FRANÇAIS ENGLISH

cea leti

CRAB

PATENTS 7+ PATENTS

Guaranteed secure, CRA-compliant embedded systems

What it is

CEA-Leti drew on its knowledge of embedded systems and cybersecurity to develop CRAB, a comprehensive characterization and test bench with tools to assess the software and hardware security of embedded systems.

The wide range of tools available can be used to complete specific security analyses and tests—to ensure compliance with new regulatory requirements, for example—or to explore an embedded component's or system's resilience to cyberattacks.

The test bench can be used to determine certain digital products' level of assurance or to identify any potential regulatory compliance issues.

What it can do

With the EU Cyber Resilience Act (CRA) now in force, CEA-Leti's test bench responds to the current and future cybersecurity needs of:

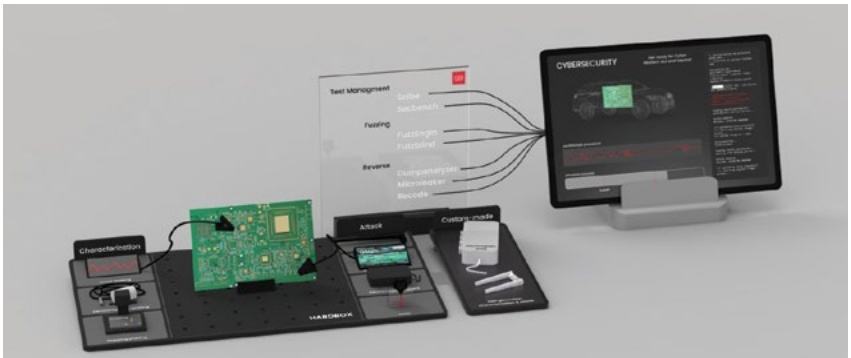
- **Manufacturers of digital products subject to CRA requirements**: CEA-Leti's test bench is suitable for all products with digital elements subject to the regulation.
- **Traditional security compliance assessment providers**: Testing and certification organizations can use CEA-Leti's test bench to extend their cybersecurity capabilities and offer new services.

CEA-Leti's characterization and testing capabilities can also be used to gain a deeper understanding of threats and, therefore, determine how relevant a threat actually is, or stress test a system's resilience.

What makes it unique

CEA-Leti's test bench includes new proprietary tools and methods that can be used in addition to the testing and characterization resources currently available on the market and more effectively respond to future threats:

- High-performance, low-cost tools can be used to characterize the real and future potential of certain attacks.
- Custom development work using open-source technologies can be completed to respond to specific business or regulatory requirements.
- The tools integrated into CEA-Leti's test bench cover a wide range of security features.



▲ *CRAB demonstrator*

Working with CEA-Leti

Manufacturers of connected digital products and cybersecurity organizations concerned by CRA requirements or strict market-specific standards (medical devices, automotive, etc.) can take advantage of CEA-Leti's and security testing tools and expertise to:

- Analyze an existing system to identify any potential compliance issues.
- Ensure systems being designed now respond to future requirements, with support from testing to design updates.
- Obtain recommendations and methods for a variety of specific use cases.
- Learn the skills and acquire the tools to create in-house testing capabilities with CEA-Leti's easy-to-use semi-automated tools, which can be adapted to different needs.

Complete coverage

- Side channel, laser injection, electromagnetic interference, and other hardware security tests.
- Software security testing using reverse engineering, inference, fuzzing, etc.

Scientific publications

- Loubier, T., Sauze Kadar, M., (2025). *A Multi-Model Approach to Enhance Automatic Matching of Vulnerabilities to Attack Patterns*. Secrypt.
- Vincent, U., Hiscock, T., Hely, D., (2026). *DuskFuzz: Encoding Side-Channel Information to Improve Blackbox Fuzzing*. CASCADE.

Interested in this technology?

Contact:
Marion Andrillat
marion.andrillat@cea.fr
+33 647 220 861

CEA-Leti, technology research institute
17 avenue des Martyrs, 38054 Grenoble Cedex 9, France
cea-leti.com

@CEA-Leti

Research for industrial innovation