Hardware Hacking

ب854.75 جنيه

Yusuf Hegazy
@hegzploit
https://hegz.io/hw.pdf

$ whoami

- ECE Graduate
- Low Level Hacker
- CTFs w/ 0xL4ugh https://discord.gg/JyCGhgDnCq
- Currently doing HW Stuff

Who is this for?

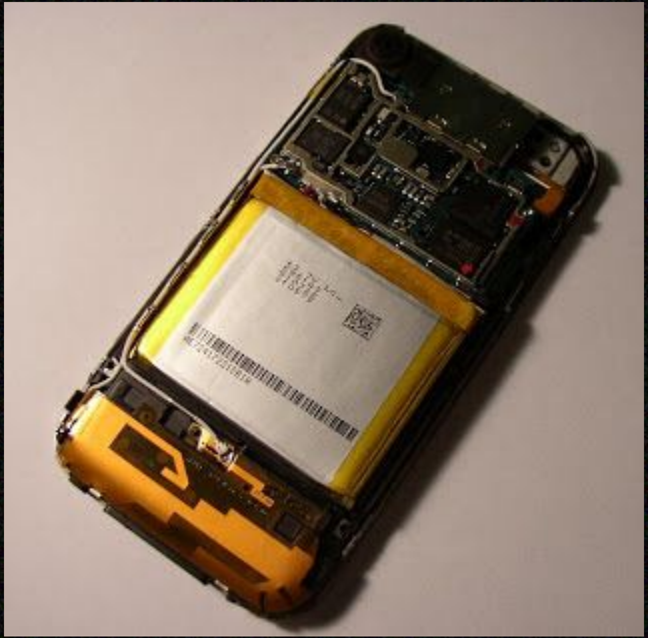
- No knowledge of hardware-related topics
- Knows basic hardware concepts but nothing about hardware hacking
- Has some knowledge of hardware hacking and is interested in learning more

Case Study: World’s First Unlocked iPhone (2007)

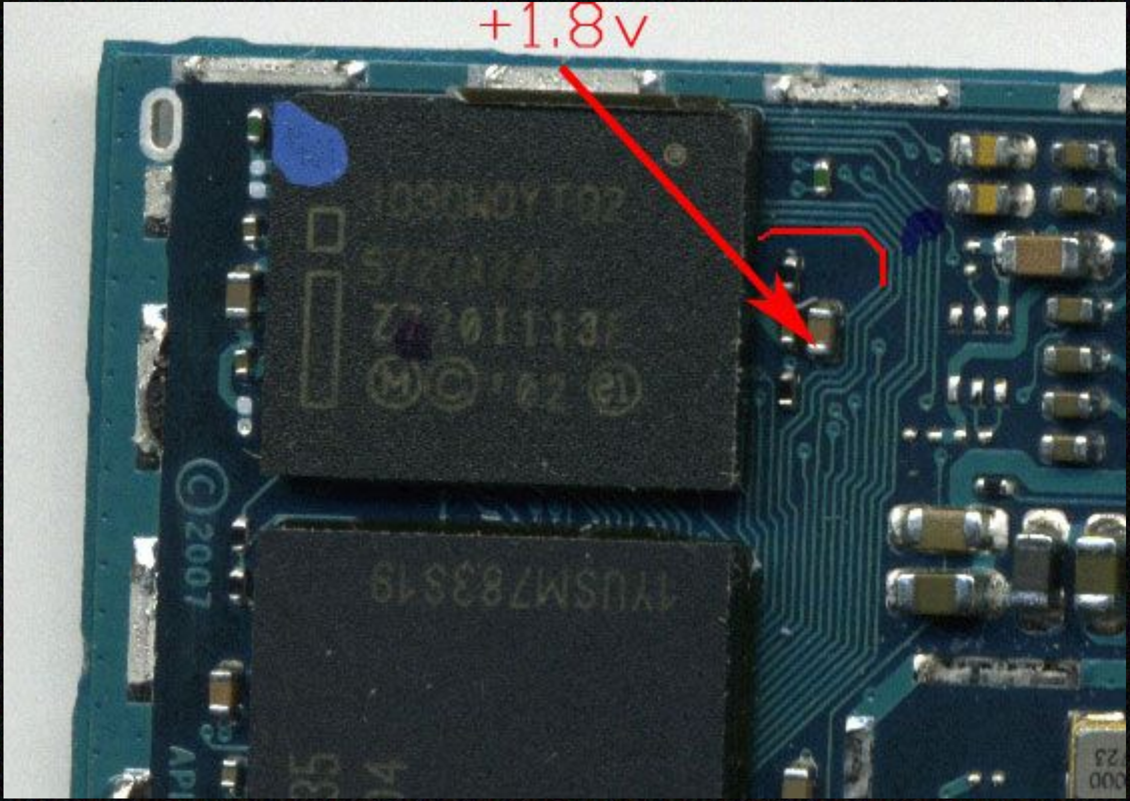
https://web.archive.org/web/20180707204147im_/http://3.bp.blogspot.com/_NJ4JFBfr1tY/Rs3ATDhDtyI/AAAAAAAAALI/BTZgOOSRN0Q/s320/finished.JPG

