Penetration Testing

Karamba Security

Karamba Security's Penetration Testing services enable OEMs and Tier 1 suppliers to uncover critical cyber vulnerabilities and validate the final release before SOP.

We pentest images and interfaces of the vehicle, subsystems, and component software levels, identifying and prioritizing weaknesses according to the ISO/SAE 21434 standard.

With a track record of dozens of pentesting projects, our team of experts identifies vulnerabilities and explains cyber-attack scenarios. After weaknesses are identified, our team prioritizes their fixes according to possible exploit impact and likelihood and then updates the TARA as needed.

Pentesting Objectives

To develop the required ISO/SAE 21434 Work Products (WP-10-05, WP-10-06, WP 10-07, WP-11-01) Karamba performs Verification and Validation tests:

- Verify that cybersecurity mitigations are in place as planned, and are actually effective against hacking!
- Confirm a minimized level of weaknesses and vulnerabilities in the release candidate, including design-level weaknesses (whether identified or not in the TARA).

Examples of the pentest scope that usually delivers the most value to the OEM and Tier 1 in addressing the standards expectations and reducing risk levels:

- Test in-vehicle connectivity (CAN, Lin, Ethernet)
- Firmware upgrade process
- HSM + Key management
- Secure Boot
- Diagnostics
- OS/BSW, VM, and external libraries

Pentesting Methods

To accomplish the standard's objectives, and being practical about cybersecurity testing, Karamba recommends using a “Gray Box” approach, in which there is assistance to the external tester with documentation, images and keys. This approach saves time and reduces budgets and allows the pentesters to identify many findings with reasonable efforts.

Karamba's researchers can also perform “Black Box” testing in which they mimic the attack on the vehicle and provide a superficial “status report” in the eyes of an expert attacker. This method is usually more expensive, and it does not provide all WPs required by the standard.

Another service can include “White Box” in which Karamba performs testing based on code review. This method is the most accurate and valuable for developer teams, however it is slow and expensive and might not be needed, given the CAL risk level of the component.

Pentesting in Practice

Stage 1 - Setup:

- Reading all relevant documents and understanding the target system behavior and possible security focus area.
- Setting up the testing environment to simulate attack scenarios, including all automotive interfaces and connections to the pentest tools. Such tools include the proven tools and scripts used by Karamba on multiple automotive pentesting projects.
- Karamba's Cybersecurity Lab setup is used whenever possible, to reduce costs and assure consistency among projects.

Stage 2 - Fuzzing and Interface testing:

Other important and common techniques include fuzzing by sending invalid random data into the unit, causing it to crash and reveal bug flaws. Vulnerability assessment, identifying any vulnerability in the image.

Stage 3 - Reverse engineering:

Researching the actual binary image of the components provides deep understanding of the interface testing results, and can identify vulnerabilities in the implementation of the application or the security mitigations.

The binary research stage requires a deep understanding of embedded software and brings to light Karamba's unique expertise in embedded development and security research techniques.

Stage 4 - Report and presentation:

Throughout the testing process, working closely with R&D and sharing findings, Karamba supports agile development methods and adjustments of priorities in the final released version.

At the end of the project, Karamba's team reviews the results with the customer and offers reports, guidance, and remediations best suited to the customer's needs.

The findings report includes:

- Approach and findings
- Test methods and tools
- Details of vulnerabilities found with their severity
- Recommended fixes and improvements

This report can then be submitted as part of the UN R155 Work Products package.

Karamba Security's Pentesting is just one of our End-to-End Product Security Portfolio elements that enable our customers to discover, mitigate and manage security vulnerabilities in their ECUs and vehicle types. Enabling customers to expedite their compliance with cybersecurity standards without slowing down innovation, Karamba leverages automated tools and a cost-effective pragmatic approach.