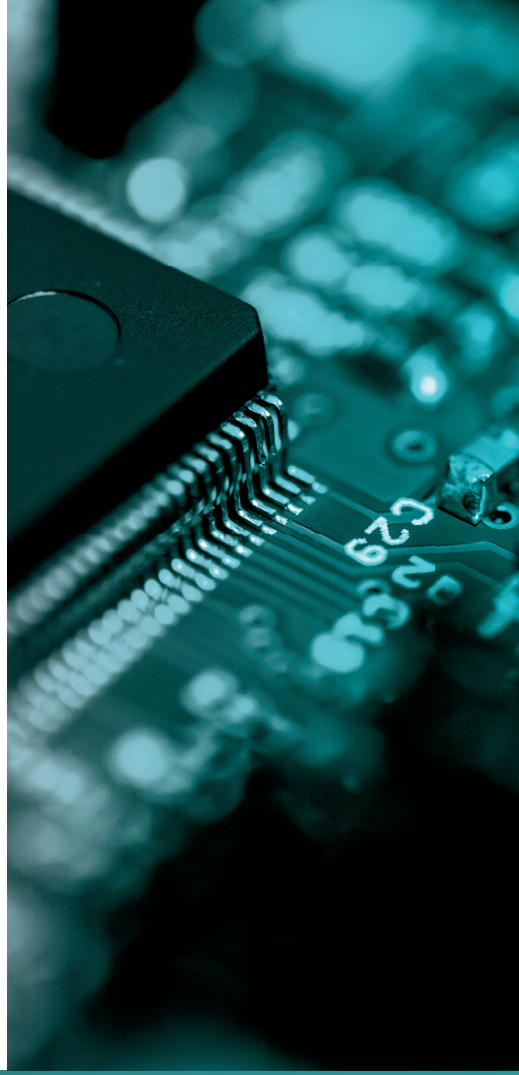
emproof
embedded security

Embedded security

No longer inconsequential



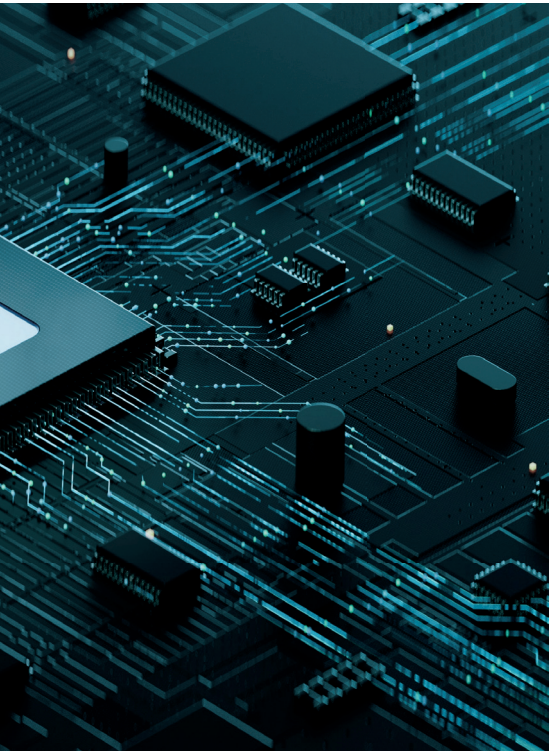
Introduction

Cybersecurity is not an optional investment in the evolving digital age. The ubiquity of embedded systems is growing exponentially. However, the threat levels continue to develop at a rapid rate and the demand for a holistic response to safety and security is more important than ever.

Since the introduction of the EU Cyber Resilience Act and US National Cybersecurity Strategy, which together bolster cybersecurity rules to ensure more secure hardware and software products, embedded security is now a must-have. Not only by your board but by government agencies as well globally.

Embedded devices are at risk, targeted by IP thieves and malicious attackers. Embedded systems don't follow one set of rules. They work with different hardware, toolchains and operating systems.

Mission-critical embedded systems are insufficiently protected.



The current reality is:

- There are practical methods for accessing and attacking embedded devices.
- Attacking embedded devices is profitable.
- User and manufacturer inaction is incentivised.

There is a need to establish sufficiently flexible and resilient systems so that they can rapidly adapt to hazards and new dangers.

