispatched in 1 business day

Price: US$ 3.36

Ship From: CN Warehouse

Shipping: **Free shipping** to United States via Standard Shipping
7-20 business days

Quantity: 1 Wholesale Inquiry

Order this & earn 3 Banggood points

Buy it now | Add cart

Add to Wish List (860 Adds)

Supported chip list:

AT89S51, AT89S52, AT89S53, AT89S8252

ATTiny12(L), ATTiny13(V), ATTiny15(L), ATTiny24(V), ATTiny25(V), ATTiny26(L), ATTiny2313(V), ATTiny44(V), ATTiny45(V), ATTiny84(V), ATTiny85(V), AT90S2313(L), AT90S2323(L), AT90S2343(L), AT90S1200(L), AT90S8515(L), AT90S8535(L), ATMEGA48(V), ATMEGA8(L), ATMEGA88(V), ATMEGA8515(L), ATMEGA8535(L), ATMEGA16(L), ATMEGA162(V), ATMEGA163(L), ATMEGA164(V), ATMEGA165(V), ATMEGA168(V), ATMEGA169(V), ATMEGA169P(V), ATMEGA32(L), ATMEGA324(V), ATMEGA325(V), ATMEGA3250(V), ATMEGA329(V), ATMEGA3290(V), ATMEGA64(L), ATMEGA640(V), ATMEGA644(V), ATMEGA645(V), ATMEGA6450(V), ATMEGA649(V) ATMEGA6490(V), ATMEGA128(L), ATMEGA1280(V), ATMEGA1281(V), ATMEGA2560(V), ATMEGA2561(V), AT90CAN32, AT90CAN64, AT90CAN128, AT90PWM2(B),

“Disassembly” Code

- avr-objdump
- reAVR
- AtmelStudio

```
        out   p22,r17       ; EEPROM address High
        out   p21,r16       ; EEPROM address Low
        out   p20,r18       ; EEPROM Data register
        sbi   p1F,b2        ; EEPROM Master Write Enable

        sbi   p1F,b1        ; EEPROM Write
        sei
        ret

L0255:
        sbi   PORTB,b2   ; Trigger Pot "enable"
        sbi   PORTD,b1   ; Battery thermistor enable
         rcall      L0191
         rcall      L025D
L0259:
        ldi   r16,k02
        sts   D006F,r16
        ret
```

Live Demo

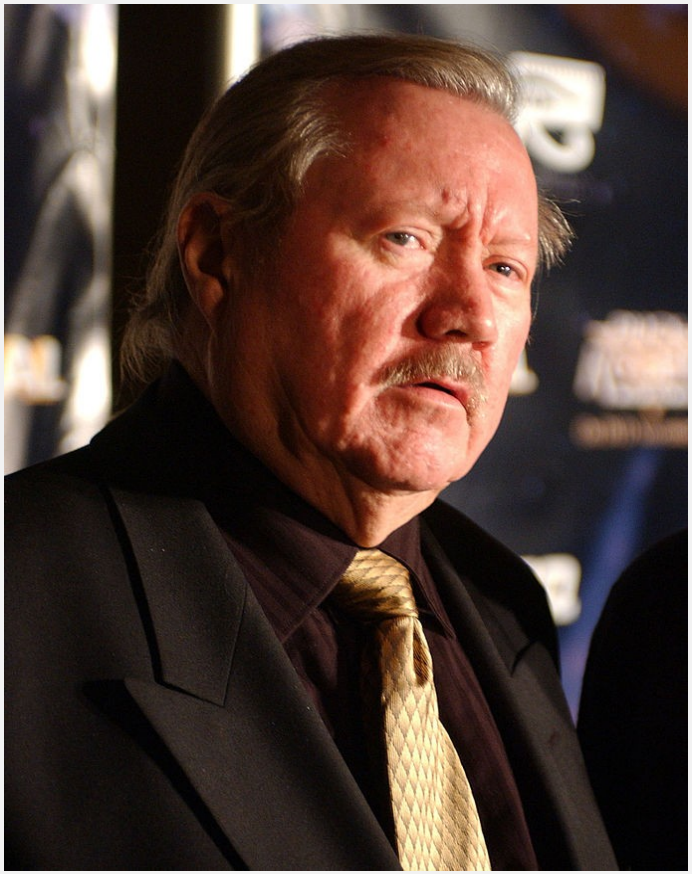
- Moved SPI port outside for easy demo access
- Pull firmware & verify hash
- Push Malware
- Verify hash

What is this?

