Technische Universität München
Lehrstuhl für
Netzarchitekturen & Netzdienste
Prof. Dr. Georg Carle

20.04.2011

Bachelor-/ Masterarbeit

Inline Fuzzing

Discovery of defects in protocol implementations

Motivation

Implementations of ***application-level protocols*** are often not extensively tested, in particular regarding the handling of incoming messages which are erroneous and do not follow the expected format. As a result, defects in the logic or implementation of the protocol risk to remain undetected. If these bugs represent security flaws, they may be exploited by an attacker. In the worst case, sending a single specially-crafted message may be sufficient to cause a buffer overflow and inject malicious code.

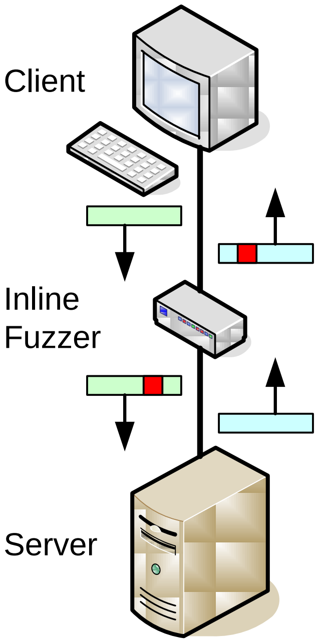
"Fuzzing" covers techniques for testing the behavior of applications in the presence of unusual or invalid input data. Most existing protocol fuzzers rely on a-priori knowledge of the considered protocol in order to generate messages with specific uncommon field values. Since such knowledge is often not available for proprietary protocols, this thesis deals with the manipulation of existing traffic on the wire using heuristics and statistics gained from the original traffic.

Task Description

The first objective is to develop a customizable and easy-to-use ***inline fuzzer*** which allows manipulating messages exchanged between two end systems (e.g. between client and server). The fuzzer shall also be able to monitor the behavior of the end systems and detect when an the end system has crashed (e.g. due to a manipulated message).

The second objective is to conceive and implement several ***fuzzing algorithms*** which apply different modifications to the packets. The decision about how to modify the packets may rely on heuristics and statistics gathered from previous observations of the communication.

The effectiveness of the inline fuzzer shall be demonstrated by testing the robustness of existing network application.



Requirements

Linux skills, programming skills in C/C++

Contact

Lothar Braun, Gerhard Münz (Siemens CERT)
Email: braun@net.in.tum.de   Tel.: 289-18010