Can formal specifications help?

Lenore Zuck (University of Illinois Chicago)

Ken McMillan (University of Texas at Austin)

Some uses of formal specifications

- Unambiguous documentation for users and implementers
  - Interface contract
- Conformance testing
  - Run-time monitoring
  - Automatic test case generation
- Formal proof of correctness properties
  - Even without formal proofs, formal specifications are very useful!

Example: Specification of QUIC

- Formal wire specification of (a subset of) QUIC
  - Detailed enough to execute the protocol and interact with implementations
  - Automatically tested compliance four server implementations with the spec
- Discovered numerous errors caused by:
  - Misinterpretation of the RFC's
  - Ambiguities in the RFC's
  - Low-level coding errors
- Some were exploitable!
  - For example, client can read uninitialized memory of server

Takeaways

- Interoperability testing is not enough
  - Misses compliance failures
  - Leads to ossification and future security issues (e.g. SSL)
- Formal specification can be a solution
  - Allows us to detect compliance failures early
- There are hard trade-offs between uses
  - Readability *vs* testing *vs* formal proof
  - More work is needed!

We would like to understand how to integrate formal specifications into the IEFTF process. If you're interested in this topic, please join us at the side meeting of the Usable Formal Methods Research Group!