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

Ella Luedeke
School of Computing
University of North Florida
Jacksonville, FL, USA
n01553443@unf.edu
0009-0003-3375-8934

Meera Sridhar
Department of Software and Information Systems
University of North Carolina at Charlotte
Charlotte, NC, USA
msridhar@charlotte.edu
0000-0002-7508-5024

Harini Ramaprasad
College of Computing and Informatics
University of North Carolina at Charlotte
Charlotte, NC, USA
hramapra@charlotte.edu
0000-0002-1598-4677

Abstract—This work introduces InfraLearn, a gamified learning platform designed to teach non-computer science students a foundational background in cybersecurity for critical infrastructure. InfraLearn simulates attacks on a Distributed Energy Resource (DER) device, modeled after the Enphase Gateway solar monitor and implemented using a Flask-based API. Three prototype scenarios are developed: API spoofing, unauthorized remote shut-downs, and Living-off-the-Land (LoTL) downgrade exploitation. These scenarios are derived from real-world vulnerabilities in DER systems and integrated into a narrative-driven, web-based platform. Students interact with pre-configured virtual machines, guided code templates, and checkpoint quizzes, with optional AI support that reinforces comprehension while minimizing the need for prior programming experience. By situating cybersecurity concepts within the context of energy systems, InfraLearn has the potential to make abstract threats tangible and emphasizes the ethical application of defensive skills. This work demonstrates a scalable approach to engaging future engineers in securing critical infrastructure.

Keywords—*Critical Infrastructure, Cybersecurity, Gamified Learning, Interactive*

I. INTRODUCTION

The digitization and increased Internet-connectivity of the power grid is expanding its attack surface rapidly, creating unprecedented new vulnerabilities in systems once considered isolated and secure [1]. With the shift towards decentralized grids, the number of *Distributed Energy Resources (DERs)*, such as solar panels and wind turbines, is growing exponentially, making them prime targets for cyberattacks [2]. These systems often lack the robust security measures found in traditional, centralized power plants, making them particularly susceptible to exploitation [3], [4]. Exploitation of DER systems can lead to physical disruptions, economic losses, and even threats to public safety [5]. Real-world examples, such as those detailed by Waylon Grange in his analysis of Enphase Gateway vulnerabilities, underscore the feasibility and impact of these attacks [6].

Traditional cybersecurity education has been unable to keep up with these rapid changes in the field of cybersecurity [7], and frequently fails to provide the practical context and hands-on experience necessary for effective learning [8]. Solutions such as *gamification*, which is the application of game-design elements and game principles in non-game contexts, have been shown to improve learning outcomes, student engagement, and motivation in various educational settings [9]. Existing gamified frameworks for cybersecurity education exist but are not specifically tailored to the challenges of the limited and decentralized security of DERs.

Our work targets students in non-*computer science* (CS) disciplines, particularly those in power and electrical engineering. These students are the future designers and operators of critical energy infrastructure, yet they typically receive limited formal education in cybersecurity [10]. We recognize that while these students may not be interested in becoming professional programmers or penetration testers, they require a fundamental understanding of digital threats to build and maintain secure systems. We design our modules to be accessible to learners with little-to-no programming experience, providing a guided, hands-on introduction to key concepts integrated into their courses. By contextualizing cybersecurity within their own field, we make the material more relevant and engaging, equipping future engineers with the skills they need to defend critical infrastructure.

InfraLearn explicitly encourages the use *Artificial Intelligence (AI)* tools (e.g, code copilots or chat-based LLMs) in the instructions of the modules to debug syntax errors, clarify error messages, and provide explanations, improving student outcomes by providing personalized feedback and support [11]. In this work, we present a gamified platform, InfraLearn, for teaching and learning critical infrastructure cybersecurity in an engaging way. InfraLearn is an evolution of previous work, Criminal Investigations, a web-based, gamified

©2026 The Author(s) | Creative Commons CC BY 4.0

framework that delivers cybersecurity education to students, with prototype activities in IoT firmware reverse engineering [12]. In this work, we extend Criminal Investigations with DER-focused modules and simulated experiences packaged into one platform, InfraLearn. InfraLearn combines two key components: a DER simulation environment that supports realistic cyberattacks and Criminal Investigations.

InfraLearn structures the student experience through Criminal Investigations, guiding them through attack scenarios and providing scaffolding and feedback to support conceptual understanding. Our DER simulator models a widely used DER system, the Enphase energy system [13]. The Enphase solar energy system consists of a set of *Microinverters*, which convert the direct current (DC) output of individual solar panels into alternating current (AC), and a *Gateway*, which serves as the system's communication hub. The Gateway collects performance data from each Microinverter, transmits it to the cloud for monitoring, and can issue remote control commands, such as curtailing or disabling energy output [14].

The main contributions of this work are as follows:

- **A DER-focused, gamified cybersecurity platform:** InfraLearn fills a gap left by existing gamified tools by providing a DER simulation environment that models the Enphase Gateway for critical infrastructure education.
- **Tailored curriculum for non-CS students:** A pre-configured *Virtual Machine (VM)*, guided code templates, and narrative context make cybersecurity concepts accessible to power and electrical engineering students with little computing experience.
- **Educationally adapted attack scenarios:** Three prototype scenarios adapted for educational use and selected for relevance: *Application Programming Interface (API)* spoofing, remote shutdown attacks, and *Living-off-the-Land (LoTL)* attacks.
- **Scalable web-based delivery:** Integration of these scenarios into Criminal Investigations, designed to enhance engagement and learning outcomes.
- **AI-assisted learning integration:** Rather than embedding AI, InfraLearn explicitly motivates students to use external copilots and chatbots for debugging and explanation, fostering AI literacy while keeping the platform lightweight.