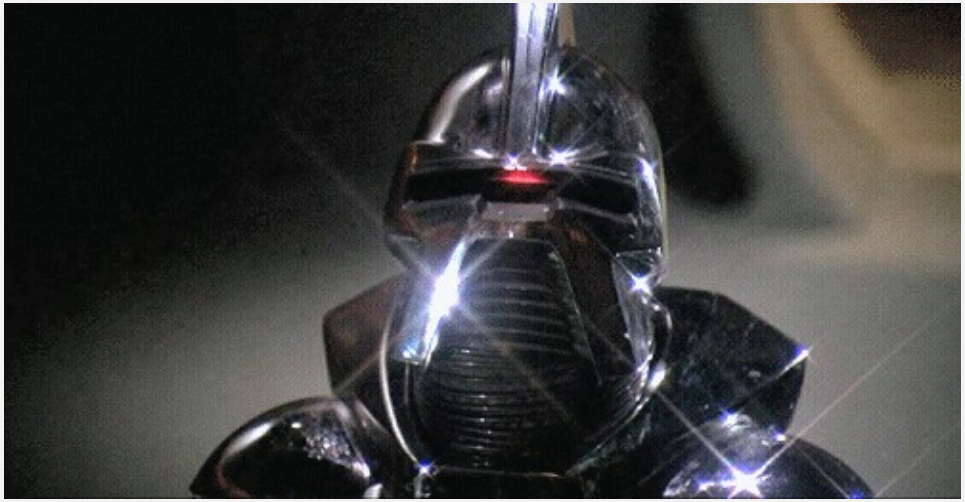
Larson Scanner

Glen Larson - Producer and writer, he created:

- Buck Rogers in the 25th Century
- Quincy, M.E.
- B. J. and the Bear
- The Fall Guy
- Magnum P.I.
- Knight Rider
- Battlestar Galactica

