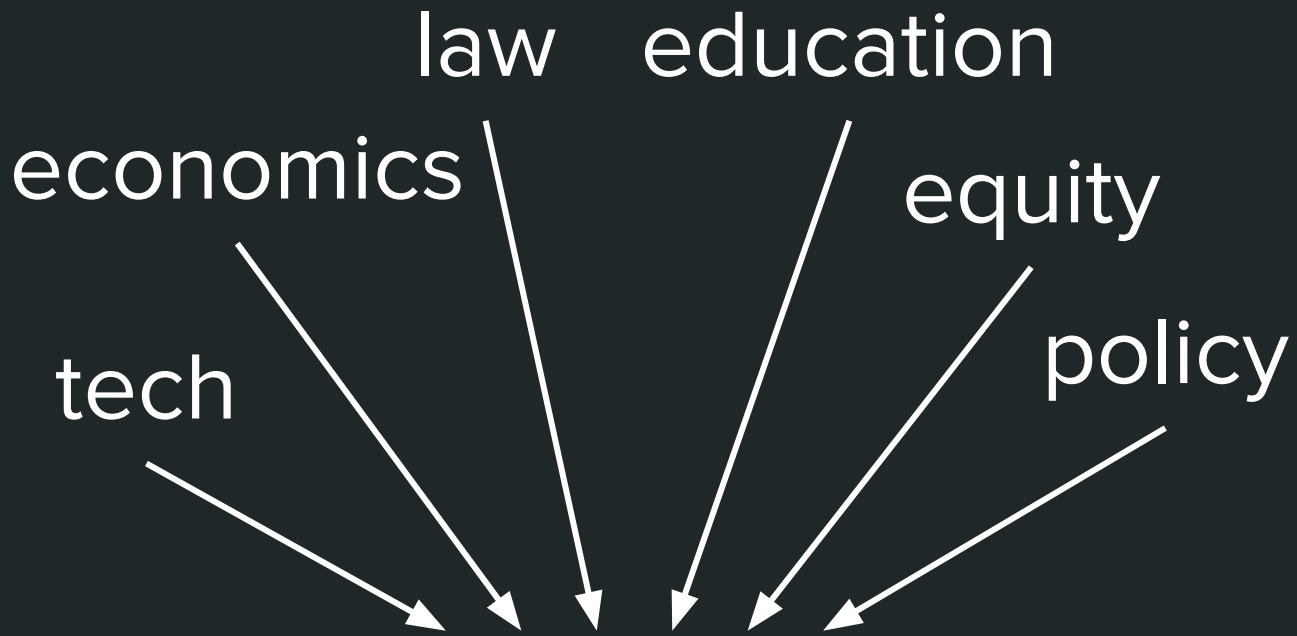
Mechanism Design for Hardware Security

CCC Visioning Workshop Kickoff



Create mechanisms to improve the state of hardware security

Thanks CCC/CRA!

Workshop Co-Organizers

Ask Questions and *Share Related Articles and Ideas* on slack here: https://tinyurl.com/hw-mech-design

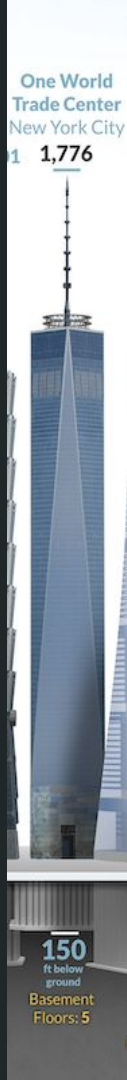
Prof. Simha Sethumadhavan
Columbia University
simha@columbia.edu