Roadmap. Section II reviews approaches with existing literature, including gamified learning and critical infrastructure security. Section III details the InfraLearn system, explaining its architecture, workflow, and core components. Section IV outlines the design of the activity modules and their pedagogical goals. Section V discusses implications, limitations, and directions for future work. Section VI concludes.

II. RELATED WORKS

The field of cybersecurity education is expanding as the need for it grows, with a growing focus on innovative methods to train professionals outside of computer science disciplines. Our work is situated within this context, building upon established pedagogical principles and addressing a specific gap in critical infrastructure cybersecurity training for non-computing students.

A. Gamified Learning

Gamified learning is a powerful and effective pedagogical approach in education, especially in e-learning [15]. It addresses the limitations of traditional methods by making material more approachable and engaging through game design principles such as narrative, challenges, and rewards [16]. As a result, higher education increasingly incorporates it in online learning environments to support self-directed learning [17]. Likewise, a rise in gamified learning is present in cybersecurity education due to the challenges of motivating students in conventional training [18].

Cyber ranges, environments that represent realistic scenarios, and *capture-the-flag (CTF)* competitions, where students compete in cybersecurity technical challenges, are examples of successful gamified tools [19], [20]. These platforms offer invaluable hands-on security training by immersing learners in a simulated, competitive environment [21]. However, many of these tools often require at least some base technical knowledge and as such are not always accessible to non-computer science students [22]. Websites like TryHackMe provide more approachable content, with courses designed for beginners and experts alike [23], but they lack niche topics such as DER security.

A few frameworks have targeted critical infrastructure scenarios: for example, SimSpace provides gamified OT cyber ranges, the SWaT Security Showdown (S3) focuses on ICS security through CTF exercises, and platforms like CyberCIEGE and KYPO Cyber Range allow interactive practice relevant to CI contexts [24]–[27]. These frameworks are typically sector-specific and assume prior technical knowledge, as evident in the documentation and target audience, which limits accessibility to students outside computer science disciplines. This gap motivates the need for more inclusive gamified solutions, such as InfraLearn, which combine realistic scenarios with assisted experiences for non-CS learners.

B. Critical Infrastructure Security Education

While gamified approaches have been explored, broader educational initiatives are also emerging to address the urgent need to protect critical infrastructure from cyberattacks. Traditional engineering education and power engineering focuses heavily on operational aspects and other engineering principles, with less emphasis on cybersecurity [28]. The *Cyber-Informed Engineering (CIE)* program, a collaborative effort among the U.S Department of Energy (DoE), Office of Cybersecurity, Energy Security, and Emergency Response

©2026 The Author(s) | Creative Commons CC BY 4.0

(CESER), the Idaho National Laboratory (INL), and the National Renewable Energy Laboratory (NREL), is a key initiative addressing this gap [29]. The program aims to educate engineers in ways that are applicable to their skill sets to make decisions that improve cybersecurity outcomes [30].

Several academic works that focus on critical infrastructure security education also contribute to this area. Xie *et al.* develops educational modules based on a cyber-distribution system testbed, enabling students to engage with realistic power system operations and examine vulnerabilities in a hands-on environment. This work highlights the importance of experiential learning to bridge theory and practice in *Cyber–Physical Systems (CPS)* [31]. Similarly, Foreman *et al.* designs *Industrial Control Systems (ICS)* cybersecurity modules for engineering education, offering foundational instruction alongside laboratory exercises to build familiarity with ICS security challenges [32]. These modules emphasize the workforce development needs for protecting critical infrastructure. Beyond ICS-focused materials, Chou presents an interactive learning system for general cybersecurity education, leveraging engagement and active learning strategies to improve student comprehension of security concepts [33].

Unlike existing general and gamified cybersecurity frameworks for critical infrastructure, InfraLearn offers an interactive, narrative-driven platform that lowers the barrier to entry and addresses a critical gap in education. While other frameworks require esoteric knowledge or expensive hardware, we eliminate those requirements by delivering a single platform that students can run on their own computers that incorporates student support into the design. Furthermore, our approach uniquely combines realistic power engineering contexts with gamified elements to broaden access and reduce technical barriers. We draw inspiration from previous gamification efforts in computing and interactive learning systems to create a platform that is not only effective but also highly accessible for use in a variety of educational settings.

III. INFRALEARN OVERVIEW AND WORKFLOW

In this section, we describe the architecture and workflow of the InfraLearn platform, highlighting the integration of Criminal Investigations. InfraLearn is designed to provide a structured and hands-on learning experience that makes learning about complex topics like DER security engaging and accessible. We design the modules for students with limited to no prior programming experience. Students are only expected to possess a basic understanding of using a computer and navigating a graphical user interface. The content is planned so that students will learn the basics of APIs naturally as they progress through the modules.

