



UNIVERSITY OF NORTH CAROLINA
CHARLOTTE



Teaching Critical Infrastructure Security Through Interactive Experiences: Modeling Cyberattacks in Gamified Learning

Ella Luedeke^{1*}³, Meera Sridhar¹, Harini Ramaprasad²

¹Department of Software and Information Systems, University of North Carolina at Charlotte, Charlotte, NC, USA

²College of Computing and Informatics, University of North Carolina at Charlotte, Charlotte, NC, USA

³Current affiliation: University of North Florida (work conducted as REU student at UNC Charlotte)

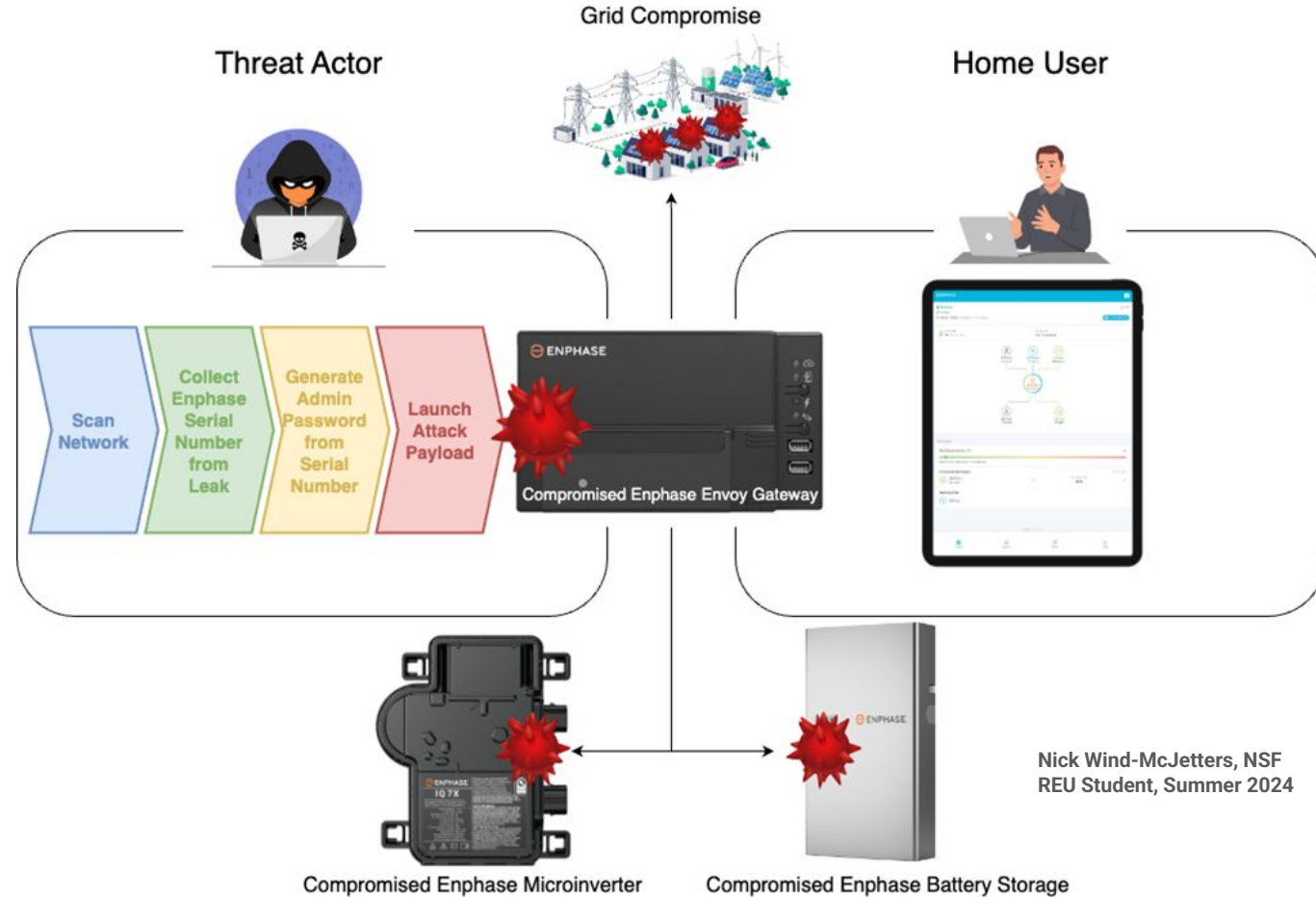
*Work supported in part by NSF-CNS #2244424, UNC Charlotte and UNC System



