What is the project
Defensive system for Linux-based IoT devices against Mirai (and related variants) using code signing to validate authenticity and integrity of executables. We also plan to leverage our defense system to code sign scripts and libraries.

Why is tackling this project important
Mirai infects 600,000 vulnerable IoT devices, in 164 countries, and the number of IoT devices is growing. New Mirai variants are frequently spotted in the wild. Many IoT devices like routers and smart TVs run Linux-based OS, so developing a generic code signing mechanism for Linux IoT devices against Mirai will have widespread applications.

How do you plan on tackling the project
March 8th - March 14th

- Research on code signing
- Setup development environment (emulators, frameworks, target devices)
- generate signatures for executables
- Decide when to sign the executables
- Test the system with Mirai's executable on our system and ensure integrity of the system.

March 15th - March 28th

- Research on library/script attacks on a linux system.
- Start testing binary variants Mirai against defense system in sandbox
- Generate signatures for scripts.
- Expand the signature checking mechanism to check scripts.
- Test the selected library attack on our system and ensure integrity of the system.

March 26th weekend

- Practice demo
- Write the report.

List of 3 sets of deliverables (I'll take these under advisement when grading, but I don't promise to strictly abide by them):
Set of deliverables that will yield a passing grade

- Develop a defense for linux based iot systems by initially verifying the integrity of the executables before running them on the system.
- Demonstrate defense against routers running openWRT firmware

Set of deliverables that will yield an A grade

- Leverage the defense system by expanding the code signing to scripts/libraries.
- Demonstrate defense against other non-router IoT devices

Set of deliverables that shows work clearly beyond an A

- Successfully defend against 5+ Mirai variants, and possibly other IoT malware
- Prevent/detect malware infection at initial exploit, before executing payload

Link to a git repository where you'll keep all the code, documentation, and development through the project.

- https://github.com/jyotsna-penumaka/EC700-Bravo2