Poster: Upcycling Computing Hardware Equipment for Security Education

Steven Ngo, Joshua Garcia
Informatics Dept.
University of California, Irvine
skngo1@uci.edu, joshug4@uci.edu

***Abstract*—Security education often requires a network environment for real-world, hands-on learning and experimentation (e.g., simulating a corporate network for penetration testing or testing configurations and defenses). Cloud services, self-hosted infrastructure (*homelabs*), and cyber ranges are all viable solutions to supporting such hands-on learning, but each has its advantages and disadvantages regarding convenience, skills learned, financial and administrative barriers, and learning curve. From a collaboration we have been cultivating since January 2024 with the National Upcycled Computing Collective, a non-profit organization that upcycles thrown-out IT infrastructure, we will explore a novel application of such equipment for security education. We will employ a mixed-method approach using semi-structured interviews, surveys, and empirical analysis and will develop models of the partnership between the non-profit and college-affiliated student organizations. We aim for our research plan to identify benefits, challenges, and findings that would enable a similar or greater degree of success for other educational and research institutions.**

***Index Terms*—security education, qualitative thematic analysis, user studies for security, upcycled technology, sustainability**

I. Introduction and Background

Going beyond lectures and rote learning to acquire hands-on practical knowledge within security education often requires a network environment that can be used to set up real-world services, applications, and servers for learners to experiment with [1], [2]. Having a network environment can enable setting up security configurations and defenses, conducting legal penetration tests and red-team exercises, and testing open-source and custom-made tools and scripts for offensive or defensive purposes. Cloud services can assist with the development and maintenance of network environments for security education purposes, but these come at a recurring cost, have terms of service that may restrict certain actions to hinder learning, and do not allow for complete control of the environment.

Homelabs—i.e., self-hosted information technology (IT) infrastructure and devices used to create small-scale, on-premise network environments—are built and maintained by security practitioners often out of their own homes for learning and experimentation [1], [3]. While homelabs may require an initial investment in hardware and come with a learning curve to set up and maintain, they can be used without restriction by a service provider. Although cloud services may be more convenient, learners miss out on hands-on experience of the fundamentals (e.g., networking, operating systems) that serve as the basis for more advanced education or research in IT, security, and development operations.

Homelabs are for usage at the individual level, and there exist education-oriented *cyber ranges* that provide IT infrastructure to power wide-scale security education in schools and universities [4]. The development and maintenance of such cyber ranges require extensive funding and are often managed at a few levels above students, preventing the acquisition of skills from direct access to computing and server infrastructure and creating administrative barriers. This state of affairs leaves opportunities open for solutions to scalable, hands-on security education and access to network environments.

IT teams and departments follow an IT equipment lifecycle to manage their organizations' infrastructure that powers everything digitally connected. These lifecycles include the procurement, installation, operation, maintenance, and disposal of IT equipment that happens every few years (e.g., every 3-5 years) to refresh IT infrastructure for performance, security, scalability, and financial purposes [5], [6]. When IT teams have to refresh their infrastructure, the old equipment does have to be disposed of in some way; some get recycled or donated, but a majority become electronic waste (e-waste), which wastes recoverable natural resources and contributes to environmental pollution. In 2022, 62 million tons of e-waste were produced, and only $\sim$22% of it was recycled, and the rest was estimated to be worth $62 billion USD [7].

The **N**ational **U**pcycled **C**omputing **C**ollective (NUCC), a non-profit organization that transforms e-waste into higher-quality items, or *upcycles* them, powers security education in student organizations and clubs in higher education by providing upcycled computing hardware equipment. Since January 2024, we have cultivated a collaboration with NUCC to explore the current utilization and further potential of upcycled equipment for security education. We aim to investigate the following research questions in our exploratory study of the usage of upcycled equipment for security education:

RQ1: How can upcycled computing hardware equipment be utilized specifically for security education?

RQ2: What are the benefits, challenges, and future directions of upcycled equipment for security education?

II. Methodology and Early Findings

To investigate **RQ1** and **RQ2**, we will employ a mixed-method approach, which includes semi-structured interviews, surveys, and empirical analysis to gather qualitative and quan-

titative data. Research participants in the aforementioned qualitative studies will include college students, alumni, faculty, and non-affiliated hobbyists who have received upcycled computing hardware equipment from NUCC. College-affiliated participants will come from a range of higher education institutions with varying focuses, including R1-research, teaching-focused, and community colleges. Many college-affiliated participants are also associated with college-affiliated student organizations and clubs, many of which are centered around security education and ethical hacking. Non-college-affiliated participants are either college alumni formerly affiliated with a student organization or hobbyists with a high interest in security and ethical hacking but are currently in a non-security-relevant career. We will conduct these studies in accordance with the human subjects research protection policies and procedures from our institution's institutional review board.

We will conduct extensive interviews with NUCC's key decision-makers to gather in-depth data and insights on their procedures for acquiring computing hardware equipment, preparing and upcycling it into usable equipment, and coordinating with their beneficiaries (i.e., college-affiliated student organizations) to set up and maintain received equipment. We will also explore their motivations, long-term goals, and challenges when working with their beneficiaries. Using these insights, we will propose and develop a partnership model between NUCC and student organizations and a maturity model to represent the different phases of the partnership.

The partnership model will be characterized by the benefits, motivations, and challenges between NUCC and student organizations. The maturity model will be represented as a lifecycle, starting when NUCC and a student organization first make contact and reaching a high-maturity partnership allowing a student organization to assist other organizations in making contact and establishing their infrastructure. These models will be references for other academics and educators to facilitate the creation of new partnerships to equip students with computing equipment that would usually become e-waste.