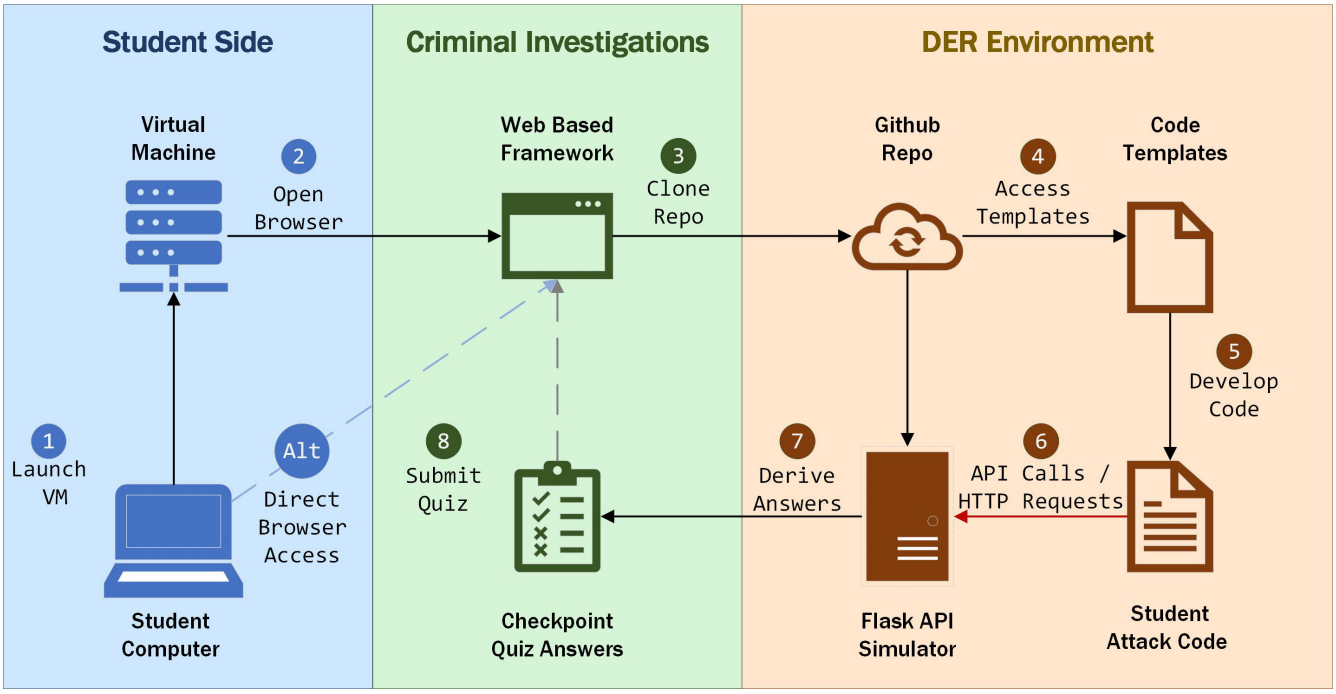

Fig. 1. A visualization of the student's journey through InfraLearn's system, from their computer to Criminal Investigations' framework and into the DER simulated environment.

A. *InfraLearn Layout*

InfraLearn consists of three key sections that work in tandem to deliver the curriculum: the (i) student side, (ii) the Criminal Investigations gamified framework, (iii) and the DER environment.

1. **Student Side.** The student side, as shown in the left panel of Figure 1, contains the pre-configured VM that ensures no real-world risk, isolating all simulated attacks and the development environment from the student's host machine and the broader internet.
2. **Criminal Investigations.** Criminal Investigations, seen in the middle panel of Figure 1, delivers the narrative, activity module instructions, and quizzes. Its integration into InfraLearn enables consistent knowledge reinforcement and supports the exploratory nature of adversarial thinking.
3. **DER Environment.** The DER environment, visualized in the right panel of Figure 1, models the target of the exercises. It consists of a GitHub-hosted repository containing a Flask-based API simulator, pre-built code templates, and reference solutions for instructors. The simulator exposes realistic endpoints for login, inverter data retrieval, and power control, giving students a safe environment to practice constructing, exploiting, and defending against malicious API requests.

B. *Criminal Investigations Background*

Criminal Investigations, developed in prior work, is a web-based framework for cybersecurity education that leverages gamification to address challenges of engagement, accessibility, and learning in advanced topics such as *Internet-of-Things (IoT)* security [12]. The prototype activity focuses on reverse engineering IoT firmware and exemplifies the potential of the gamification approach. Within Criminal Investigations, students engage in a narrative-driven investigation, apply technical tools in a guided environment, and receive immediate feedback tied to clear learning objectives.

Criminal Investigations has undergone a pilot deployment as an extra-credit module in one undergraduate/early graduate game design course and three undergraduate operating systems and networking course sections in Spring 2021. The full course module included instructional content, an interactive activity with nine tasks delivered through Criminal Investigations, a quiz, and pre-/post-surveys. A total of 36 students completed at least one task and feedback survey and 23 completed all nine tasks.

Evaluation data consisted of Likert-scale and free-response questions, which were categorized into negative, neutral, and positive responses using both manual grouping and automated sentiment analysis with NLTK's VADER [34]. Results were analyzed with approval from the University of North Carolina at Charlotte's Institutional Review Board (IRB) along dimensions of user interface and accessibility, student learning, and student engagement. Over 50% of the students had positive responses to all but one question related to engagement, while learning outcomes showed mixed responses, with feedback indicating a need for clearer instructions and additional learning content.

Overall feedback was encouraging and informed subsequent improvements implemented in InfraLearn, including refactoring the framework to a more modular architecture and refining instructional materials [12]. Features such as experience points, checkpoints, and instant feedback sustain student interest and provided continuous reinforcement of progress [35], [36].

C. *Student Workflow*

The student workflow, summarized visually in Figure 1, guides learners through a structured, iterative process. Students begin by launching a pre-configured **virtual machine (VM)** (1). Once inside the VM, the student opens a web browser to access the **Criminal Investigations website** (2). Alternatively, this framework can be directly accessed from the student's host machine. The instructions within the framework prompt the student to clone the project's **GitHub repository** directly onto their virtual machine (3). Following these instructions, the student starts the **Flask API server** from the cloned repository (4). This server launches a mock API that mimics a real-world DER gateway, establishing the active target for their simulated attacks.

The student navigates to the provided **code templates** within the cloned repository. Using documentation, Just-in-Time hints from Criminal Investigations, and the option to use AI chatbots for debugging assistance, they fill in the missing sections of the code (5). This hands-on process solidifies their understanding of how API calls and HTTP requests are constructed and exploited. The code templates are designed to integrate seamlessly with InfraLearn's front-end, which is built with React JS [37] and is backed by a MongoDB [38] database.

