Sustainability is a Security Problem

ACM Conference on Computer and Communications Security (CCS)
November 8, 2022

Patrick McDaniel, Tsun-Ming Shih Professor of Computer Sciences

UW-Madison School of Computer, Data & Information Sciences

As a species? …

Where are we?

Why are we here?

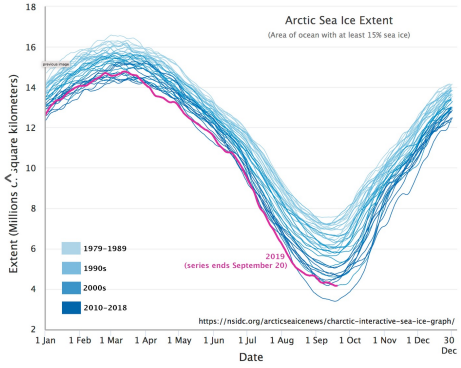
What can/must we do about it?

360,000 years, 10,000 years, 200 years, 25 years …

no serious person can deny we are at a pivotal point in human (and earth's) existence

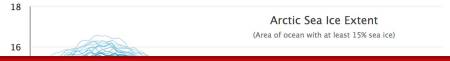
A moment in time …

- Human mismanagement of our world has led to (among other things):
  - Climate change
  - Widespread pollution of the oceans
  - Acidification of land and water
  - Ozone loss
  - Desertization
  - And loss of biodiversity



A moment in time …

- Human mismanagement of our world has led to (among other things):
  - Climate change
  - Widespread pollution of the oceans
  - Acidification of land and water
  - Ozone loss
  - Desertization
  - And loss of biodiversity



Scary fact Bingo:

- There's more carbon dioxide in our atmosphere than at any time in human history
- Average wildlife populations have dropped by 60 per cent in just over 40 years
- Plastic production in 2019 was at its largest in history (368 million metric tons)

A moment in time …

- But *we have* made meaningful progress
  - We have cut the 4C estimate in half to about 2C (and about 1/2 the reduction was due revising models to be more realistic)
  - Costs of renewables has dropped by 85% for solar
  - 90% of the global population lives in places where new renewable power would be cheaper than new dirty power
  - 90% of the world's G.D.P. and over 80% of global emissions are now governed by net-zero *pledges*
- Approaching: "renewable singularity", action needed

Liebreich: Peak Emissions Are Closer Than You Think – and Here's Why, Michael Liebreich, BloombergNEF, 2019.

what now

What is sustainability?

- Sustainability addresses the global challenges we face, including poverty, inequality, *climate change*, *environmental degradation*, peace, and justice.
- In its purest (idealized and simplified) form, sustainability is the practice of living without having lasting impacts on the natural world.
  - Net-zero is one manifestation of this concept – e.g.,
    - Use as much water as we collect and safely process
    - Emissions must be offset by other processes that remove a like amount of pollution (e.g., carbon capture)
    - Tree cultivated for industry must be offset by planting another tree

Question for society: how do we change our behaviors and processes to achieve these goals?

Computational Sustainability

- Computational sustainability is an emerging field of computer science (and engineering, …) which "Computer and information scientists join forces with other fields to help solve societal and environmental challenges facing humanity, in pursuit of a sustainable future."

  > "Our vision is that computer scientists can and should play a key role in helping address societal and environmental challenges in pursuit of a sustainable future, while also advancing computer science as a discipline." [Gomes19]

- Computational sustainability problems relate to uncertainty, machine learning, optimization, remote sensing, and decision making.
  - Applied computer science lying at the nexus of problems and solutions addressing key societal and environmental challenges.

