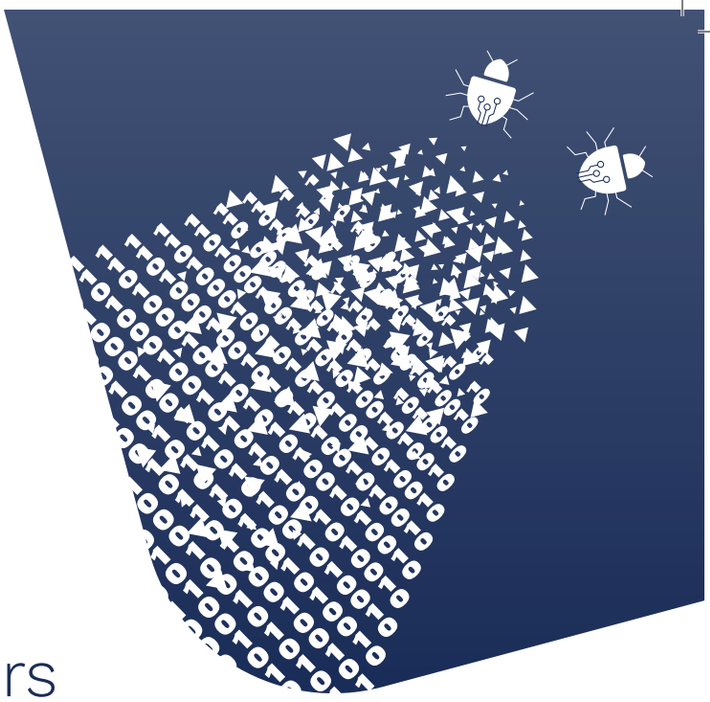
KUDELSKI IOT THINGS



CYBERSECURITY RISK MANAGEMENT

Fuzz Testing for Automotive Manufacturers

New vehicles are becoming increasingly connected and software based. The number of semiconductor components in vehicles is expected to quadruple over the next few years, driving new security regulations in an industry where security expertise is already scarce. Increased connection increases the attack surface that hackers can exploit to threaten automotive security and safety. Fuzz testing is a technique that consist in injecting the system under test with a large number of inputs with the aim of finding vulnerabilities.

BENEFITS

Advantages of Fuzz Testing

Automation
Save time and resources compared to manual testing.

Customization
Target specific vulnerabilities or areas of the surface or software that you need to test.

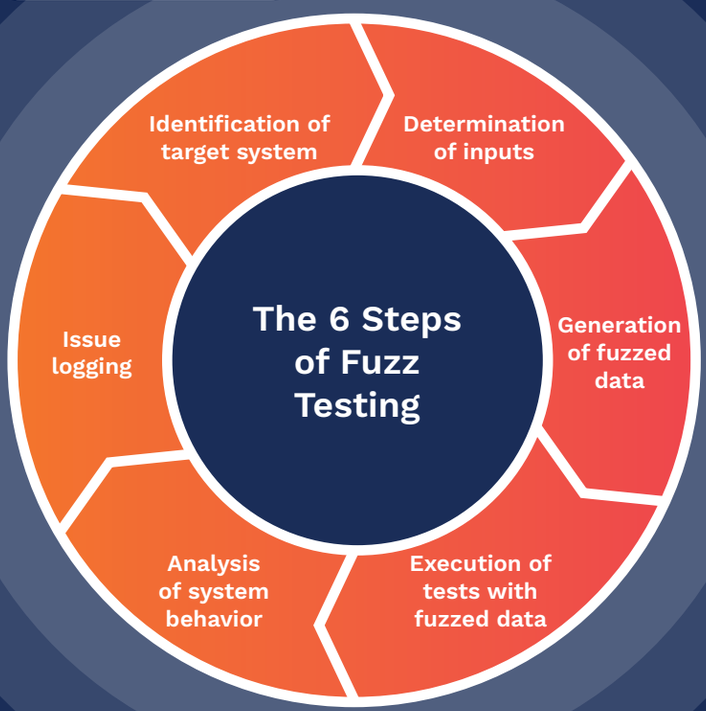
Scalability
Test your entire program or software rather than just small parts of it.

Integration
Incorporate fuzz testing into an overall testing strategy.

WHY US

Expert IoT Security Lab

1. Qualified, certified, industry-experienced security penetration and fuzz testers.
2. Breadth and depth of testing including the most advanced realworld attack scenarios.
3. Close collaboration and constant communication with client to achieve testing goals on time.



APPROACH

How we engage

1 Define Scope & Goals
We meet with the client to determine testing objectives, scope, and rules of engagement.

2 Execute Fuzz Testing
We plan and implement the process, from test cases to delivery, failure examination, and fix determination.

3 Prepare Deliverables
We carry out technical and business impact analysis to develop recommendations.

4 Report & Recommend
We present actionable, prioritized recommendations to key stakeholders and deliver final report with full analysis.

5 Test and Validate
We can retest vulnerabilities to verify that recommended remediation action plans were indeed successful and that no other vulnerabilities have been introduced during the remediation phase.

OUTCOMES

What we deliver

Fuzz testing results can vary depending on the specific goals and objectives of the testing, which will be unique to each client and testing plan. Some potential outcomes of fuzz testing include:

1 Identify Vulnerabilities
Fuzz testing can help identify security vulnerabilities, such as buffer overflows or injection attacks, that could be exploited by attackers.

2 Identify Program Failures
Fuzz testing can help identify failures in a program's functionality, such as crashes or hangs, that may occur when the program is exposed to invalid or unexpected inputs.

3 Generate Test Cases
Fuzz testing can generate test cases that can be used to validate the correctness and reliability of a program.

4 Improve Program Robustness
By identifying and addressing vulnerabilities and failures, fuzz testing can help improve the overall robustness and reliability of a program.

5 Provide Test Evidence
Fuzz testing can provide evidence that a program has been thoroughly tested, which can be useful for demonstrating compliance with industry standards or regulations.

DELIVERABLES

Executive summary
An overview of the most significant strengths and weaknesses of the security measures pertaining to the assets in scope.

Technical Findings
A technical listing of vulnerabilities identified, their exploitation, and potential business risk.

Actionable insights
Vulnerabilities are prioritized with a global ranking, in order to highlight remediation actions with the greatest impact.

Attack Scenarios
A high-level conclusion that helps the CISO communicate effectively with the Board about security priorities.

v1.2

Contact us: info@kudelski-iot.com