CENTER FOR
DIGITAL SAFETY & SECURITY

AUSTRIAN INSTITUTE OF TECHNOLOGY

MACHINE-CODE ANALYZER - SEMI-AUTOMATED ANALYSIS OF MACHINE CODE

CHALLENGE: HIDDEN FUNCTIONALITY

Running any **third-party software** requires you to have trust in the software supplier not to have added any hidden functionality that could endanger your business, or delivered a product full of systematic weaknesses that an attacker can exploit. Especially when dealing with software that uses cryptographic algorithms it is important to check whether there are no such **hidden weaknesses**.

Techniques like penetration testing, fuzzing, etc., offered by AIT, help to reduce risks involved, however, to gain the highest level of confidence in the software, investment in manual analysis is necessary. This is an expensive and time-consuming process, often carried out on the machine code level, as the source code of the software usually is not available.

AIT's Machine-Code Analyzer is a tool helping you with this analysis, as it is able to point out program-locations in need of further inspection and program-locations without this need.

HOW IT WORKS

AIT's Machine Code Analyzer takes an **application and a set of machine-readable requirements as inputs**. It runs the application and watches the execution. It looks at the dataflow inside the application, at the use of memory locations, and generally monitors the control flow coverage and checks whether the application meets the requirements specified. This way it can point out potentially unsafe instructions, information leaks, and other critical issues.

In addition to this, the tool will automatically create new program inputs so that the next run of the application will go down paths in the control flow graph that have never been taken before. This way, the tool is able to **discover functionality hidden in the application**, triggered with special inputs only.

KEY FEATURES

- **Maximum confidence** gain through machine code analysis
- Focus on **cryptography algorithms** in programs
- **Automation** of your program analysis workflow

THE TEAM

The Dependable Systems Engineering research group at the AIT Austrian Institute of Technology has a systematic understanding of the development process of safety-critical and dependable systems. The group's expertise ranges from developing new standards, over providing workflow support, to verification & validation activities like testing and runtime verification.

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
Willibald Krenn
Tel +43(0) 50550 4109
Giefinggasse 4, 1210 Wien
willibald.krenn@ait.ac.at
www.ait.ac.at