

"A Static Analysis Technique for the Detection of TOCTTOU Vulnerabilities"

Abstract

Software quality is the cause of many vulnerabilities. Using ASTLOG, I built highly accurate call graph and control flow graph generators. The graphs were fed to another program which looked for TOCTTOU file access race condition vulnerabilities (a.k.a. /tmp races). The final product highlighted possibly vulnerable code segments. Future work includes building an ASTLOG workalike for other compilers, expanding the type of vulnerabilities searched for, and implementing data flow analysis in order to improving the accuracy of the search tool.

Thesis available at <http://atlantis.cs.ucdavis.edu/~anguiano>.