Step 1

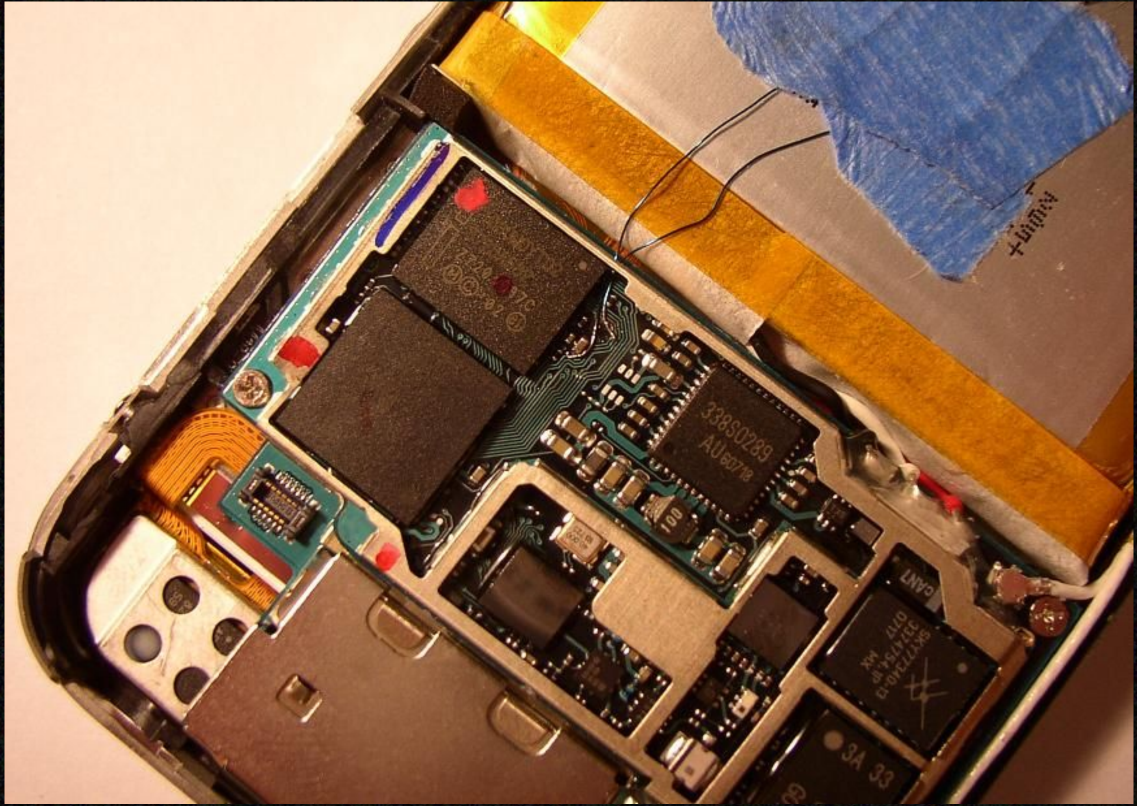
Step 2



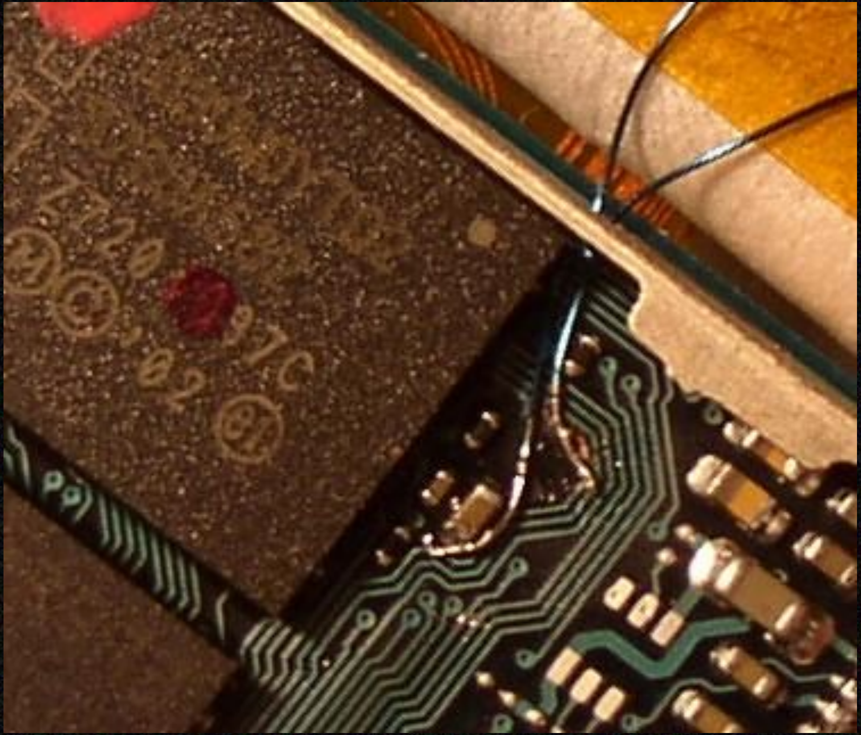
Step 3

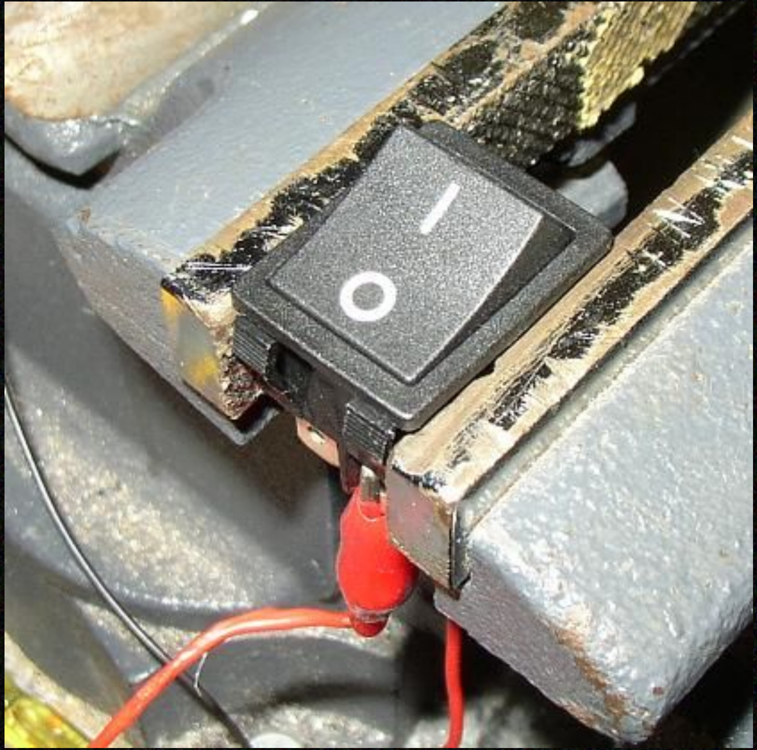


Step 3



Step 3





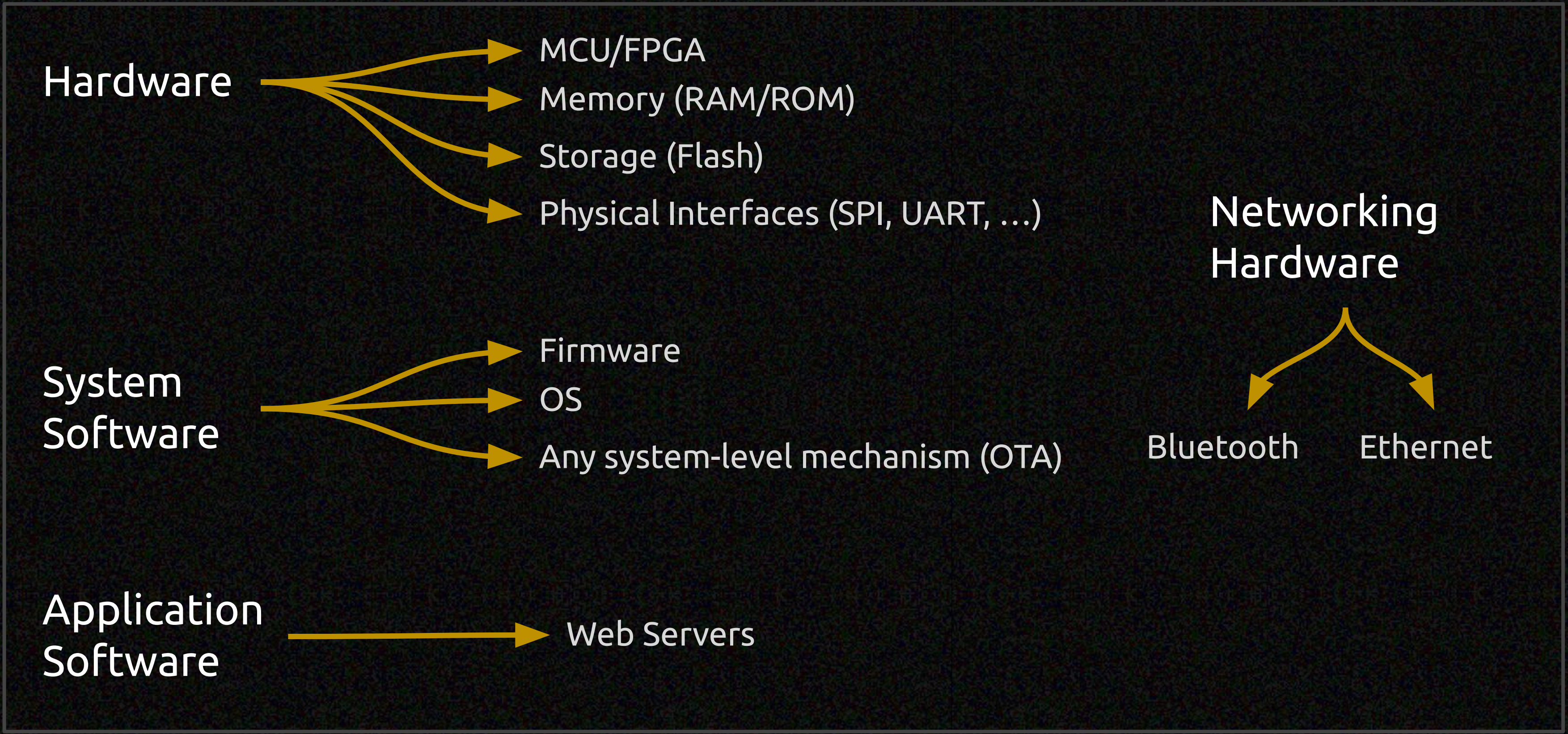
Step 4,5,6,7,8,9,10

1. Dump firmware → `nor.bin`
2. Erase the baseband firmware
3. Patch `nor.bin`
4. Reflash the patched firmware along with the file `testcode.bb`
5. Now using the hardware switch, we can run arbitrary code on the baseband `testcode.bb`
6. Run `AT+CLCK="PN",0,"00000000"` to unlock!

Skills Involved

- Electronics
  - Circuits
  - Digital Logic
- Embedded Systems
  - Navigating Datasheets
  - Writing/Reading Embedded Code
  - Communication Protocols (SPI, UART, I2C, JTAG, etc…)
- Lab Skills
  - Soldering/Desoldering
  - Reverse Engineering PCBs

Device Properties



Hardware

- MCU/FPGA
- Memory (RAM/ROM)
- Storage (Flash)
- Physical Interfaces (SPI, UART, …)

System Software

- Firmware
- OS
- Any system-level mechanism (OTA)

