2026 ASEE ANNUAL CONFERENCE June 21–24, 2026 | Charlotte Convention Center, NC

Host Sponsor UNC Charlotte

Paper ID #51011

Teaching Device Security Through Physical Testbeds: A Hands-on Approach to Engineering Education and Workforce Development

Dr. Lauren Linkous, Virginia Commonwealth University

Dr. Lauren Linkous is a Postdoctoral Research Associate specializing in Machine Learning, electromagnetics, and automation. She received her Ph.D. in Engineering from Virginia Commonwealth University. She has extensive teaching experience across electrical engineering and computer science, including courses in circuits, medical device security, electromagnetics, and machine learning. She has developed curricula on RF optimization, AI/LLM applications, and wireless communication, guiding students through hands-on labs with industry-standard tools. She also holds an M.S. in Computer Science and dual B.S. degrees in Electrical Engineering and Physics from VCU.

Mr. Erwin Karincic, Virginia Commonwealth University

Erwin Karincic received B.S. and M.S. degrees in Computer Engineering from Virginia Commonwealth University (VCU) in 2020 and 2021, respectively. He is currently pursuing a Ph.D. degree from Virginia Commonwealth University. He is an experienced security researcher with focus on reverse engineering and exploit development. An avid learner in many different fields, his research interests are cyber security, reverse engineering, exploit development, Internet of Things, software defined radio, antenna analysis, and design. He currently holds 27 cyber security certifications.

Dr. Erdem Topsakal, Virginia Commonwealth University

Teaching Device Security Through Physical Testbeds: A Hands-on Approach to Engineering Education and Workforce Development

Abstract

Traditional cybersecurity education emphasizes theoretical knowledge and case study analysis, which inadequately prepares students for real-world embedded security challenges and current workforce demands in critical industries such as healthcare. This work reports on an eight-semester implementation of a hands-on, research-based approach for teaching embedded systems security to undergraduate students through a medical device hardware testbed. The curriculum is delivered as a multi-semester undergraduate elective course at a four-year university; it adapts the Course-based Undergraduate Research Experience (CURE) model within a Vertically Integrated Projects (VIP) program structure, where students work across multiple semesters with peers, graduate student mentors, and faculty to gain authentic research experience in device security assessments.

This work details the pedagogical framework and teaching strategies supporting this testbed-centered experiential learning implementation. Core instructional activities include hardware-based programming in Python and C/C++ for device interfacing, device disassembly and hardware analysis, wireless communication security with software-defined radio experimentation, and vulnerability analysis of software and firmware. Instructional materials are organized into differentiated learning pathways that accommodate varying student backgrounds and are scaffolded to ensure appropriate challenge levels.

Assessment data demonstrates improvements in technical competency and workforce readiness, with students developing the cross-disciplinary skills demanded by employers in embedded security fields. Students report increased confidence in hands-on security analysis and complete research projects for portfolios showcasing applied skills. The vertically integrated structure benefits student retention, with continuing undergraduate students developing mentorship skills while reinforcing their technical knowledge. Reflections on course effectiveness and applicability to other courses are included. Teaching strategies, assessment techniques, and sample tutorials are included as supplementary material.

1 Introduction

As embedded systems become increasingly prevalent across critical industries such as healthcare, automotive, and industrial control, integrating device security into undergraduate education has become essential to meet current workforce demands [1, 2, 3]. Traditional educational approaches in engineering programs typically emphasize theoretical knowledge and case study analysis, which inadequately prepare students for the complexities of real-world embedded security challenges [1, 4, 5]. The gap between classroom instruction and industry requirements has become particularly pronounced in specialized domains like medical device security, where practitioners must possess both theoretical understanding and practical skills in hardware

analysis, wireless communications, and vulnerability assessments [2]. To address this disparity, educational institutions are increasingly adopting laboratory-based curricula that provide students with hands-on experience in authentic scenarios using real devices.

This work reports on an eight-semester implementation of a hands-on, research-based experiential learning approach for teaching embedded systems security to undergraduate students through a medical device security focused testbed. This includes providing background to students from undergraduate majors not typically aligned with security research. We describe the development and refinement of an adaptive curriculum framework deployed as a multi-semester undergraduate elective course at Virginia Commonwealth University (VCU), a public four-year research institution in Richmond, VA, USA.

Our pedagogical approach adapts the CURE framework through VCU's VIP program structure, which enables undergraduate students to work across multiple semesters within a research laboratory alongside graduate student mentors and faculty. In this work, we focus on one team within the principal investigator's (PI) research group. This research group typically features several interdisciplinary teams within the same course section. The course blends research-based and laboratory-based approaches, teaching applied experimental techniques and systematic methodologies for investigating device-level security. This is primarily done through core activities including hardware-based programming in Python and C/C++ for device interfacing, physical device disassembly and hardware analysis, wireless communication security, and vulnerability analysis of software and device firmware. Instructional materials are organized into differentiated learning pathways that accommodate varying student backgrounds and are scaffolded to ensure appropriate challenge levels for all participants [6].

Over eight semesters, we have collected assessment data demonstrating improvements in student technical competency, research skills, and workforce readiness. Students report increased confidence in hands-on security and device analysis and successfully complete research projects for portfolios showcasing applied skills. In the PI's research group, and the broader department, the vertically integrated structure particularly benefits student retention, with continuing students developing mentorship capabilities while reinforcing their technical knowledge. Graduate student mentors gain valuable pedagogical experience, and faculty benefit from sustained research collaboration with motivated undergraduate contributors. Instructional materials created in this course have also been adopted and applied by instructors of other courses at VCU.

