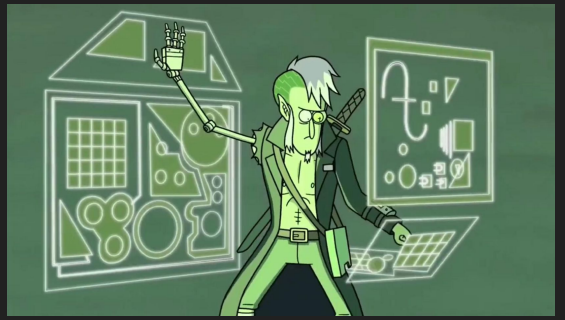
Intro To HardWare

By Noah

UMASS CYBERSEC CLUB

What is Hardware Hacking

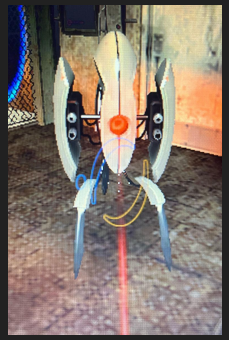


What is **Hacking**?

Most people associate hacking with software.

Software hacking targets vulnerabilities in software, hardware hacking targets weaknesses in the circuit board the software is running on.

What is an **Embedded System**?



Where do we see them?

What can we get out of hacking them?

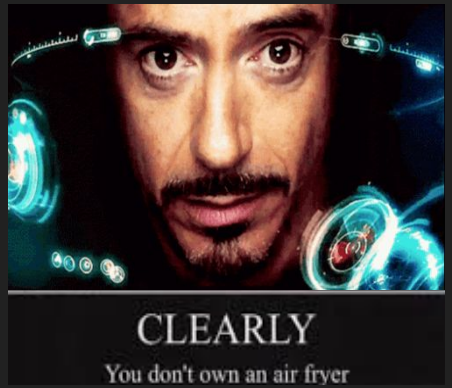
UMASS CYBERSEC CLUB

Embedded Systems - Definition

Laptops, Desktops, PCs: general purpose

Embedded Systems: specialized to perform specific tasks

Must be optimized for cost, power usage, speed, and size



UMASS CYBERSEC CLUB

Applications of Hardware Hacking

- **Jailbreaking** - smartphones, game consoles, IoT devices
- **Device Repair / Data Recovery** - cooked laptop/console
- **Diagnostics** - read sensor values (ex: car engine temp)
- **Key Extraction** - breaking cryptography
- **Reverse Engineering** - source code of device's firmware

We will focus on Key Extraction, Reverse Engineering, and Jailbreaking

Gaining access to functionality or secrets hidden from the user

UMASS CYBERSEC CLUB

Key Extraction

Devices create and store keys all the time - **Why is this necessary?**

Security runs on cryptography. (Confidentiality, Integrity, Authentication)

It is extremely important that secret keys remain secret

Impersonation, theft, malice >:)

Ex: Hardware Crypto Wallets

UMASS CYBERSEC CLUB

Key Extraction

If keys are secure in software, they may not be in hardware

How do keys get extracted from hardware?

UMASS CYBERSEC CLUB

Side Channel Analysis and Implementation Attacks

Implementation attacks target the way hardware was implemented

What is a **Side Channel**?

Power analysis - differences in power consumption based on input

Timing analysis - measuring how much time an operation takes

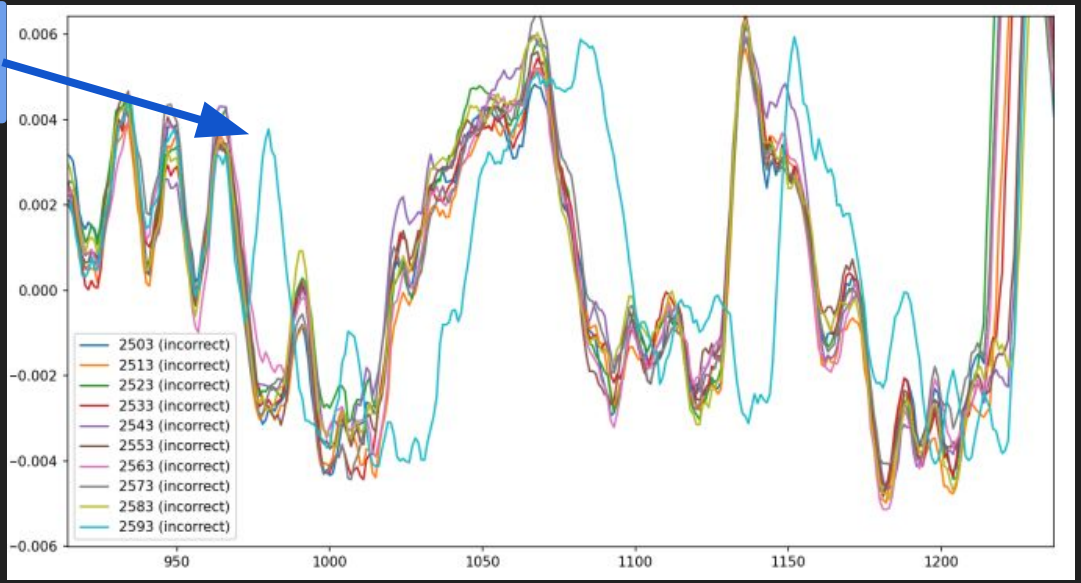
Fault injection - if we inject failures into components what can we learn?

