SIGPwny

Embedded SP2026 • 2026-01-21

eCTF Introduction

Prof. Kirill Levchenko, Jake Mayer, Nikhil Date, Swetha Karthikeyan, Krishnan Shankar

Jake Mayer

- SIGPwny Admin & Embedded co-lead for '24 & '25
- CS, Math major
- Fun fact: I was rejected from UIUC

Swetha Karthikeyan

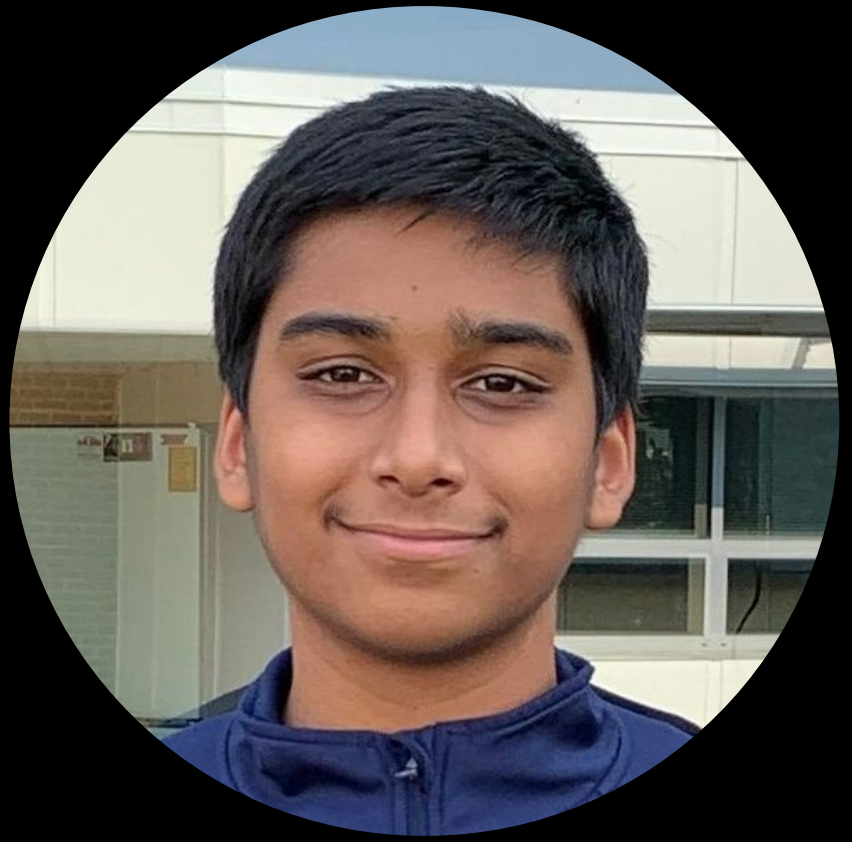
- Admin & embedded lead in SIGPwny
- Junior in Computer Engineering
- Fun fact: I play the violin and used to be in the university orchestra

Nikhil Date

- Admin
- Computer Science
- Fact: I lived in Columbus last summer

Krishnan Shankar

- SIGPwny Admin
- Computer Engineering ‘28
- Fun fact: I’m from the Washington, D.C Area



Announcements

- eCTF Kickoff last Wednesday
  - Rules
  - Boards

- eCTF Individual Registration
  - Register with MITRE for eCTF
  - Form

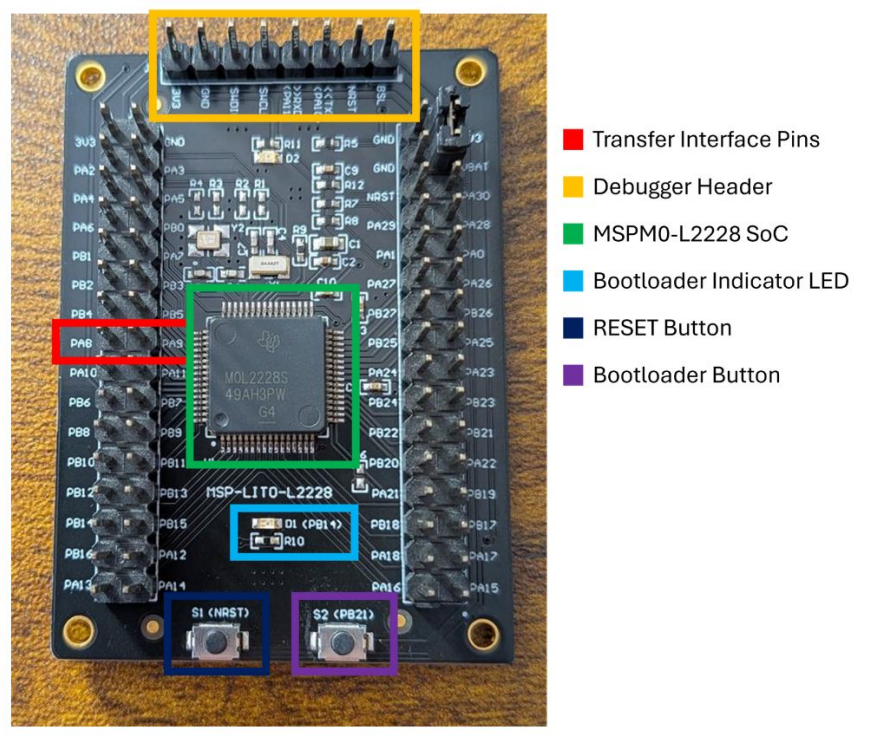
- Embedded Team Form
  - Added subteam preference question. You can edit your response.
  - Form

