LogicFuzzer Cybersecurity Framework

Accurate and reliable detection of process-destabilizing malware for PLC-based systems

Inventors at Georgia Tech have developed a cybersecurity framework called LogicFuzzer that aims to provide safeguards for programmable logic controller (PLC)-based systems susceptible to malware and malicious code. The framework offers a novel method of overcoming techniques that cybercriminals could use to hide malicious capabilities of code or program inserted into a PLC's memory. Specifically, automation representation techniques model program behavior and perform analyses to determine if specific physical processes are being targeted. LogicFuzzer also helps to determine if any program present in the PLC has malicious intent and should be isolated and destroyed. Initial testing demonstrates 98.9% accuracy in detecting the presence of malicious code.

LogicFuzzer works by combining binary analysis, fuzzing, and automaton theory. It first parses the binary programmable logic, extracting specific elements for further analysis when needed. It then creates a high-level data structure from the binary elements, which becomes an emulator for the code execution environment. A fuzzer then generates a complete behavioral model of the PLC program in the form of an automaton. This enables prediction of which process corresponds to the automaton. Finally, the detector component identifies unsafe states and the corresponding paths in the industrial process where these states could apply. This allows LogicFuzzer to quickly identify malicious code, and action is taken to activate the necessary safeguards.

Summary Bullets

- **Accurate**: Demonstrates high reliability in identifying the presence of malicious code and programs
- **Robust**: Identifies malware even if the attacker hides the malicious behavior (e.g., by using a logic bomb), since it is agnostic to large timer or counter values set to hide malicious code segments
- **Easy to use**: Eliminates the need for a training stage and requires only the binary program rather than source code

Solution Advantages

- **Accurate**: Demonstrates high reliability in identifying the presence of malicious code and programs
- **Robust**: Identifies malware even if the attacker hides the malicious behavior (e.g., by using a logic bomb), since it is agnostic to large timer or counter values set to hide malicious code segments
- **Easy to use**: Eliminates the need for a training stage and requires only the binary program rather than source code

- **Risk lowering**: Avoids the requirement for a run-time environment during usage, which may reduce the cost and risk associated with operation of physical industrial equipment and any damage incurred due to possible malware attacks
- **Reliable**: Demonstrates efficacy even when used in increasingly complex PLC programs

Potential Commercial Applications

- Manufacturing, production, and related operations (e.g., cement, glass, paper)
- Energy processing (e.g., oil, gas, petrochemicals)
- Control systems in buildings (e.g., escalators, elevators)
- Any PLC-based industrial control system

Background and More Information

PLCs are computers commonly used in industrial applications for automation of electrical, mechanical, or hybrid processes and are frequently utilized to manage and control power consumption by different equipment, particularly in manufacturing. These computers perform critical functions such as monitoring, measuring, and recording to assist in starting and stopping processes and help ensure robust and flexible manufacturing capabilities for myriad industries.

As state-supported and other cybercriminal activities increase, enhanced security for operations involving PLCs is needed in order to avoid disastrous effects. In particular, large-scale industrial applications ranging from electrical utilities to oil and gas refineries use PLCs, and malware attacks on those systems could result in catastrophic losses. Unfortunately, other methods of securing PLCs from malicious code have shortcomings that may keep them from providing the full and necessary level of protection. Current methods tend to be passive and react to anomalies after they appear or when certain conditions known as logic bombs occur. This makes it easy for system administrators to be fooled by long delays before a triggering event occurs. This can sometimes be overcome by analyzing source code, but it can be difficult to access, and timely analyses may be a challenge. By contrast, LogicFuzzer addresses these shortcomings by offering a proactive method of identifying malicious code in PLC-based systems without the need for source code or training stages. It scans binary PLC programs to detect malicious behaviors with a high degree of universality that requires little contextual information about the underlying physical processes.

Inventors

- Qinchen Gu
  Research Assistant - Georgia Tech Communications Assurance and Performance Group
- Dr. Raheem Beyah
  Dean and Southern Company Chair - Georgia Tech College of Engineering

IP Status

The following patent application has published : US20230050691A1

Publications

, -

Images

Visit the Technology here:
LogicFuzzer Cybersecurity Framework