[Gomes19] *Computational sustainability: computing for a better world and a sustainable future*, Gomes et al, Comm. of the ACM, Vol. 62, No. 9, Aug 2019.

we are the problem

Jevon's Paradox and Pigou's Externalities …

- Jevon's Paradox: Humans will consume whatever resources are made available to them. When resources become more plentiful (or more efficiently consumed), demand will rise as a result … [see the lesson of *hybrid cars*]
  - Also known as the *conspicuous consumption law*
- In the 19th century, Arthur Pigou explored how the use of resources creates *externalities*—costs forced on others caused by consumption.
  - Pigovian tax—tax on those who create externalities to offset those costs, which indirectly creates incentives (and markets) for resource consumption strategies that benefit society as a whole
  - Pigou was amongst the first to posit society must create structures to foster sound policy for consumption …

Solutions to address sustainability

- Regulatory structures
  - U.S. Department of Transportation's National Highway Traffic Safety Administration, Corporate Average Fuel Economy standards require an industry-wide fleet average of approximately 49 mpg for passenger cars and light trucks in model year 2026.
- Impact (e.g., emissions) tax*
  - London Ultra Low Emissions Zone - LEZ emission standards or you must pay a £12.50 daily charge to drive inside the zone.
- Sustainability credit markets
  - European Union Emissions Trading System - a maximum (cap) is set on the amount of greenhouse gases that can be emitted. Credits are awarded and can be freely traded. Installations must monitor and report their CO2 emissions.

* Can also be framed as subsidies (incentives)

Where sustainability measures fail …

- Beginning in the 2000s, the Volkswagen installed emissions software on 11 million cars worldwide that had dual-mode logic.

  - In test mode, the engine to operate in compliance with regulatory requirements such as those provided by the EPA .
  - When driven normally, the engine would significantly change the fuel pressure, modify the injection timing, and change the exhaust-gas recirculation ratios.
  - The nitrogen-oxide (NOx) during normal driving was up to 40X the US federal limit.
- They were caught (researchers from WVU), fined, shamed …

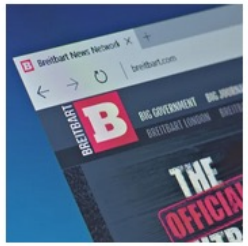
Why don’t we have sustainability now?*

- Misinformation
- Lack of enforcement
- Sustainability information gap

The former head of EPA’s Office of Enforcement and Compliance Assurance under the Obama administration wrote, “*most environmental policy practitioners, including government regulators, regulated companies, legislators, academics, and advocates—assume[] compliance*.”

Did NASA ‘Admit’ Climate Change Is Caused by Changes in Earth’s Orbit, Not Humans?
At issue are so-called Milankovich cycles, which describe three periodic variations in the way the...

(misinformation)



Do Hundreds of Papers Published in 2017 ‘Prove’ That Global Warming is a Myth?
An article stakes its claim on a regurgitation of false information from a blogger who...

(misinformation)

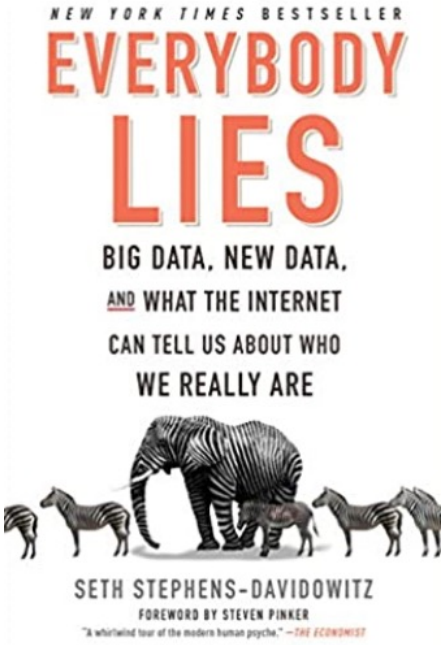
Peer-Reviewed Study Proves All Recent Global Warming Fabricated by Climatologists?
A blog post, even if you like it and it is presented in downloadable PDF...

(misinformation)

*Focusing on technology here, from security perspective.

The problem

1. Every solution to sustainability (regulations, tax/subsidy, and market) require that information be trustworthy.
2. Economics (and history) shows that many will cheat (e.g., misreport).
3. Thus, all sustainability measures and systems must be modeled as systems under threat.