The Critical Infrastructure Crisis



- Power grid digitization = Larger attack surface
- Distributed Energy Resources (DERs) lack the strong security of traditional power plants
- Power engineering students aren't often taught cybersecurity fundamentals



Nick Wind-McJetters, NSF REU Student, Summer 2024



The Gap

Existing Tools

- **Type of Tools:** CTFs, Cyber Ranges, Labs
- **Barrier to Entry:** Assumes programming skills
- **General Topics:** Rarely cover DERs

InfraLearn

- **Gamification:** Engaging features sustain interest
- **Tailored Curriculum:** Guided learning for non-computing students
- **Interactive Learning:** Hands-on learning related to DERs

Criminal Investigations Background

Pedagogical Strategies:

- Compelling narrative
- Just-in-time learning content delivery
- Knowledge checkpoints to assess student preparation
- Hands-on tasks / activities
- Rewards such as eXperience Points (XP) to motivate student

Adapted for Power Engineering Students



CESAR
CENTER FOR ENERGY
SECURITY AND RELIABILITY

Player:
XP: 0

MENU

HELP

DETECTIVE:

Hello, I'm Detective Mahina Brown. I've requested help of the university's cyber security students in investigating a case that happened here. A college student is suspected of hacking multiple IoT

SYSTEM:

What information would you like to find?

1

3

4

5

6

7

8

9

SYSTEM:

Compression is the process of encoding information using fewer bits than the original representation. Since embedded devices have less resources including a small memory, on-the-fly decompression of previously compressed firmware reduces the data load and minimizes the number of accesses to long-term storage during boot or wake-up. This, in turn, reduces the energy (and the delay) during this critical phase of operation.

SYSTEM:

