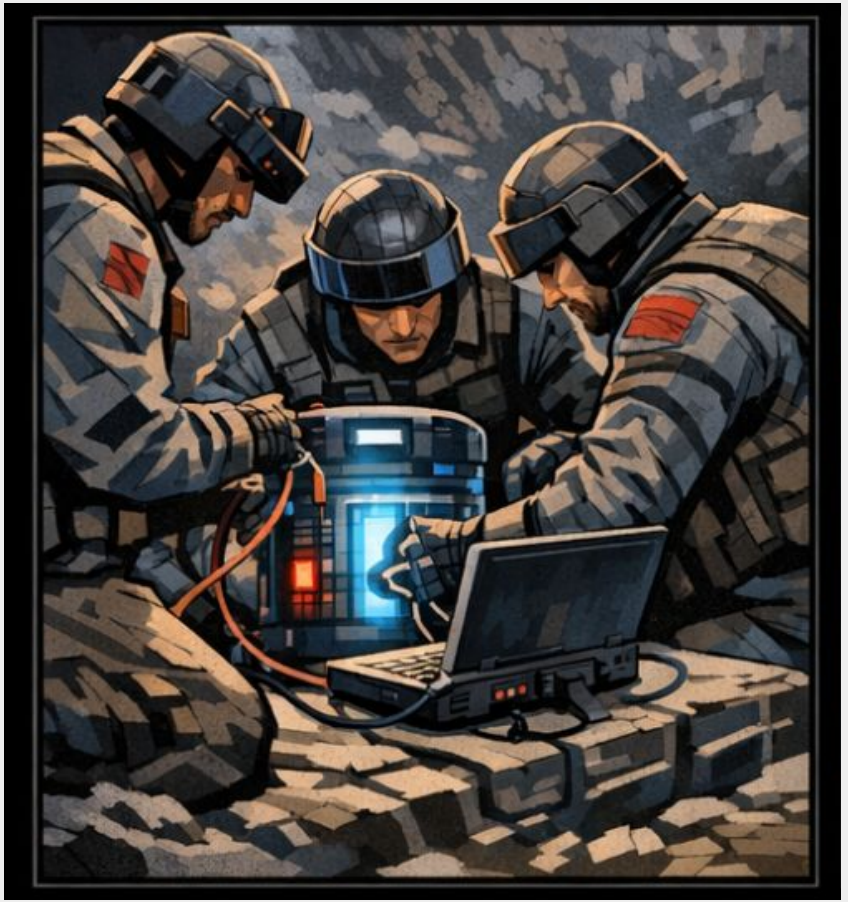
UNSW SYDNEY

Assignment: Hardware CTF

26T1

Hammond Pearce

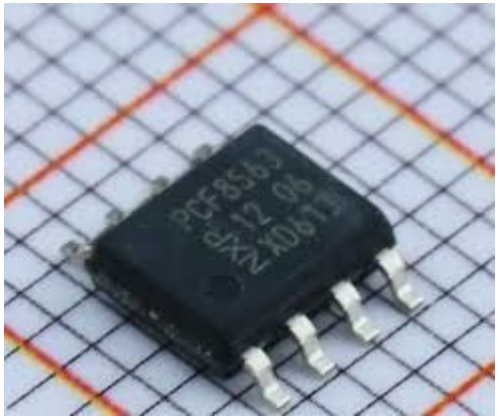


“Time”: important in many digital systems

- Enables data tracking
  - (important for e.g. banking)
- Enables serialization and sequencing
  - Data reassembled in correct order
- Security and authentication
  - Timestamps provide validation information
- Industrial automation
  - Control of real-world physical systems
- Can be used for positioning (e.g. GPS)
  - And also relativity compensation!

Real-time Clocks

- Modern computers have RTCs which maintain the time even after power-off



Time-based Security Applications

- Internet “HTTPS” traffic is protected by TLS, which uses time:
  - Certificate validity checks (Not before, Not after)
  - Revocation status (thisUpdate, nextUpdate)
  - Prevent Replay attacks
  - Minimise compromised key usage

More Time-based Security Applications

Self-destruct timer is a feature in Telegram that can only be used for messages in 'Secret Chats' and for media in private cloud chats. Through this feature, you can send messages that disappear after a set time.

