Tracing the Bugs  
(Visualization of Software Vulnerabilities)

Motivation
Allegedly small software implementations, such as an off by one-write here, and a missing boundary check over there often result in devastating security vulnerabilities. Buffer Overflows, and Integer overflows, are two of the most prominent members of this class of problems.
In this project we want to design, and implement a tool-chain for visualizing the effects of buffer overflows (and possibly integer overflows) in context of small vulnerable test programs. The input for the toolchain should be suitably annotate , simple C programs. The output should be an easy to understand, interactive visualization of the contained exploit.

Project Description

Goals
• Investigate usability of the Low-Level Virtual Machine (LLVM) framework as basis for your toolchain
• Design and implement a prototype of the exploit visualization tool-chain

Background
• Good C and C++ programming skills
• Skills in graphical user interface and/or web user interface
• Interest in software vulnerabilities, compilers, assembly code

Deliverables
• Tool prototype (source code in GIT repository)
• Documentation/Tech Report
• Short presentation (15-20 min)

Scope and Credits
Studies: ☑ INF ☑ SEW ☑ TEL ☑ MATH
The scope, effort, and credits of this project are scalable for 1-2 participants.

Advisor/Contact
Johannes.Winter@iaik.tugraz.at