Power Analysis to Crack a Padlock (that blows up after 50 incorrect guesses)

We have a padlock with a 4-digit pin

We can monitor the power consumption of the circuit

Blue line = 2593.



Example from a CS 564 Cyber Effects homework

Assume we already know the 1st two digits (2,5,X,X)

What is the 3rd digit based on this trace? 25XX

Why?

UMASS CYBERSEC CLUB

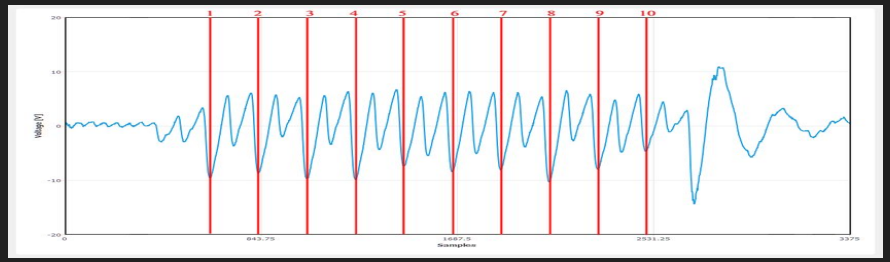
Power Analysis and Cryptography

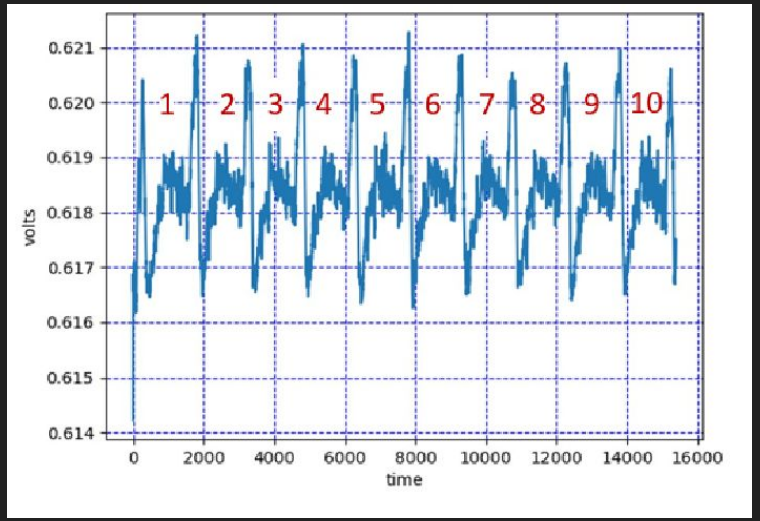
Cryptographic keys are great targets for power analysis / side channel attacks

Not feasible to crack these keys with brute force or math 

AES: common encryption algorithm, key size = 128, 192, 256 bits

AES-128 does 10 rounds of encryption





Through SPA we can recognize the pattern

Other analysis methods can determine the key

UMASS CYBERSEC CLUB

Video here explains AES algorithm: https://asecuritysite.com/subjects/chapter88

Fault Injection

Many ways to disrupt a device during operation

Voltage pulses, modifying clock signal, extreme temperature, lasers!!!

Goal is to put the device / software into an undefined state

This can leak info, skip security checks, and more

Raspberry Pi put out a challenge to hack the RP2350

Using Fault Injections, this guy won $20,000

https://media.ccc.de/v/38c3-hacking-the-rp2350

this was not the guy

UMASS CYBERSEC CLUB

Reverse Engineering

If you wanted to change how a device functions, what would you change?

What determines how a device operates?

