

Simulation and Visualization of Software Exploits

Motivation

Buffer overflows and finite arithmetic effects are still one of the major sources of security critical software bugs. In research and education we face the challenge of demonstrating and explaining these attack vectors to a wide audience in a reproducible and easy-to-understand way.

We started to implement a small simulator for the ARM Thumb instruction set, which provides instrumentation facilities for memory and registers accesses. In order to use this simulator for demonstration of software exploits, we need to *visualize* the effects of the exploits in an intuitive manner.

Project description

Goals

Develop and test a tool for visualization of software exploits.

Tasks

Design an easy to use graphical user interface for the simulator.

Develop methods to visualize the effects of software exploits on memory, registers and control flow.

Evaluate the visualization techniques using small vulnerable programs which contain typical implementation bugs. (buffer overflows, integer overflows, ...)



[Image source: <http://www.stevenbrown.ca/blog/archives/225>] (CC BY-NC-SA 2.5)

Deliverables

Source code of the prototype (GIT repository)

Documentation

Presentation (10-20min)

Master Project

Studies: ✓ INF ✓ SEW ✓ TEL ✓ Tech. Math.

Prerequisites

Interest in software exploits and bugs

Basic knowledge of the C# programming language

Contact

Daniel Hein <daniel.hein@iaik.tugraz.at>

Johannes Winter <johannes.winter@iaik.tugraz.at>