The key contributions of this work are as follows:

1. We provide an in-depth examination of one institution's evolution in teaching embedded security, providing a temporal perspective on curriculum adaptation, student outcomes, and pedagogical refinement.
2. We describe a synthesis of peer mentoring structures as applied to STEM topics, analyzing their application to cybersecurity education and documenting benefits for student retention and skill development.
3. We provide a critical examination of which pedagogical elements from the case study are generalizable to other institutions, course formats, and technical domains, with considerations of resource requirements and constraints.

4. We provide access to supplementary material, including lesson methodology, supporting tools, and sample tutorials.

This work is organized as follows: Section 2 surveys the current state-of-the-art, with consideration towards undergraduate engineering implementation. Section 3 provides an overview of the program implemented at the university where this course is provided, and other variations within the university. Section 4 discusses course objectives, student outcomes, and provides references to sample student work. Section 5 contains information on the online repository and publicly available course materials. Finally, Section 6 concludes this work.

2 Background

Modern healthcare operation and delivery depends extensively on networked medical devices, with embedded systems now integral to all parts of conventional treatment. This includes patient monitoring, diagnostic imaging, therapeutic delivery, surgical procedures, equipment tracking, and personnel organization. The proliferation of connected medical devices has transformed clinical care while simultaneously expanding the attack surface for potential security vulnerabilities [2, 3, 7, 8]. Entry points for malicious actors now exist in commonplace technology from insulin pumps and pacemakers to infusion systems and ventilators, all of which incorporate complex embedded computing systems that communicate wirelessly, interface with electronic health records, and operate continuously in life-sustaining roles [2, 7].

The convergence of traditional medical device functionality with network connectivity and data exchange capabilities has created a cyber security challenge that extends beyond conventional IT security concerns [1, 8, 9]. In 2015, it was reported that 94% of health care organizations had been the victim of a cyber attack [3]; more recently, it was reported that 13% of healthcare organizations experienced a ransomware attack within 2024 [10]. Cybersecurity is no longer applicable to only infrastructure, modern security concerns now include implantable devices with advanced attack vectors [8, 11], which have seen recalls in recent years such as the FDA recalls of approximately 465,000 pacemakers in 2017 [12], and alerts issued for Medtronic insulin pump vulnerabilities in 2019 [13], which was reportedly the first recall of a diabetes device due to cyber security risks. To fully address modern-day medical technology requires specialized knowledge of both embedded systems architecture and healthcare-specific constraints.

Traditional cybersecurity education has predominantly relied on lecture-based instruction supplemented by controlled laboratory exercises and case study analysis. These approaches effectively convey theoretical foundations and allow students to build foundational skills while examining documented security incidents. Case studies are particularly valuable for illustrating vulnerabilities and attack scenarios, providing students with structured narratives that demonstrate how security incidents unfold and are resolved. However, this instructional format inherently presents security challenges as completed stories with identified problems, solutions, and outcomes. This composition may limit opportunities for students to develop the investigative instincts, troubleshooting persistence, and iterative problem-solving approaches required when confronting novel or poorly documented security issues in professional settings. As modern medical device security continues to evolve, the workforce increasingly demands engineers and problem solvers who can navigate the intersection of hardware engineering, software

development, wireless communications, regulatory compliance, and domain-specific operational constraints. This demand requires a demographic that benefits strongly from experiential learning opportunities alongside traditional instruction.

The CURE model is a pedagogical framework that integrates authentic research activities into undergraduate coursework, providing students with investigative experiences traditionally reserved for graduate programs or summer research internships. This model has been broadly implemented, and well reported, by educators across fields [4, 5, 14, 15, 16, 17, 18]. When implemented, it has a direct, positive impact on student learning outcomes, particularly in developing scientific thinking skills, technical competencies, and research self-efficacy. This model is well-suited for embedded security education because vulnerability assessment of medical devices inherently involves unknown outcomes. This open-endedness requires students to engage in genuine investigation where answers cannot be predetermined by instructors. Medical device security also provides broadly relevant research questions with direct societal impact on patient safety and healthcare infrastructure, increasing student motivation while allowing undergraduate contributions to address real-world security gaps in operational technology [1].

The course featured in this work is part of the VIP program, where research is structured in semester-long courses where undergraduate students work with faculty and graduate students on long-term, multi-semester research projects. Project teams are often multidisciplinary across both academic majors and projects, and may have multiple faculty overseeing a course. This program builds on the concept of the CURE model, among others, to introduce emphasis on multidisciplinary projects, collaboration between students of different academic backgrounds, and mentorship opportunities for faculty and graduate students. The VIP structure has demonstrated success in developing both technical competencies and professional skills, with evidence showing improved student retention [19, 20, 21, 22, 23]. The elective credit VIP course is a popular course in the College of Engineering at the four-year university where this work is focused. Some project teams within the department have run uninterrupted for over 15 years, with rotating groups of students iterating on projects and publications. The course section discussed in this work leverages both the CURE and VIP frameworks to create a medical device security research experience that combines authentic investigation with vertically integrated mentoring.

The Medical Device Security Testbed at VCU provides students with access to authentic research infrastructure containing over 50 network capable medical devices, ranging from patient monitors and electrocardiogram (ECG) systems to ultrasound machines and IoT devices with known vulnerabilities. Alongside this, the testbed provides more than 60 commercial tools including software-defined radios (SDRs), hardware debugging interfaces, and reverse engineering equipment. This infrastructure supports student research across offensive security and penetration testing, secure-by-design device analysis, and machine learning applications for patient-specific device customization. The authentic research environment enables students to progress beyond simulated exercises to contribute meaningful security assessments of real-world healthcare technology.