Counterfeit components that have been reverse-engineered not only affect a company's bottom line but could also have a devastating impact on brand credibility and reputation in a world with billions of connected devices.

Emproof delivers high levels of security and IP integrity for embedded systems, using unique techniques that protect algorithms and data while securing the entire device.

Our solution, Emproof Nyx, prevents reverse engineering, securing your valuable intellectual property and protecting against exploitation.

Companies lose $200bn per year due to product piracy and cyber-attacks.

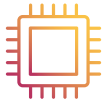
What is embedded security?

Embedded security focuses on preventing malicious access and use of embedded systems providing mechanisms to protect a system from all types of malicious behaviour.

The Internet of Things boom has brought with it an explosion of embedded devices. Typically, these devices are limited to one function, with little security because of limited resource. Which means there are billions of embedded devices in use that have limited protection, and this will only increase over time.

You'll find them in: industrial IoT and machines, consumer electronics, healthcare technology, aviation and automotive devices to name a few.

IoT: Use of smart meters is rising, however, as these devices are connected to the cloud, if one is compromised, it could have a ripple effect on the entire company infrastructure.



Semiconductor: The bootloader is often targeted by attackers to gain unauthorised access to the system, load malicious firmware, or disable additional security checks.

Automotive: Protecting automotive IP is critical to the success of the automotive industry, as it allows manufacturers to maintain a competitive edge and continue to innovate.

Scan the QR code to see all our use cases
www.emproof.com/use-cases

An end-to-end approach

Like security in most IT fields, embedded system security requires an end-to-end approach that includes addressing security issues during the design phase. Security considerations should include the cost of an attack on an embedded system, the cost of an attack on the company and the number of possible attack vectors.

To prevent attacks on embedded systems, software developers should:

- Regularly update firmware.
- Limit access to embedded systems to a need-to-use basis.
- Provide a way for network administrators to monitor connections to and from embedded systems.
- Use a third-party security management system – such as **Emproof Nyx**.

Do malicious hackers target embedded systems?

Yes, absolutely. It's well known that large computer and networking systems, servers, and data centres use a variety of industry-standard techniques to protect themselves from cyber-attacks.

However, embedded systems can be particularly vulnerable to these attacks because they often have limited resources and fixed functionality.

Additionally, because these systems are often interconnected with other devices and systems, a security breach in an embedded device can provide an attacker with access to an entire infrastructure. This emphasises the need for robust security measures to protect embedded systems from cyber-attacks.

Tesla jailbreak unlocks theft of in-car paid features

Tesla cars are susceptible to a nearly irreversible jailbreak of their onboard infotainment systems that would allow owners to unlock a bevy of paid in-car features for free.

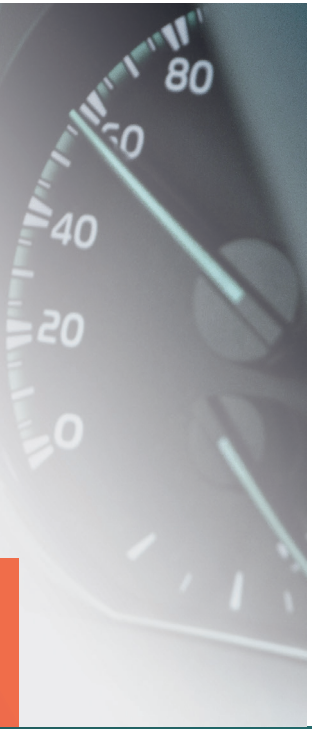
Through reverse engineering software attackers can uncover the underlying technology and circumvent the paid features for their own benefit or distribution to others. This not only results in financial losses for the manufacturer, but also undermines their competitive advantage. It is essential to deploy advanced software security into these systems to ensure overall protection and application reliability.

www.darkreading.com/application-security/tesla-jailbreak-unlocks-theft-in-car-paid-features

USE CASE: Paid features

This use case highlights how protecting paid features in cars is becoming increasingly pressing as manufacturers seek new ways to monetise their products.

What are the typical threats seen in an embedded device?



Denial of service Software bugs such as memory corruptions can be used to overload the system or cause system crashes – this can be prevented by using exploit mitigation.

IP theft Generic term for theft of intellectual property that can be repurposed and reused allowing illegally copied versions to be produced.