More Time-based Security Applications

SECURE FILE IMPORT

SecuriRAM_

Unique USB drive with automatic secure erase

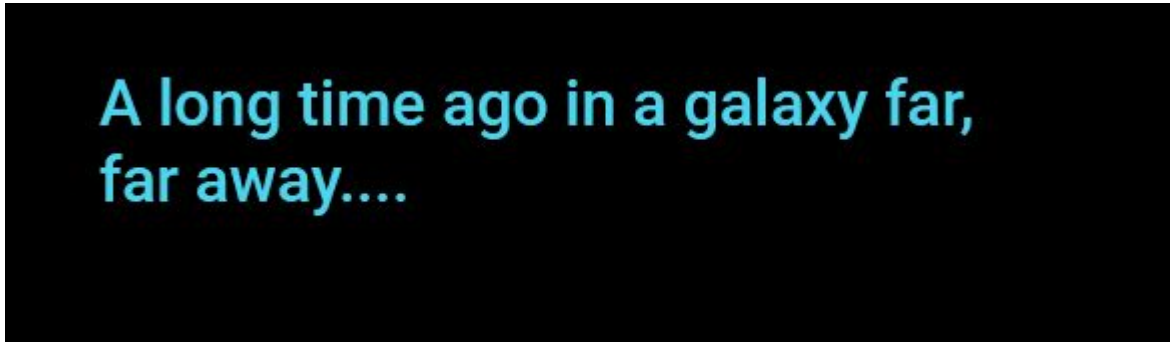
SecuriRAM is a self-erasing USB drive designed to transport sensitive information between security domains.

Contact us | Specifications

SecuriRAM offers a unique ability to completely erase all its content, either manually or automatically after 24h.

… and a long, long time ago,

some other people needed to transfer data too



https://starwarsintrogenerator.com/scroller?u=2cj35mca


The OUTER RIM - Moments after a REBEL AMBUSH
WE'RE HIT!
THAT SHIP CARRIES A DATA CORE.
NO MATTER. IT IS SECURE.
BOOM !!


WE HAVE THE CORE! ... UH OH, "SELF-DESTRUCT"?
THERE'S MULTIPLE DEFENSES. EVERYTHING WILL BE GONE AFTER TWO, MAX THREE MINUTES. GUARANTEED.
FOR YOUR SAKE, I HOPE YOU ARE RIGHT.
Well, is he? YOUR TASK: Stop the core from SELF-DESTRUCTING!

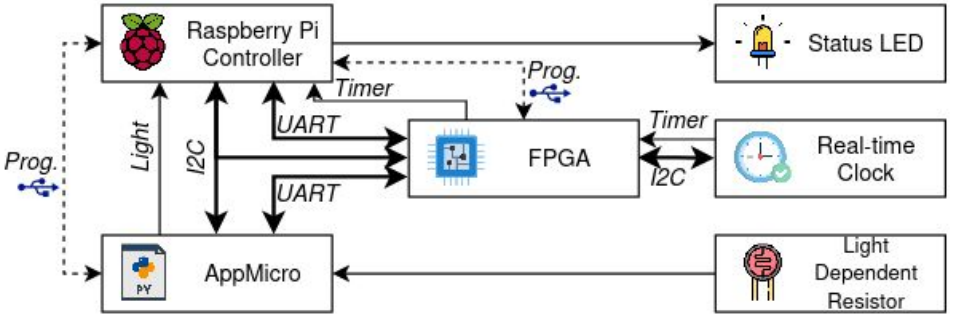
Rebel Intelligence:

We need that data!