Students working in this testbed come from diverse academic backgrounds, including many from the biomedical engineering program, who possess strong domain knowledge but limited exposure to low-level hardware programming or security concepts. Exposing students to authentic research

experiences outside their primary major allows them to develop the interdisciplinary fluency essential for addressing complex security challenges while simultaneously building technical depth through hands-on experimentation with real devices. This experiential approach enables students to encounter the ambiguity, resource constraints, and iterative investigation processes characteristic of professional security research.

3 Course Design

This section describes the implementation of a VIP course focused on medical device security research within a specialized testbed environment. The course structure, curriculum design, and basic student demographics are detailed across eight semesters of operation from Spring 2022 through Fall 2025, following the course's post-pandemic reconstitution.

3.1 Course Description

The VIP course in this work is a semester-long elective credit course under a faculty PI that undergraduates may take for either 1 or 2 credit hours per semester. Students must earn a total of 4 credit hours with a minimum grade of C in order for these credits to be eligible to count toward a technical or departmental elective. Students can take a maximum of 8 credit hours of VIP as technical elective credits in their degree program. More restrictive requirements may be imposed by individual departments, and prerequisites for specific projects are managed by the individual course PIs.

The PI for the course in this work has several VIP teams divided based on topic. Undergraduate student teams are typically 2-5 students led by a PhD student in their second year or later. All student teams are active in one of several research spaces, where their shared responsibilities are to find and analyze publications, validate and recreate experiments, and propose their own experiments. Individual teams have their own specific objectives, but all teams are responsible for submitting (1) semester-long project documentation of their research and activities, (2) a midterm semester report, and (3) a final written report accompanied by a group presentation. Teams meet weekly with their graduate student mentor for updates, hands-on lessons, and supervised laboratory research.

3.2 Testbed Instructional Environment

The project team described in this work operates out of a medical device security themed testbed designed to replicate a hospital environment and network infrastructure [24]. The Medical Device Security Testbed at VCU provides students with access to authentic research infrastructure that enables investigation of real-world security vulnerabilities in operational healthcare technology. The testbed contains over 50 medical devices on an isolated network configured for testing, ranging from portable equipment such as patient monitors, Continuous Positive Airway Pressure (CPAP) machines, and ECG systems to stationary devices including an ultrasound machine and Wi-Fi enabled hospital bed. An assortment of common IoT devices have been selected based on known vulnerabilities, including baby monitors and wearable medical sensors for ECGs, heart rate, pulse and blood oxygen, and glucose monitoring. This diverse device inventory allows students to encounter the heterogeneous technology landscape characteristic of modern healthcare

environments. Devices are acquired without medical data and verified clear before student use. A responsible disclosure process is in place to handle any vulnerabilities students may discover.

Within this testbed environment, students develop competencies across several foundational areas. Core skills include basic microcontroller programming, sensor data collection, and wireless data transmission and reception using SDRs for wireless protocol analysis. Students receive instruction in device and electrical safety protocols essential for medical device teardown and analysis, ensuring safe handling of powered equipment and proper use of laboratory instruments. Hardware analysis skills encompass PCB design interpretation, hardware interface identification, and circuit tracing techniques. Students progress to reverse engineering methodologies using industry-standard commercial tools, including oscilloscopes, function generators, logic analyzers, and specialized debugging interfaces. This infrastructure supports student research across three focus areas: offensive security and penetration testing to identify vulnerabilities and recommend mitigations, secure-by-design device analysis incorporating multi-level safety monitoring, and machine learning applications for customizing device operation based on patient-specific biometrics. More than 60 commercial tools are available for student and collaborator use within the testbed. The authentic research environment allows students to progress beyond simulated exercises to contribute meaningful security assessments of real-world healthcare technology.

Beyond the VIP team, this testbed supports collaborative workforce development efforts and research partnerships. The facility hosts workshops, outreach events, tours, and instructional activities that expose students to real-world equipment and scenarios. This includes collaborations with other faculty for hands-on course assignments using the equipment for applications unrelated to security, as well as joint publications on specific vulnerabilities and attack vectors. Graduate students have leveraged the testbed to develop curricula based on its resources, pilot these materials within the facility, and deploy them in external instructional and workforce development programs [25, 26, 27, 28].

3.3 Ethics and Responsible Disclosure

Students working within the testbed participate in discussions of the ethical handling of medical devices and personal data. While devices purchased for testbed experimentation were acquired from authorized vendors with data sanitation policies, the risk of extracting potentially identifiable information from a used or refurbished device is non-zero. Policies are in place for disclosure to the PI and the device vendor or reseller. The vulnerability disclosure policy for students and collaborators follows a similar process through the PI and device companies.

There is a zero-tolerance policy in place for wireless experimentation on medical devices outside of anechoic chambers and other shielded environments.

3.4 Post-COVID-19 Restructure

This elective course was downsized during the COVID-19 pandemic when the university moved to virtual instruction in the Spring 2020 semester. Students already enrolled in the course were allowed to continue in order to fulfill their credit requirements, but new students were not

accepted due to the nature of the course being reliant on hands-on instruction in a research laboratory.

Following the university's return to predominantly in-person instruction in Fall 2021, the course was reconstituted with a new cohort of undergraduate students, including the project team that this work focuses on. While several graduate student mentors within the PI's research group had prior experience with the VIP program structure, the research team also integrated newly admitted graduate students during this period. The Fall 2021 restart necessitated the formation of new project teams and research initiatives to accommodate the refreshed participant composition.

The following sections detail the implementation and outcomes specifically for the project team working within the hardware-based medical device security testbed under the PI's supervision.

