Keynote Address: Sustainability is a Security Problem

Patrick McDaniel
University of Wisconsin-Madison

ACM Reference Format:
Patrick McDaniel. 2022. Keynote Address: Sustainability is a Security Problem. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS '22), November 7–11, 2022, Los Angeles, CA, USA.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3548606.3559396

It is undeniable that we are at pivotal point in human existence. Humans as a species have grown in population and infrastructure to the point where our collective actions are impacting nearly every living thing and natural process on Earth. The direct impacts are myriad: to list a few, crises such as climate change, mass extinctions (and the attendant loss of biodiversity), ocean acidification, soil and water contamination and degradation are now visible and growing in severity. Indirect impacts on the global population such as starvation, disease, natural disasters, and global reduction of quality of life are accelerating. We have reached a point where our current model of living is unsustainable. If we don't take action now we will face ever increasing consequences and eventually reach a point where life as we know it on Earth will not be possible.

So what can we do to achieve a sustainable lifestyle on earth? In this address I will reflect on that question and, perhaps surprisingly, observe that sustainability can only be achieved when framed as a (physical and cyber) security problem.

We first have to define what it means to be sustainable. In its purest (idealized and simplified) form, sustainability is the practice of living without having lasting impacts on the natural world. Terms like net-zero demonstrate this concept – for example, we should only use as much water as we collect and safely process, emissions created during energy generation must be offset by other processes that remove a like amount of pollution, and any tree cultivated for industry must be offset by planting another tree. A society that can do this for all of our resources can exist indefinitely. The United Nations interestingly frames it in terms of our responsibility to future generations, where they stated that sustainability is "meeting the needs of the present without compromising the ability of future generations to meet their own needs" [1].

How society decides to achieve sustainability is very much an open question. Regulatory structures, market incentives, education campaigns, among many strategies all seek to alter the actions of individuals or organization to align with sustainability goals. This has worked in many cases, but yet we are nowhere close to addressing the crisis before us. With all this action, then why aren't we making more progress?

The problem is people (and by extension organizations). Philosopher Thomas Hobbs observed in the absence of governance, humans will behave selfishly [2]. Put another way, humans (in general) are greedy algorithms that will do what is best for them unless there are sufficient controls (either regulations or incentives). Modern economic theory supports this view of society, particularly as it relates to sustainability.

Consider the case of the car maker Volkswagen's emissions scandal in 2015 [3]. In 2006, Volkswagen introduced a new catalytic converter in its diesel engines and promoted it as a "green technology". However, the converter was essentially a failure and could not provide the advertised emission controls at the performance expected by the consumers. So, engineers at the company programmed the converter to only operate in green mode when it detected it was under test—in effect they cheated by only providing green technology when being measured for environmental impact. This device was manufactured over years and deployed in over 11 million vehicles. On the road, the device was horrific; the VW Jetta exceeded US emissions limits by a factor of 15 to 35 in measured tests. Volkswagen was eventually caught and fined billions across the globe and was required to recall vehicles and pay customers enormous settlements.

Other approaches that thwart sustainability goals are more subtle. One such approach—dubbed by some as greenwashing—is an organization's way of using PR to suggest that sustainability goals are being met while not actually making any real progress [4]. For example, oil companies such as BP have mislead the public about their sustainability goals and behaviors, Starbucks created a straw-less lid that contained more plastic than the original straw and lid, and Coca-Cola (ranked as the world's largest plastic polluter in 2020) promoted it was going to be more plastic free while making little or no progress in altering their production. Similar sustainability thwarting behavior commonly occurs at the consumer (disabling of eco-friendly technology on vehicles) or national levels (governments mis-representing emissions, population, and pollution information). Computation itself, most notably in cloud data centers, has been touted as both the path to sustainability and the cause of enormous environmental impacts.

All of these events signal that many organizations (like people) will do what benefits them—often at the expense of the planet. Therefore, it is essential that the global community have verifiable sustainability. Regulations and market incentives without public verifiability will not—and cannot—provide the kinds of guarantees we need to have a sustainable future. We have found that self-reporting, best effort measurement and anything less than complete verifiable control of sustainability will fail.

That is why sustainability is a security problem. Any technology that can achieve sustainability exists within a world with users (society, us), adversaries (people and organizations that would seek to misrepresent sustainability metrics or behaviors and those that

CCS '22, November 7–11, 2022, Los Angeles, CA, USA

ACM ISBN 978-1-4503-9450-5/22/11.
https://doi.org/10.1145/3548606.3559396

would seek to disable or circumvent the use of sustainability verification), threats, threat surfaces, and security and privacy goals. Hence, we must treat future systems for sustainability as systems under threat.

And as it turns out, there is no community better equipped to help design resilient sustainability systems than ours. That is my call to action. We must develop technologies that support this mission—develop primitives that allow domain experts to construct and operate these systems and verify the results. Securing sustainable systems must be a goal of this community.

So what might this new sub-field of security look like? It would certainly build upon recent advances and known primitives for achieving security and privacy goals in hostile environments. For example, trusted execution environments might provide the third party verifiability of systems operation, block chains may provide traceability of goods and consumption in numerous contexts, and secure multiparty computation may provide structures for organizations to produce proofs of sustainability while preventing the exposure of sensitive data. But we must start by understanding the goals, methods, and limitations of sustainability processes–we cannot do this in a vacuum, but must work with scientists, engineers, policy-makers, and the public to achieve our shared goal of a sustainable society.

The remainder of this talk will explore what a sub-field of security might look like; what technologies will likely be useful, what the goals of that field would look like, and what new challenges it presents. Lastly I will revisit how developed technologies can be integrated into sound policy. I strongly believe that this community can be an important (and indeed essential) participant in reversing the failures to date and advancing our world into a more sustainable future. Failing to act is not a viable option.

REFERENCES

[1] UNWCED: United Nations World Commission and Development. Report of the world commission on environment and development: Our common future (brundtland report). *United Nations General Assembly document*, A/42/427:1–300, 1987.
[2] Thomas Hobbes, 1588-1679. *Leviathan, or, The matter, form, and power of a commonwealth ecclesiastical and civil.* London : Printed for Andrew Crooke. 1651., 1651.
[3] Russell Hotten. Volkswagen: The scandal explained. *British Broadcast Company*, dec 2015.
[4] Deena Robinson. 10 Companies Called Out For Greenwashing, July 2022.

Speaker Bio: Patrick McDaniel is the Tsun-Ming Shih Professor of Computer Sciences in the School of Computer, Data and Information Sciences at the University of Wisconsin-Madison. Professor McDaniel is a Fellow of the IEEE, ACM and AAAS, a recipient of the SIGOPS Hall of Fame Award and SIGSAC Outstanding Innovation Award, and the director of the NSF Frontier Center for Trustworthy Machine Learning. He also served as the program manager and lead scientist for the Army Research Laboratory's Cyber-Security Collaborative Research Alliance from 2013 to 2018. Patrick's research focuses on a wide range of topics in computer and network security and technical public policy. Prior to joining Wisconsin in 2022, he was the William L. Weiss Professor of Information and Communications Technology and Director of the Institute for Networking and Security Research at Pennsylvania State University.

Research Interests: Dr. McDaniel's research focuses on a wide range of topics in computer and network security and technical public policy, with particular interests in mobile device security, the security of machine learning, systems, program analysis for security, sustainability, and election systems.