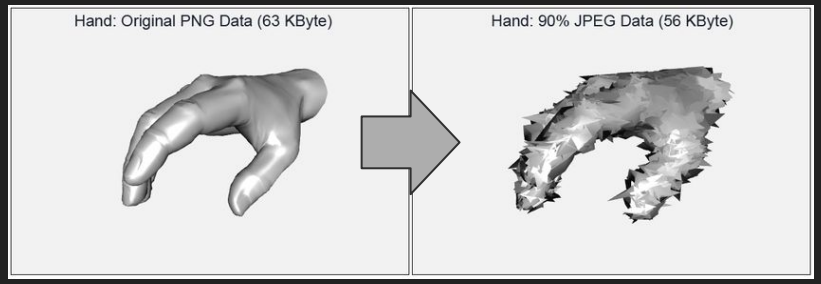
Where do the instructions come from?

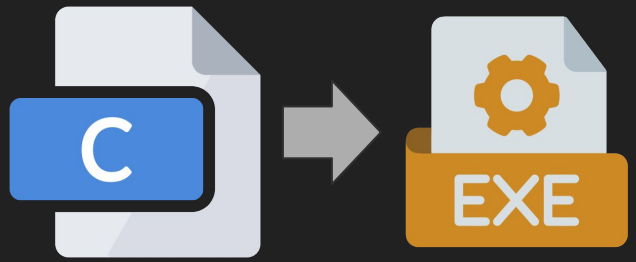
Reverse Engineering

Embedded devices run firmware which dictates how they function

Firmware is usually a compiled executable

Compilation is a lossy process (no comments, no source code, just binary)





Reverse engineering = building the source code using ASM and context

UMASS CYBERSEC CLUB

DirectTV Cracked Smart Cards and “Black Sunday (2001)”

- Throughout the 90s, DirectTV used smart cards to decrypt their broadcasted signals based on user subscription
- Hackers reverse engineered the smartcards, giving them access to manually editing the subscription information, obtaining all content for free
- Cloned and sold 100,000 “H cards”
- DirectTV knew about the issue but didn’t do anything, until...

SuperBowl Sunday 2001 - DirectTV puts out an update that destroys all H cards

UMASS CYBERSEC CLUB

https://slashdot.org/story/01/01/25/1343218/DirecTVs-Secret-War-On-Hackers

Jailbreaking

smartphones, game consoles, streaming boxes, routers, ect.

What is jailbreaking?

Why might someone do this?

UMASS CYBERSEC CLUB

Jailbreaking

smartphones, game consoles, streaming boxes, routers, ect.

What is jailbreaking? - Gaining access to blocked features on a device

Why might someone do this?

Jailbreaking

smartphones, game consoles, streaming boxes, routers, ect.

What is jailbreaking? - Gaining access to blocked features on a device

Why might someone do this? - lots of reasons

- Gain full access to hardware
- Run unsigned code (iPhone, Xbox)
- Customization
- Enable disabled features (ex. debug interface)

How? - manipulate bootloader to boot into a non-sandboxed environment

Boot Code

When a computer starts up, it doesn't know what to do

Boot code (usually stored in ROM) runs on startup to:

- Initialize hardware
- Load OS into memory
- OS takes over from there

Sometimes users are given the option to boot from other places...

Jailbreaking the Xbox 360 - “Reset Glitch Hack (2011)”

jailbreaking a 360 was a low cost way to obtain a linux machine with decent specs

An Xbox is just a computer, and we want a computer

When it starts up, boot code in ROM initializes components

It will allow a user to boot from disk drive with a disk that contains Microsoft signed code

Otherwise, it boots normally into a restricted virtual environment (Xbox menu)

How can we get past this?

What tools do we have available?

UMASS CYBERSEC CLUB

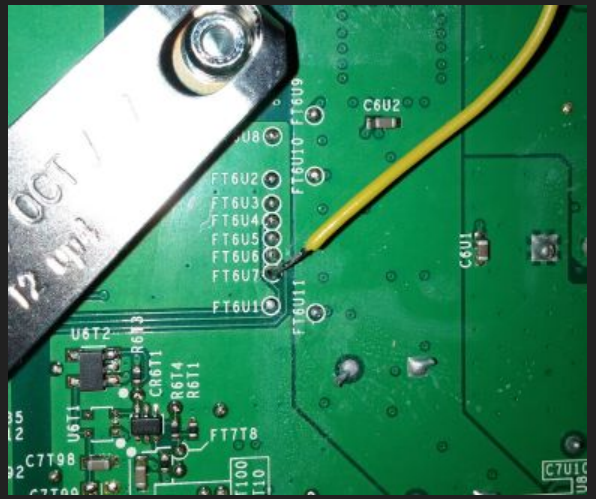
https://www.blackhat.com/docs/eu-15/materials/eu-15-Giller-Implementing-Electrical-Glitching-Attacks.pdf

