Abstract

This thesis presents new methods contributing to the area of software security. Both offensive and defensive methods are proposed, where the offensive methods presented in this thesis mostly deal with how an attacker can embed malicious code in a stealthy manner, and the defensive methods aims at detecting some form of attack.

The first approach deals with how a virtual machine can be detected and we discuss its use as both an offensive as well as a defensive method. We develop a proof-of-concept that aims to demonstrate how the technique works in practice.

Next we implement a GlobalPlatform compatible RPC mechanism utilizing both a hypervisor and SELinux and provide some benchmarks for both solutions.

Following this we will look at timestamping of data on a massive scale and how by utilizing the blockchain of the Bitcoin network, we can gain Byzantine fault tolerance for the Keyless Signing Infrastructure.

Then we will look at methods for obfuscating code by overlapping assembly instructions in machine code. We do this both by crafting custom no-operation instructions in the binary, but also provide a method to accomplish this in the source code when that source code will be compiled via a deterministic building process to produce the expected binaries.

Finally this thesis will conclude with a method for detecting Return Oriented Programming attacks by analyzing the raw data of a network stream.