After running the completed script (6) and observing its effects on the simulated environment, the student returns to Criminal Investigations to answer checkpoint and discussion questions (8), drawing on insights gained from their observations (7). These assessments verify their understanding and successful execution of the attack simulation.

D. *Student Learning Features*

Narrative and Just-in-Time Content Delivery. InfraLearn leverages Criminal Investigations's narrative-driven approach, adapted to model a real-world FBI/DHS joint task force that combats critical infrastructure cybersecurity [39]. This contextualizes the attacks in a way that encourages critical thinking about real-world consequences for critical energy infrastructure. *Just-in-Time content delivery*, a pedagogical approach that aims to engage students by providing them with the information they need to know precisely when they need it,

is used to ensure key concepts are absorbed in the most relevant context [40].

Checkpoint Quizzes. InfraLearn also integrates Criminal Investigations's multiple choice checkpoint questions, known as Knowledge Checkpoints. These quizzes are intended to verify comprehension before students are allowed to progress. Gamification aspects like *experience points (XP)* are incorporated to engage students and provide a sense of achievement.

Code Templates. Partially completed Python code templates containing function definitions, import statements, and logging scaffolding and derived from the completed attacks are given to the students. Students complete missing sections that aim to increase their understanding of API endpoints, HTTP requests, and parsing responses. Additionally, students are encouraged to use documentation, hints, and AI-assisted tools to receive debugging guidance. The goal is to allow students to focus on the conceptual material and reduce barriers for learners new to programming.

IV. ACTIVITY MODULES

This section introduces three hands-on activity modules that model real-world vulnerabilities in DER systems: an API Spoof attack, a Remote Shutdown exploit, and a LoTL firmware downgrade. Together, the modules emphasize how attacks targeting the digital infrastructure—the *Information Technology (IT)*—can cause tangible impacts on the physical devices that produce and deliver energy—the *Operational Technology (OT)*. We deliver the modules through Criminal Investigations, and place the students in adversarial roles as they work through reconnaissance, exploitation, and mitigation steps. Each activity links directly to real-world vulnerabilities, ensuring that students gain both technical knowledge and an understanding of the broader cybersecurity implications.

Figure 2 illustrates the modeled DER environment and highlights the attack surface targeted by each module. The left panel represents the home electrical network, including the PV emulator, Enphase Microinverters, and battery storage connected through an electrical junction box. The right panel represents the home local area network, where the Enphase Envoy Gateway communicates with the Enphase mobile application and cloud services through a wireless router. Colored overlays indicate the focus of each module: green for the API Spoof Attack, red for the Remote Shutdown Attack, and yellow for the LoTL Attack. The student's access point is shown at the bottom. Together, these components illustrate how software exploits can propagate from IT systems to OT devices, affecting physical power production.

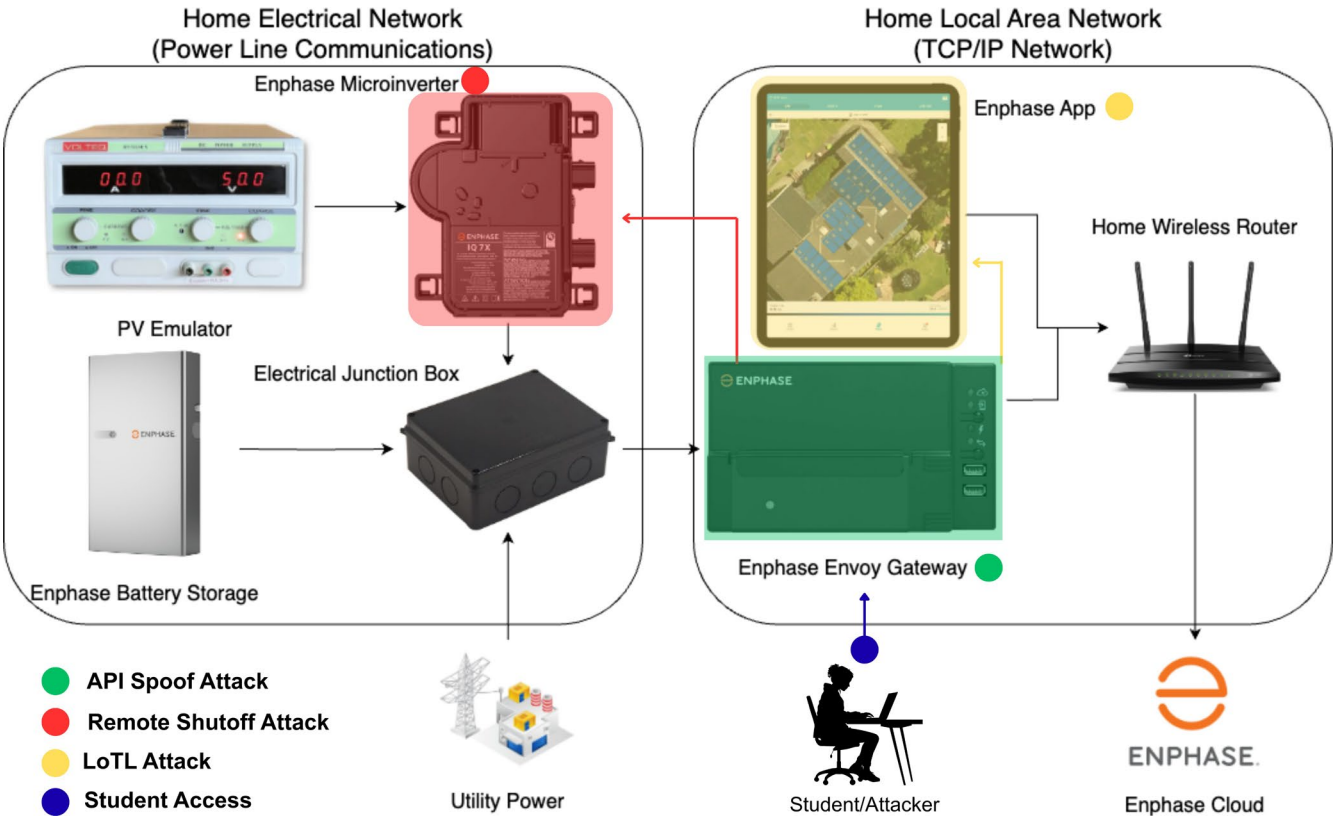

Fig. 2. Attack environment that represents a home solar system.