Prof. Tim Sherwood
University of California, Santa Barbara
sherwood@cs.ucsb.edu

Agenda

- Why a visioning workshop?
- The multidimensional space
- Q&A

Strong security demands a strong hardware foundation

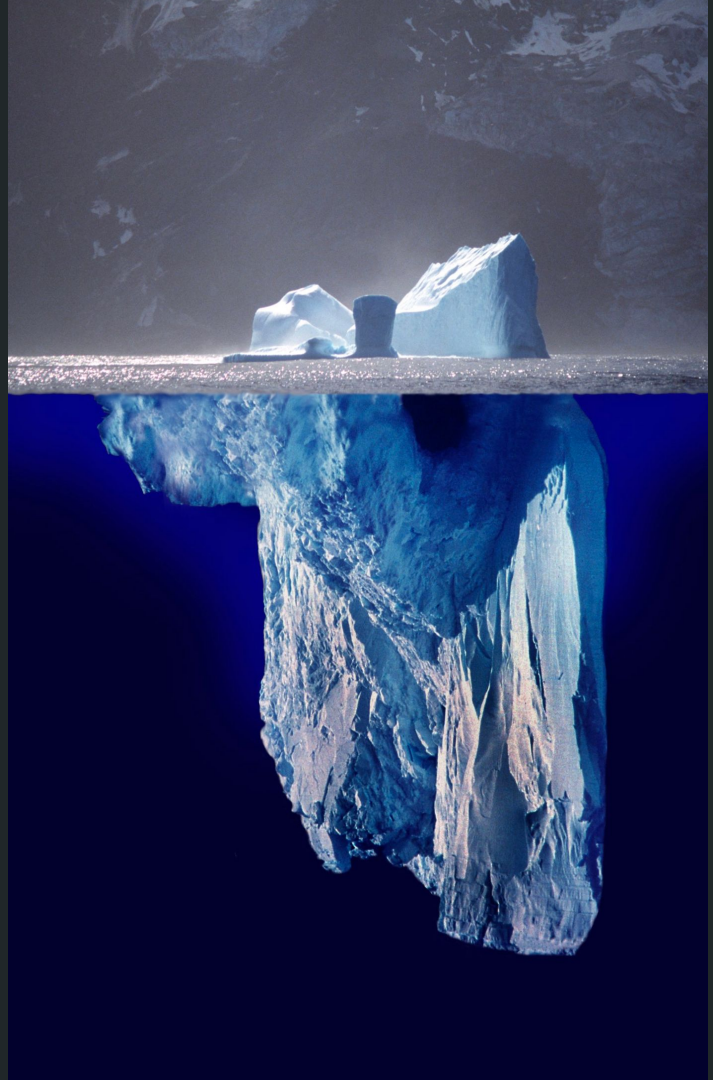


Hardware is Hard

The New York Times

Researchers Discover Two Major Flaws in the World's Computers

As Chips Shrink, Rowhammer Attacks Get Harder to Stop



Many Conflicting Goals and Issues

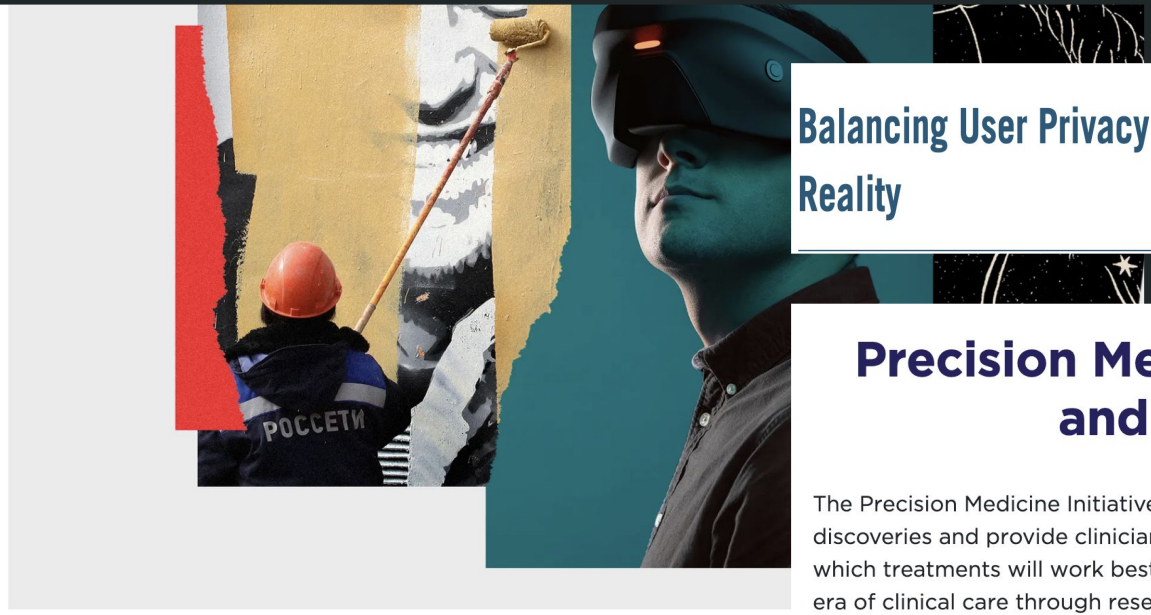


PHOTO-ILLUSTRATION: SAM WHITNEY; GETTY IMAGES

Balancing User Privacy and Innovation in Augmented and Virtual Reality

Precision Medicine Initiative: Privacy and Trust Principles

The Precision Medicine Initiative (PMI) launched in January 2015 to accelerate "biomedical discoveries and provide clinicians with new tools, knowledge, and therapies to select which treatments will work best for which patients." Precision medicine is enabling a new era of clinical care through research, technology, and policies that empower patients, researchers, and providers to work together toward development of individualized care