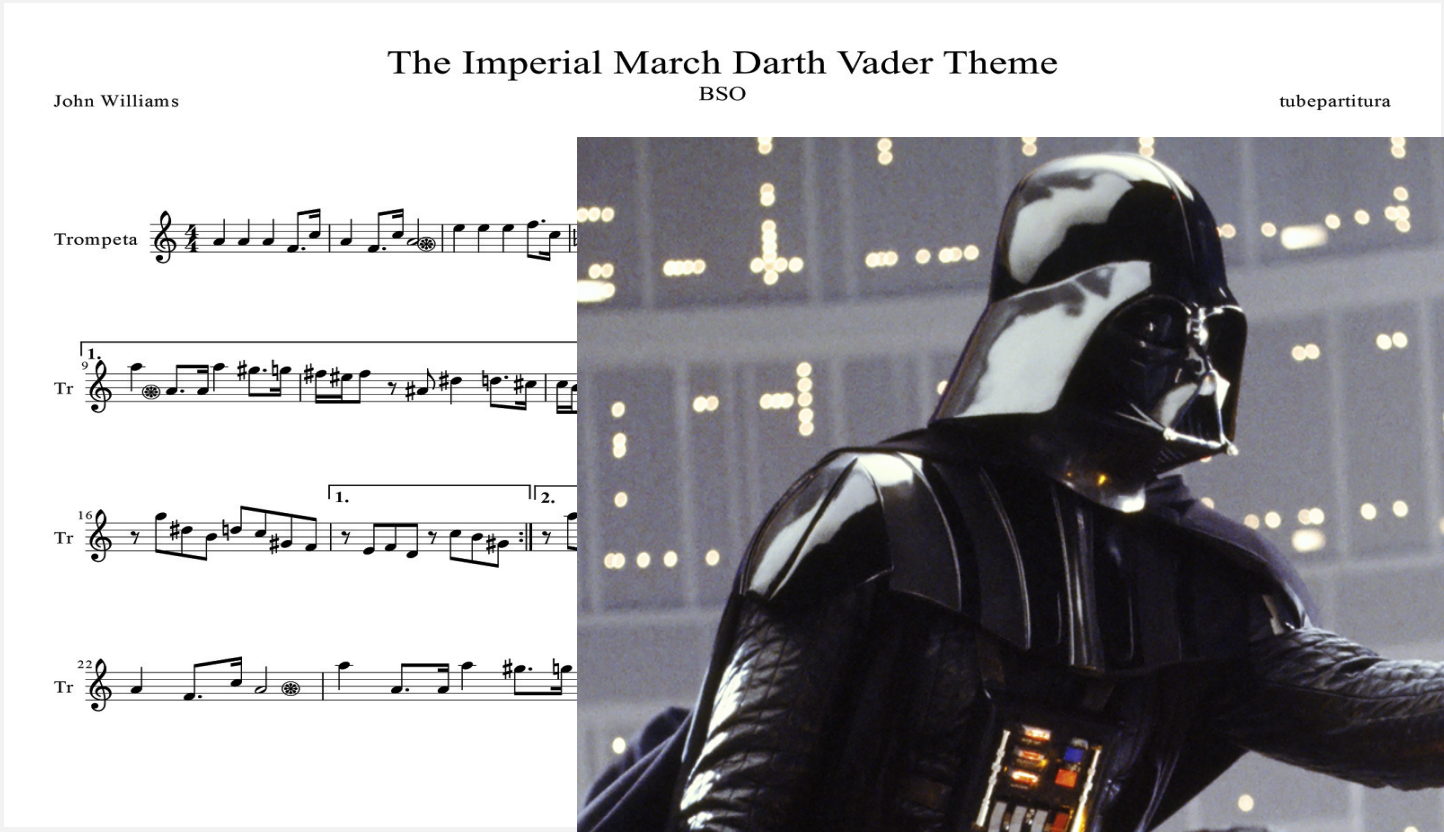


A.I.



!

Name that tune



Impractical attack ?

- Air Gap – no attack path
- No financial consequences
- No effect on other systems