A. API Spoof Attack

Spoofing attacks involve falsifying data or identity information with the goal of misleading a target system [41]. In this module, students explore how spoofing can compromise data integrity by forging API responses. The activity module is based on CVE-2020-25754 [42], where the Enphase Gateway derives its administrator password from a publicly available serial number using a predictable algorithm. Attackers can exploit this weakness to authenticate and modify inverter telemetry data [6].

Students assume a reconnaissance role, where their mission is to investigate and recreate a suspected data manipulation event. The checkpoint quizzes, embedded throughout the module, ensure students can articulate why predictable passwords and weak authentication are critical vulnerabilities. Through this exercise, students gain firsthand experience with a data integrity attack and how falsified telemetry can undermine grid management.

1) Attack Steps: Students issue a `GET` request to the `info` endpoint to retrieve the device serial number. They compute the administrator password by hashing the serial number with SHA-256 and truncating the result to eight characters. Using the derived password, they authenticate through `/api/login` and obtain a session token. They then enumerate inverter data from `/api/v1/production/inverters` and send POST requests that overwrite watt values with artificially high numbers. Finally, they confirm the tampered results by re-querying `/api/v1/production`.

B. Remote Shutdown Attack

Remote shutdown exploits represent a form of attack in which an adversary can force a device offline, preventing it from performing its intended function [43]. This module models CVE-2020-21880 [44], which allows improper neutralization of special elements in the Enphase Gateway through an endpoint. The endpoint that controls the inverter's operational state does not require authentication [45]. This illustrates a significant lapse in security design, as it allows a remote, unauthenticated attacker to disrupt power production. This attack exploits a lack of access control to remotely shut down a physical device, the Enphase Microinverters. The narrative puts the student in the role of a task force member trying to prevent a potential blackout. Checkpoint questions for this module assess understanding of `GET` vs. `POST` operations, recognition of access control flaws, and the operational impacts of remotely disabling DER devices. The module reinforces that the absence of explicit authentication is a vulnerability as significant as using weak credentials. Through guided discussion, students consider the implications of such an attack at scale: an adversary could target multiple inverters or entire arrays, causing sudden drops in energy output and potentially destabilizing localized grid segments. Students also examine why leaving control endpoints unauthenticated is a severe risk, especially in systems exposed to the public internet.

1) Attack Steps: Students first send a `GET` request to the endpoint to observe the inverter's current state, typically `"powerForcedOff"`: false in the initial setup. To execute the attack, they send a POST request to the same endpoint, setting the JSON field `"powerForcedOff": true`. The simulation updates the inverter's status in the backend database, and a follow-up `GET` request confirms that power production has been disabled.

C. LoTL Attack

LoTL attacks abuse the system's own trusted tools and features against it, making it difficult to detect [46]. These attacks often utilize built-in utilities such as PowerShell, *Windows Management Instrumentation (WMI)*, and PsExec to execute commands and scripts without introducing external malicious files [47]. One such example is a firmware downgrade vulnerability, where an adversary can reinstall a previous version of the firmware using legitimate system update mechanisms [48].

This module demonstrates this firmware downgrade vulnerability inspired by CVE-2025-8321, where attackers use legitimate installer functionality to install an outdated firmware version to Tesla Wall Connector devices [49].

The narrative frames this as a *Trojan Horse* investigation, where students must discover how an attacker used a seemingly harmless feature for malicious purposes. Checkpoint questions for this module focus on identifying why LoTL attacks are stealthy, distinguishing between malicious and legitimate use of maintenance features, and recognizing the importance of firmware verification in critical infrastructure. The given discussion questions ask students to think of detection and prevention strategies.

1) Attack Steps: Students begin by repeating the reconnaissance and authentication process from the first activity: retrieving the device's serial number, deriving the administrator password, and logging in. The exploitation targets the `/installer/upgrade/start` endpoint, which in a production environment would allow authenticated users to install firmware updates.

In the simulation, students craft a `POST` request containing a JSON payload with a firmware url field. Instead of pointing to a new, secure firmware release, the payload references an older, intentionally "legacy" version.

The simulated API responds as if the downgrade has completed successfully, reporting the downgraded version and a success message. Students are prompted to consider how this could be exploited in practice—an attacker could reintroduce vulnerabilities that had been patched in later releases, or even use legacy versions with known backdoors.

V. DISCUSSION

By focusing on contextualized, real-world scenarios, this work aims to bridge the gap between cybersecurity and power systems education. The three activity modules, with

©2026 The Author(s) | Creative Commons CC BY 4.0

embedded learning features, are designed to make adversarial thinking approachable for students in power systems courses.

The integration of these activity modules into the Criminal Investigations framework supports an investigative workflow that encourages exploration and reflection. By leveraging narrative context, checkpoints, and guided technical tasks, InfraLearn is intended to foster conceptual understanding of how digital attacks on IT systems can impact physical OT infrastructure, rather than assuming mastery of these concepts. An additional contribution of this work is the explicit encouragement of AI-assisted problem solving. While InfraLearn itself does not embed AI features, the platform is intentionally designed to be compatible with AI tools, such as chatbots and code copilots, through prompting in the activity instructions and code templates. Students are encouraged to leverage these tools to receive natural language explanations, troubleshoot syntax issues, and explore alternative approaches to the guided exercises. This not only reflects modern engineering workflows but also promotes the development of AI literacy as a complementary skill.