Jailbreaking the Xbox 360 - “Reset Glitch Hack (2011)”

jailbreaking a 360 was a low cost way to obtain a linux machine with decent specs

Xbox 360 Boot Process:

1. Start executing code from secure memory to initialize components
2. Read (modified) secondary boot code from disk drive
3. Verify cryptographic signature of code - **What is this?**
4. If signature verification of secondary boot code passes, continue
5. Start executing secondary boot code



Exposed pin interface:

CPU_PLL_BYPASS - slows processor to 520 khz (makes timing easier)

RESET - clears active thread (skips instruction)

POST Bus - gives diagnostic codes at important boot stages

Which of these seem useful?
When should we use?

UMASS CYBERSEC CLUB

https://www.blackhat.com/docs/eu-15/materials/eu-15-Giller-Implementing-Electrical-Glitching-Attacks.pdf

Jailbreaking the Xbox 360 - “Reset Glitch Hack (2011)”

jailbreaking a 360 was a low cost way to obtain a linux machine with decent specs

Xbox 360 Boot Process:

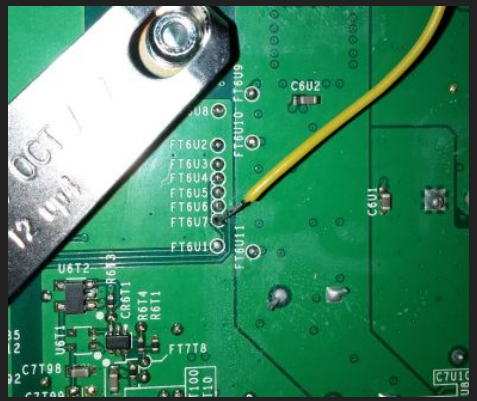
1. Start executing code from secure memory to initialize components
2. Read (modified) secondary boot code from disk drive
3. Verify cryptographic signature of code - **What is this?**
4. If signature verification of secondary boot code passes, continue
5. Start executing secondary boot code

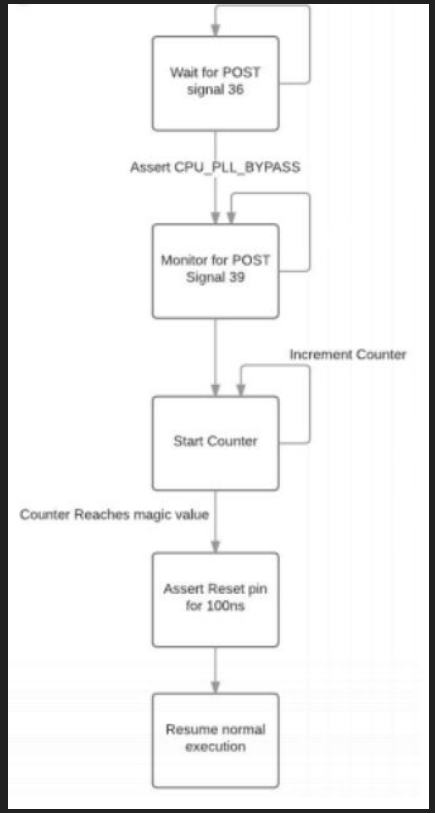
Exposed pin interface:

CPU_PLL_BYPASS - slows processor to 520 khz

RESET - clears active thread (skips instruction)

POST Bus - gives diagnostic codes at important boot stages





https://www.blackhat.com/docs/eu-15/materials/eu-15-Giller-Implementing-Electrical-Glitching-Attacks.pdf

UMASS CYBERSEC CLUB

How Can You Start Hacking?

Better learn how to swim lil gup

Need a good understanding of computers, embedded systems, programming, circuits, tools, ect.