Subteams

- Design subteams - working on submission for design phase
- Attack subteams - prepping for attack phase, utilizing custom PCB
  - Fault Injection
  - Side Channel Analysis
- Less priority on automation anymore since 2026 scoring doesn’t reward first blood
- Based on team needs and interests, we will assign people to subteams

eCTF 2026 Challenge

- This year, the challenge is developing a Hardware Security Module (HSM) for securely storing and transferring chip fabrication files
- Development platform is Texas Instruments MSP-LITO-L2228 with MSPM0L2228 MCU



eCTF 2026 Challenge

- We need to implement the HSM, which can store “files”
- File has a
    - “Group ID”
    - UUID
    - Name
    - Contents
- HSM needs to support
    - Reading files to host
    - Writing files from host
    - Transferring files to another HSM
- We have per-group permissions for read, write receive
- Each device also has a 6-hex digit PIN

Security Requirements

Security Requirement 1

An attacker should not be able to perform any file action without a validly provisioned HSM with the permissions to perform that action on files belonging to that group.

The attacker should not be able to read files from an HSM without the read permission. The attacker should not be able to create files without the write permission. The attacker should not be able to receive files from other HSMs without the receive permission. The receive permission also applies to interrogate, meaning that the interrogated device should only return metadata about files for which the requesting device has the receive permission.

Security Requirement 2

No PIN-protected action should be able to be completed by a user without prior knowledge of the PIN

This includes confidentiality of the PIN. The HSM should not expose information about its PIN to any unauthorized user.

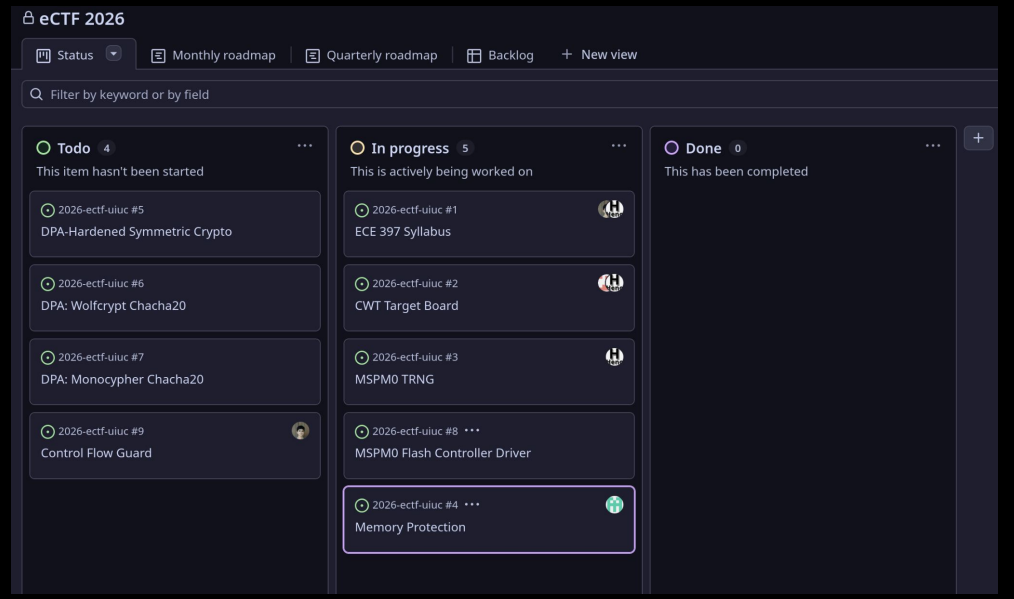
Security Requirement 3

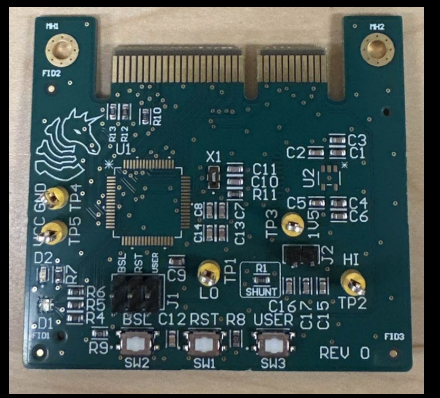
An HSM should not successfully receive any file that was not generated by another valid HSM with write permissions for that group

This includes protecting file integrity from being compromised in any way by an attacker.

What we've been working on

- Boards arrived
  - We may need a second revision to match competition boards
- Some work on HAL
  - TRNG driver upstreamed
  - Flash controller WIP
- Some talk about security measures
  - Stack canary works!
  - Further mitigations hypothesized





ECE 397

- We will be offering 2 hours of individual study credit with Professor Kirill Levchenko
- Credit is given for contributing to our eCTF team and completing some assignments
- Syllabus

eCTF Design Brainstorming

Next Meetings

2026-01-24 • **This Saturday**

- eCTF Design
- Make design decisions

2026-01-28 • **Next Wednesday**

- eCTF Design Wrap Up
- Our design doc should be finalized by the end of the meeting

2026-02-25 • **Some Wednesday**

- eCTF Handoff
- First day we can submit our design, we should be ready in advance

Meeting content can be found at sigpwny.com/meetings.

SIGPwny