Key extraction Private cryptographic keys protecting a company's valuable IP, communications are extractable from the software enabling further attacks on device and company.

Malware Malicious software such as botnets and crypto lockers which are intentionally designed to cause disruption to a device.

Non-fixable bugs Software bugs that cannot be fixed due to read only memory restrictions can be exploited during the lifetime of the device.

Reverse engineering A method of analysing a systems structure and inter-relationships to enable the creation of a representation in a different form or higher level of abstraction.

Zero-day exploits These are software bugs that are unknown to the vendor that have been found by an attacker but cannot be leveraged due to exploit mitigation techniques.

The importance of hardware security and Emproof Nyx

Hardware features like secure boot, security modules, and fuse bits create a strong defense against physical attacks and unauthorised firmware access. However, they fall short in addressing software vulnerabilities such as memory corruption exploits and reverse engineering threats.

By integrating software-level protections, developers can fortify firmware against runtime attacks while safeguarding intellectual property. A combined hardware-software security approach ensures a robust, multilayered defense that mitigates risks from all angles.

Trusted execution platforms (TEE) Arm TrustZone and similar TEEs provide hardware-based isolation, ensuring sensitive operations run in a secure environment separate from untrusted software. However, they do not inherently prevent memory corruption exploits or protect firmware from reverse engineering, leaving vulnerabilities exposed. Emproof Nyx mitigates attacks in both secure and normal worlds while preventing IP theft and analysis through various reverse engineering protections. Together, TrustZone and Emproof Nyx create a comprehensive defense, combining hardware isolation with robust software protections.

Fuse bits, hardware debug lockdown and JTAG security
Fuse bits and JTAG lockdown block direct firmware access but can often be bypassed through side-channels or fault attacks. Emproof Nyx will protect the firmware even if these hardware measures fail and the binary can be extracted and reverse engineered. Integrating Emproof Nyx with fuse bits, debug lockdown, or JTAG security creates a robust, multilayered defense against both physical and software attacks.

Secure boot and root of trust systems ensure only trusted firmware loads by verifying its integrity at startup but does not protect against runtime attacks or reverse engineering. Once firmware is in memory, it can still be dumped, analysed, or exploited. Here, Emproof Nyx prevents memory corruption with runtime protections and safeguards firmware through its unique protections. Emproof Nyx can also enhance the bootloader itself, strengthening the entire secure boot process against tampering and reverse engineering.

Hardware security modules protect cryptographic keys but do not prevent reverse engineering or runtime exploits, leaving the broader firmware exposed. Emproof Nyx complements systems with hardware security modules (HSMs) by mitigating memory corruption attacks and shielding firmware from reverse engineering. This ensures that while HSMs secure keys, Emproof Nyx safeguards proprietary code and system integrity. Integrating Emproof Nyx with an HSM creates a comprehensive defense, combining hardware-based key security with robust firmware protection.

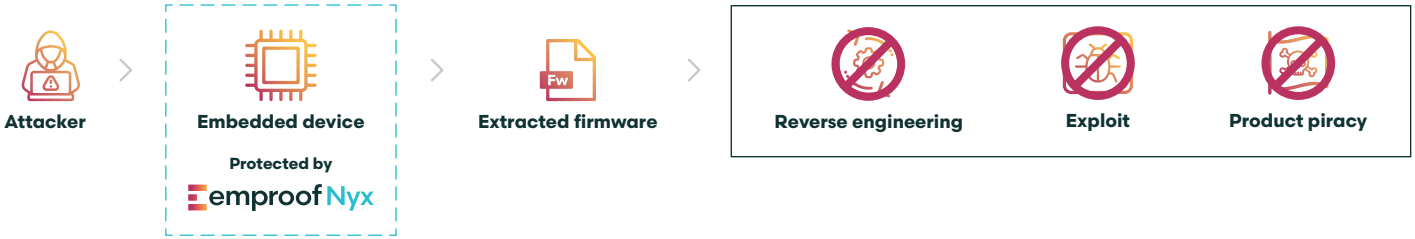
Cryptographic accelerators speed up secure operations but do not inherently protect the rest of the firmware from runtime exploits or reverse engineering. Attackers who compromise system code can still intercept or misuse calls to the accelerator, leaving critical functions exposed. Emproof Nyx closes these gaps by hardening the firmware. Together, accelerators and Emproof Nyx deliver a holistic security strategy, combining hardware performance with robust software protection for sensitive cryptographic operations.

