Mechanism Design for Improving Hardware Security Workshop Orientation Q&A

Is participation in the workshop limited to the U.S.?

No, anyone is welcome to participate.

Many of your examples were closely tied to societal impact / policy, etc. Are you explicitly looking for ideas/discussion that draw those connections? Would an engineering-only pitch (e.g., here's a widget/opportunity to improve performance) be a poor fit for a whitepaper?

This is a great question — certainly engineering-only solutions are an important piece of what we are after. We mostly want to recognize that engineering-only solutions exist in a much more complex problem space. If you change the performance or cost or effectiveness of a solution it will have impact on these many other aspects and I think one of the things we would hope to see is for us to take a moment and maybe think a little about what those impacts might be and some eagerness to engage with others that might help us understand that deeper space.

Do you see open-source hardware designs as building blocks for secure hardware systems which can provide security and/or privacy guarantees? Just like how crypto standards are open? Or is that not profitable enough?

Another great question, and open-source is a great example of something that cuts across different aspects of the problem (e.g. economic, community, transparency) and there are things to learn from the open-source software community and unique challenges in the space of hardware (e.g. the difficulty of patching). I won't share my take, because really we want to hear yours! This would be a great example of a topic for a whitepaper.

What is the impact of coming up with these thought areas/topics to improve hardware security? How's it going to get adopted or what's your strategy?

I thought @Ann Schwartz Drobnis had a wonderful answer to this in the video chat, but the long story short is that here is where CCC/CRA expertise and connections are so incredibly valuable. Everything produced will be public but also making sure the right people are informed and have every opportunity for their thinking to be influenced by what we end up doing is one of the many things they do best.

Who does this report go to at the end?

As a community organization everything the CCC does is public, so it'll be posted on our website, then blogged and we make sure that it gets into the hands of the right people at NSF and other agencies that would make sense. We take all the ideas presented at the workshop, put it together, and then run it by everyone who was at the workshop so it's a community consensus.