Cryptol: Writing a specification

Description A good specification expresses precisely what a function, hardware module, or system component is supposed to do. A lot of effort goes into defining a specification but the benefit is that if implementations can be verified against a specification then there is high confidence that the implementation is correct. A good specification depends on the language of specification – obviously, the C language would never be considered as a suitable language for writing specifications. The Cryptol language has been designed with specification writing in mind. Written on top of Haskell, Cryptol is a Functional and Declarative language. Pointers and pointer arithmetic are not the coder's worry, nor is execution control. Therefore, generally one can write a specification in Cryptol that one is confident about. The downside is learning how to use the language for this purpose can be difficult, especially when working with the Software Analysis Workbench which will be discussed in later lessons.

Purpose See how to write specifications in the Cryptol language.

Audience This module is intended for:

1 The general public
2 K-12 and college classes on cyber defense
3 preparation for proficiency in the use of tools and a computing environment suitable for the study of cyber defense

Objectives After completing the module:

1 Learners will have seen several different kinds of specification in Cryptol
2 Learners will know how to write Cryptol theorems to prove specification properties
3 Learners will know how to evaluate their specifications: do they work as intended?

Keywords verification, property, theorem, SMT, SAT solver, specification, confidence

Category cybersecurity > education

Delivery java applets and written documentation in pdf format

Team John Franco and Ethan Link

Assessment The applets provide the means for experimentation. Questions are asked in the documentation that help with the set up of experiments. The ideas that learners come up with is evidence that the module was successful.

Workflow No particular schedule was established

Environment All materials are contained in a single jar file. The jar file can be run on any computer where java version 14 or higher and some pdf reader such as acroread or evince are available. The jar file may be executed in the cyber range or learners may download the jar file (which is considered to be an executable file) and run it on their personal computers.