Workshop on Cybersecurity and Sustainability

DAVID BARRERA, Carleton University, Canada
MAXWELL KELEHER, Carleton University, Canada
SONIA CHIASSON, Carleton University, Canada

As awareness of environmental sustainability issues continues to grow, sustainable HCI has expanded into adjacent fields identifying new opportunities for bringing change. Cybersecurity is one such field where sustainability has only recently seen interest, primarily from the standpoint of securing the technical infrastructure that supports sustainability initiatives. However, the link between cybersecurity and sustainability is much more complex, and the way that the two fields interact is not yet well understood. This workshop will bring together researchers in the fields of sustainable HCI and cybersecurity to explore this critical intersection. Specifically, through brief tutorials and breakout sessions, participants will work together to identify cybersecurity practices that can inadvertently undermine sustainability efforts. Participants will also collaboratively critique and improve existing design processes that prioritize cybersecurity over sustainability as a core principle.

1 Introduction

Cybersecurity plays a key role in practically all aspects of the digital world, and as more devices become internet-connected, cybersecurity only becomes more deeply entrenched in everyday life. Indeed, the security and privacy of data captured and used by our devices is important, but it is becoming increasingly evident that security and privacy are being considered in isolation, sometimes to the detriment of environmental sustainability. In a short 2023 workshop paper, Kocksch and Sørenson [3] challenge the HCI community to explore the relationship between sustainability and security in the context of digital technologies. To our knowledge, theirs is the first published paper to solicit deeper research exploring the intersection of sustainability and cybersecurity.

Consider a low-end internet of things (IoT[1]) device being designed today. In addition to all the UI/UX choices and basic performance and functionality goals, the designers of this device must also make a number of cybersecurity choices which directly or indirectly impact its sustainability. For example:

- If digital certificates are to be used for authenticating cloud servers (a standard practice), certificate expiry dates must be chosen, and a mechanism to update the certificate before expiry must be developed. Failure to update the certificate would prevent the device from functioning correctly, encouraging its early disposal.
- Designers may want to prevent attackers from understanding the inner-workings of the device, and may use software or hardware locks to prevent reverse-engineering. While these protections may help keep the device secure while it is supported, these types of protections make it difficult for third parties to give the device a second/extended life after the vendor inevitably goes out of business [1].

Each of the choices made shapes the IoT device into what it will be for the rest of its life, and these choices often create hard dependencies on software and hardware that cannot easily be changed. Manufacturers can amplify these

[0]This is the author's personal copy. The definitive version can be found at https://dl.acm.org/doi/10.1145/3715335.3744896.
[1]While the cybersecurity/sustainability problem impacts all devices that use hardware and software, we find IoT to be an easy to understand application domain for experts and non-experts alike.

Authors' Contact Information: David Barrera, School of Computer Science, Carleton University, Canada; Maxwell Keleher, School of Computer Science, Carleton University, Canada; Sonia Chiasson, School of Computer Science, Carleton University, Canada.

2025. Manuscript submitted to ACM

challenges by making choices that artificially limit product lifespans (e.g., through planned obsolescence [5]). We believe cybersecurity decisions made without sustainability consideration can similarly limit the device's lifespan. When these choices are made incorrectly, devices become vulnerable to attack, and if the vendor is unwilling or unable to create a fix, the device risks becoming electronic waste (e-waste).

Moreover, design decisions that de-emphasize repair and maintenance likely contribute to the consumer perceptions that IoT devices are disposable [4]. Many IoT devices are designed such that repair is difficult or infeasible [6]. When users are unable to repair or replace parts on IoT devices, they may discard that device [2], which has significant sustainability implications. This disposable mindset also has implications for device security; first, it means that security decisions may be made expecting a relatively short maintenance horizon, and second, it means that each of these disposed devices could potentially leak user data if precise disposal procedures are not followed. How can we address issues of sustainability with IoT device design while maintaining security?

