Software Analysis Workbench: Application to SHA256

Description Illustrate how SAW is used to show equivalence between implementations of C functions comprising a SHA256 digest solution and SHA256 specifications written in Cryptol. A collection of helpers for arrays, pointers and more is developed and used.

Purpose Begin getting familiar with constructs that can be used in SAW scripts. This is a followon to the previous lab. A learner will be able to solve this by referring to the solution to that lab.

Audience This module is intended for:

1 The general public
2 K-12 and college classes on Cyber Defense and Math Logic
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 Learner will know what SHA256 is and have C code for it
2 Learner will have created a Cryptol specification compatible with a C function that produces a digest.
3 Learner will have used helper utilities and built-in commands to prove equivalence of Cryptol specification with the C implementation

Keywords SHA256, Cryptol, Software Analysis Workbench, Formal Verification, Equivalence, Hash function, SHA256 Digest

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 11 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.