Interdisciplinary Project

Static and dynamic security testing of an embedded device actively used in industry (AISEC)

Nowadays, many security vulnerabilities in software are found either via static application security testing (SAST) or via dynamic methods such as fuzzing. Depending on the target, however, both methods have limitations and require different amount of effort to be set up.

Your task will be to set up a SAST-tool developed at AISEC and an established opensource fuzzing-tool on an embedded device actively used in industry that handles network traffic. This device is running a common Linux kernel with custom extensions written in C/C++. For fuzzing purposes, suitable interfaces for virtualization are provided.

Once set up, the results of both security testing methods should be analyzed and harmonized.

Prerequisites

• Basic programming experience (C/C++)
• Ability to work self-directed and systematically
• Experience and knowledge in security testing is an asset
• Experience with Linux is an asset

If you are interested and would like to know more, please refer to the persons mentioned below.

Please send your application with current CV and transcript of records to:

Contact

Hannah Schmid
Ferdinand Jarisch
Tel.: +49 89 322-9986-130
Tel.: +49 89 322-9986-166
E-mail: hannah.schmid@aisec.fraunhofer.de
E-mail: ferdinand.jarisch@aisec.fraunhofer.de

Fraunhofer Research Institute for Applied and Integrated Security AISEC
Department Product Protection and Industrial Security
Lichtenbergstraße 11, 85748 Garching near Munich, Germany https://www.aisec.fraunhofer.de

Advisors

Georg Sigl
Hannah Schmid, Ferdinand Jarisch (Fraunhofer AISEC)