Side-channel protections address physical or analog vectors, but software-level vulnerabilities remain a risk. Emproof Nyx ensures that even if attackers circumvent or are indifferent to side-channel mitigations, they still face significant barriers to exploitation and reverse engineering of the firmware.

How attackers proceed and how Emproof Nyx can help

How attackers proceed: In a typical scenario, attackers dump firmware from embedded devices, enabling reverse engineering using tools like Ghidra or IDAPro. This helps find exploits to compromise devices or analyse intellectual property for counterfeiting.

How Emproof Nyx can help: Emproof Nyx is integrated seamlessly into deployment processes, safeguarding embedded firmware. It automatically analyses binaries, fortifying them against reverse engineering. This shields against IP theft and exploit discovery.



Commercial benefits of the Emproof Nyx suite

We are at the forefront of embedded security. Emproof Nyx software is easy to integrate and provides security without compromise, protecting embedded devices throughout the lifecycle even when only 10% overhead or less is available*.

Our functional safety-compliant anti-piracy technology can:

- **Lower project costs** – best-in-class prevention for a yearly licensing fee of less than the cost of a single software developer.
- **Help develop products faster** – import over 30 combined years of software security expertise to your embedded devices in 5 minutes.

Code protection
Prevents reverse engineering and subsequent IP theft

Security hardening
Detects and secures against exploitation attacks

emproof Nyx

ISO 26262 (ASIL B) certification for functional safety in automotive components.

* Based on various technical discussions with our industry contacts.

Emproof Nyx product overview

Emproof Nyx protects applications and firmware from cyber threats with advanced binary transformation, preventing reverse engineering, IP theft, and exploits in memory-unsafe languages like C/C++.

Emproof Nyx ProtectSuite is the complete protection from reverse engineering and hacking attempts for all embedded systems and hardware devices.

Reverse engineering protection: Attackers use tools like Ghidra, IDA Pro, and Binary Ninja to analyse software binaries. Emproof Nyx employs obfuscation, anti-debugging/emulation, anti-tamper and integrity checks to hinder reverse engineering and protect your valuable code, algorithms and sensitive data – such as keys or AI models.

Hacking protection: Emproof Nyx secures embedded systems using C/C++ or other memory-unsafe languages, including ARM Cortex-M and RISC-V devices. Ideal for connected devices, unsupported compilers (e.g., GCC/Clang), and bare-metal/RTOS environments.