Application Software

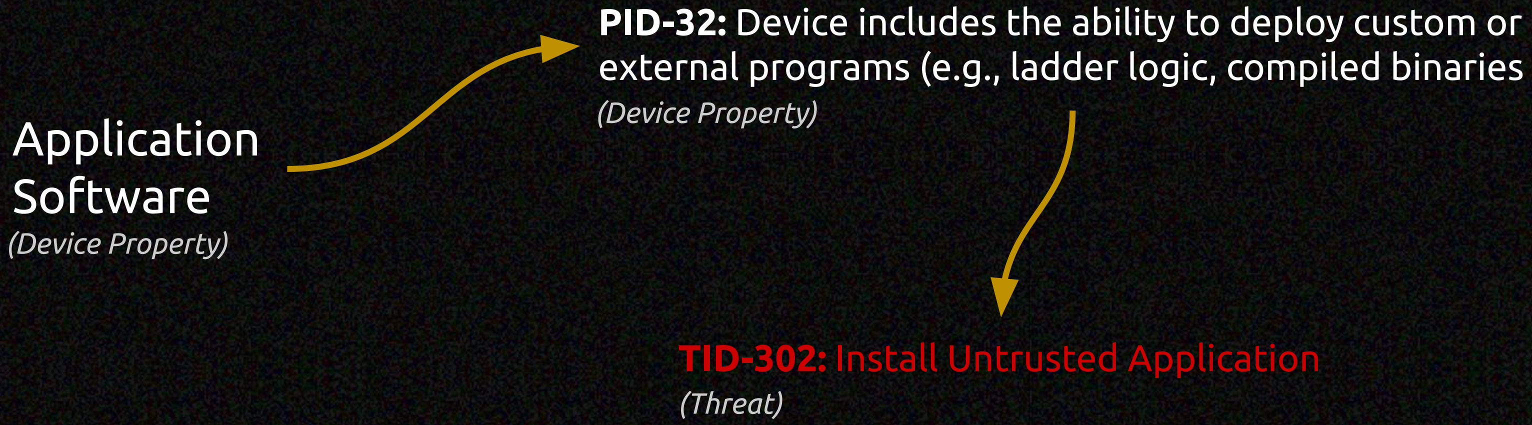
- Web Servers

Networking Hardware

- Bluetooth
- Ethernet

https://emb3d.mitre.org/assets/EMB3D_Paper_09-23-24.pdf

Threat Mapping



Application Software

(Device Property)

PID-32: Device includes the ability to deploy custom or external programs (e.g., ladder logic, compiled binaries

(Device Property)

TID-302: Install Untrusted Application

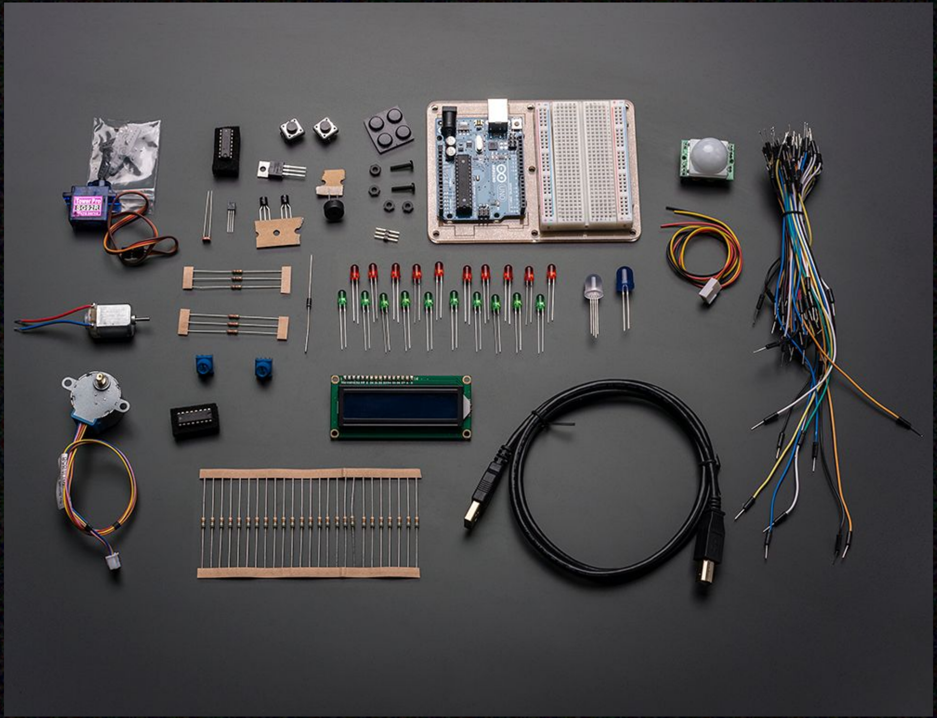
(Threat)

