The Center for Cyber Defenders

Expanding computer security knowledge

Analyzing Software Vulnerabilities

Raisa Ifquat, University of Southern California
Caroline Kish, Georgia Institute of Technology

SAND2018-7596D

Project Mentor: Shelley Leger

Problem Statement:

Software vulnerabilities are often difficult to detect because the same type of vulnerability can present itself in a variety of ways across different contexts. The results from analyzing a large data set, such as the 2016 DARPA Cyber Grand Challenge (CGC) binaries, can help train and evaluate tools and processes for vulnerability identification. The small CGC binaries emulate multiple real world software applications and include known vulnerabilities, but they are not standardized to support easy analysis of the binaries.

Objectives and Approach:

- Modify the CGC binaries to create a data set that can be used for vulnerability analysis
- Conduct vulnerability analysis on source code and binaries from the DARPA CGC data set
- Find a method to isolate and test each vulnerability within each challenge
- Document a process to capture results from analyzing the vulnerabilities using existing methods such as static analysis tools or code auditing

Results

- Modified build process for the DARPA Cyber Grand Challenge binaries to allow code auditors / researchers to build the binaries based on vulnerability
- Added options to allow researchers to change the binaries and add or remove vulnerabilities as desired
- Documented vulnerability analysis of two binaries, leveraging the human as a starting point to standardize results reporting throughout the process of tracing and patching bugs in code

Impact and Benefits:

The results of our work can be used to support software vulnerability analysis, specifically in improving current analysis tools and augmenting machine learning data.

- Ease the process of automating testing and verification of vulnerability analysis tools
- Use the resulting data to contribute to machine learning efforts in detecting and correcting software vulnerabilities
- Use detailed annotations to support manual code analysis of additional software samples

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2017-XXXXC.