/TLDR - Sustainability without security is doomed to fail.

we must innovate our way to sustainability

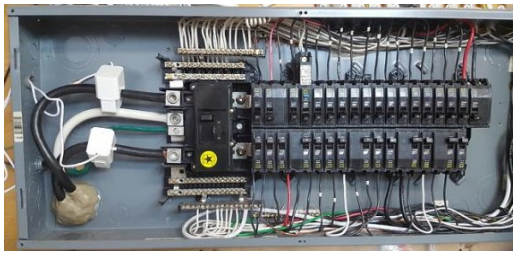
What now?

- The existential question (quite literally) for the security community is how do we solve the problems these technologies need?

Gomes et al. (and others) have suggested security plays a role, but we don't know what it is.

Observation: all sustainability requires “data”*

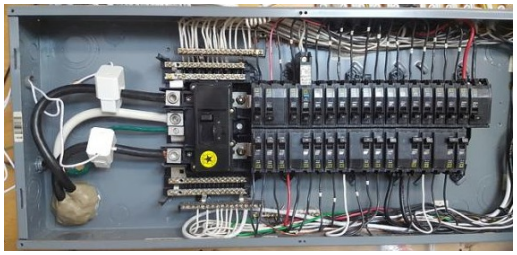
- All sustainability efforts require verifiable data
  - Verifiable consumption, use, construction, occupancy, provenance …
- The central challenges is that people, governments, and scientists do not have the data to monitor, regulate, study, and achieve sustainable goals.
- Thus, the (or a) security question is how do we acquire and maintain data in a trustworthy manner.



*Observationally, this is the most frequently cited issue in sustainability is : better/more/accurate data

Observation: all sustainability requires “data”*

- All sustainability efforts require verifiable data
  - Verifiable consumption, use, construction, occupancy, provenance …
- The central challenges is that people, governments, and scientists do not have the data to monitor, regulate, study, and achieve sustainable goals.
- Thus, the (or a) security question is how do we acquire and maintain data in a trustworthy manner.

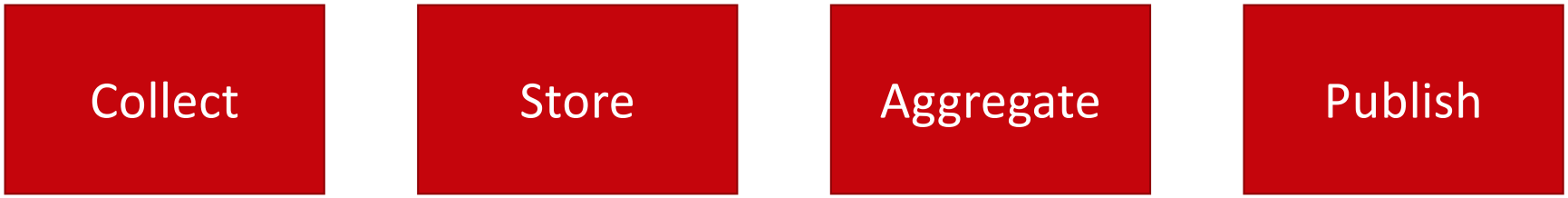


From here on we are going to treat all collection metrics that support regulation/incentives/enforcement of sustainability goals generically as “data”

*Observationally, this is the most frequently cited issue in sustainability is : better/more/accurate data

The sustainability metric pipeline …

- Trustworthy sustainability thus requires an end-to-end architecture (or many) for collection, storage, aggregation (or other processing), and use of sustainability metrics *in situ*
  - Each of these steps in the pipeline lead to unique challenges



Q: What are the security challenges of providing these capabilities in a trustworthy way?

What does trustworthy mean in this context?

1. All data must be verifiable to its accuracy, source, time, and location
2. Data must be complete and timely (available)
3. Data cannot be altered or removed (but maybe aggregated?)
4. Anyone should be able to view data and measure compliance
5. Collected data should not disclose private information
   - E.g., intellectual property, process secrets, user activities, location, etc.
6. Data (and the impacts of its collection/use) must be fair to all communities
7. Should not require trust in a singular entity/organization ~ everyone (from citizen scientists to corporations) should be able to validate independently

Sustainability data principles: Accurate, Complete, Timely, Public, Privacy Preserving, Fair, and Trust Agnostic