A. Classroom Implementation

The activity modules are designed for classroom implementation, with instructors facilitating group discussion and reflection questions to reinforce key concepts. InfraLearn is intended to be a foundational component of a broader OT Cybersecurity program, rather than a standalone training solution.

This program is being developed in alignment with the University of North Carolina at Charlotte's *Center for Energy Security and Reliability (CESAR),* which is dedicated to pioneering research and innovation to develop a secure, carbon-neutral power grid for the future [50].

Through CESAR's collaboration with industry partners, InfraLearn may be incorporated into professional development or certificate-based training as the platform matures. By aligning academic instruction with the practical needs of the energy sector, InfraLearn is expected to support students and provide a scalable framework for up-skilling current engineers in Cyber-Informed Engineering principles [29].

B. Deployment Timeline and Evaluation

InfraLearn is slated for a phased deployment to evaluate its pedagogical effectiveness. The initial pilot deployment is expected to occur in Fall 2026 within a graduate-level cybersecurity course focused on operational technology. This cohort will consist of Master's students with prior cybersecurity exposure, allowing for early qualitative feedback on usability, clarity of instructions, and technical realism before being given broader audiences.

Following refinement informed by pilot feedback, InfraLearn is planned to be integrated into a regularly scheduled course in Spring 2027. At this stage, the platform may also be extended to an industry and interdisciplinary audience through CESAR-affiliated certificate or professional development programs.

Evaluation of InfraLearn's educational impact will be conducted with appropriate IRB approval. Drawing from prior assessment methodologies used in Criminal Investigations, we plan to employ two primary instruments:

1. **Experience Surveys.** To assess the engaging nature of the gamified tool and student motivation.
2. **Pre-test/Post-test Knowledge Checks.** To quantify technical gains and verify that students have mastered the foundational concepts of DER security.

We expect these outcomes to demonstrate improved adversarial thinking and technical competency in DER security, which reflects InfraLearn's objectives. This work is designed to be a concrete, replicable model for incorporating cybersecurity education into power engineering programs through a combination of gamification and hands-on experimentation.

C. Mapping to Adversarial Frameworks

Currently, our prototype scenarios (API Spoofing, Remote Shutdown, and LoTL) are designed to align to the initial stages of the *cyber kill chain*, the process coined by Lockheed Martin in which perpetrators carry out cyberattacks [51], [52]. Specifically, the steps of the activity modules cover Reconnaissance and Exploitation.

As InfraLearn develops, we plan to transition from single-point exploits to more complex, multi-step attacks. Future iterations of our curriculum will further map activity modules to industry-standard frameworks like the Lockheed Martin cyber kill chain and the MITRE ATT&CK for ICS, a knowledge base of cyberattacks and techniques [53]. Additionally, we will incorporate the ICS Cyber Kill Chain defined by the SANS Institute, which provides a specialized model for understanding adversary campaigns specifically targeting Industrial Control Systems [54]. These frameworks will guide the development of more sophisticated attacks, such as *Distributed Denial-of-Service (DDoS)* and supply chain attacks.

VI. CONCLUSIONS AND FUTURE WORK

This work presents a novel set of gamified activities to educate non-CS students in cybersecurity principles as they relate to DERs. The platform emphasizes accessibility, engagement, and relevance to critical infrastructure. By simulating real-world attacks on a model of a solar energy device, the modules provide an interactive learning environment that goes beyond theoretical concepts. The approach represents a significant step toward equipping future engineers with the knowledge and practical skills necessary to secure distributed energy systems against emerging digital threats.

As mentioned in Section V, future work will involve classroom implementation and user studies with power engineering students to gather data on learning outcomes,

©2026 The Author(s) | Creative Commons CC BY 4.0

student engagement, and usability. We also plan to expand our library of attacks to include more complex scenarios to expose students to a wider range of realistic threats and help them develop higher-order problem-solving skills relevant to modern cybersecurity challenges [55], [56]. In future iterations, we aim to integrate AI more directly into InfraLearn by embedding a context-aware hint system or adaptive feedback agent within the platform. This could further personalize the learning experience and provide real-time, targeted assistance to students as they work through challenging concepts.

ACKNOWLEDGEMENT

This research was supported in part by NSF award #2244424

REFERENCES

[1] B. Paul, A. Sarker, S. H. Abhi, S. K. Das, M. F. Ali, M. M. Islam, M. R. Islam, S. I. Moyeen, M. F. Rahman Badal, M. H. Ahamed, S. K. Sarker, P. Das, M. M. Hasan, and N. Saqib, "Potential smart grid vulnerabilities to cyber attacks: Current threats and existing mitigation strategies," *Heliyon*, vol. 10, no. 19, p. e37980, 2024.

[2] U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response and Office of Energy Efficiency and Renewable Energy, "Cybersecurity considerations for distributed energy resources on the u.s. electric grid," U.S. Department of Energy, Tech. Rep., Oct 2022.

[3] I. Zografopoulos, N. D. Hatziargyriou, and C. Konstantinou, "Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations," *IEEE Systems Journal*, vol. 17, no. 4, pp. 6695–6709, 2023.

[4] J. Chen, J. Yan, A. Kemmeugne, M. Kassouf, and M. Debbabi, "Cybersecurity of distributed energy resource systems in the smart grid: A survey," *Applied Energy*, vol. 383, p. 125364, 2025.

[5] E. Viganò, M. Loi, and E. Yaghmaei, *Cybersecurity of Critical Infrastructure*. Springer International Publishing, 09 2019.

[6] W. Grange, "His power level is over 9000! vulnerabilities in solar panel controllers," RSA Conference, May 2021.