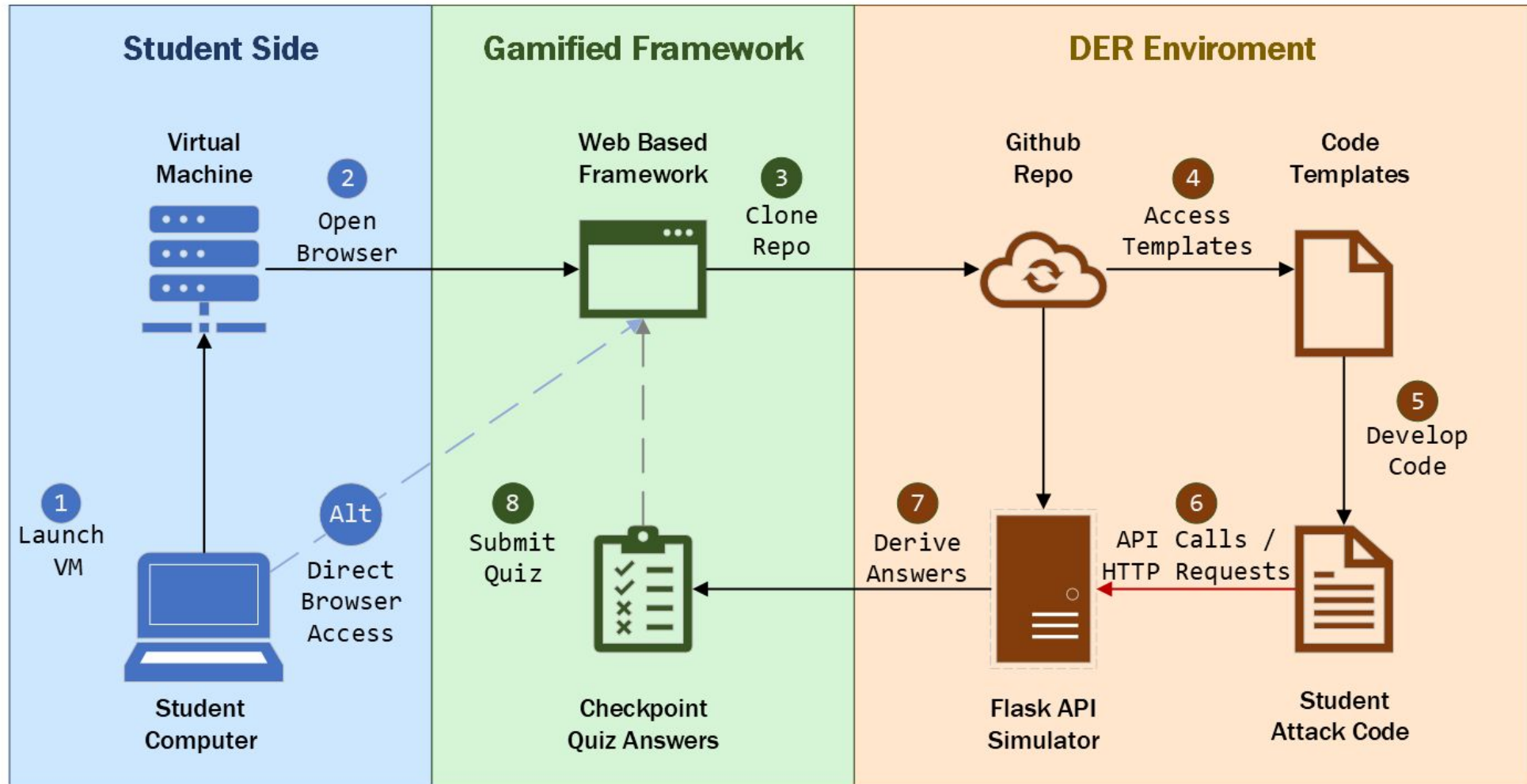
Use binwalk to identify the compression schemes used to compress different components of the firmware, such as: kernel, filesystem, bootloader, etc. Make sure you can decompress the file or component for analysis.