Personal projects (ex. Arduino based embedded system)

UMASS CYBERSEC CLUB

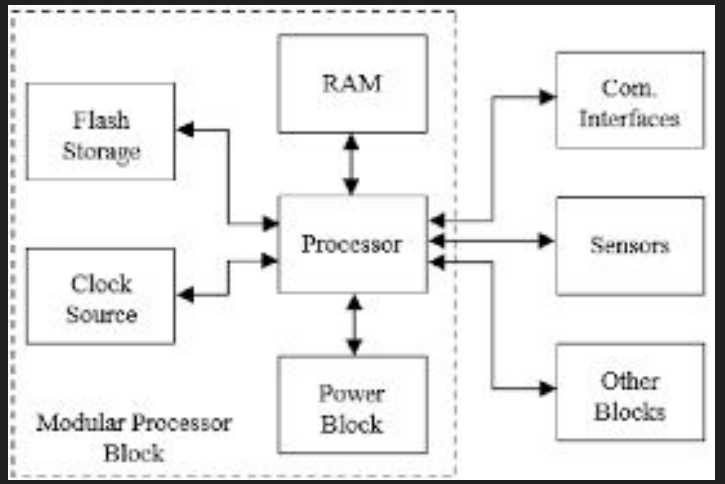
Parts of an Embedded System

Microcontroller - processor that runs firmware

Memory - stores firmware + other data

Clock - generates timing signal

Power Supply/Management - powers components



Sensors/Actuators - how system interacts with physical environment

Communication Modules - WiFi, Bluetooth, RF, Ethernet, USB

I/O interfaces - GPIO, ADC/DAC, UART, JTAG (debug)

Parts of an Embedded System - Microcontrollers (MCU)

Digital devices need to perform operations/computations —> Processor required

Microcontrollers usually contain all components they need to function

The microprocessor (MPU) is the processor of the microcontroller

- Does operations/calculations

Parts of an Embedded System - Memory

Memory comes in many forms

- RAM
- ROM
- EPROM
- Volatile vs Non-Volatile

Data is stored here

Parts of an Embedded System - Input/Output

Serial Communication: 1 bit at a time

Reading data:

GPIO

ADC / DAC

Communication and Debugging:

UART

JTAG

UMASS CYBERSEC CLUB

What is a PCB?

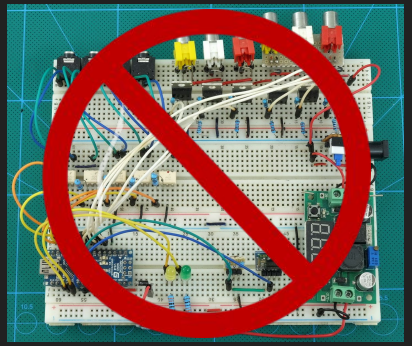
In Hardware Hacking, you will almost always be dealing with PCBs

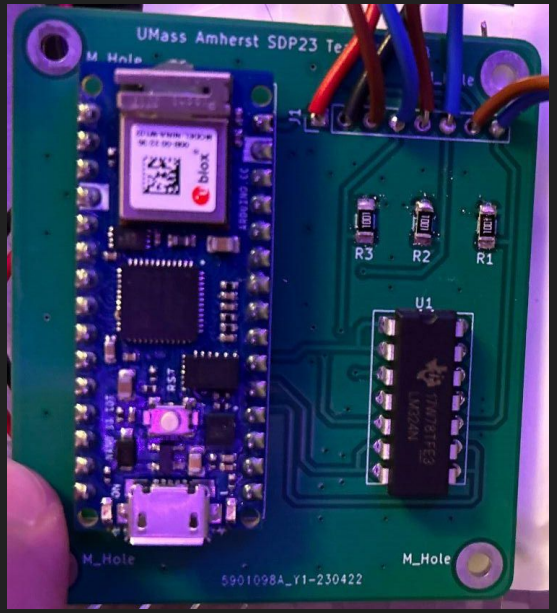
Printed Circuit Board

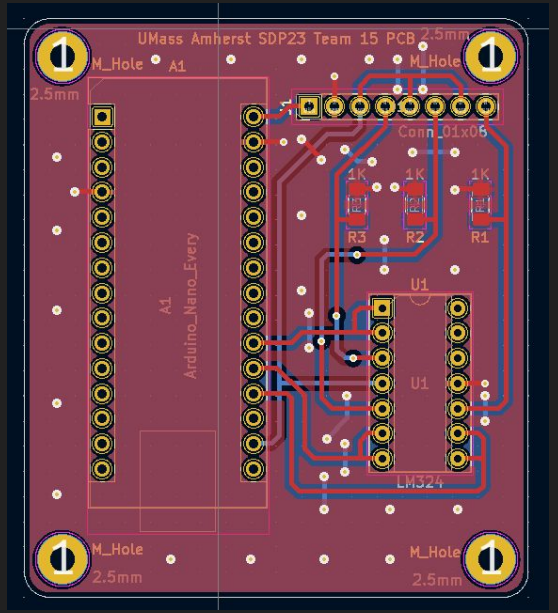
Houses circuit components and connects them

Found in almost all electronic devices

Why do we use PCBs over breadboards in real life devices?







