Research Spotlight Forum

8.6.19 Cybersecurity

Software Assurance at the Georgia Tech Research Institute (GTRI)

PRESENTED BY:

Joel Odom, SWA Branch Head, odom@gatech.edu

Sandia National Laboratories | Georgia Institute of Technology | The University of New Mexico | Illinois | NM State University | Purdue University | New Mexico Tech | The University of Texas at Austin

SAND2018-14303 O

ABOUT THE GTRI SOFTWARE ASSURANCE BRANCH

Dynamic Analysis

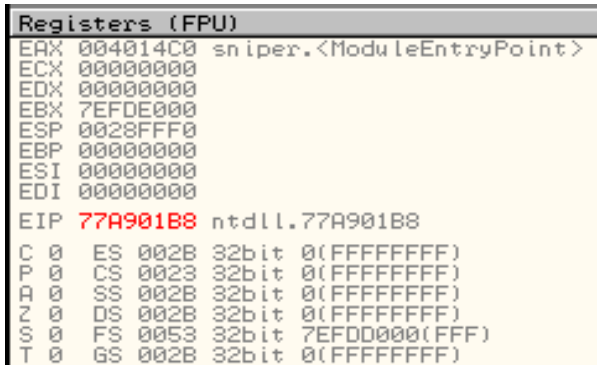
- Intelligent Fuzzing Using Debugging & Instrumentation
- Enterprise & Embedded Operating Systems
- Virtualized & Bare Metal Analysis

Static Analysis

- COTS Tools (Ghidra, IDA Pro, Coverity, ….)
- Custom Tools
- Symbolic Analysis of Binaries

Reverse Engineering

- Identify and Verify Software Functionality
- Perform Grey Box Analysis
- Enterprise & Embedded Systems
- Identify Vulnerabilities & Demonstrate Exploits



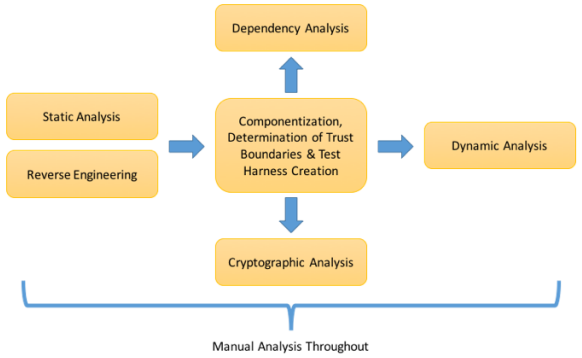
Keywords:

Software Assurance, Fuzzing, Reverse Engineering, Dynamic Analysis, Static Analysis

CURRENT WORK IN CYBERSECURITY

Software Analysis at GTRI

Software security analysis is inherently a task that requires technically skilled expertise. The following diagram shows the typical flow of a software security analysis at GTRI. The other quadrants on this chart discuss particular tools and capabilities that GTRI uses to perform more in depth analysis with less labor.

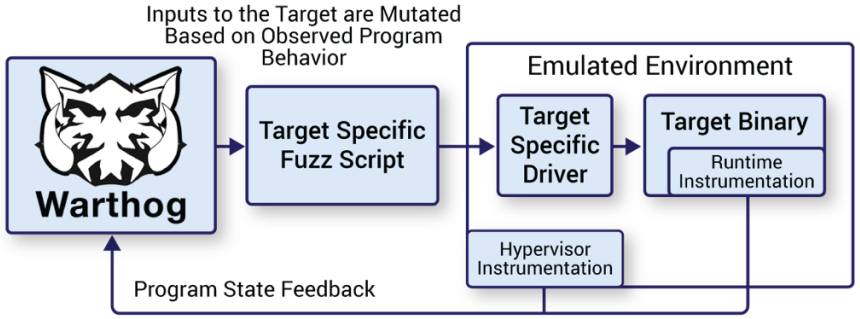


Human-Machine Cooperative Cyber Vulnerability Discovery Project

- Fuzz testing is effective at finding shallow bugs but can struggle to find bugs that require deep, complicated conditions.
- Our research combines concolic execution with analyst intuition, focusing the fuzzing on portions of the application likely to contain vulnerabilities.
- The automated tool prompts a user for help, learning what user input tends to provide the best results for driving the fuzzer.
- The human-machine cooperative cyber vulnerability discovery project was funded by GTRI IRAD funds, was matured with sponsor funds, and is currently at about TRL 5.