Heeding Kocksch and Sørenson's challenge [3], this workshop seeks to bring together researchers from all areas of HCI and cybersecurity to collaborate on the many facets of this problem. Our goals extend beyond identifying cybersecurity choices that can lead premature obsolescence of devices; we aim to jointly build a robust understanding of software and hardware design methodologies rooted in participants' research experience, and identify opportunities for injecting sustainability advice into the design process itself. We expect the inclusion of participants in diverse areas of HCI and cybersecurity will broaden the scope and impact of our research agenda and lead to future interdisciplinary collaborations.

2 Workshop Outline

We intend for a highly interactive full-day workshop where participants have opportunity to engage in several activities, meet other researchers, and collaboratively brainstorm ways to address the cybersecurity and sustainability challenge.

Duration and Format. 1 day, in-person format.

Introduction and Background Session. With the understanding that many HCI participants won't necessarily be well-versed in cybersecurity concepts, we'll first present a few examples of how IoT devices rely on cybersecurity protections to operate securely. We'll then briefly connect the cybersecurity and sustainability domains with real-world examples of products that have become e-waste due to shortsighted cybersecurity decisions.

Collaborative Breakout Sessions. The remainder of the workshop will feature 3 breakout sessions where participants will be assigned to groups of 5-7 participants. We'll aim to create groups having diversity in terms of domain expertise and experience to encourage interactions that consider multiple perspectives. We will shuffle groups between breakout sessions so that individuals have the opportunity to be part of different groups and hear different perspectives.

Participants will be given an activity and work collaboratively to solve the problem or answer a question. These activities will last around 25 minutes, and when time is up, we will regroup with a moderator to guide the presentation and discussion of each group's findings. During the breakout sessions, workshop organizers will float between groups, answering questions, and providing assistance where necessary. We expect each session, including introductory explanation, hands-on break-out activity, and presentations to last 50 minutes.

Discussion and Conclusion Session. We'll allocate a final general discussion session timeslot to allow for participant feedback and arriving at shared conclusions. As a group, we will discuss potential paths forward and identify opportunities for collaboration.

3 Workshop Goals and Anticipated Outcomes

We envision the following goals for our workshop:

(1) Reflect on trade-offs and inter-dependence of cybersecurity and sustainability. The workshop aims to identify specific cybersecurity practices that could negatively impact sustainability efforts, and vice-versa.
(2) Critique and improve design processes: Participants will collaboratively examine and improve existing design processes, focusing on how security and sustainability could be mutually supported.
(3) Foster interdisciplinary collaboration: The workshop seeks to broaden the scope of research and encourage future collaborations between sustainable HCI and cybersecurity researchers.

Given the immaturity of research combining the two domains, one anticipated outcome is to **collaboratively develop a research agenda** that identifies promising areas for improvement. Another outcome is to **plan interdisciplinary collaborations** and grow the community of researchers thinking about this emerging interdisciplinary area.

4 Workshop Organization

David Barrera is an associate professor in the School of Computer Science at Carleton University and co-director of the Carleton Internet Security Lab (CISL). He has previously done research on next-generation internet architectures and mobile operating system security. His current interests are on IoT security and sustainability.
Maxwell Keleher is a PhD student in the School of Computer Science at Carleton University. He has a Bachelor's of Computing from Queen's University, a Master's of Computer Science (HCI) from Carleton and has previously worked as a software engineer at Microsoft. His research has focused on deceptive design patterns, and the effect of perceiving devices as social actors on privacy attitudes. His PhD aims to propose design guidelines for sustainable IoT cybersecurity design.
Sonia Chiasson is a full professor in the School of Computer Science at Carleton University and director of Carleton's Human Oriented Research in Usable Security (CHORUS). Her interdisciplinary research interests lie at the intersection of human-computer interaction (HCI), computer security, and privacy. She is also co-director of Carleton University's interdisciplinary HCI Graduate program.

