TCIPG

Trustworthy Cyber Infrastructure for the Power Grid

Fuzz-testing of Proprietary SCADA/Control Network Protocols

tcipg.org

Overview and Problem Statement

Power control network asset owners may suspect that their equipment's proprietary protocols are susceptible to attacks via malformed crafted inputs, but lack the means of testing their assets and prioritizing them for protective measures (other than ordering expensive and specialized penetration tests). *Fuzzing* is a methodology for performing such testing; however, most fuzzing tools were developed for different environments and tasks (such as vulnerability development) and do not fit power network scenarios. Additionally, many tools assume that a specification of the targeted protocol is available, which is not the case for proprietary control protocols. Our LZfuzz addresses both the need for fuzzing proprietary protocols, and the specific features of a power control network environment.

Research Objectives

- Give SCADA/control network asset owners a simple way to test their assets for brittleness.
- Develop algorithms to efficiently fuzz proprietary SCADA protocols without specification or with only rudimentary specifications.
- Implement necessary network scaffolding to fuzz software/hardware that cannot be intrusively instrumented.
- **Smart Grid Application Area:** Securing control networks, in particular control center equipment and LANs such as energy management servers, front end systems, and analyst workstations.

Technical Description and Solution Approach

- LZfuzz creates a "network pipe" to intercept, analyze, and mutate targeted traffic, and does not require instrumentation of the targeted computers.
- LZfuzz uses a variant of the Lempel-Ziv compression algorithm to derive an approximate partitioning of a proprietary protocol's payload into "tokens," which it then fuzzes using a set of heuristics. Currently, these heuristics are provided by the GPF fuzzer.

Results and Benefits

- **Partnerships and External Interactions:** Used in network security assessment at a major power company.
- **Technology Readiness Level:** Beta.

Researchers

- Sergey Bratus, sergey@cs.dartmouth.edu
- Rebecca Shapiro, bx@cs.dartmouth.edu
- Sean W. Smith, sws@cs.dartmouth.edu
- Edmond Rogers, ejrogers@illinois.edu

funded by the U.S. Department of Energy and the U.S. Department of Homeland Security