Digest: Description of Math Logic with Examples

Description Overview of Math Logic: what is it, why is it useful. Specifications and properties of code/algorithms/circuits. Simple example of Binary Search shows how a vulnerability that existed for decades without discovery can be discovered with Math logic via Cryptol. A fix is developed and proven to eliminate the vulnerability.

Purpose Motivate and prepare participants for the remaining lessons. The goal is to convince participants that Math Logic embodies a collection of tools that should be added to tools currently used to validate correctness and analyze code and circuits, especially from unknown sources.

Audience This module is intended for:

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

Objectives After completing the module:

1 Understand what Math Logic is and why it is important
2 Understand what a specification is and how to write one in Cryptol
3 Understand how a specification my be used to prove properties of hardware and software
4 Know who is currently using Math Logic wisely – Amazon, NASA, NSA, etc.

Keywords Math Logic, SMT Solver, SAT solver, ITP Solver, ATP solver, Propositional Logic, First Order Logic, Cryptol, Yices, ABC, Z3, CVC4, Boolector

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.