- **Regan Robertson** Mod • 15 days ago
  The recording of the live panel and closing remarks will be added to the site by tomorrow morning.
  - Reply
  - Share ›

Regan Robertson Mod • 15 days ago

We had some great questions come through the Q&A, and some were answered by the panelists and some wrote in the answers.

Renato 02:47 PM
Kevin, would it be the case to verify the specs of a processor model before actually crating the hardware and even having it on soft (FPGA) to be verified and validated? This can also be used to help eliminate side channels

Kevin Hamlen 02:48 PM
Yes, that's certainly a direction that I'd like to see explored more. I'm not a hardware expert, but I've been told that sometimes that's not feasible, though. For example, there are hardware "errata" that reveal a performance issue that wouldn't appear in a functional correctness spec, and that suggest a workaround that the functional correctness spec says is not a valid operation. :) So the answer to those sorts of issues might be to retroactive derive an improve spec that accommodates the workaround rather than discover the performance issue before the hardware ships.

Renato 02:50 PM
Agreed, but some side channels that came from good ideas such as speculation execution would have been found, if the design itself was seen as an exercise in security validation (as we are trying to do with software)

Kevin Hamlen 02:52 PM
Yes, certainly true. That's why I favor an "all of the above" approach. We should apply formal methods directly to hardware to the extent possible, yet recognize that inevitably there will be idiosyncrasies that were not part of the formal spec but become issues after release. So we need viable backup plans too, which can derive a more complete, trustworthy model from already-released hardware.

Douglas Schafer 03:05 PM
So, what are perceived as limitations for verification? For example, our favorite industry practice of code re-use, re-packaging, etc. for time and cost savings?

How often and under what conditions would you say are pragmatic for use of FM in larger systems-of-systems? This question has been answered live

Ray Richards 03:10 PM
I agree that deriving the spec has value. Note that Common Criteria at EAL5 has formal specifications, but semiformal (whatever that means) proofs. Everytime I have been involved in building a model of an existing system, we found bugs. (comment, not a question.)

Ray Richards 03:12 PM
Sergey, what is the weirdest weird machine that your are aware of? This question has been answered live

Jacob Saina 03:12 PM
Do you expect formal methods to become a rote component of software development for every day developers? In what sort of timeline? (5 years, 20 years, ...)? This question has been answered live

Jacob Saina 03:18 PM
If we are able to verify functionality from binary, do we trade away obfuscation (i.e. defense against reverse engineering)?

Sergey Bratus 03:21 PM
I'd say that the effectiveness of obfuscation tends to be overestimated. The tradeoff will favor verifiability, I'd say

Gernot Heiser 03:23 PM
Security by obscurity = no security

Jacob Saina 03:23 PM
alternatively, do we gain a tool for reverse engineering binaries?