Rebel intelligence

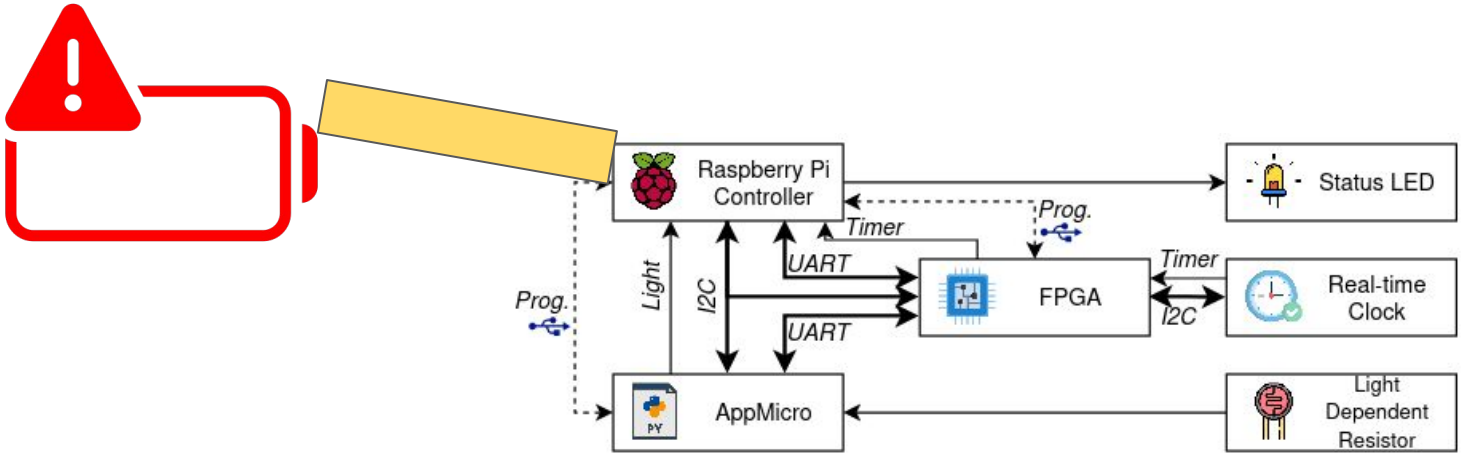
The DATA CORE is based on the Hackster platform

The data is stored in a Raspberry Pi's RAM



Rebel intelligence

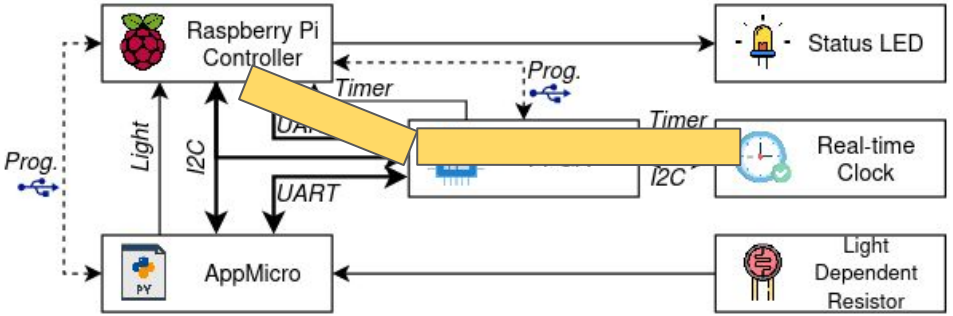
If it loses power, it will delete the stored data



Rebel intelligence

The Raspberry Pi is connected to an RTC over I2C and GPIO

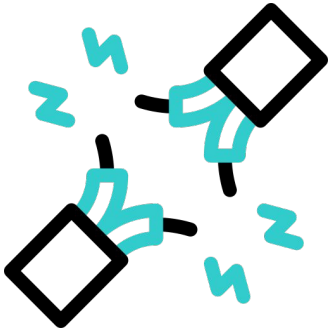
After 2 minutes, it will delete the stored data

