PRESS RELEASE

For Immediate Release

Exposing Embedded Security Gaps: Emproof at Embedded World 2025

Emproof
Hall 4, Booth 4-139c
Embedded World 2025, Nuremberg
11-13th March 2025

18th February 2025 – Emproof will be at Embedded World next month to highlight the growing threat of reverse engineering in embedded systems and demonstrate how manufacturers can better protect their devices from exploitation.

Many OEMs rely on encryption and hardware security, but attackers are increasingly bypassing these measures by exploiting vulnerabilities in software. Using widely available tools like Ghidra, hackers can extract cryptographic keys, steal intellectual property, and modify firmware, often without needing advanced technical expertise. As these threats grow, regulatory bodies are introducing stricter security requirements for embedded systems.

At Embedded World, visitors to Hall 4, Booth 4-139c can explore practical ways to strengthen software security and ensure compliance with evolving regulations. Experts from Emproof will demonstrate how embedded developers and manufacturers can protect their firmware against reverse engineering, code injection, and other emerging threats, without disrupting workflows or requiring access to source code.

With regulatory deadlines such as the Cyber Resilience Act (CRA) approaching, compliance is an increasing concern. Independent testing by Cetome has confirmed that Emproof Nyx, a binary-level security solution, reduces attack surfaces and helps mitigate security incidents, offering a practical path to meeting regulatory requirements. Designed to work across architectures including RISC-V, ARM, Tri-Core, and x86_64, Emproof Nyx enables manufacturers to implement robust software security without disrupting their existing embedded system designs.

For those wanting a deeper understanding of reverse engineering risks, Nils Albartus, Embedded Security Specialist at Emproof, will present *Demystifying Reverse Engineering Attacks on Embedded Devices* on 11th March at 12:00 PM as part of the Safety & Security session (Session 3.1). His talk will break down how attackers analyse embedded software, what tools they use, and how businesses can stay ahead with effective mitigation strategies.

<ENDS>

Image caption: Attackers bypass OEM security measures through software vulnerabilities.

About Emproof

Emproof was founded at Germany's Ruhr-Universität Bochum, a top international university and research institute with a global reputation for its work in developing innovative measures against cyberattacks. Founders Marc Fyrbiak, Phillip Koppe and Tim Blazytko met at the university while researching IT security. Emproof's solution Emproof Nyx delivers high levels of security and IP integrity for embedded systems, using unique techniques that protect algorithms and data while securing the entire device. It prevents reverse engineering, secures intellectual property and protects against exploitation attacks. Hardware and software agnostic, Emproof Nyx, can be implemented at any stage of the product lifecycle, saving time, money and resources.

Bio Nils Albartus

Nils Albartus is an embedded security specialist at Emproof and a PhD candidate at the Max Planck Institute for Security and Privacy in Bochum, Germany. With a broad expertise in embedded systems and a specialization in reverse engineering, he focuses on developing robust protections against reverse engineering tactics. Beyond his technical endeavors, Nils is committed to educating both professionals and students in effective security practices, nurturing the development of future security experts.

For more information, visit www.emproof.com

For editorial enquiries, please email: melanie@kava-agency.com