3.5 Course Demographics

The VIP course run by the faculty PI, including the project team in this work, had approximately 60 undergraduate students contribute to active research projects during the Spring 2022 - Fall 2025 time frame. This number includes graduate students, undergraduate student volunteers, and undergraduate students enrolled in the course for elective credit. Undergraduate volunteers fell into several categories: (1) students seeking short-term experience or topic exposure without a multi-semester commitment (typically one semester), (2) students completing existing projects while experiencing scheduling conflicts with classes or work, (3) students finishing projects requiring less than a full semester, and (4) recent graduates completing publication work. Summer research was conducted by graduate students only. Undergraduate volunteers had no required weekly or semester-long time commitments and could participate in research activities as their schedules allowed, though they were not expected to contribute at the same level as enrolled students. All student contributions were recognized in resulting research outputs and publications.

The students on the project team in this work were not typically volunteers. The table below, 1, presents their demographic data by semester, which mirrors that of the PI's broader VIP team. Despite being housed in Electrical and Computer Engineering, the course's biomedical security focus drew substantial enrollment from Biomedical Engineering students, particularly those in the instrumentation specialization. During this period, one student transferred to another university and did not complete all three semesters. Another student took two semesters of co-op, and then finished the third semester of VIP.

3.6 Curriculum Design and Program Outcomes

A set of modular instructional units has been developed and maintained for this course since 2020, with at least one unit added each semester following student testing and feedback. Each unit consists of 3-5 lectures accompanied by at least three hands-on activities and demonstrations, culminating in a team project. Depending on student background, units typically require 2-5 weeks to complete, though some teams demonstrate sufficient proficiency to skip introductory material and proceed directly to advanced content.

Table 1: Course enrollment and student demographics across eight semesters

Metric	Spr 2022	Fall 2022	Spr 2023	Fall 2023	Spr 2024	Fall 2024	Spr 2025	Fall 2025
Total Students	2	3	3	4	3	5	7	7
Volunteers	0	0	0	0	0	1	2	2
Returning Students	1	1	3	2	1	2	5	5
Major	CS (1), ECE (1)	BME (2), ECE (1)	BME (2), ECE (1)	BME (3), ECE (1)	BME (2), ECE (1)	BME (1), ECE (3), MATH (1)	BME (5), ECE (1), MATH (1)	BME (5), ECE (1), MATH (1)
Academic Year	Sph(1), Sr(1)	Jr (3)	Jr (3)	Fr(1), Sr(2)	Fr(1), Sr(2)	Jr (5), Sr(2)	Jr (5), Sr(2)	Sr (5), Grad (2)

The unit collection includes both sequential series that build on prior knowledge and standalone modules that can be taught independently. Unit difficulty can be adjusted for students working at varying levels or, in some cases, substituted with related advanced units. Units are adapted to each semester's theme, though core instructional content remains largely consistent. For instance, a firmware extraction unit can be completed using either a known vulnerable device or a microcontroller designed for such purpose depending on student competency. Open-source hardware is often used in entry-level units to provide students opportunities to experiment with equipment that is less costly to replace.

Over eight semesters of implementation, several key observations have emerged regarding curriculum effectiveness and student outcomes. The vertically integrated structure has demonstrated particular value for student retention and long-term engagement. Multiple undergraduate students who began in the VIP program continued into graduate studies, with several remaining in the same research laboratory, a trajectory that speaks to both the quality of research experience and the mentorship relationships developed through the program. Other VIP alumni have pursued industry positions in embedded security or applied skills developed in the course to adjacent technical fields.

While some students are recruited from courses taught by program instructors, the PI's course section employs an informal interview process in which interested students tour the laboratory, observe ongoing projects, and meet graduate student mentors. This process has positively influenced student retention, enabling students to more accurately gauge their interest and topic compatibility before committing. These selection factors should be considered when generalizing findings to other institutional contexts.

The longevity of the program, running continuously with iterating student cohorts, provides evidence of its sustainability and adaptability. Curriculum adaptations have been driven by both student feedback and evolving research directions, with the modular unit structure enabling responsive updates without complete course redesign. Faculty have benefited from sustained research collaboration with motivated undergraduates, with students contributing to

peer-reviewed publications during their time in the program [29, 30, 31].

3.7 Course Material and Implementation

The course material is organized into four primary categories that collectively address the competencies required for embedded device security research. The hardware-based programming category introduces students to Python and C/C++ for device interfacing, microcontroller programming, and sensor data collection, with students progressing from basic scripting to developing custom tools for interacting with medical device hardware and communication protocols. The wireless communication and software-defined radio category covers signal capture, analysis, and interpretation for protocols such as Bluetooth, Wi-Fi, and proprietary RF communications, emphasizing both theoretical foundations of signal processing and practical skills with SDR hardware and software tools. The device disassembly and hardware analysis category builds reverse engineering competencies through safe teardown procedures, PCB analysis, circuit tracing, and hardware interface identification using industry-standard tools. Finally, the vulnerability analysis and attack surface assessment category teaches systematic approaches to identifying security weaknesses in software and firmware, integrating concepts from the other categories to enable comprehensive security assessment.

Units from these categories are combined each semester around thematic topics that provide coherence and real-world context for the technical skills being developed. Semester topics have included Linux basics and state machine programming with hardware (Spring 2022), memory forensics and automating medical device memory dumps (Fall 2022), unintentional RF emissions and RF detection of bitcoin miners (Spring 2023), electrical characterization of infected devices and wireless communications design (Fall 2023), wireless hospital asset tracking and wearable biometric sensing for patients (Spring 2024), hardware reverse engineering and serial communications (Fall 2024), reverse engineering circuitry and large language models for engineering applications (Spring 2025), firmware extraction and machine learning (Fall 2025). Moving forward, the current semester (Spring 2026) will focus on hardware interfacing, data streams, and wireless communications.