Security for sustainability in five challenges …

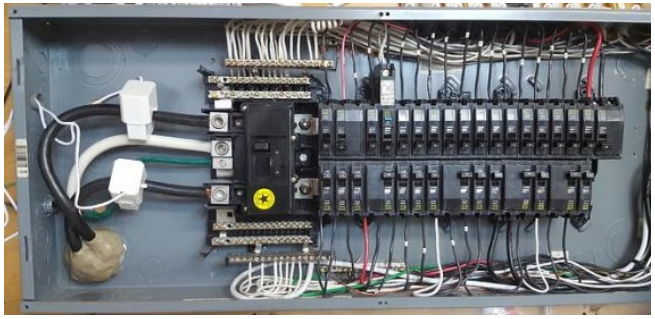
Challenge: Verifiable Data Collection

- Vision: Public readable, verifiable sensor readings – architecture and systems to collect sustainability in adversarial settings
  - Scale from small, low power devices to enterprise or greater settings (data-centers)
  - Generate proofs of use/construction retrievable by authorized parties (or public)
    - Time, place, compliance, metrics …
  - Tamper-proof (or resistant) construction, i.e., must operate in adversarial deployments
  - Verifiable implementation
- Exemplar study: TEE-based OS extension to report process usage
  - Reports usage statistics in form of signed proofs, or proof systems that can be queried
  - Small, formally verified implementation
  - Challenges:
    - Proof/proof system construction
    - How to get accurate (unforgeable) information from kernel
    - Installation on untrusted platforms
    - Ensuring availability

Potential security area: formal methods, OS security, verifiable computation, cryptography, hardware security, IoT and sensor network security, …

Challenge: Privacy-Preserving Data Collection

- Vision: Sensor disclosure of sustainability metrics that preserves privacy*
  - Prevention of disclosure of location, behavior, intellectual property, systems
  - Possibly using trained models



- Exemplar study: TEE-based multiparty computation proving compliance
  - Observer perform MPC with sensor device to obtain sensor reading
  - Small, formally verified implementation
  - Challenges:
    - Computational costs: particularly with lost cost/power platforms
    - MPC compliance circuits/algorithms
    - Side channel leakage

Potential security areas: multiparty computation, differential privacy, cryptography, hardware security, oblivious-X, ….

* These goals may conflict with previous challenge.

Challenge: Verifiable Private Data Aggregations

- Vision: Construct proofs of computation of units of sustainability metrics
  - Perform aggregation, summary, or other function on data whose result do not disclose information about the underlying data
  - Aggregations must provide (provably) accurate higher-level data without exposing underlying sensitive information
  - E.g., proofs of compliance of manufacturing process without exposing unit wise behaviors or specific metrics
- Exemplar study: Crypto proof for compliance of sustainability
  - Setup: k trusted devices in environment produce verifiable proofs P of use which are given to prover environment
  - Prover environment takes P and generates proof Q that P (e.g., sum of P) is compliant with some policy (e.g., P<c, where c is some usage cap)
  - Verifier uses Q to prove compliance without learning anything about P

Potential security areas: multiparty computation, differential privacy, zero-knowledge proofs, homomorphic encryption, robust machine learning, ….

Challenge: Public Sustainability Ledgers

- Vision: Creating public ledger of sustainability data
  - Metrics (raw or aggregated) posted to ledger
  - Record non-sensor data
    - Carbon credit allocations, sales, and expenditures
  - Public must be able to read and add to ledger
  - Low cost, complete set of measurements
  - Prevent side channels, etc.

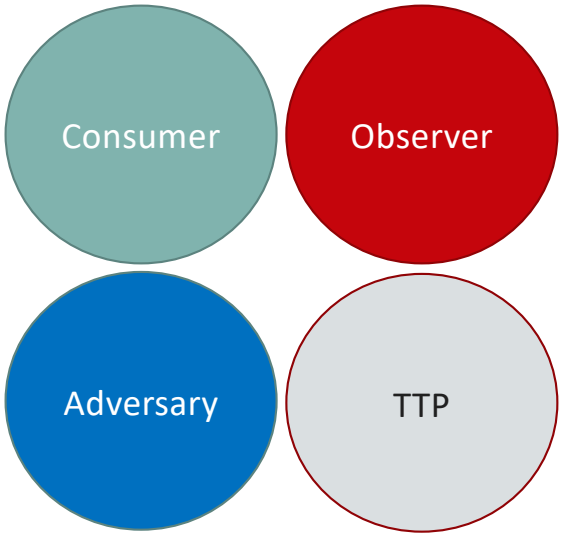
Callback: Accurate, Complete, Timely, Public, Privacy Preserving, Fair, and Trust Agnostic