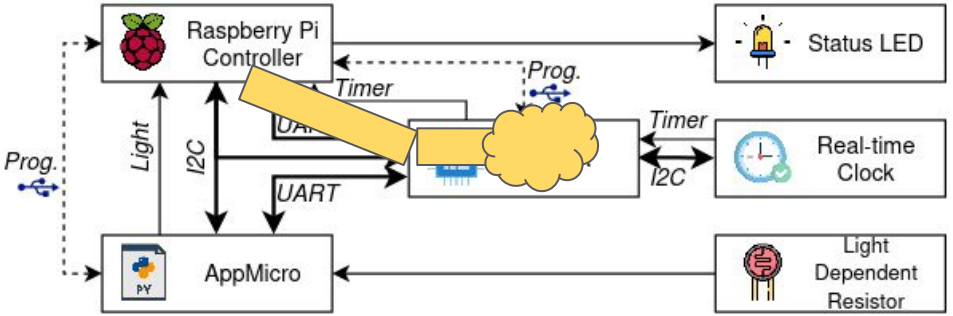


Rebel intelligence

The Raspberry Pi is connected to an RTC over I2C

If the RTC faults,
it will delete the data

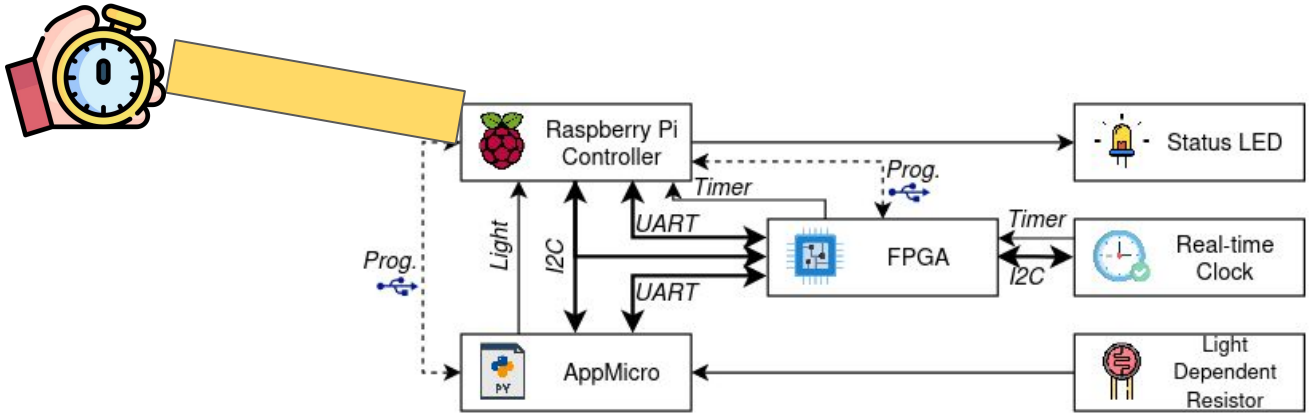




Rebel intelligence

The Raspberry Pi is connected to a second software timer

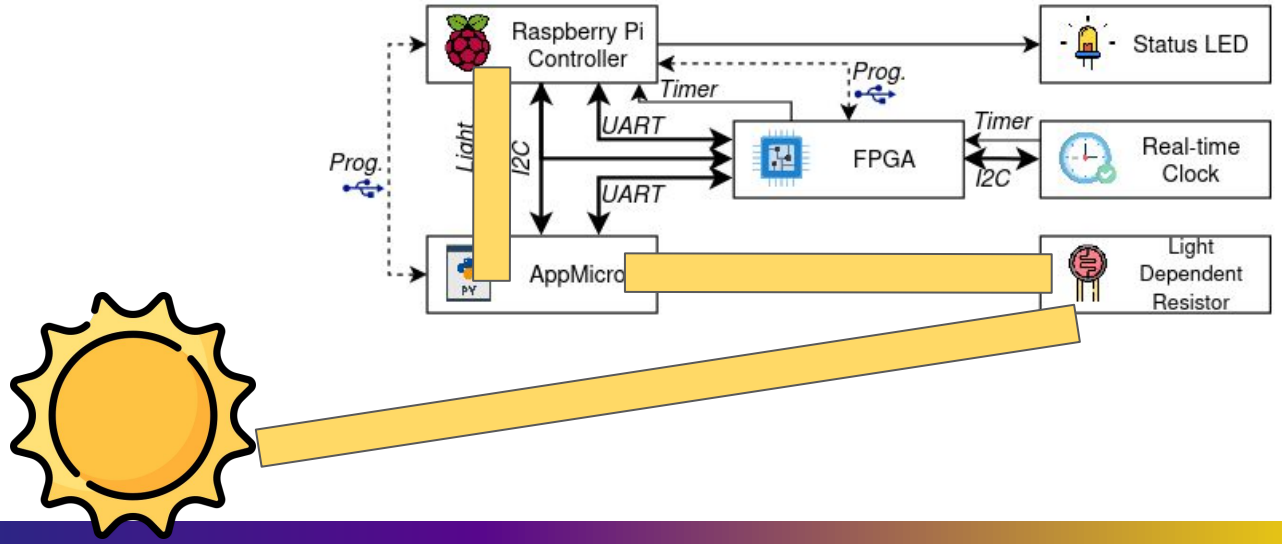
If it has been 3 minutes, it will delete the data



