Library of Reconfigurable Immersive Attack and Defend Scenarios for Cybersecurity Research and Workforce Development

PI – R. A. Borrelli
IGEM Grant #23-001

Reporting period
07/01/24 - 12/31/24

Summary of progress towards proposed milestones I

Increased enrollment on the Idaho Falls campus	Employed three graduate students Heidi Codling, Henok Tadele, Tollan Berhanu. All are first generation college students and/or underrepresented students. Updated courses with hands-on, realistic activities. Received overwhelmingly positive student reviews and observed increased engagement. Drastically increased student participation to Cybersecurity courses. CYB 340 - Network Defense (from 6 students in Y2023 to 31 in Y2025).

Summary of progress towards proposed milestones II

Adversary-As-A-Service	Extended RADICL with additional power to support containerized network elements e.g., routers, switches, vulnerable servers, and malicious hosts. Implemented three alternative scenarios demonstrating different types of adversarial activity. Ransomware attack (Wannacry). Students learn to detect ransomware activity and analyze encryption behavior and propagation patterns. Distributed Denial of Service attack (Mirai). Students learn to analyze network traffic for DDoS patterns and implement defensive measures such as firewalls and load balancers. Data Exfiltration via Covert Channels (Heartbleed). Students recognize covert data exfiltration techniques and implement monitoring and alerting for anomalous traffic. Zero effort to setup by students and step-by-step guides with the scenarios are provided. Easy to define benign infrastructure of various scales and select desired attack.

Summary of progress towards proposed milestones III

Electrical grid with distributed generation and RTDS	Development began of the laboratory focused on power system communication and control systems Matching funds provided by UI to procure the real-time digital grid simulator
Private cloud environment	Support a large number of concurrently connected students ($>$ 100) performing scenarios that simulate large networks. Secure environment to perform attacks. No fear of attacks leaking to the outside world. Students do not have to pay for the infrastructure or share their private data. Offer security scenarios as-a-service.
Advanced Manufacturing Trainer	ISU procured an advance manufacturing trainer with PLC, HMI, conveyor, and robotic arm The trainer allows for realistic teaching and research related to industrial cybersecurity

Summary of progress towards proposed milestones IV

Industrial network security proficiency assessment	Student researchers began design of a hands-on industrial networking security proficiency evaluation The researchers developed a scenario, network diagram, software list, task list, and scoring rubric This exam will be used as an assessment instrument for students in the ISU industrial cybersecurity program
Curriculum Guidance Document	ISU, INL, DOE, and International Society of Automation published a 125-page document 'Curricular Guidance: Industrial Cybersecurity Knowledge' describing 559 terms that form a foundational body of knowledge for an OT security professional. The document is helpful for students, instructors, administrators and working professionals. A paper describing the effort to create the document won best paper at the 28th Colloquium for Information Systems Security Education.

Summary of progress towards proposed milestones V

Harvest strategy	ISU and University of Idaho won a $2.875M award from the National Institute of Standards and Technology to further the industrial cybersecurity research lab capability and enhance the research infrastructure at the UIIF Accepted pre-proposal DOE EPSCoR with ISU, and BSU. The project capitalizes on the infrastructure to support industrial metaverse educational scenarios.

Summary of expenditures and budget performance

Key insights

Expenditures on budget and in accordance with requirements

Year 2 – $532872

Challenges & Changes

Lack of personnel

Project moving along with change in PI

Category	Budgeted	Spent	±
Salary	$69038	$8798	$51816
Fringe	$11720	$120	$
Irregular help	$12960	$ –	$12960
Operational expenses	$29830	$ –	$29830
Capital equipment (over $5K)	$180000	$ –	$180000
Small equipment (under $5K)	$70000	$ –	$70000
Tuition	$26452	$6141	$20310
Subaward	$300000	$ –	$300000

Projection of work in next reporting period I

Integrate real-life cyberphysical components to RADICL in a hardware-in-the-loop fashion (lead: co-PI Kolias).

Implement two additional educational scenarios that replicate the Stuxnet and Trisis/Triton incidents (lead: co-PI Kolias).

Expose the RADICL service (and all implemented scenarios) as a remotely accessible service to ISU and selected Idaho Colleges (lead: co-PI Kolias).

Present demo at Engineering EXPO (lead: co-PI Kolias).

Move existing industrial cybersecurity courseware into an online delivery format (ISU)

Work with Idaho secondary teachers to deploy curricular materials into high schools (ISU)

Projection of work in next reporting period II

Propose graduate certificate in industrial cybersecurity to Idaho State Board of Education (ISU)

Deploy motor control trainers into the lab (ISU)

Test deployment of industrial networking security proficiency assessment (ISU)

Design hands-on control systems fundamentals proficiency exam (ISU)