Hall et. al, SIGCE '22



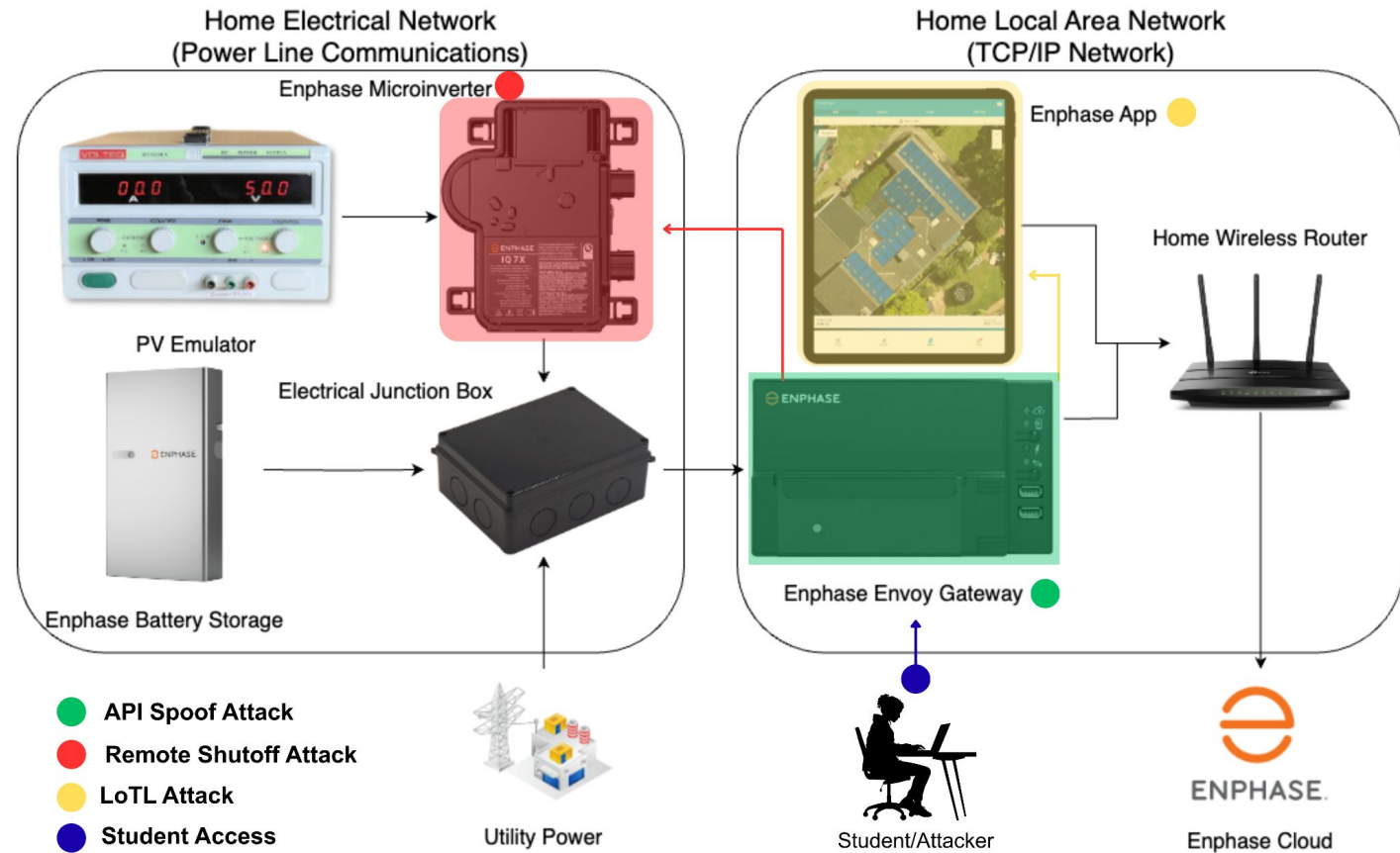
UNIVERSITY OF NORTH CAROLINA
CHARLOTTE

InfraLearn as a Solution



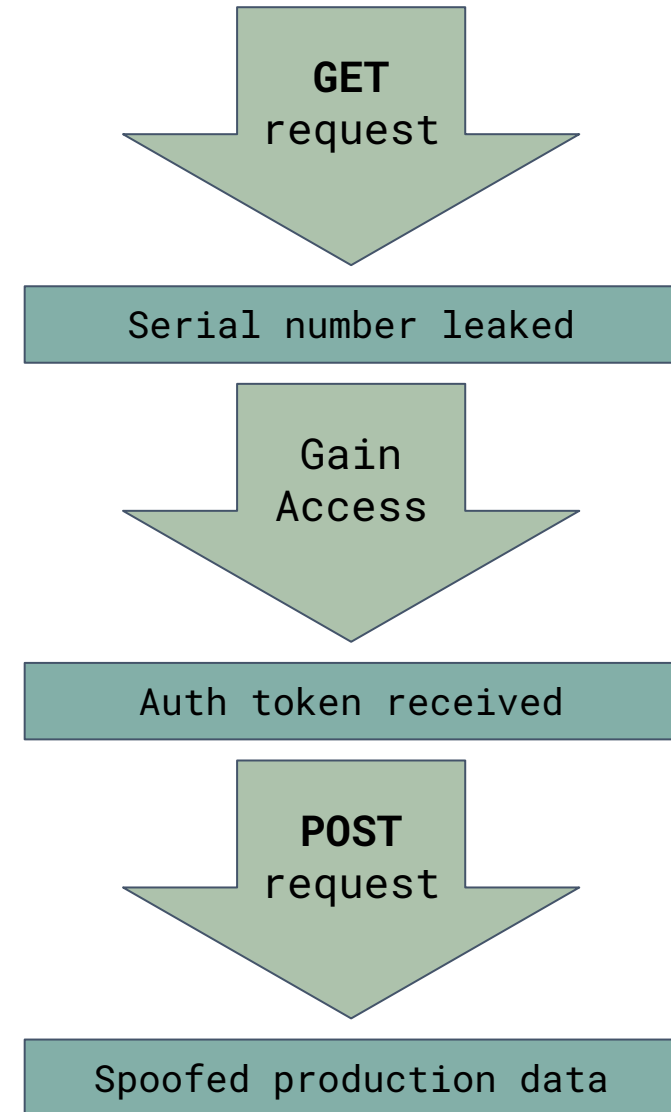
Activity Modules

- Each activity models a real-world cybersecurity problem, targeting different parts of the Home Electrical Network