Warthog for Dynamic Program Analysis

Warthog is a cross platform dynamic analysis tool. Its key feature is its ability to fuzz different kinds of software targets, from enterprise to embedded targets. Proven operating systems include Windows, VxWorks, Linux and iOS.



Additional Software Analysis Tools & Techniques

- PiNetSim is a network services simulator developed by GTRI that allows us to mimic network services for realistic software analysis.
- Falafel is a FORTRAN static code analysis tool developed by GTRI.
- PITA is a static type analysis tool for Python developed by GTRI.
- GTRI is actively conducting research into debloating software libraries, particularly those that implement network protocols.
- GTRI has extensive experience in software reverse engineering (enterprise, embedded, and cyber-physical) for the purpose of security analysis.
- GTRI and GT's ECE have extensive experience in hardware emulation for the purpose of automated security analysis.

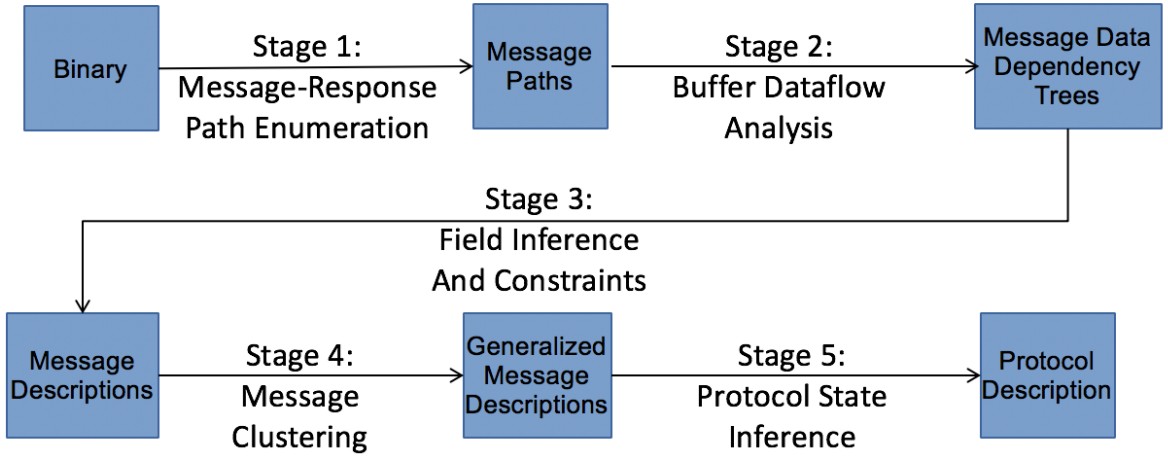
FUNDING SOURCES

Funding Sources Include the U.S. Government and Industry

- Primarily Department of Defense
- Industry Work Includes eVoting Security Funded by Smartmatic

Collaborations With Sandia National Labs

- Collaboration with Sandia Cyber Group on Automated Reverse Engineering
- New Collaboration with Sandia Kansas City Campus



RESEARCH NEEDS

GTRI seeks to "bridge the paper gap." We want to take fundamental research from academia and bring it to our sponsors to meet their operational needs. To this end, we welcome collaborations from academia wherein academia provides fundamental research and GTRI helps to operationalize that research. Of primary interest are:

- We seek technologies that can help to automate binary analysis. For example, plugins to Ghidra that can make a reverse engineer's job easier are welcome.
- When academia wants to work with the government, we can help. We understand working with the government and have various contracts in place that make this easy. We can also deal with the security requirements of the government.
- It has been a pleasure working with Sandia on cybersecurity problems. Expanded SNL collaboration is welcome.