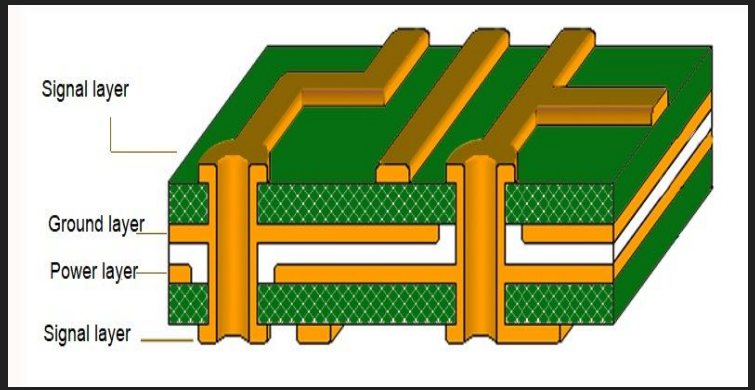
UMASS CYBERSEC CLUB

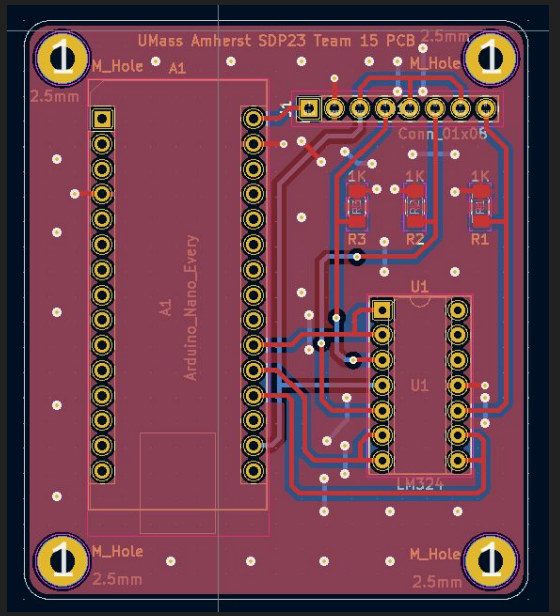
PCB Layout:

PCB is usually just the full embedded system, but condensed

PCB layers:

- Gnd Plane
- Pwr Plane
- Signal Traces
- Insulation Layers
- Silkscreen Labels





Structures:

Planes, Traces, Vias, Through Holes

UMASS CYBERSEC CLUB

Analyzing PCBs (Static Analysis Only, Dynamic is out of scope)

Steps:

1. Establish Overall goal - dumping firmware, gaining debug access, ect.
2. Search Online - sometimes somebody else has already done this work
3. Examine PCB visually - read labels, part numbers, identify components
4. Understand Circuit - find datasheets for components, build image of circuit
5. Locate Points of Interest - debug pins, flash memory, ect.

Components generally have part numbers, you can usually find their datasheet containing specs and pin layout online

Helpful to search <part_number> “pinout” or “datasheet” for components

Do the following ~5 minutes: and let me know if you have questions

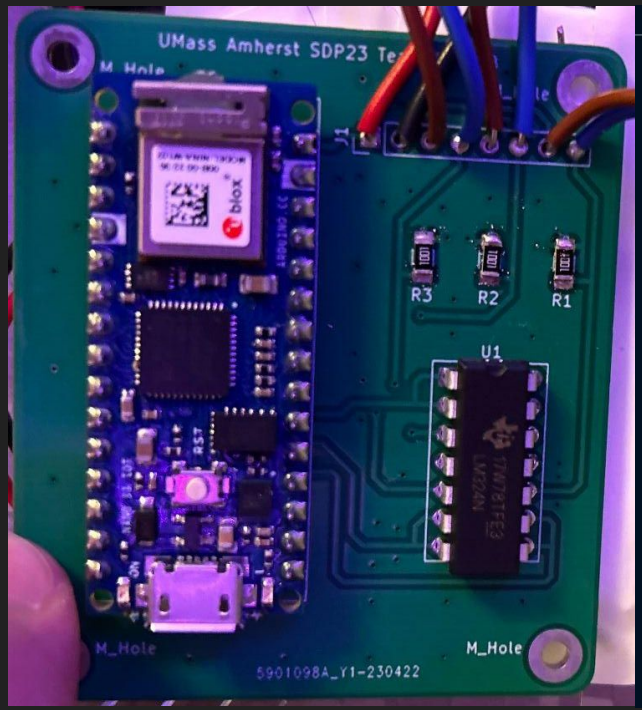
You have enough info to find everything, even if it's not fully labeled (Google stuff)