- Example of firmware in unexpected places

Supply Chain

- Interdiction

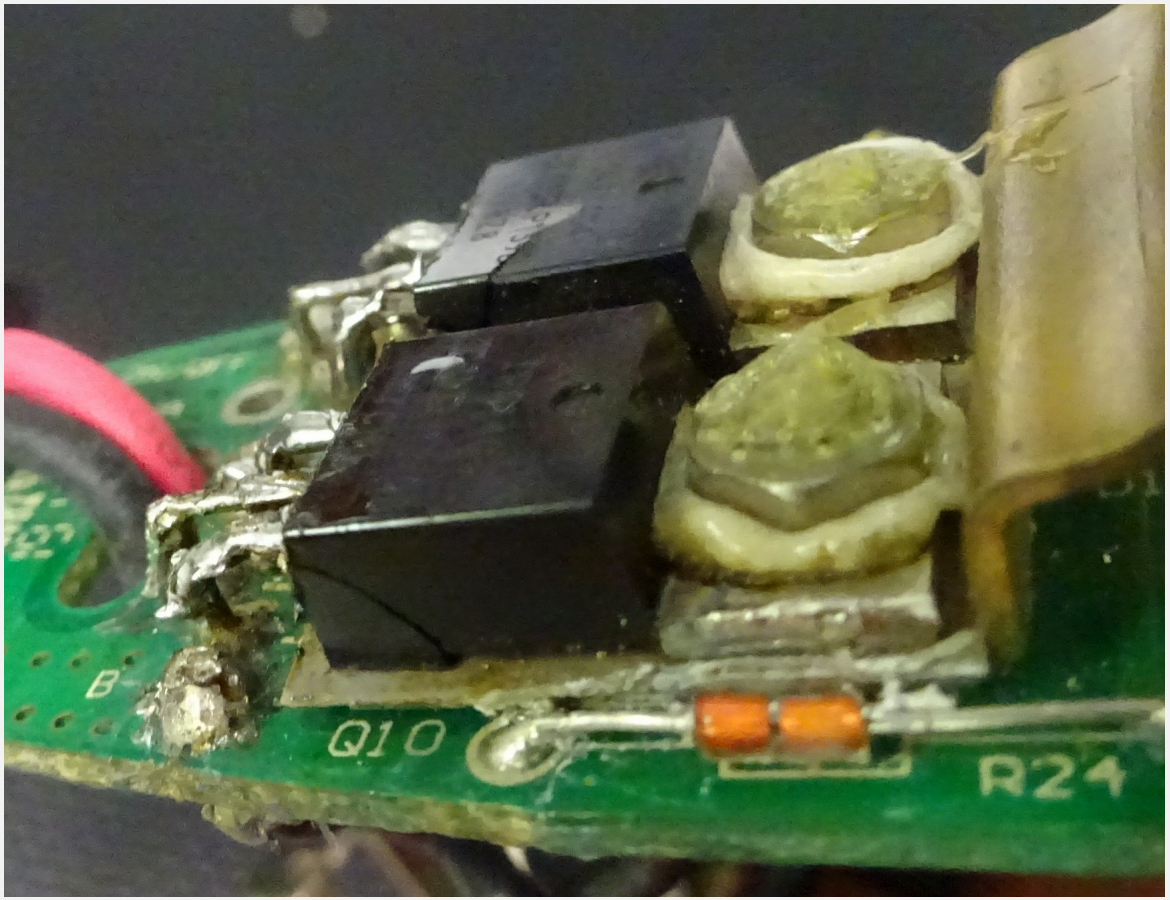
  “Professionally made in China by Milwaukee Electric Tool, PRC”