Rebel intelligence

The Raspberry Pi is connected to a light sensor

If it detects light, it will delete the data



Rebel intelligence

How do we get at the data?

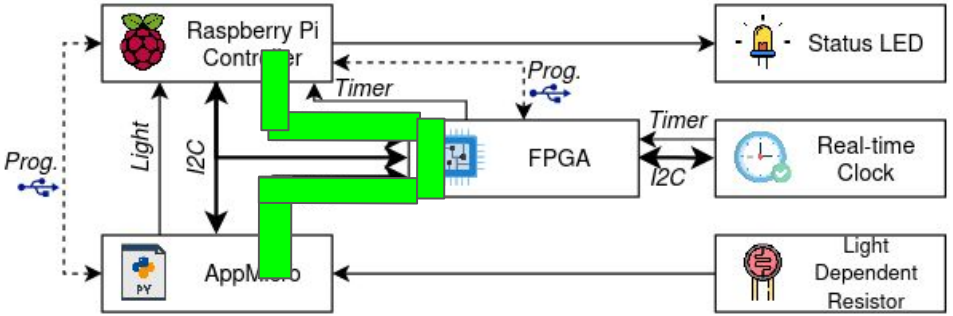
There is only “one way”

Rebel intelligence

How do we get at the data?

There is only “one way”

A disarm command over UART

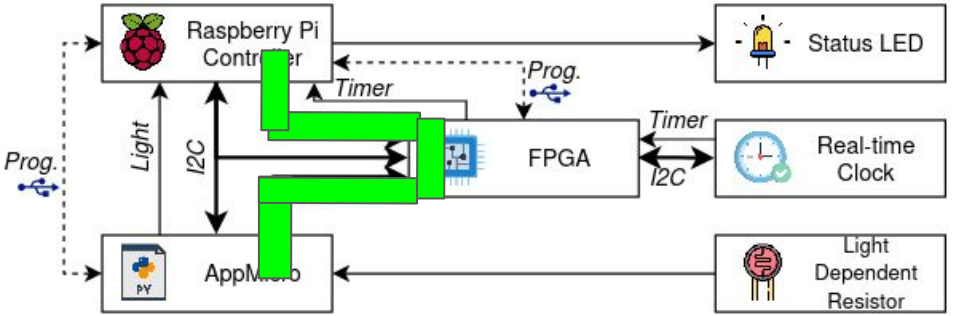


But this needs a password!

Rebel intelligence

How do we get the password?

Fortunately, **it is short! - just three digits**



Rebel intelligence

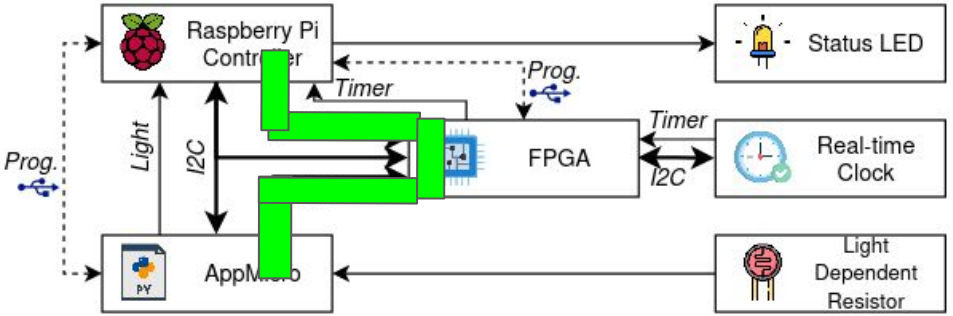
How do we get the password?