We will also conduct interviews with NUCC's beneficiaries to gather data on what they have been able to do with the upcycled equipment, particularly regarding security education, and also inquire into their motivations and challenges. After each interview, we will undergo open coding to identify themes to organize our findings and assist in determining when thematic saturation is achieved. After saturation, we will use the themes to create questions for a follow-up survey with our interviewees to seek their opinions on themes that may not have come up in individual interviews.

We will conduct an empirical analysis of the operations and activities NUCC's beneficiaries have enabled and empowered using the upcycled equipment. With permission, we will directly access the servers and networks the beneficiaries may have set up and request any relevant materials, reports, or notes of past activities for analysis. This analysis will be done in parallel with the semi-structured interviews.

The first author also has participant and non-participant observations from their involvement in a student organization with a relatively mature partnership with NUCC. These observations stem from frequent discussions with NUCC's members, participation in their events and leadership, and attendance at events where the organization's members and NUCC's key decision-makers are present.

Fig. 1. Upcycled server to support a cybersecurity student club at UCI.

Fig. 1 is a picture of a server rack composed primarily of upcycled equipment gifted to a cybersecurity student club at an R1 institution by NUCC. The current equipment in the server rack has been roughly estimated to be worth ∼$10,000 USD, but this specific club spent less than $3,000 USD over the past 3 years of their own budget to purchase parts that NUCC did not have. The equipment has enabled the members of the club to achieve national-level success at a top cyber defense competition, create at least six mock corporate networks for blue teaming and red teaming exercises, and dozens of accessible, hands-on security-focused workshops to teach other students (e.g., intro to pentesting, password cracking, malware reverse engineering). We aim for our research plan to identify benefits, challenges, and findings that would enable a similar or greater degree of success for other institutions.

References

[1] D. Tomaschik, "Building a Home Lab for Offensive Security & Security Research," 2017. [Online]. Available: https://systemoverlord.com/2017/10/24/building-a-home-lab-for-offensive-security-basics.html

[2] J. Simpson and A. Brantly, "Security Simulations in Undergraduate Education: A Review," in *Journal of Cybersecurity Education, Research, and Practice*. Kennesaw State University, 2022. [Online]. Available: https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=1086&context=jcerp

[3] C. Dadiyala, P. Tangade, G. Singh, V. Bhutada, A. Bhattad, N. Partani, and R. Jangid, "Designing and implementing an effective cybersecurity home lab for detection and monitoring," in *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 2023, pp. 1–8.

[4] Virginia Cyber Range, "Virginia Cyber Range." [Online]. Available: https://www.virginiacyberrange.org/

[5] Matrix-NDI, "Maximizing Efficiency: The 3-5 Year IT Infrastructure Refresh Cycle," 2024. [Online]. Available: https://www.matrix-ndi.com/resources/maximizing-efficiency-the-three-to-five-year-it-infrastructure-refresh-cycle/

[6] J. Kuehne, "Keeping Devices Refreshed Is Critical to a Healthy and Modern IT Ecosystem," 2024. [Online]. Available: https://edtechmagazine.com/k12/article/2024/05/keeping-devices-refreshed-critical-healthy-and-modern-it-ecosystem

[7] United Nations Institute for Training and Research, "The global E-waste Monitor 2024 – Electronic Waste Rising Five Times Faster than Documented E-waste Recycling: UN," 2024. [Online]. Available: https://ewastemonitor.info/the-global-e-waste-monitor-2024/

Upcycled Computing Hardware Equipment for Security Education

Steven Ngo, Joshua Garcia
Informatics Department, School of Information & Computer Sciences
UC Irvine
skngo1@uci.edu, joshug4@uci.edu

Background

We aim to enable a realistic, hands-on security education experience *with network environments*:

- Setting up **real-world** applications and services for testing
- Conducting pentests and red teaming **simulated** corporate networks
- Testing **custom-made** scripts and tools

Existing solutions:

- Cloud providers (e.g., AWS, GCP)
- Self-hosted infrastructure (*homelabs*)
- Cyber ranges

But we want a **scalable**, **low-budget** solution that provides **direct access** to the infrastructure for students.

Idea: IT teams throw out computing hardware when refreshing IT infrastructure

Concept: *Upcycling* - transforming electronic waste (E-waste) into higher-quality items

RQ1: How can ***upcycled computing hardware equipment*** be utilized ***specifically for security education***?

RQ2: What are the ***benefits***, ***challenges***, and ***future directions*** of utilizing upcycled equipment for security education?

Methodology

Non-profit partner: **National Upcycled Computing Collective (NUCC)**

NUCC has supplied upcycled equipment to ***student-run clubs*** at:

- 3 R1 institutions
- 3 Teaching-focused institutions
- 2 Community colleges

We use a **mixed-methods approach**:

- semi-structured interviews
- open coding & thematic analysis
- follow-up surveys + supplementary empirical analysis

In-Progress/Early Findings

Some of what the upcycled equipment has enabled:

- **National-level success** at a top cyber defense competition
- Creation of at least 6 **mock corporate networks**
  - Supports blue and red team exercises with teams of 8 students
- Dozens of **accessible, hands-on workshops** to teach other students

Specs

Storage Server - 4TB HDD, 512GB SSD cache

Virtual Servers - 2x 192GB RAM, 8x 250GB SSD

Networking - 2x UniFi 24-port Switches

Server rack of upcycled equipment; supports the operations of a cybersecurity student club at an R1 institution. This club spent only ~$3,000 USD of their budget across 3 years.