🔗 Properties Mapper | MITRE EMB3D™

Starting your journey in hardware hacking

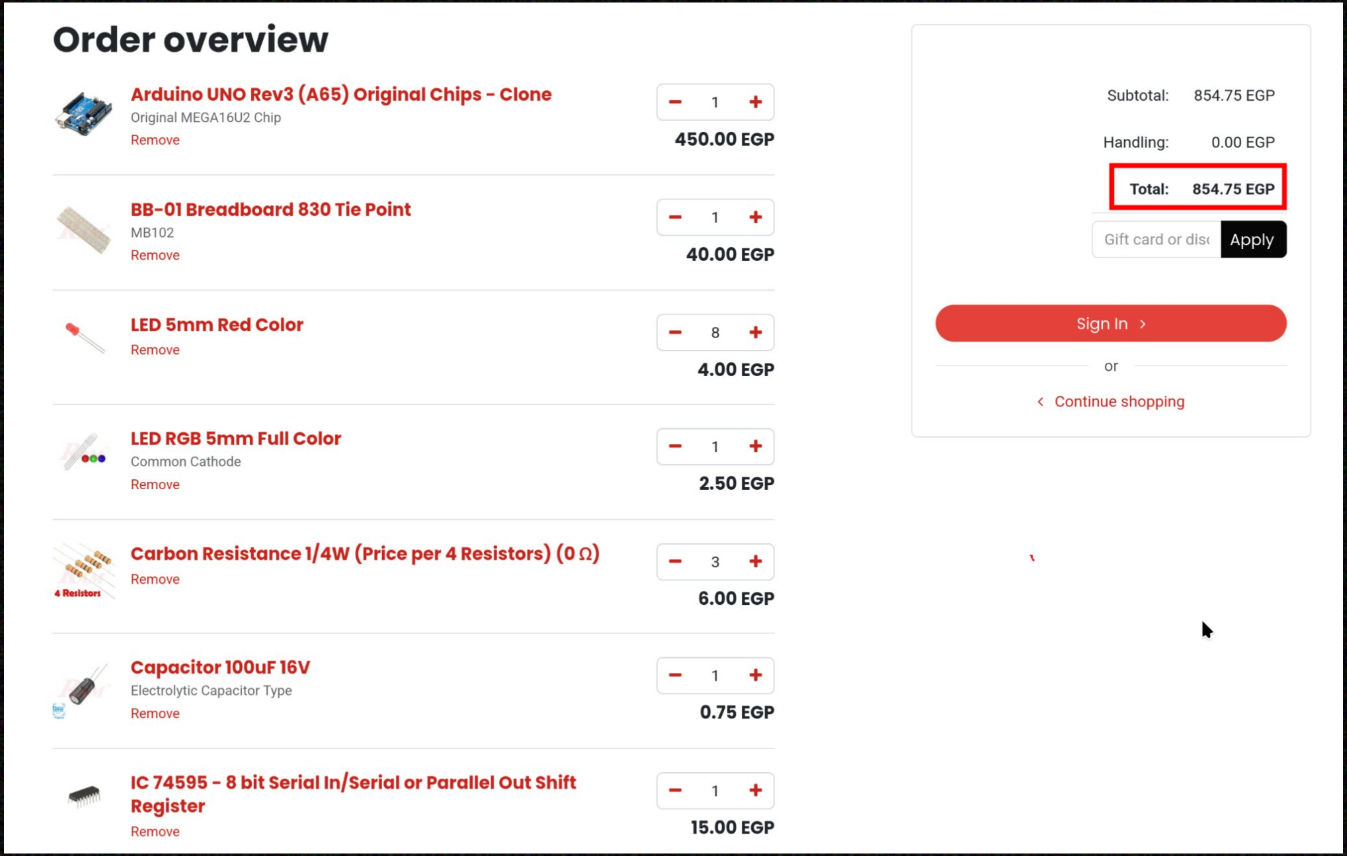
Required Parts:

- Arduino
- Breadboard
- Jumper wires
- LEDs
- Resistors
- Motors
- ICs
- Buttons