The modular unit structure allows flexible adaptation to each semester's thematic focus while maintaining consistent learning objectives across the four content categories. For example, the hardware-based programming units can be applied to Linux basics and state machine development (Spring 2022), automated memory dump collection (Fall 2022), or interfacing with wearable biometric sensors (Spring 2024). With this model, the core programming competencies remain constant while the application context changes. Similarly, wireless communication units support investigations of unintentional RF emissions from bitcoin miners (Spring 2023), asset tracking systems (Spring 2024), or contemporary wireless protocols (Spring 2026). Hardware analysis units scaffold from basic device teardown in early semesters to advanced circuit reverse engineering (Spring 2025) and firmware extraction (Fall 2025), with unit difficulty adjusted based on cohort experience and topic complexity. This approach enables students entering at different semesters to build foundational skills through introductory units while more experienced students tackle advanced applications aligned with the semester theme. The firmware extraction unit exemplifies this flexibility: it can be delivered using Arduino hardware for students requiring foundational experience or applied to vulnerable medical devices for advanced investigation,

ensuring appropriate challenge levels regardless of the semester's specific focus. Samples of this material is provided open-source at [6], and discussed further in Section 4.3. More of our published material is available at [25, 26, 27, 28, 32].

4 Outcomes and Assessment

At multiple points in the semester, both student and course outcomes are assessed to evaluate (1) student competency in the material, (2) student confidence in their mastery of topics, and (3) if the course material as planned still meets the course outcomes outlined at the beginning of the course. These evaluations occur at least monthly, with more substantial reflection at midterms to evaluate student work against halfway-point goals for the course. However, weekly check-ins during the one-hour group lecture serve as an early identifier to detect students struggling with concepts or assignments.

As the team featured in this work is project-centered rather than assessment or presentation-centered, there is flexibility for adaptation in lesson plans not typically seen in traditional or larger classrooms. In this work, individual units served as natural pivot points for adjusting topics or difficulty levels based on student progress and comprehension.

Student assessment in terms of grades is based on submitted assignments (team and individual), final group presentations, documentation (team and individual), and engagement with course material. The grading philosophy strongly encourages students to attempt work and iterate rather than achieving perfect results on the first attempt. This mirrors the actual research process, where methodology is often more important than immediate results, and trains undergraduate students in practices that transfer to workforce contexts. Final group presentations are used to share research topics and progress with the other teams in the PI's course, and to give students opportunity to practice discussing their research with new audiences.

Standard quantitative assessment includes semester-long project documentation of research and activities, a midterm report, and a final written report accompanied by a group presentation. Teams meet weekly with their graduate student mentor for updates, hands-on lessons, and supervised laboratory research, with the mentor tracking attendance and engagement.

In practice, students are also graded on their improved competency for applying industry standard tools to the exploratory process. Students gain experience with Keysight and Teledyne LeCroy wireless measurement equipment for advanced RF analysis. They are also introduced to ETS-Lindgren anechoic chambers and automated measurement systems for isolation testing and signal characterization. Industry standard tools such as Ida Pro, Binary Ninja, Linux-based penetration testing tools are available for usage on lab provided computers isolated via LAN. Using appropriate hardware for physical interfacing (Tigard, Bus Pirate, JTAGulator, etc.), logic analyzers (Saleae line), and device probing (oscilloscopes, multimeters, etc.), is included in practical student evaluations as part of the course grade.

4.1 Meeting Learning Outcomes

This course consistently addresses four ABET student outcomes that align with the research-based, hands-on nature of embedded security education [33]:

1) An ability to identify, formulate, and solve complex engineering problems by applying principles of engineering, science, and mathematics

4) An ability to recognize ethical and professional responsibilities in engineering situations and make informed judgments, which must consider the impact of engineering solutions in global, economic, environmental, and societal contexts

5) An ability to function effectively on a team whose members together provide leadership, create a collaborative environment, establish goals, plan tasks, and meet objectives

7) An ability to acquire and apply new knowledge as needed, using appropriate learning strategies

Additional ABET outcomes are addressed secondarily depending on the specific units and semester topics. When working with medical devices and cross-disciplinary students, some experimental units are deliberately structured to prioritize foundational skill development over open-ended exploration, affecting which outcomes receive emphasis in a given semester.

Student comprehension is evaluated through multiple assessment mechanisms throughout the semester. Technical competency is measured through hands-on practical demonstrations where students must successfully complete device interfacing tasks, wireless signal capture and analysis exercises, and vulnerability identification challenges. Written documentation and reports are evaluated for both technical accuracy and the student's ability to articulate complex security concepts to varied audiences.

Student confidence and engagement are assessed through both self-reported measures and observed behavior. At the beginning and end of each semester, students discuss their confidence in specific technical skills covered by the course material and identify ideas for growth. These self-assessments are compared against observed performance during laboratory sessions and project work. Graduate student mentors provide qualitative observations on student engagement, noting indicators such as question-asking behavior, willingness to attempt challenging tasks, and initiative in proposing research directions.

Engagement metrics also include attendance and retention data. Weekly meeting attendance is tracked by graduate student mentors and patterns of disengagement are addressed early through individual check-ins. Semester-to-semester retention within the VIP program serves as a longer-term indicator of student engagement, with returning students demonstrating sustained interest and providing mentorship to newer team members.

4.2 Student Feedback

Student feedback is collected through the semester during the weekly meetings and formally at the end of the semester through course evaluations. Feedback has been organized into four primary categories that inform ongoing curriculum development.

Course Topics and Student Interest. Feedback regarding course topics has been consistently positive across all eight semesters. Students report high levels of engagement with the material, citing the real-world applicability and hands-on nature of the work as primary motivators. However, as an elective course, the program inherently attracts students with pre-existing interest

in security and hardware topics, which likely contributes to these favorable responses on the topic material.