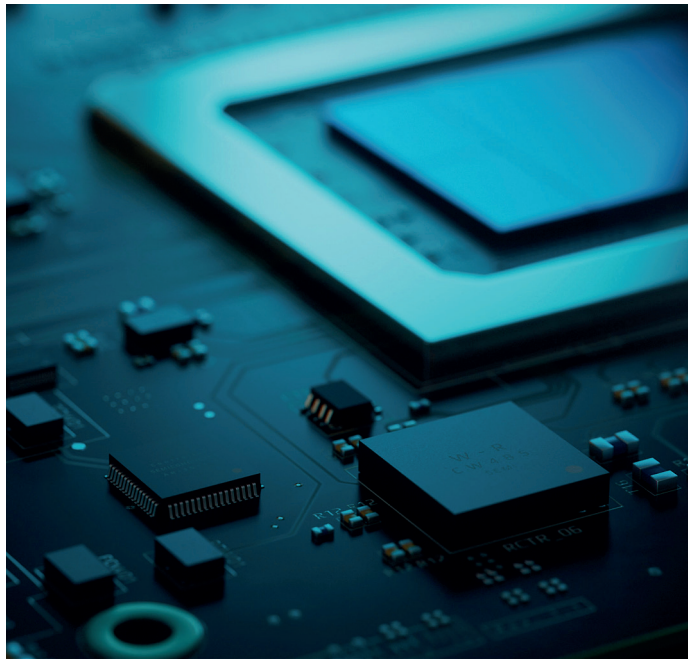
emproof Nyx

	ProtectSuite				
	Reverse engineering protection			Hacking protection	
	Code protection	Key protection	AI protection	Exploit mitigation	Bootloader protection
Reverse engineering-based attacks					
IP theft/cloning	✓	✓ [1]	✓ [2]	–	✓ [3]
Tampering attacks	✓	✓ [1]	✓ [2]	–	✓ [3]
Debugging/emulation attacks	✓	✓ [1]	✓ [2]	–	✓ [3]
Private key/API token theft	–	✓	–	–	–
Hardcoded password protection	–	✓	–	–	–
AI/ML model stealing	–	–	✓	–	–
AI/ML algorithm protection	–	–	✓	–	–
Hacking-based attacks					
C/C++: buffer overflow attacks	–	–	–	✓	–
C/C++: memory corruption attacks	–	–	–	✓	–
Bootloader fail attacks	–	–	–	–	✓
Bootloader tampering attacks	–	–	–	–	✓

1. Crypto only, **2.** AI only, **3.** Bootloader only

Summary

- Threat levels continue to develop at a rapid rate and demand for a holistic response to safety and security is more important than ever.
- Companies lose $200bn per year due to product piracy and cyber-attacks.
- An embedded system is a programmable hardware component with a minimal operating system and software.
- Embedded system security is a strategic approach to protecting software running on embedded systems from attack.
- Emproof delivers high levels of security and IP integrity for embedded systems, using unique techniques that protect algorithms and data while securing the entire device.
- Emproof Nyx helps all affected sectors to meet security requirements and guarantee protection of embedded systems.



About Emproof

The Emproof story began in 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.

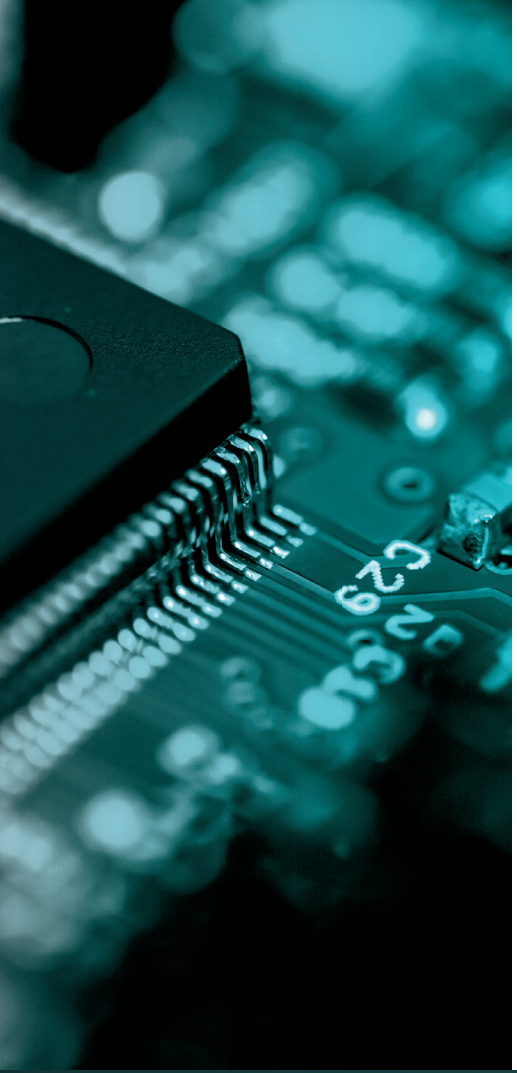
Founders of Emproof, Marc Fyrbiak, Phillip Koppe and Tim Blazytko met here while researching IT security. Marc worked on the hardware security side, while Philipp and Tim focused on research in software security.

During various research projects interrogating system vulnerabilities, they noted the weaknesses associated with embedded system security.

They also recognised the serious implications of such vulnerabilities in an increasingly connected world.

The answer, they realised, is not redesigning a system but adding protection from the outside. Protection that takes up only a tiny fraction of programming or software space but that nevertheless makes attacks difficult or impossible. It's a unique approach and, we think, the only effective one for the fragmentation inherent in embedded systems.

"Our goal is to build a sustainable company that provides ubiquitous, robust and cost-effective software security for all embedded systems."
Marc Fyrbiak, Chief Product Officer



emproof

emproof.com | contact@emproof.com

emproof
embeddedaward2023
Winner: Software

emproof
Recognized by ENTERPRISE SECURITY
TOP CYBER SECURITY SOLUTIONS PROVIDER IN EUROPE 2022