[7] S. Ramezanian and V. Niemi, "Cybersecurity education in universities: A comprehensive guide to curriculum development," *IEEE Access*, vol. 12, pp. 61 741–61 766, Apr 2024.

[8] D. Huitema and A. Wong, "A case study in gamification for a cybersecurity education program: A game for cryptography," 2025.

[9] P. Buckley and E. Doyle, "Gamification and student motivation," *Interactive Learning Environments*, vol. 24, no. 6, pp. 1162–1175, 2016.

[10] S. Park, R. Kamali-Sarvestani, J. Giraldo, H. Nademi, and M. Parvania, "Importance of cyber-physical security training in electrical engineering education," in *2024 ASEE Annual Conference & Exposition*, ser. Modern Teaching Strategies in Engineering, 2024.

[11] Q. Xu, Y. Liu, and X. Li, "Unlocking student potential: How ai-driven personalized feedback shapes goal achievement, self-efficacy, and learning engagement through a self-determination lens," *Learning and Motivation*, vol. 91, p. 102138, 2025.

[12] J. G. Hall, A. Mohanty, P. Murarisetty, N. D. Nguyen, J. C. Bahamón, H. Ramaprasad, and M. Sridhar, "Criminal investigations: An interactive experience to improve student engagement and achievement in cybersecurity courses," in *Proceedings of the 53rd ACM Technical Symposium on Computer Science Education V. 1*, ser. SIGCSE 2022. New York, NY, USA: ACM, 2022, pp. 491–497.

[13] Enphase Energy, "IQ gateway," https://enphase.com/en-au/store/communication/iq-gateway, 2025, accessed: 2025-09-19.

[14] E. Energy, "How does the enphase home energy system work?" https://support.enphase.com/s/article/how-does-the-enphase-energy-system-work, 2023, accessed: 2025-09-18.

[15] A. N. Saleem, N. M. Noori, and F. Ozdamli, "Gamification applications in e-learning: A literature review," *Tech Know Learn*, vol. 27, pp. 139–159, 2022.

[16] A. Khaldi, R. Bouzidi, and F. Nader, "Gamification of e-learning in higher education: a systematic literature review," *Smart Learning Environments*, vol. 10, p. 10, 2023.

[17] K. Palaniappan and N. M. Noor, "Gamification strategy to support self-directed learning in an online learning environment," *International Journal of Emerging Technologies in Learning (iJET)*, vol. 17, no. 3, pp. 104–116, February 2022.

[18] A. Carreiro, C. Silva, and M. Antunes, "The use of gamification on cybersecurity awareness of healthcare professionals," *Procedia Computer Science*, vol. 239, pp. 526–533, 2024, cENTERIS – International Conference on ENTERprise Information Systems / ProjMAN - International Conference on Project MANagement / HCist - International Conference on Health and Social Care Information Systems and Technologies 2023.

[19] N. Chouliaras, G. Kittes, I. Kantzavelou, L. Maglaras, G. Pantziou, and M. A. Ferrag, "Cyber ranges and testbeds for education, training, and research," *Applied Sciences*, vol. 11, no. 4, 2021.

[20] A. H. A. Hanafi, H. Rokman, A. D. Ibrahim, Z.-A. Ibrahim, M. N. A. Zawawi, and F. A. Rahim, "A ctf-based approach in cyber security education for secondary school students," *European Journal of Computer Science and Information Technology (EJCSIT)*, vol. 7, no. 1, 2021, published 2021-10-22.

[21] S. V. Cole, "Impact of capture the flag (ctf)-style vs. traditional exercises in an introductory computer security class," in *Proceedings of the 27th ACM Conference on Innovation and Technology in Computer Science Education Vol. 1*, ser. ITiCSE '22. New York, NY, USA: Association for Computing Machinery, 2022, p. 470–476.

[22] V. Ford, A. Siraj, A. Haynes, and E. Brown, "Capture the flag unplugged: an offline cyber competition," in Proceedings of the *48th ACM Technical Symposium on Computer Science Education Technical Symposium on Computer Science Education*, ser. SIGCSE '17. New York, NY, USA: Association for Computing Machinery, 2017, p. 225–230. [Online]. Available: https://doi.org/10.1145/3017680.3017783

[23] TryHackMe, "Tryhackme: Learn cybersecurity through real-world challenges," https://tryhackme.com/, accessed: 2025-08-28.

[24] SimSpace, "Gamified cyber ranges: Revolutionizing ot cybersecurity training," 2025. [Online]. Available: https://simspace.com/blog/gamified-cyber-ranges-revolutionizing-ot-cybersecurity-training/

[25] D. Antonioli, "The swat security showdown (s3) ctfs," 2017. [Online]. Available: https://francozappa.github.io/files/slides/cps-spc17.pdf

[26] Naval Postgraduate School, "Cyberciege - center for cybersecurity and cyber operations," 2025. [Online]. Available: https://nps.edu/web/c3o/cyberciege

[27] Masaryk University, "Kypo cyber range platform," 2025. [Online]. Available: https://crp.kypo.muni.cz/

[28] G. F. Reed and W. E. Stanchina, "Smart grid education models for modern electric power system engineering curriculum," in *IEEE PES General Meeting*, 2010, pp. 1–5.

[29] Office of Cybersecurity, Energy Security, and Emergency Response, "Building the next generation of cyber-informed engineers and engineering designs," https://www.energy.gov/ceser/articles/building-next-generation-cyber-informed-engineers-and-engineering-designs-0, Dec. 2024, accessed: 2025-08-29.