- Physical access attacks
- Air gapped

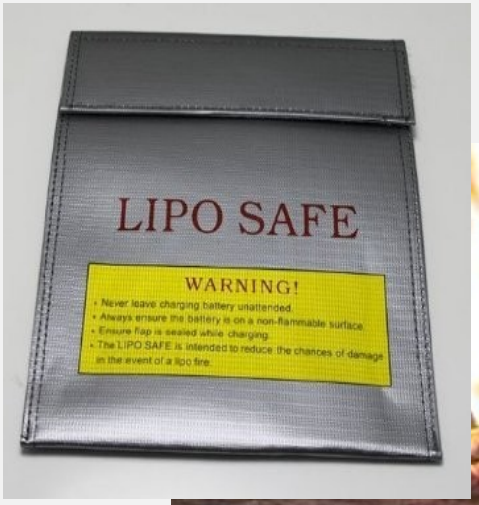
MOSFET Magic Smoke

MOSFET Specs

- 202 Amps continuous
- 808 Amps pulsed
- Un-software-modified e-bay purchase



Thermal Protection Override

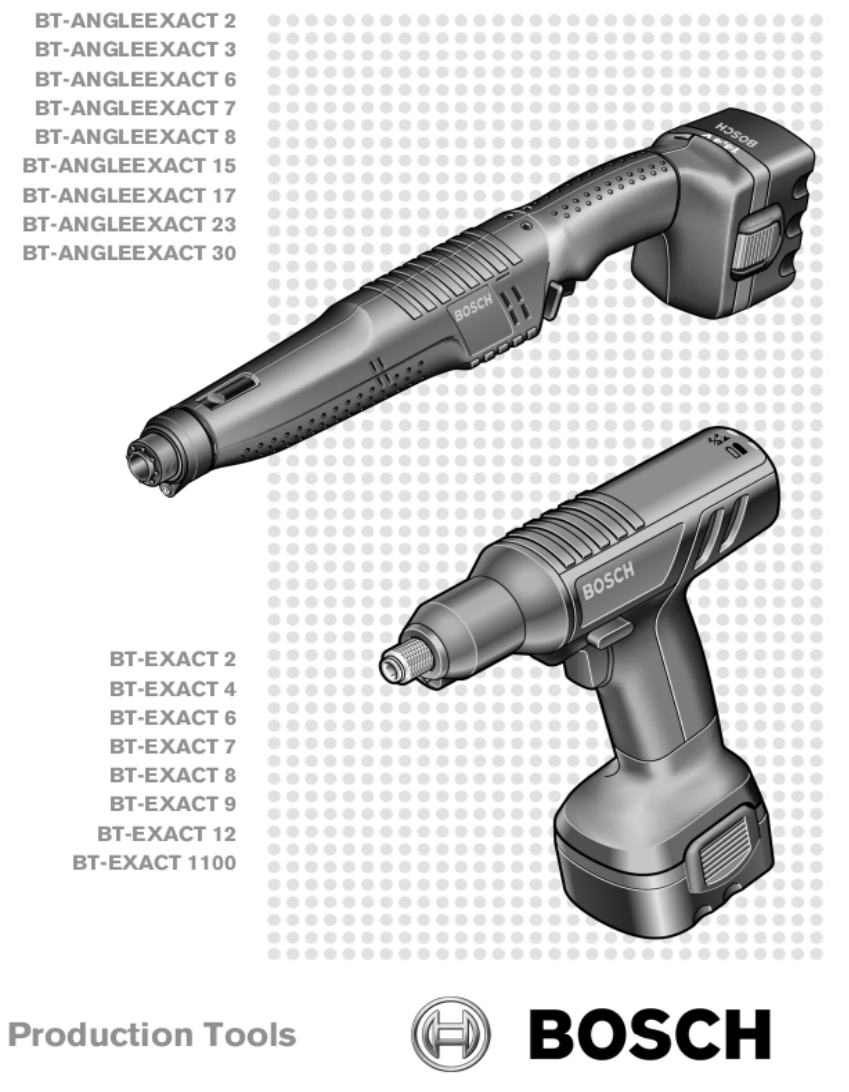


FoxGuard Solutions®

Impractical attack ?

- Air Gap – no attack path
- No financial consequences
- No effect on other systems
- Example of firmware in unexpected places

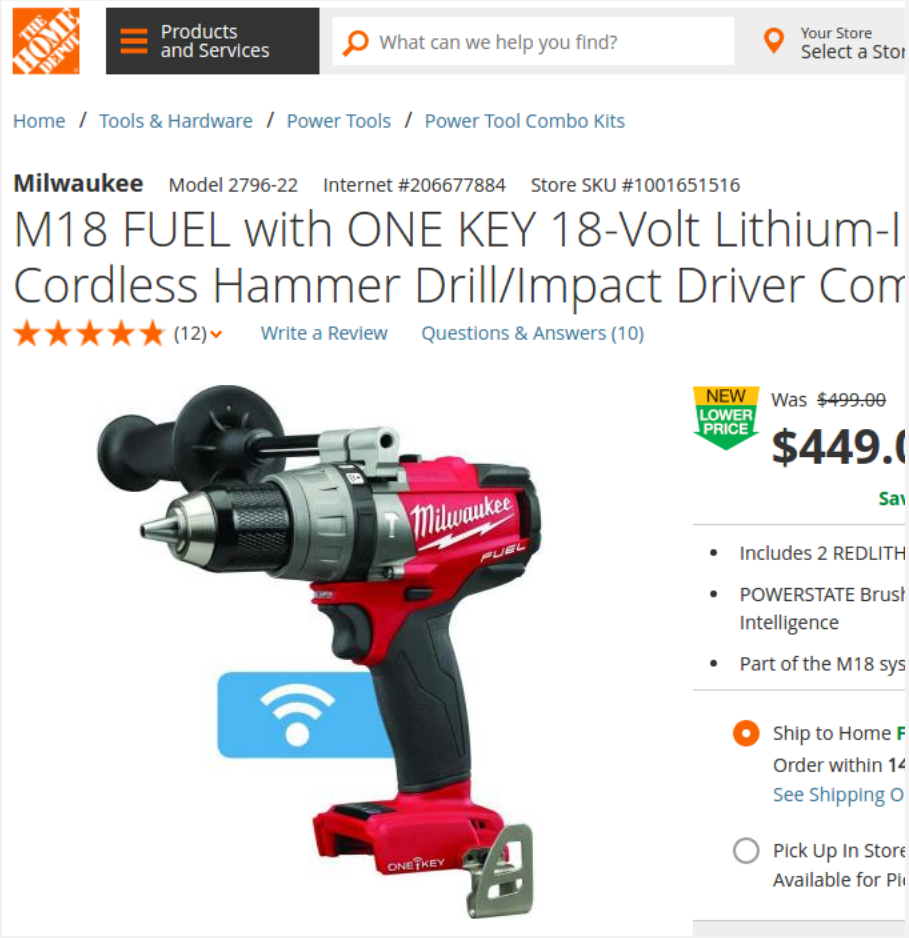
Airgap ?