- Exemplar study: Leverage, for example, Azure confidential ledger to build data center sustainability log
  - Allocate device energy credits
  - Collect data and insert usage and credit expenditures
  - Develop policies, detect usage overages
  - Simulate (or implement) credit sales, insert as transactions in ledger

Potential security areas: blockchain, secure distributed consensus, smart-contracts, ….

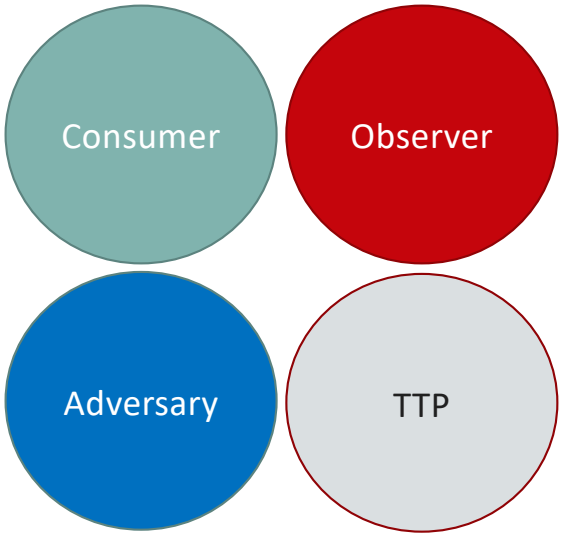
Challenge: The sustainability game …

- The consumer (system, environment, factory, etc.)
- The observer (e.g., regulator, citizen scientist, government, the public)
- The adversary (anyone who would interfere with the observer/consumer interaction)
  - Cheater consumer (Volkswagen)
  - Cheater observer (corrupt government)
  - Outsider adversary (disrupting person, organization, etc.)
- Trusted Third Party (provider of devices, etc.)
  - Trying to avoid these where possible, but need some root of trust (or roots of trust)



The secure sustainability game …

- Goals:
  - The non-adversarial consumer and observer want accurate and complete representation of sustainability metrics
  - The adversary want (1) inaccurate metrics to be collected, or (2) metrics not to be collected (or delayed)
- Moves:
  - Collect (or deploy/un-deploy collection)
  - Incentivize (offer reward, tax, or credit)
- Optimize: what is the optimal strategy for deploying/collecting sensors in a particular environment (e.g., data centers)?



Challenge: Others

- No matter what area of security you are working, it is important to sustainability
- Secure machine learning:
  - AI/ML for optimizing environments for sustainability goals (in adversarial settings)
  - Building robust models for consumption or production regulation and optimization
- Hardware security:
  - Trust zones in processors, IoT, sensors, etc.
  - Enforcing energy budgets on processes
- Software security:
  - Develop sustainability languages (which provably enforce and report metrics)
- Formal methods:
  - Can we prove that implementations comply with policy
  - Can we prove that implementations (or collections of implementations) achieve a sustainability goal optimal
- Network security:
  - Develop protocols (or services) that control sustainable goals (energy use) in the presence of an adversary (amplification resistance)
- Usable security:
  - Provide interfaces that allow users control how much information related to sustainable goals is presented (and the privacy risks therein)

Summary

- The challenge before us is to provide trustworthy sustainability data:
  - Making data collection verifiable (accurate, timely, and immutable)
  - Making data collection and use privacy preserving and fair
  - Supporting publicly accessible information on sustainability
  - Provide optimal strategies for sustainability infrastructure deployment

- If we provide even partial answers to these five challenges (which are multifaceted in their own right), we can put verifiable data into the hands of the people and organizations who can achieve sustainability.

Contact: mcdaniel@cs.wisc.edu