- The activities demonstrate how digital (IT) threats can directly impact physical infrastructure (OT)



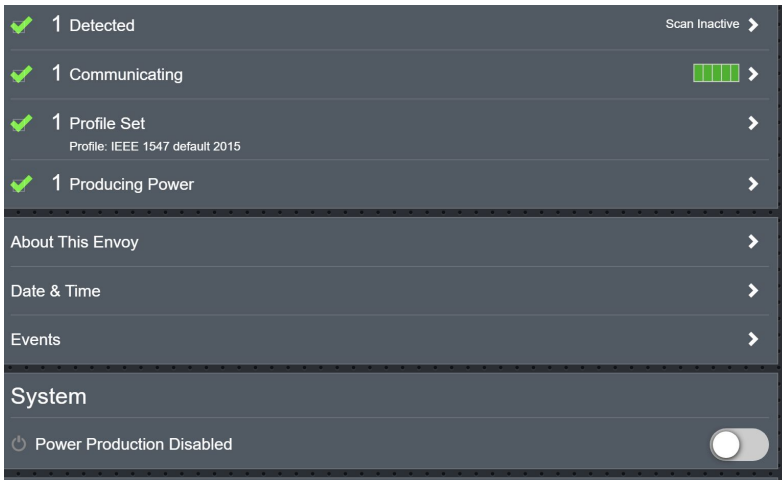
API Spoof Attack

- This activity is based on CVE-2020-25754
- In this activity, students explore how spoofing can compromise data integrity by forging API responses