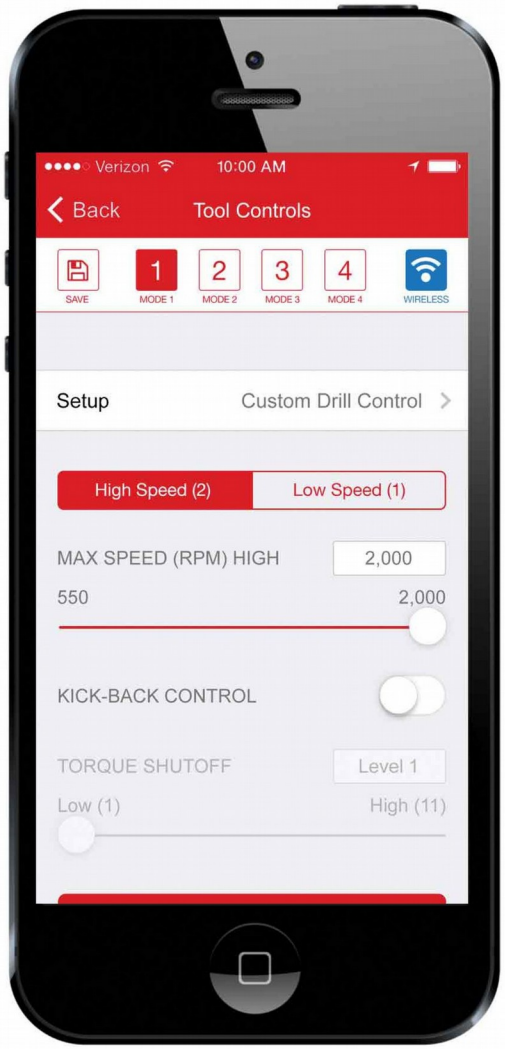


"Without access point EXAConnecT, screwdrivers of the series BT-EXACT and BT-ANGLEEXACT cannot be put into operation: ***The screwdrivers are locked when they are delivered and can be unlocked only by access point EXAConnecT. "***

"The Bluetooth EXACT Cordless Screwdriving system thinks for itself. The BT-EXACT tool takes its commands from the EXAConnecT controller, which stores the work in progress in real time. ***The system can talk to and take commands from external devices like a PLC... "***

