Lehrstuhl für Sicherheit in der Informatik
Prof. Dr. Claudia Eckert

Fraunhofer AISEC

Bachelor's/Master's thesis in collaboration with Fraunhofer Research Institute AISEC

Construction of a Highly Vulnerable Executable for ARM Linux Platforms

Date: *August 8, 2017*

Description

Memory errors, such as buffer overflows or use-after-free errors, are vulnerabilities in unsafe programming languages (e.g. C or C++) which are commonly used as starting point for different kinds of low-level exploits. Simple code injection on the stack, Return-oriented Programming (ROP) and information leaks are examples of exploits enabled by memory errors.

To secure systems and programs against those attacks, many different defensive strategies have been proposed. Some of those techniques, such as Data Execution Prevention (DEP), Stack Canaries and Address Space Layout Randomization (ASLR), are widely adopted in state-of-the-art systems. The adoption of other defensive mechanisms, such as fine-grained Control Flow Integrity (CFI) or memory safety extensions for C and C++, is hindered by their performance penalty and sometimes unclear security margin. While performance can be tested quite easily using one of many available benchmarks, it is typically difficult to quantify the security gained by using a specific mechanism.

The goal of this thesis is the construction of a highly vulnerable executable for ARM Linux platforms, similar but not limited to the functionality of RIPE for x86[1]. The resulting testbed can be used to evaluate and compare the effectiveness of memory error defense mechanisms. The binary should be able to test exploits of varying complexity on itself reaching from simple code injection over ROP to data-only exploits.

Requirements

- Ability to work independently and accurately
- Good C programming skills
- Basic knowledge of exploit techniques, ARM assembly and Linux
- Strong interest in advanced exploit techniques, defensive strategies and ARM architecture

Contact

Julian Horsch
E-Mail: julian.horsch@aisec.fraunhofer.de

Fraunhofer Institute for Applied and Integrated Security (AISEC)
Parkring 4, 85748 Garching (near Munich), Germany

[1] https://github.com/johnwilander/RIPE