DARREN SHOU IDEAS 09.02.2021 08:00 AM

I Want My Daughter to Live in a Better Metaverse

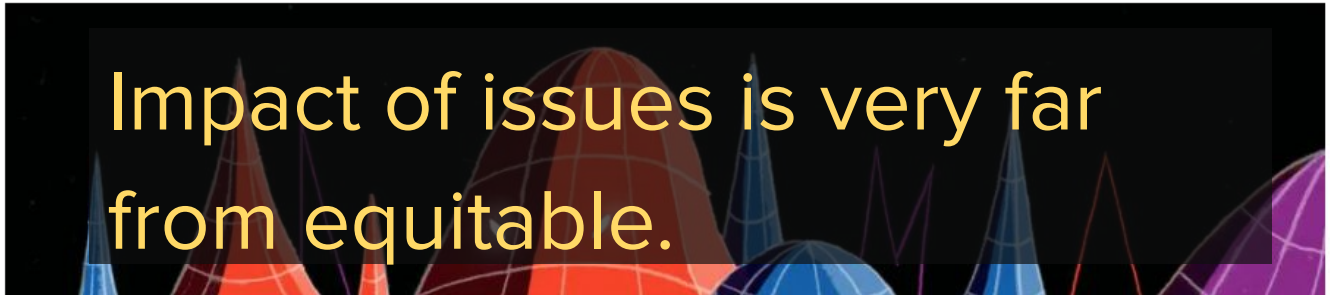
The metaverse could be beautiful. But left unchecked, it will further fragment reality and make us even more polarized.

https://www.nytimes.com/2019/04/25/opinion/privacy-poverty.html

The Devastating Consequences of Being Poor in the Digital Age

When someone who is living paycheck to paycheck falls victim to an online fraud or a breach, the cascade of repercussions can be devastating.

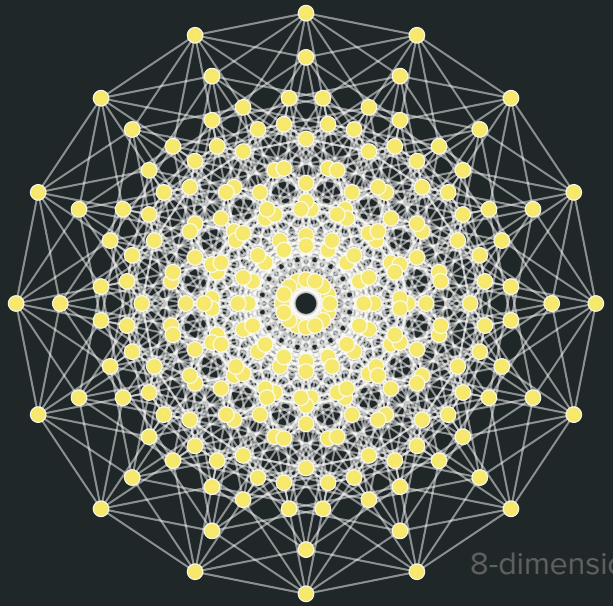
April 25, 2019



How do current policies and market structures disincentive hardware oriented security solutions?

How do we fix this: what technical and policy frameworks are necessary to make progress in this area?

Stakeholder concerns are not currently aligning in a useful way!



8-dimensional "cube"

Security Effectiveness
Enforceability
Cost of Ownership
Cost of Development
Environmental Impact
Ethical and Legal
Equity and Justice
Usability

A visioning workshop is a chance to ask the big questions

What are the mechanisms necessary to enforce a government mandate that says that X% of the performance or cost should be set aside for security? What mechanisms are necessary to determine X? How often should X be determined?

Is there a quantitative approach for the organization to use up this security budget? How would this be enforced on user systems? Are there alternate government mandates that are actionable and can be supported technically?

A visioning workshop is a chance to ask the big questions

What incentives and frameworks are necessary to patch hardware bugs in a timely manner?

Is there an equitable way to proportion the benefits of security and impacts of security attacks? What hardware support, if any, is necessary to facilitate this process?

What education/certification requirements are necessary for increasing the awareness and application of hardware security solutions?

A visioning workshop is a chance to ask the big questions

How do we establish a chain of responsibility for malicious and negligent action while also maintaining privacy?

How can hardware innovations (e.g. U2F tokens) fundamentally impact software dark economies?

What questions should we *really* be asking?

Next Steps

- Join the slack channel
  - Share useful articles and thoughts

- Submit white paper by April 15th 2022
  - Workshop in June in NYC

https://cra.org/ccc/events/mechanism-design-for-improving-hardware-security/

About the workshop

- The workshop will bring together a diverse group of thinkers to help chart a future for hardware security and hopes to include security experts, economists, and anyone else that will inform and understanding of what that future might look like and how we get there.

- The plan is an in-person workshop in NY on, or around, June 10th. Workshop attendance will be by an invitation from CCC and travel expenses will be available for select participants.

- As is tradition in CCC, we seek short white papers to help create an agenda for the workshop and select attendees.

- An additional goal of the workshop is to prepare a report summarizing key findings of our meeting for the broader community.

Whitepapers

- Our hope is whitepapers express a vision for the future, or describe some important research challenges, that stretch our communities understanding of what it means to be an effective security approach.

- We are particularly interested in ideas that include the perspective of diverse stakeholders and communities and are done in with full consideration of the deeply multidimensional space any solution occupies (e.g. across effectiveness, equity, usability, etc..)

- We also welcome critical evaluations of the status quo, discussion of policy considerations, economic or process theories that could inform effective change-making, and generally any perspective that help inform others on this set of problems.

Thank you!

Please stay for some Q&A