For students taking this course as a cross-disciplinary elective, interest has been driven primarily by the opportunity to work hands-on with medical devices rather than purely by security concerns. While cybersecurity motivates all course participants, the opportunity to reverse engineer and physically engage with medical devices in a laboratory setting often serves as the stronger draw, particularly for biomedical engineering students.

Difficulty of Materials. The most substantive feedback has concerned the difficulty of course materials, particularly given the cross-disciplinary nature of the project team. Students entering without functional programming experience, whether from previous coursework or independent learning, have reported frustration during early weeks due to the steep learning curve required to participate meaningfully in device interfacing and analysis tasks. This barrier has been partially addressed through differentiated learning pathways and peer mentoring from returning students, though it remains an area of ongoing curriculum refinement. Semesters with higher proportions of returning students have shown smoother onboarding for new participants, as experienced team members provide informal support alongside structured instruction.

Student Confidence. Student confidence metrics have shown positive trends, with end-of-semester self-assessments consistently higher than beginning-of-semester baselines across technical skill areas. Students report feeling more capable of approaching unfamiliar security challenges and more comfortable with the iterative, exploratory nature of research work.

Cross-disciplinary students particularly report increased confidence in their understanding of fundamental concepts such as circuits and electronics. While this gain is most pronounced among students from outside the ECE department where the course is hosted, building these foundational competencies across diverse academic backgrounds is an intentional course design goal.

Student Mastery and Application. Feedback on mastery and application of course topics presents a nuanced picture that varies by student trajectory and timing of enrollment. Several program alumni have continued into graduate studies in related fields or secured industry positions where they directly apply skills developed in the course. However, the program also serves students who enroll primarily out of intellectual curiosity rather than career alignment, and these students may not directly apply the technical skills in their subsequent professional work.

Application of Material beyond VIP. More immediate application of learned skills occurs for junior and senior students, who frequently transfer course material to concurrent coursework and capstone projects. The repeated reinforcement of wiring, circuits, wireless communication, and sensor integration through hands-on demonstrations provides immediately applicable skills. Programming experience proves particularly transferable, with students consistently applying concepts across multiple courses. Students who worked with Arduinos in VIP units preferentially selected Arduino platforms for projects in other courses, and those who used Python in VIP units chose Python over MATLAB when given the option in their other classes. When surveyed about these technology choices, students attributed them to the active, hands-on experience in the elective course, noting that tools were already configured and familiar from VIP work, lowering barriers to adoption in other contexts.

Instructors in other courses have also adopted units developed within the VIP course outlined in this work. Popular topics included Arduino-based sensor projects (wireless transmission, sensor data analysis), machine learning demonstrations (EMG-based grip identification, signal processing), patch antenna design, and firmware extraction. Several instructors were influenced by their undergraduate student TAs having either taken the VIP course, toured the research lab, or attended lectures as guests.

4.3 Student Work Samples

Extended samples of course materials and student work are provided open-source at [6]. This repository contains tutorials for material, some of which was created by students for the course as their documentation grade, while others were created by graduate student mentors. Not all semesters are equally represented in the repository, as topics such as machine learning, large language models, and pure research investigations produced fewer visual or tutorial-based artifacts suitable for public sharing. Key unit modules for this course have been released as standalone exercises that can be adopted by other instructors. Additional published materials from the program, including semester-long laboratory and activity series, are available at [25, 26, 27, 28, 32].

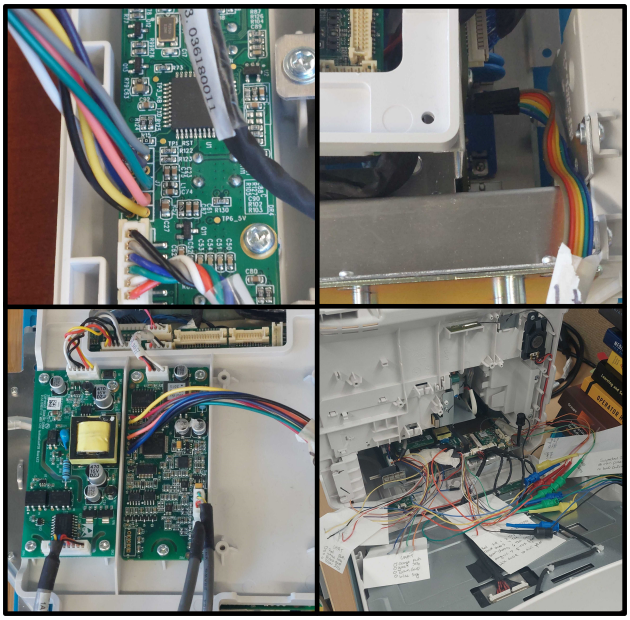

Figure 1: Four views of a disassembled patient monitor with wires connected to debug ports for interfacing with the device and understanding data transfer

Figure 1 shows an example of student work involving a patient monitor. The student disassembled the device, identified standard and proprietary interface ports, and worked on firmware extraction. Unintentional RF emissions were also investigated. This device subsequently served as a teaching platform for other students, demonstrating common hardware interfacing methods, PCB design principles, and patient-critical power distribution techniques.