https://learn.adafruit.com/groups/learn-arduino

Cost

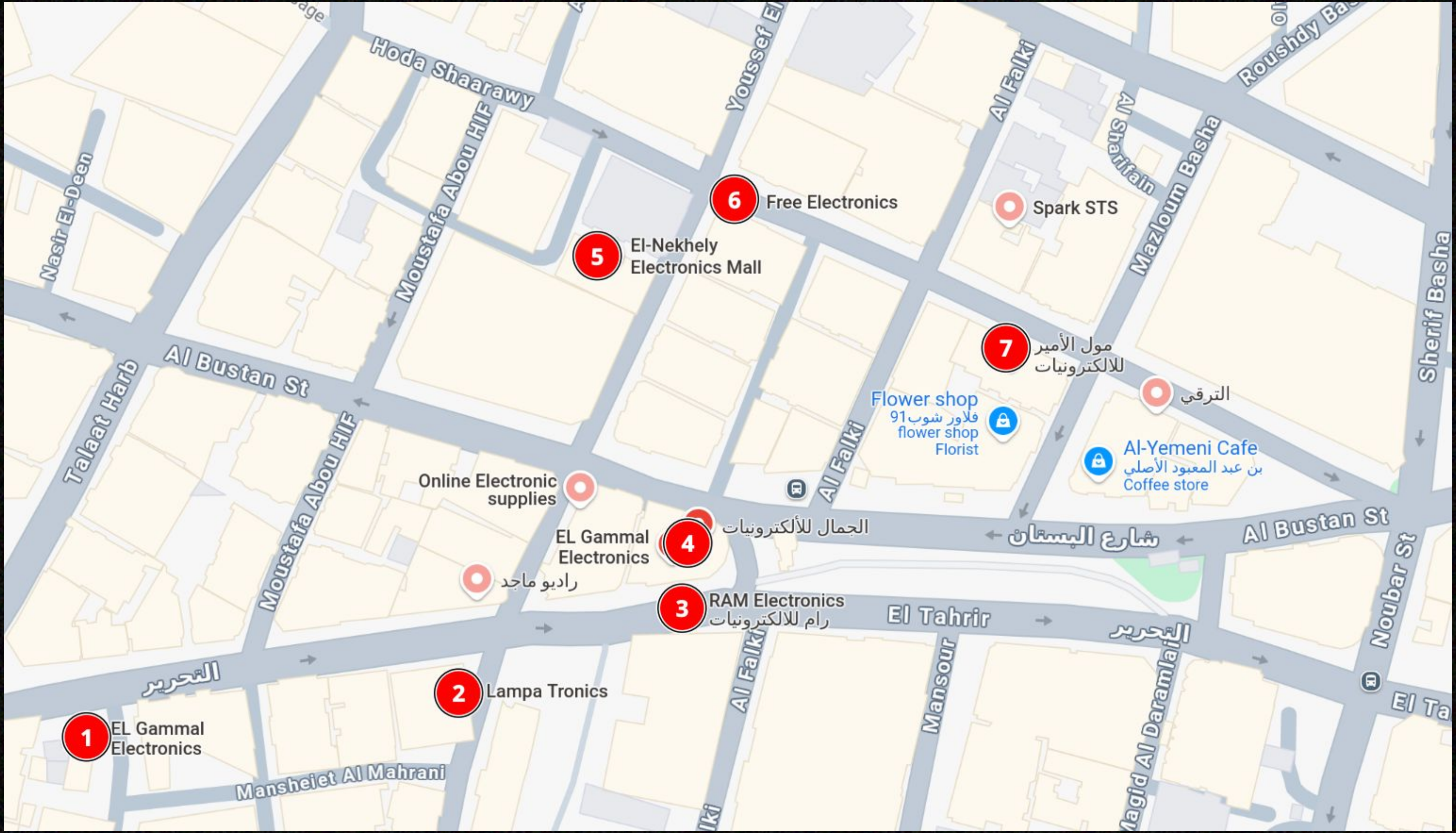


Order overview

Arduino UNO Rev3 (A65) Original Chips - Clone Original MEGA16U2 Chip Remove	− 1 +	**450.00 EGP**
BB-01 Breadboard 830 Tie Point MB102 Remove	− 1 +	**40.00 EGP**
LED 5mm Red Color Remove	− 8 +	**4.00 EGP**
LED RGB 5mm Full Color Common Cathode Remove	− 1 +	**2.50 EGP**
Carbon Resistance 1/4W (Price per 4 Resistors) (0 Ω) Remove	− 3 +	**6.00 EGP**
Capacitor 100uF 16V Electrolytic Capacitor Type Remove	− 1 +	**0.75 EGP**
IC 74595 - 8 bit Serial In/Serial or Parallel Out Shift Register Remove	− 1 +	**15.00 EGP**

Subtotal:	854.75 EGP
Handling:	0.00 EGP
Total:	**854.75 EGP**

Where to get البضاعة?



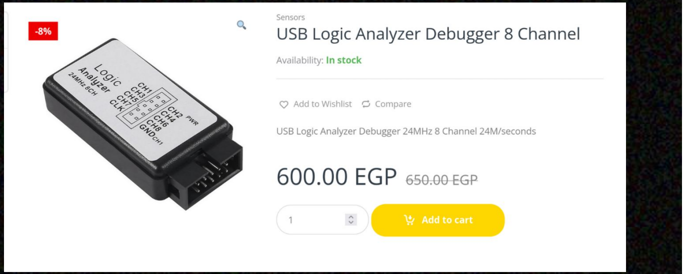
Online Simulators

- https://wokwi.com/
- https://www.falstad.com/circuit/circuitjs.html

Next Steps: Hacking Your First Device

Steps:

1. Pick target
2. Buy more بضاعة
   a. Cheap Logic Analyzer
   b. Multimeter
   c. SPI Programmer
   d. UART Interface (USB-TTL)
   e. Soldering Iron
   f. MCU (RPI, Arduino, ESP32, …)
3. Recon
4. Dump Firmware
5. Analysis/Reverse Engineering



