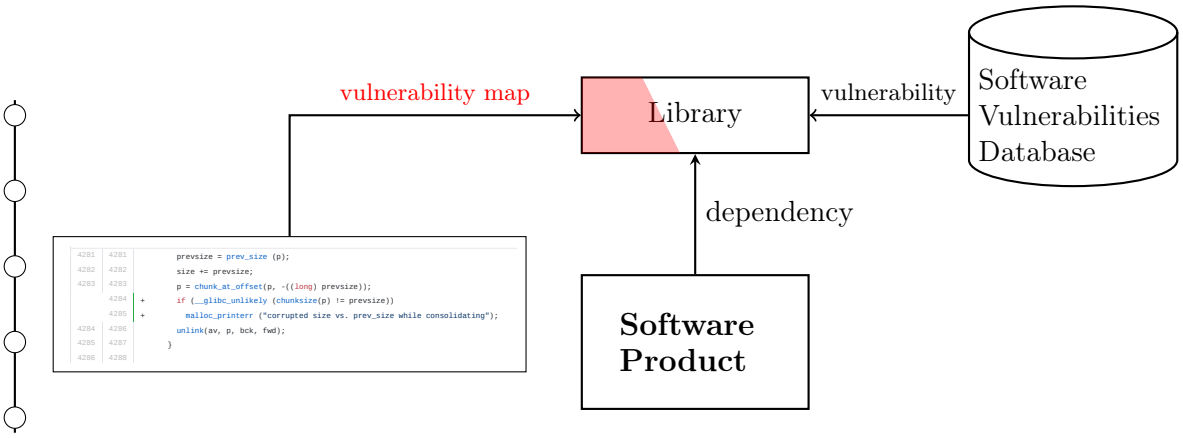
Exjobb: Refining Security Vulnerability Detection

17 december 2018

Wanted: One or two students interested in software security and program analysis. At least one of you should have taken the Compilers course.



Each year, security researchers find tens of thousands of new vulnerabilities in existing software. Embedded software developers often rely on tools and libraries that are affected by these vulnerabilities, but it can be hard for the developers to stay on top of all the latest security developments. The SECONDS project here at LTH has developed a technique that:

- Analyses program build files
- Extracts dependencies and version identifiers
- Compares the dependencies + versions against a vulnerability database

While the project has been commercially successful, it reports some *false positives*: if a library has a security vulnerability, it is often only a small part of the library that is affected.

In this project, you will refine the existing solution by applying program analysis techniques:

- Build a tool to analyse which parts of a library were affected by a vulnerability:
  - Compute differences between known-insecure and known-fixed versions
  - Identify affected functions and their callers
  - Build a library vulnerability map
- Build a tool to scan programs with your vulnerability maps
- Evaluate your work with programs that depend on libraries with known vulnerabilities

This is a joint project between EIT (Martin Hell, martin.hell@eit.lth.se), Software Engineering (Martin Höst, martin.host@cs.lth.se), and Software Development & Environments (Christoph Reichenbach, christoph.reichenbach@cs.lth.se). Contact us for details!