Review of 'A HYBRID TECHNIQUE FOR SQL INJECTION ATTACKS DETECTION AND PREVENTION' and 'Using Static and Runtime Analysis to Improve Developer Productivity and Product Quality'

Qing Peng

The paper begins with static analysis, which prevents problems from entering the main code stream and ensures that any new code is up to standard. Using techniques such as abstract syntax tree (AST) validation and code path analysis, static analysis tools can uncover security vulnerabilities, logic errors, implementation defects, and other problems, both at the developer's desktop and at system build time. The paper then explores runtime analysis, which developers can perform during module development and system integration to catch any problems missed by static analysis. Runtime analysis not only detects pointer errors and other violations, but also helps optimize utilization of CPU cycles, RAM, flash memory, and other resources. The paper then discusses how developers can combine static and runtime analysis to prevent regressions as a product matures. This two-pronged approach helps to eliminate most problems early in the development cycle, when they cost least to fix.

In the article of "A HYBRID TECHNIQUE FOR SQL INJECTION ATTACKS DETECTION AND PREVENTION"(referred as "hybrid techniques" in this article), the author came up with a technique combining static and runtime SQL queries analysis to detect and prevent various types of SQL injection attacks(SQLIAs). And in the article of "Using Static and Runtime Analysis to Improve Developer Productivity and Product Quality"(referred as "static and runtime analysis" in this article), the author began with static analysis, and then explored runtime analysis, and discuss how developers can combine static and runtime analysis to prevent regressions as a product matures. "hybrid techniques" focused on creating a hybrid technique, while "static and runtime analysis" focused on the analysis and comparison of static and runtime analysis.

Since "hybrid techniques" created a technique to solve the problem of SQL injection, it introduced what is SQL injection at first to give the readers a background. "Hybrid techniques" illustrated why is SQL injection attacks a common problem for web applications, and it mentioned that there was no method that can cover the whole wywtem from being attacked by SQL injection. "Hybrid techniques" came up with the first mechanism to handle the security of database, which is to ensure the access is well controlled. And it categorized attackers into several types, analyzed the methods they usually use to attack the database systems. However, "static and runtime analysis" focused on the static and runtime analysis, so it introduced to the readers about the two techniques at first.

"Hybrid techniques" briefly compared the three types of aspects to detect and prevent SQLIAs, including static analysis, runtime analysis and static and runtime analysis. While "static and runtime analysis" gave detailed analysis about static and runtime analysis. It compared the two techniques in multiple aspects like phases, environment, labor costs and so on. "Static and runtime analysis" listed the pros and cons of the two techniques, such as static analysis can analyze existing code bases that have already been tested, but it has non-zero false positive rate; and runtime analysis generates few false positives, but it impairs realtime behavior.

"Hybrid techniques" introduced the three-tier architecture, and summerized the steps of exchanging data among the three-tier system architecture. Then it proposed a strategy that is a runtime detection and prevention methodology based on providing security controlling methodology on the database server side. There are six stages in the approach: 1. replicate system databases 2. creating "database_behaviors" database 3. redirect SQL queries 4. simple SQL syntax checking 5. virtual execution 6. SQLIA detection Then it evaluated the approach by developed it using VB .Net, and simulated the application to analyze the performance and accuracy of the detection and prevention processes. The result concluded that the hybrid technique covers all types of SQLIA and it is the only technique that prevent sthe direct attack type. While "static and runtime analysis" illustrates how it analyzed static and runtime techniques, and summarized the workflows for the two techniques, and listed the liburary instrumentation to test the techniques. After the analysis of the two techniques, it discussed the role of RTOS architecture, which can make programming errors easier todetect, isolate and resolve.

References:

[1] Graham, B., Leroux, P. N., and Landry, T. "Using Static and Runtime Analysis to Improve Developer Productivity and Product Quality," white paper, QNX Software Systems, April 2 [2] Jalal Omer Atoum and Amer Jibril Qaralleh "A HYBRID TECHNIQUE FOR SQL INJECTION ATTACKS DETECTION AND PREVENTION", Princess Sumaya University for Technology, Amman, Jord, February 2014