Sensors

USB Logic Analyzer Debugger 8 Channel

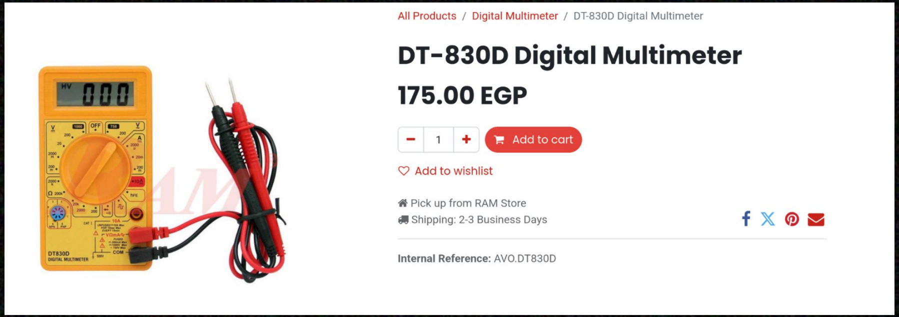
Availability: In stock

Add to Wishlist Compare

USB Logic Analyzer Debugger 24MHz 8 Channel 24M/seconds

600.00 EGP ~~650.00 EGP~~

1 Add to cart



All Products / Digital Multimeter / DT-830D Digital Multimeter

DT-830D Digital Multimeter

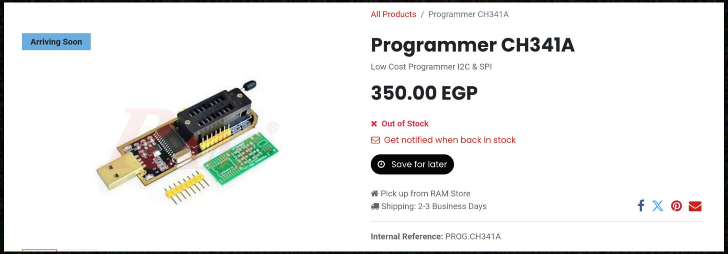
175.00 EGP

− 1 + Add to cart

Add to wishlist

Pick up from RAM Store
Shipping: 2-3 Business Days

Internal Reference: AVO.DT830D



All Products / Programmer CH341A

Programmer CH341A

Low Cost Programmer I2C & SPI

350.00 EGP

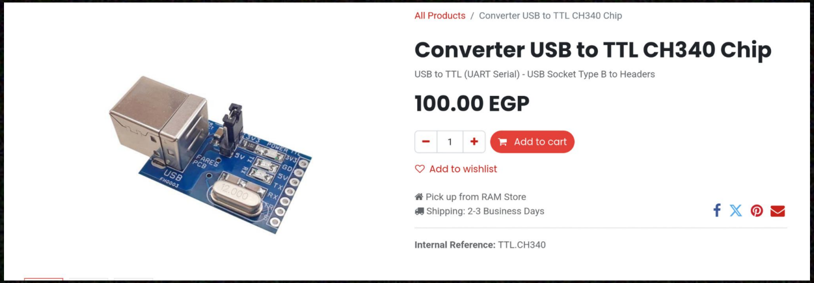
✕ Out of Stock

Get notified when back in stock

Save for later

Pick up from RAM Store
Shipping: 2-3 Business Days

Internal Reference: PROG.CH341A



All Products / Converter USB to TTL CH340 Chip

Converter USB to TTL CH340 Chip

USB to TTL (UART Serial) - USB Socket Type B to Headers

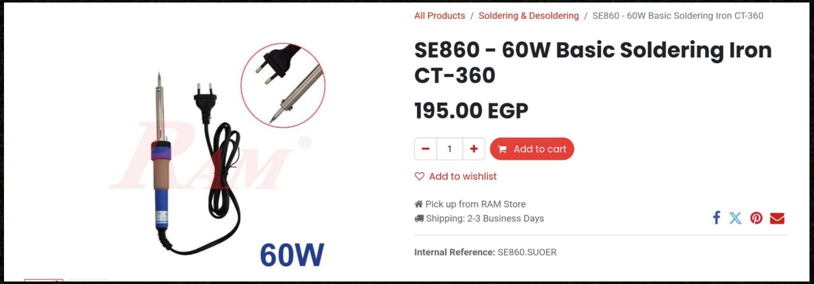
100.00 EGP

− 1 + Add to cart

Add to wishlist

Pick up from RAM Store
Shipping: 2-3 Business Days

Internal Reference: TTL.CH340



All Products / Soldering & Desoldering / SE860 - 60W Basic Soldering Iron CT-360

SE860 - 60W Basic Soldering Iron CT-360

195.00 EGP

− 1 + Add to cart

Add to wishlist

Pick up from RAM Store
Shipping: 2-3 Business Days

Internal Reference: SE860.SUOER

Case Study

https://www.hardbreak.wiki/introduction/case-study-led-to-a-cve-update

More Resources for the intermediate

- Hardware Hacking YouTube Playlist (Make Me Hack)
- Hardware Hacking Walkthroughs (Matt Brown)
- Hardware Hacking Wiki (Hardbreak)
- Practical Electronics Course
- Hardware All The Things
- More Good Stuff
- Books
  - The Hardware Hacking Handbook
  - Hacking The Xbox
  - Microcontroller Exploits
  - Power Analysis Attacks: Revealing The Secrets of Smart Cards (DPABook)
  - The Car Hacking Handbook