[30] V. L. Wright, J. P. Meng, R. S. Anderson, J. R. Gellner, L. B. Barnes, S. D. Chanoski, R. M. Edsall, M. R. Holtz, J. M. Jones, K. L. Le Blanc *et al.*, "Cyber-informed engineering implementation guide," 09 2023. [Online]. Available: https://www.osti.gov/biblio/1995796

[31] J. Xie, J. C. Bedoya, C.-C. Liu, A. Hahn, K. J. Kaur, and R. Singh, "New educational modules using a cyber-distribution system testbed," *IEEE Transactions on Power Systems*, vol. 33, no. 5, pp. 5759–5769, 2018.

[32] C. Foreman, M. Turner, and K. Perusich, "Educational modules in industrial control systems for critical infrastructure cyber security," in *2015 ASEE Annual Conference & Exposition*. ASEE, 2015, pp. 26–573.

©2026 The Author(s) | Creative Commons CC BY 4.0

[33] T .-S. Chou, "An interactive learning system for cyber security education," in *2019 Conference on Industry and Education Collaboration (CIEC)*. ASEE, 2019.

[34] S. Bird and E. Loper, "NLTK: The natural language toolkit," in *Proceedings of the ACL Interactive Poster and Demonstration Sessions*. Barcelona, Spain: Association for Computational Linguistics, Jul. 2004, pp. 214–217. [Online]. Available: https://aclanthology.org/P04-3031/

[35] K. Salen and E. Zimmerman, Rules of Play: *Game Design Fundamentals*. Cambridge, MA: The MIT Press, 2003.

[36] C. Crawford, *Chris Crawford on Game Design*. Indianapolis, IN: New Riders Publishing, 2003.

[37] Meta, "React - a javascript library for building user interfaces," https://reactjs.org, 2025, accessed: 2025-09-09.

[38] MongoDB, Inc., "MongoDB," *Official Documentation*, 2025. [Online]. Available: https://www.mongodb.com/

[39] Cybersecurity and Infrastructure Security Agency (CISA), "Russian government cyber activity targeting energy and other critical infrastructure sectors," Cybersecurity and Infrastructure Security Agency (CISA), Tech. Rep. TA18-074A, March 2018, https://www.cisa.gov/news-events/alerts/2018/03/15/russian-government-cyber-activity-targeting-energy-and-other-critical-infrastructure-sectors.

[40] E. Boese, "Just-in-time learning for the just google it era," in *Proceedings of the 47th ACM Technical Symposium on Computing Science Education*, ser. SIGCSE '16. New York, NY, USA: Association for Computing Machinery, 2016, pp. 341—-345.

[41] NIST Computer Security Resource Center, "Spoofing - glossary," NIST IR 8323r1 from CNSSI 4009-2015, 2023, https://csrc.nist.gov/glossary/term/spoofing.

[42] Enphase Energy, "CVE-2020-25754: Enphase envoy r3.x and d4.x custom pam module authentication bypass," 2020, accessed: 2025-09-18. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2020-25754

[43] S. Kulandaivel, S. Jain, J. Guajardo, and V. Sekar, "Cannon: Reliable and stealthy remote shutdown attacks via unaltered automotive micro-controllers," in *2021 IEEE Symposium on Security and Privacy (SP)*, 2021, pp. 195–210.

[44] Dutch Institute for Vulnerability Disclosure, "CVE-2024-21880: Command injection in enphase iq gateway," 2024, accessed: 2025-09-18. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2024-21880

[45] Matthew1471, "Enphase public api project," https://github.com/Matthew1471/Enphase-API/blob/main/Documentation/IQ%20Gateway%20API/IVP/Mod/EID/Mode/Power.adoc, 2024, unofficial Enphase-API documentation hosted on GitHub.

[46] F. Barr-Smith, X. Ugarte-Pedrero, M. Graziano, R. Spolaor, and I. Martinovic, "Survivalism: Systematic analysis of windows malware living-off-the-land," in *2021 IEEE Symposium on Security and Privacy (SP)*, 2021, pp. 1557–1574.

[47] U.S. Department of Health and Human Services, "Living off the land (lotl)," 2024, accessed: 2025-09-15. [Online]. Available: https://www.hhs.gov/sites/default/files/living-off-land-attacks-tlpclear.pdf

[48] MITRE Corporation, "Tid-216: Firmware update rollbacks allowed," 2025, accessed: 2025-09-15. [Online]. Available: https://emb3d.mitre.org/threats/TID-216.html

[49] Tesla, "CVE-2025-8321: Tesla wall connector firmware downgrade vulnerability," 2025, accessed: 2025-09-18. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2025-8321

[50] Center for Energy Security and Reliability (CESAR), "Center for energy security and reliability — UNC Charlotte," https://cesar.charlotte.edu/, 2026, accessed: 2026-01-19.

[51] Lockheed Martin Corporation, "The Cyber Kill Chain®," https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html, 2025, accessed: 2026-01-20.

[52] F. Skopik and T. Pahi, "Under false flag: using technical artifacts for cyber attack attribution," *Cybersecurity*, vol. 3, p. 8, 03 2020

[53] MITRE ATT&CK, "Techniques - ICS — MITRE ATT&CK®," https://attack.mitre.org/techniques/ics/, 2025, accessed: 2026-01-20.

[54] M. J. Assante and R. M. Lee, "The industrial control system cyber kill chain," SANS Institute, White Paper, 2015. [Online]. Available: https://www.sans.org/white-papers/36297

[55] L. Urciuoli, T. Männistö, J. Hintsa, and T. Khan, "Supply chain cyber security – potential threats," *Information & Security: An International Journal*, vol. 29, pp. 51–68, 01 2013.

[56] A. Singh and B. Gupta, "Distributed denial-of-service (ddos) attacks and defense mechanisms in various web-enabled computing platforms: Issues, challenges, and future research directions," *International Journal on Semantic Web and Information Systems*, vol. 18, pp. 1–43, 04 2022.

©2026 The Author(s) | Creative Commons CC BY 4.0