Figure 2 shows a student-build wireless sensor assembly featuring an Arduino Leonardo,

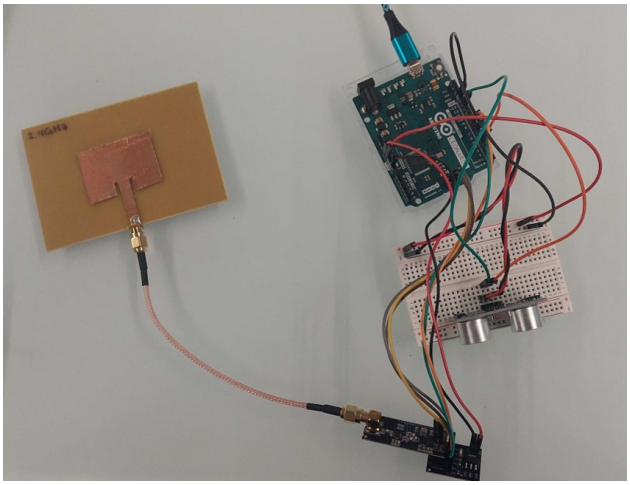

Figure 2: Student-fabricated wireless distance sensor with a custom 2.4 GHz patch antenna.

NRF24L01 transceiver module, hand-made 2.4 GHz microstrip-fed patch antenna on FR4 substrate, and a HC-SR04 Ultrasonic sensor. In this unit, students calculate antenna parameters, simulate the design with Ansys HFSS, and then fabricate the antenna. Students then wire the ultrasonic sensor to the Arduino, program data collection and analog data conversion to distance in centimeters, and transmit the data using the NRF24L01 module, bypassing the build in Wi-Fi TX/RX capabilities of the Arduino Leonardo. A receiving station displays the transmitted data on a laptop in real time.

5 Publicly Available Course Modules

Key course materials are available online at [6]. This includes example units, student work samples, and public details of testbed equipment. When applicable, related educational resources developed within the testbed are included.

6 Conclusion

This paper presents an eight-semester case study of teaching embedded systems security through a hands-on, research-based curriculum using a medical device security focused testbed. By integrating the CURE framework within a vertically integrated project structure, we created a learning environment where students engage in authentic security research while developing practical workforce-ready skills.

Our approach addresses a critical gap in traditional cybersecurity education, which often emphasizes theoretical knowledge and case study analysis at the expense of hands-on experimentation. Through hardware-based programming, device disassembly, wireless communication analysis with software-defined radios, and vulnerability assessment, students gain direct experience with the technical challenges they will encounter in professional practice. The medical device context provides both pedagogical value and societal relevance given the growing cybersecurity threats facing healthcare infrastructure.

Assessment data across eight semesters demonstrates meaningful improvements in technical competency and workforce readiness. Student reflections consistently indicate increased confidence in approaching complex security problems, and the vertically integrated mentoring structure has proven effective for student retention and knowledge transfer between cohorts. The progression from guided exercises to independent research projects enables students at different skill levels to contribute meaningfully while continuously developing their capabilities.

The pedagogical strategies, differentiated learning pathways, and assessment methods described in this work offer a transferable model for institutions seeking to strengthen practical cybersecurity education. Our experience suggests that research-based, hands-on instruction using physical security testbeds can effectively prepare students for the demands of embedded systems security work while fostering the critical thinking and adaptability that the rapidly evolving threat landscape requires.

References

[1] J.-P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, "Ethical hacking for iot: Security issues, challenges, solutions and recommendations," *Internet of Things and Cyber-Physical Systems*, vol. 3, pp. 280–308, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2667345223000238

[2] A. I. Newaz, A. K. Sikder, M. A. Rahman, and A. S. Uluagac, "A survey on security and privacy issues in modern healthcare systems: Attacks and defenses," *ACM Trans. Comput. Healthcare*, vol. 2, no. 3, Jul. 2021. [Online]. Available: https://doi.org/10.1145/3453176

[3] P. A. Williams and A. J. Woodward, "Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem," *Medical Devices: Evidence and Research*, vol. 8, pp. 305–316, 2015. [Online]. Available: https://www.tandfonline.com/doi/abs/10.2147/MDER.S50048

[4] S. Freeman, S. L. Eddy, M. McDonough, M. K. Smith, N. Okoroafor, H. Jordt, and M. P. Wenderoth, "Active learning increases student performance in science, engineering, and mathematics," *Proceedings of the National Academy of Sciences*, vol. 111, no. 23, pp. 8410–8415, 2014. [Online]. Available: https://www.pnas.org/doi/abs/10.1073/pnas.1319030111

[5] S. E. Rodenbusch, P. R. Hernandez, S. L. Simmons, and E. L. Dolan, "Early engagement in course-based research increases graduation rates and completion of science, engineering, and mathematics degrees," *CBE—Life Sciences Education*, vol. 15, no. 2, Jun 2016.

[6] L. Linkous (LC-Linkous), "Medical device security course notes." [Online]. Available: https://github.com/https://github.com/LC-Linkous/medical_device_security_course_notes

[7] K. Fu and J. Blum, "Controlling for cybersecurity risks of medical device software," *Commun. ACM*, vol. 56, no. 10, p. 35–37, Oct. 2013. [Online]. Available: https://doi.org/10.1145/2508701

[8] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel, "Pacemakers and implantable cardiac defibrillators: Software

radio attacks and zero-power defenses," in *2008 IEEE Symposium on Security and Privacy (sp 2008)*, 2008, pp. 129–142.

[9] M. Rushanan, A. D. Rubin, D. F. Kune, and C. M. Swanson, "Sok: Security and privacy in implantable medical devices and body area networks," in *2014 IEEE Symposium on Security and Privacy*, 2014, pp. 524–539.

[10] HIMSS, "2024 himss healthcare cybersecurity survey," Healthcare Information and Management Systems Society, Tech. Rep., 2024. [Online]. Available: https://www.himss.org/resources/himss-healthcare-cybersecurity-survey

[11] C. Li, A. Raghunathan, and N. K. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," in *2011 IEEE 13th International Conference on e-Health Networking, Applications and Services*, 2011, pp. 150–156.