5 Sample Schedule

09:00-09:50 - Introduction and background tutorials
09:50-10:00 - Transition Break
10:00-10:50 - Breakout 1
10:50-11:10 - Break
11:10-12:00 - Breakout 2
12:00-13:30 - Lunch
13:30-13:40 - Transition Break
13:40-14:30 - Breakout 3
14:30-14:50 - Break

14:50-16:00 - Group Discussion
16:00-16:15 - Workshop conclusion

6 Sample Call for Participation

We invite HCI researchers who have an interest in cybersecurity to participate in a workshop exploring the complex relationship between cybersecurity and sustainability. Increasingly, devices are being forced into e-waste due to shortsighted cybersecurity decisions and unwillingness to plan for failure. Many products are ending up in landfills *while still fully functional* because cybersecurity choices have either permanently locked the device, or deliberately induced an unfixable failure mode.

In this one-day workshop, participants will learn about the role that cybersecurity plays in modern IoT devices, and collaborate to identify cybersecurity choices that work in opposition to sustainability initiatives. Participants will work in groups, bringing their experience and perspectives to the discussion. They will work together to find opportunities for injecting sustainability advice during the design process, leading to devices that can remain secure and functional for longer periods of time.

We encourage participation from researchers in related areas of HCI including (but not limited to) sustainable design, behavioral science and persuasion, communication, accessibility and inclusive design, prototyping, and user experience research. We also encourage participation from members of the cybersecurity community, particularly those who have experience with IoT.

To demonstrate your interest and participate in the workshop, please submit a one-page abstract that includes:

(1) Your background, including any relevant experience.
(2) A max 200 word justification statement of why you're interested in participating in the workshop

Submissions should be formatted as ACM CHI extended abstracts and be at most 2 pages in length. These submissions will only be used to ensure suitability of participation and will not be published.

Please direct your questions and submissions to David Barrera (davidbarrera@cunet.carleton.ca). You may find additional information on the workshop at our website: https://to-be-determined

References

[1] Conner Bradley and David Barrera. 2023. Escaping Vendor Mortality: A New Paradigm for Extending IoT Device Longevity. In *New Security Paradigms Workshop*. ACM, Segovia Spain, 1–16. doi:10.1145/3633500.3633501

[2] Stacey Higginbotham. 2018. The Internet of Trash: IoT Has a Looming E-Waste Problem - IEEE Spectrum. https://spectrum.ieee.org/the-internet-of-trash-iot-has-a-looming-ewaste-problem.

[3] Laura Kocksch and Estrid Sørensen. 2023. Investigating the Sustainability-Cybersecurity Nexus in HCI as a Practical Problem: Submission to Workshop WS27: HCI for Climate Change: Imagining Sustainable Futures. In *HCI for Climate Change: Imagining Sustainable Futures: Workshop at CHI 2023*. https://sites.google.com/fbk.eu/hci-climate-change

[4] Matthew Pilling, Michael Stead, Adrian Gradinar, Christian Remy, and Thomas Macpherson-Pope. 2023. Preparing to Repair: Using Co-Design and Speculative Design Methods to Explore the Future of IoT Right-to-Repair with Citizens and Communities. In *Design for Adaptation Cumulus Conference Proceedings Detroit 2022*. Cumulus, USA, 482–501. https://www.research.ed.ac.uk/en/publications/towards-sustainable-internet-of-things-objects-design-strategies-

[5] Julio L. Rivera and Amrine Lallmahomed. 2016. Environmental implications of planned obsolescence and product lifetime: a literature review. *International Journal of Sustainable Engineering* 9, 2 (March 2016), 119–129. doi:10.1080/19397038.2015.1099757

[6] Michael Stead, Paul Coulton, Joseph Lindley, and Claire Coulton. 2019. *The Little Book of SUSTAINABILITY for the Internet of Things*. Lancaster University, Lancaster, England.