Fortunately, **it is short! - just three digits**

We can brute force!

But this takes time…

And we don't have much!



Rebel intelligence

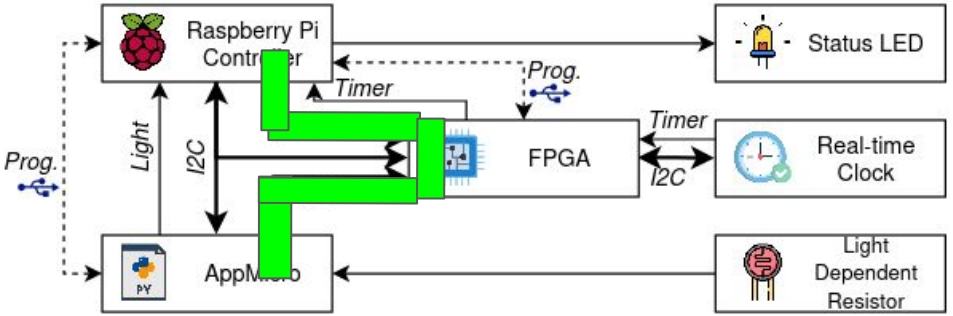
How do we get the password?

Fortunately, **it is short!**

We can brute force!

But this takes time…

And we don't have much!



How do we get more time??

Your goal:

- Find a way to disarm the DATA CORE in under three minutes

Hint: This will require a MitM attack (e.g. a Hardware Trojan)

Grading and Hurdle

Practical Demonstration: 15% (Weeks 8, 9, and/or 10)

- [5%] Delay
- [5%] Disarm
- [5%] Debrief

Report/Artifacts: 15% (3+R page IEEE 2 column format, Wk11)

- [5%] Artifacts **[checked for plagiarism]**
- [10%] Report:
  - Planning, research, and method
  - Results and reflections
  - Proposed fixes and improvements

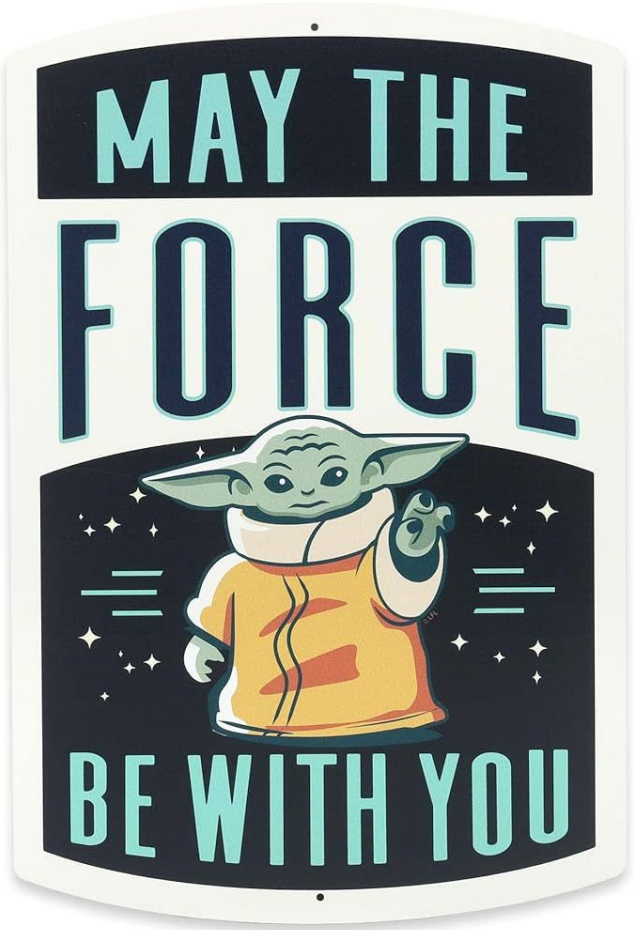
HURDLE: YOU NEED 15/30

Getting started

Details will be provided on the course website.

In general, you need to:

1. Learn how the RTC works using the AppMicro
2. Create an I2C trojan to interfere with the communication
3. Learn to deploy it quickly!
4. Overcome the other defenses…


MAY THE
FORCE
BE WITH YOU