[12] Aug 2017. [Online]. Available: https://abbott.mediaroom.com/2017-08-29-Abbott-issues-new-updates-for-implanted-cardiac-devices

[13] D. Klonoff and J. Han, "The first recall of a diabetes device because of cybersecurity risks," *Journal of Diabetes Science and Technology*, vol. 13, no. 5, p. 817–820, Jul 2019.

[14] D. A. Kolb, *Experiential learning: Experience as the source of learning and development*, 2nd ed. Pearson FT Press, 2014.

[15] L. C. Auchincloss, S. L. Laursen, J. L. Branchaw, K. Eagan, M. Graham, D. I. Hanauer, G. Lawrie, C. M. McLinn, N. Pelaez, S. Rowland, and et al., "Assessment of course-based undergraduate research experiences: A meeting report," *CBE—Life Sciences Education*, vol. 13, no. 1, p. 29–40, Mar 2014.

[16] L. A. Corwin, M. J. Graham, and E. L. Dolan, "Modeling course-based undergraduate research experiences: An agenda for future research and evaluation," *CBE—Life Sciences Education*, vol. 14, no. 1, Mar 2015.

[17] J. Bennie, K. Zhang, P. Yeh, J. C. Gill, L. Crowley, M. Bauer, and M. J. Graham, "Student interest development in course-based undergraduate research experiences (cures): A longitudinal case study analysis," *Frontiers in Education*, vol. 10, Apr 2025.

[18] Y. Zhu, C. Wang, D. I. Hanauer, and M. J. Graham, "Course-based undergraduate research experiences (cures) and student interest development: a longitudinal study investigating the roles of challenge, frustration, and meaning making," *Studies in Higher Education*, vol. 50, no. 6, pp. 1039–1054, 2025. [Online]. Available: https://doi.org/10.1080/03075079.2024.2361328

[19] J. Allebach, E. Coyle, and J. Krueger, "The vertically integrated projects (vip) program in ece at purdue: Fully integrating undergraduate education and graduate research," *2006 Annual Conference and Exposition Proceedings*, 2006.

[20] P. Rahme, G. E. Nasr, A. A. Tarhini, M. Elkhoury, and E. Fakhoury, "Bridging the gap: Integrating vertically integrated projects (vip) courses into university curricula," in *2025 ASEE Annual Conference & Exposition*. Montreal, Quebec, Canada: ASEE Conferences, Jun. 2025. [Online]. Available: https://peer.asee.org/56021

[21] N. Ramirez and C. B. Zoltowski, "First-year experiences – how the vertically integrated projects (vip) model addresses grand challenges and abet outcomes," in *2022 IEEE Frontiers in Education Conference (FIE)*, 2022, pp. 1–4.

[22] C. O. Stewart, C. Preza, and S. S. Ivey, "Two years of lessons learned from an nsf-iuse funded vertically integrated projects (vip) program at university of memphis," in *2025 ASEE Annual Conference & Exposition*. Montreal, Quebec, Canada: ASEE Conferences, Jun. 2025. [Online]. Available: https://peer.asee.org/55672

[23] M. G. Mitka, S. Narayanswamy, and I. Smith, "Developing teamwork in a multidisciplinary, multicohort curricular context: A case study of vertically integrated projects," *Journal of University Teaching and Learning Practice*, vol. 20, no. 4, Dec 2023.

[24] Commonwealth Cyber Initiative. (2024, Apr) Medical device security testbed. [Online]. Available: https://cci-cvn.org/mds/

[25] E. Karincic, L. Linkous, and E. Topsakal, "Interactive educational platform for digital modulation recognition and signal analysis," in *2026 United States National Committee of URSI National Radio Science Meeting (USNC-URSI NRSM)*, 2026.

[26] E. Karincic, L. Linkous, and E. Topsakal, "From classroom to career with practical network training," in *2024 ASEE Annual Conference and Exposition*. ASEE Conferences, 2024.

[27] E. Karincic, L. Linkous, and E. Topsakal, "Experiential radio frequency engineering education with machine learning focused signal processing labs," in *2026 ASEE Annual Conference and Exposition*, June 2026.

[28] E. Karincic, L. Linkous, and E. Topsakal, "Classroom approaches to rf education with visual-based modulation recognition labs," in *2026 ASEE Annual Conference and Exposition*, June 2026.

[29] J. Lundquist, L. Linkous, M. E. Piper, Z. Sickey, K. Zimmet, I. Mendoza, S. Suresh, and E. Topsakal, "Textile-based inkjet-printed rfids: Exploring wearable antennas in the real world [bioelectromagnetics]," *IEEE Antennas and Propagation Magazine*, vol. 66, no. 1, pp. 50–62, 2024.

[30] M. E. Piper, S. Hutson, W. Lohr, A. Milstein, M. Mangino, and E. Topsakal, "Implantable radio frequency identification tags for patient data recognition," in *2022 IEEE International Symposium on Antennas and Propagation and USNC-URSI Radio Science Meeting (AP-S/URSI)*, 2022, pp. 884–885.

[31] E. Karincic, L. Linkous, and E. Topsakal, "Generalized machine-learning particle swarm optimization antennas for cbrs," in *2023 United States National Committee of URSI National Radio Science Meeting (USNC-URSI NRSM)*, 2023.

[32] E. Karincic, E. Topsakal, and L. Linkous, "Patch antenna calculations and fabrication made simple for cyber security research," in *2023 ASEE Annual Conference & Exposition*, no. 10.18260/1-2–43974. Baltimore , Maryland: ASEE Conferences, June 2023, https://peer.asee.org/43974.

[33] ABET. (2025, Feb). [Online]. Available: https://www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-engineering-programs-2025-2026/