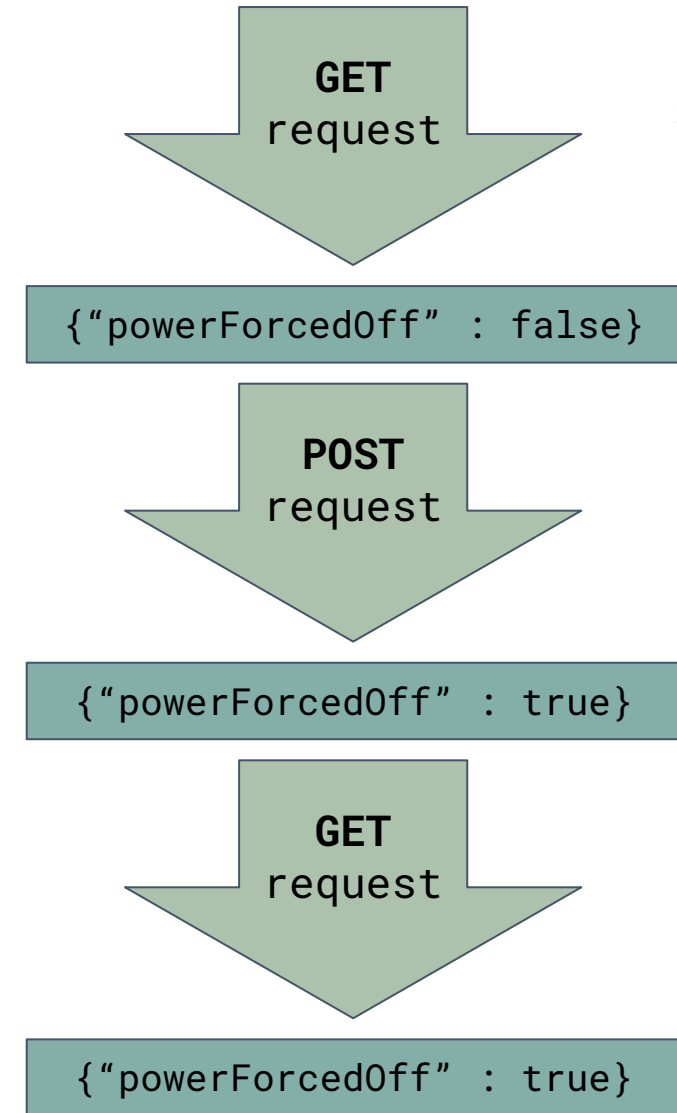


Remote Disable Attack

- This activity teaches about remote shutdown exploits (CVE-2020-21880)
- An adversary can force the device offline, preventing it from performing its intended function

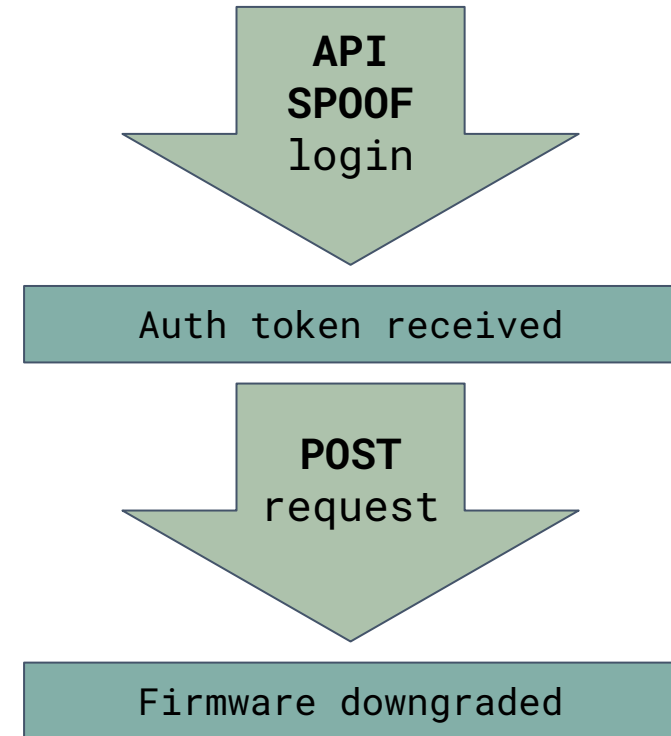


© Nicholas Wind-McJetters, CESAR



LoTL Attack

- LoTL attacks abuse the system's own trusted tools and features against it
- One such example is a firmware downgrade vulnerability
- This activity demonstrates this firmware downgrade vulnerability inspired by CVE-2025-8321



Looking Ahead

Contributions

- InfraLearn fills a gap left by existing gamified tools
- Provides a DER simulation environment that models the Enphase Gateway
- Critical infrastructure education for non-computing students.

Future Work

- User studies with power engineering students
- Gather data on learning outcomes and student engagement
- Expand our activities to other critical infrastructure sectors

Questions?

Ella Luedeke

n01553443@unf.edu