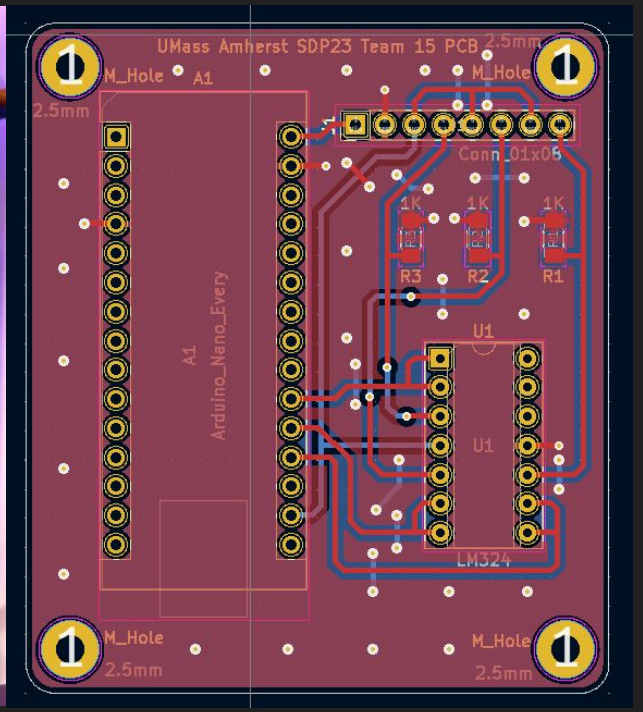
What microcontroller is this?

What kind of component is the LM324 (on the right)?

What might R1, R2, R3 be?

7 pins are used on the microcontroller. What do they do?

