SAW: Examples proving C correctness against Cryptol specifications

Description Introduction to the Software Analysis Workbench. SAW can be used to prove that functions written in C, Java or other languages are equivalent to 'golden' specifications written in Cryptol. This can be done in several ways, depending on the target language. Example functions include find the first 1 in a word, in C and Java, and Salsa20 in C.

Purpose Use the SAW tool for advanced verification tasks

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 Learner will have some understanding of what SAW can do
2 Learner will be able to orchestrate a proof of system correctness
3 Learner will be acquainted with some examples using SAW

Keywords Software Analysis Workbence, Salsa20, Find First 1, Cryptol

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.