Milwaukee One Key

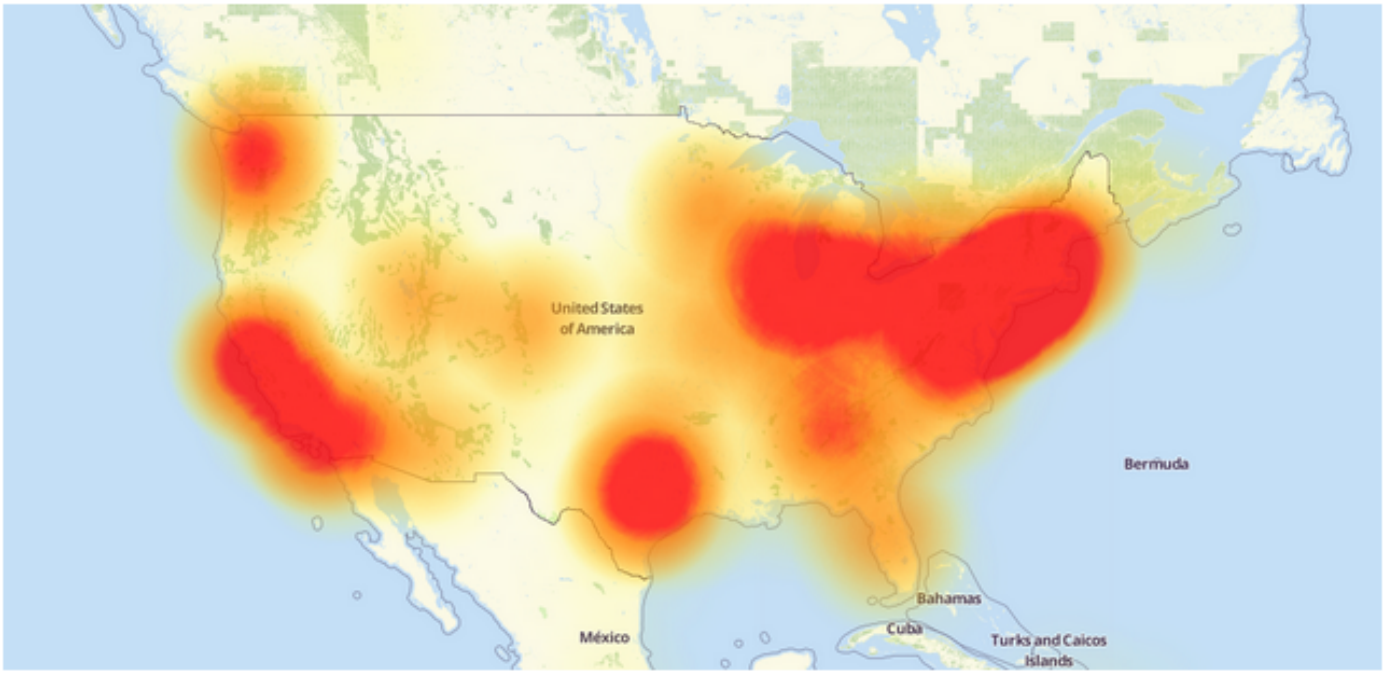
- 



FOXGUARD SOLUTIONS®

Blame the Internet of Things for today's web blackout

Flashpoint says hacked cameras and routers enabled a Mirai botnet to take out major websites on Friday.



Level3

Impractical attack ?

- Air Gap – no attack path
- No financial consequences
- No effect on other systems
- **Example of firmware in unexpected places**

Software vs. Firmware

- Firmware – noun -Permanent software programmed into a read-only memory
- Firmware is software
- It's not magic
- It's most often modifiable

By Christiaan Colen

- “Firmware” deserves all the security protections we provide for “software”
- Monta's Rule of thumb - If it “plugs in” or “has batteries” it's running firmware (and is programmable)
- Never say “Firmware” again

Tool Analysis

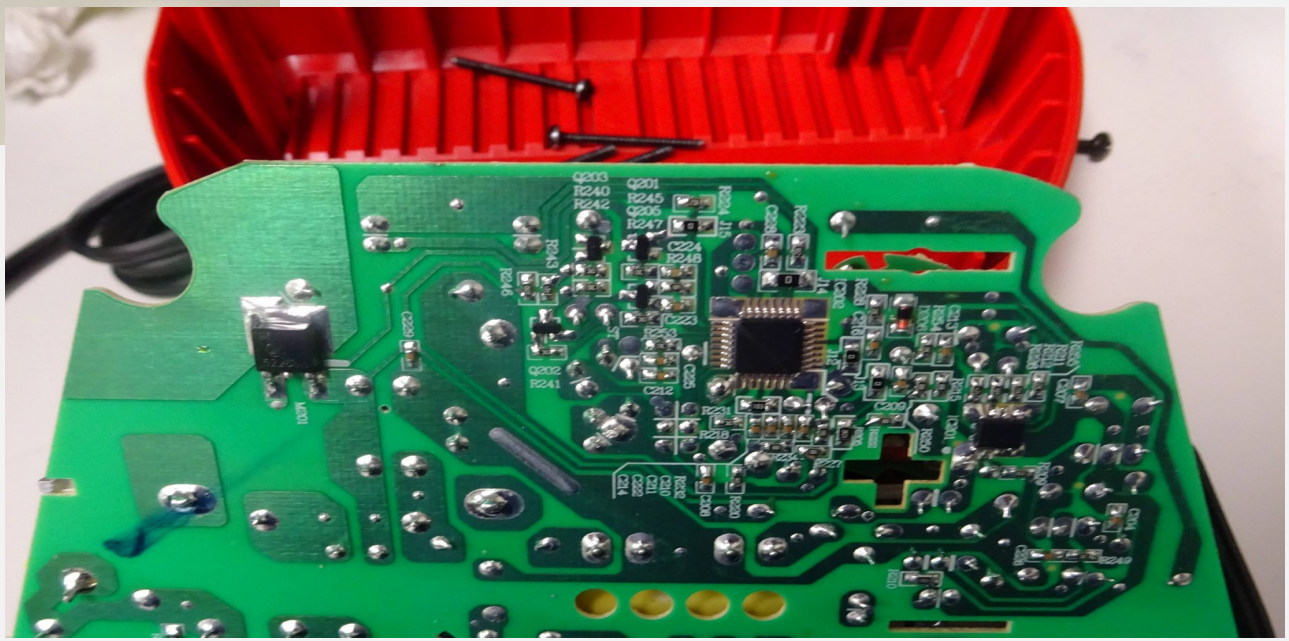
- Heatsinks
- Thermal sensors
- Conformal coating
- Not making firmware “write only” is a plus

- Publish hash for firmware
- Programming header makes it easier for me to verify the firmware on your device

Existing tools and strategies to mitigate these threats

Charger

- There is more firmware out there that you realize



FoxGuard Solutions®

FoxGuard Solutions

QUESTIONS?

Monta Elkins melkins@FoxguardSolutions.com