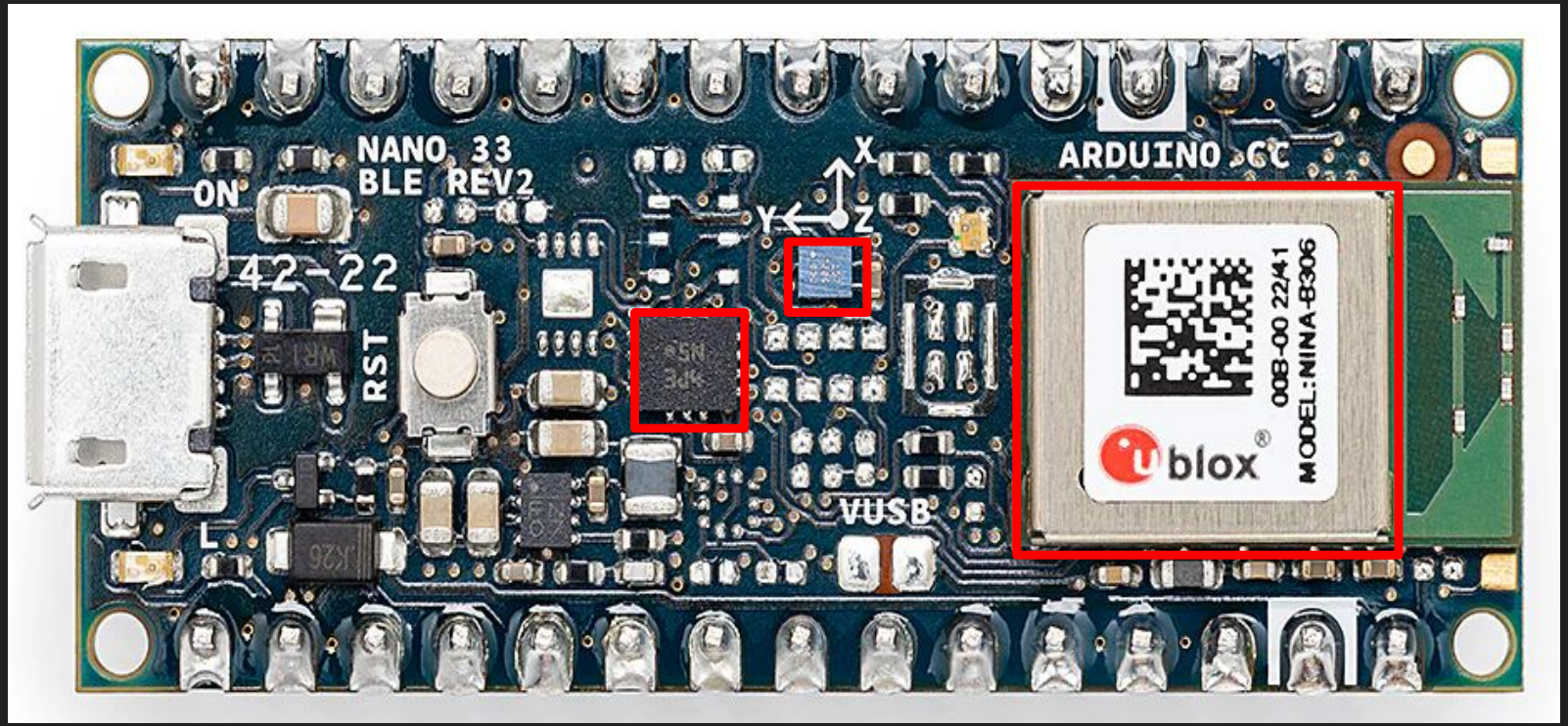




UMASS CYBERSEC CLUB

Do Another Following: Another the 5 Minutes

Identify what these components do:



UMASS CYBERSEC CLUB

Hands On Stuff

We have PCBs

Take one and try to identify components

Think about what their purpose might be in the overall system

Let me know if you have questions

UMASS CYBERSEC CLUB

Resources

If you found this stuff interesting and would like to learn more:

- Classes to take
  - ECE 231 - Intro to Embedded Systems
  - ECE 332 - Embedded Systems Lab
  - ECE 371 - Intro to Security Engineering
  - ECE 547 - Security Engineering
  - CS 256 - Make: A Hands-On Introduction to Physical Computing
  - CS 335 - Inside the Box
  - CS 564 - Cyber Effects
- Resources
  - https://www.cyberark.com/resources/threat-research-blog/an-introduction-to-hardware-hacking

UMASS CYBERSEC CLUB

NECCDC Applications open soon!

If you’re interested in blue teaming, this is a competition where you defend a simulated corporate network against industry professional hackers!

- Fill out our interest form!
- Application materials will be released next week.

Interest form

UMASS CYBERSEC CLUB

Join us for MinutemanCTF!

Where?

LGRC A112

When?

Oct 17 @ 6:00 PM

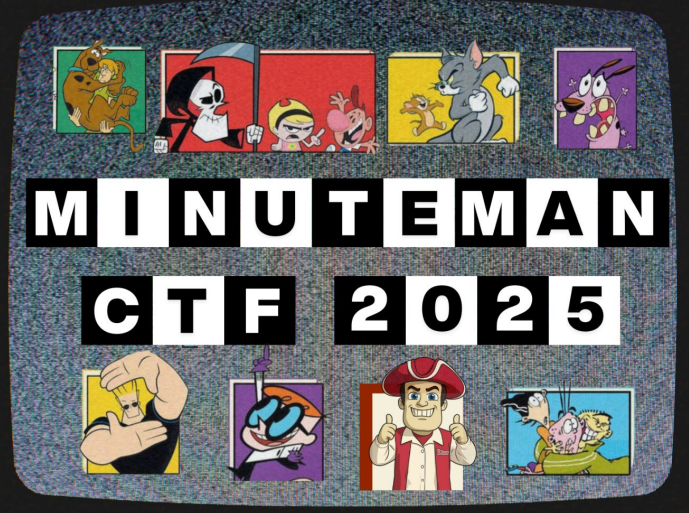
Want a challenge?

Want to see industry and professor panels?

Come play MinutemanCTF!

UMASS CYBERSEC CLUB

UMASS CYBERSEC CLUB PRESENTS



A BEGINNER FRIENDLY CAPTURE THE FLAG COMPETITION FOR UMASS AND FIVE COLLEGE STUDENTS

OCT. 17 TO OCT. 19 [AT] 6PM EST

Kickoff Event: Oct. 17 at 6:00 pm

LGRC, ROOM A112 , UMASS

Hands on learning | ARG style challenges

Panels & Talks from Faculty and Meta, Bugcrowd, Dell

PRIZES WORTH UPTO $100 AND MUCH MORE!!

Questions?

How do I learn more?
How can I get involved?
When are you guys available?

Come Up & Ask!

Resources Posted in Discord

Newsletter

Discord

Twitter

Website