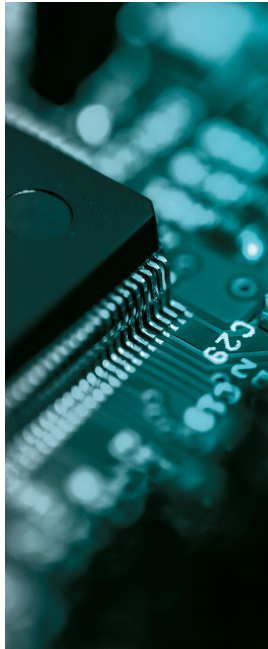# Secrets Unveiled: What Attackers Find in Embedded Systems

Tim Blazytko   Roland Marx

About Tim

- Chief Scientist, Head of Engineering & Co-Founder of Emproof

- focused on advancing embedded security solutions

- PhD in binary program analysis & reverse engineering

- training and lectures at industry conferences & universities

What's in embedded firmware?

Firmware Secrets

- hardcoded **credentials** (cryptographic keys, **passwords**, ...)

- IP addresses, domains, ...

- **keywords** that reveal **context** (e.g., network protocols)

- secret **algorithms** and **intellectual property**

DEMO

Anti Reverse Engineering

Code Obfuscation & Data Encoding

- increase **code complexity** to impede **reverse engineering** (code obfuscation)

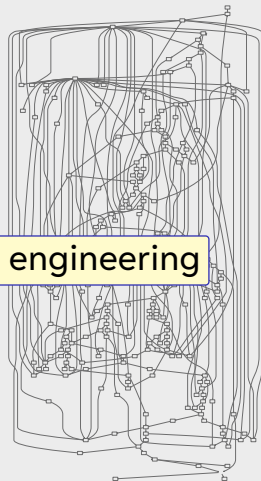- **hide keys and credentials** and decode them at **runtime**
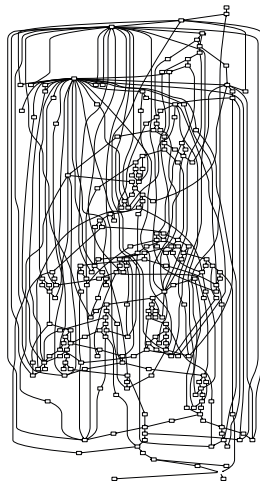
Code Obfuscation & Data Encoding

- increase **code complexity** to impede **reverse engineering** (code obfuscation)

  passive protections impede reverse engineering

- **hide keys and credentials** and decode them at **runtime**

Anti-Debug & Anti-Tamper

- observe execution environment for debuggers (anti-debug)

```
if debugger_detected() {
    terminate()
}
```

- detect code modifications (patching) by code checksumming (anti-tamper)

```
if checksum(code) != 0xd75648 {
    terminate()
}
```

Anti-Debug & Anti-Tamper

- observe execution environment for debuggers (anti-debug)

```
if debugger_detected() {
    terminate()
}
```

runtime protections to prevent analysis & modifications

- detect code modifications (patching) by code checksumming (anti-tamper)

```
if checksum(code) != 0xd75648 {
    terminate()
}
```

Demo

Home   IP Protection Demo   Exploit Mitigation Demo   Resources ▼   Back to Homepage   Contact ▼

Welcome to the Emproof Nyx Demo Centre

Here you can try our IP Protection and Exploit Mitigation solutions, as well as our open-source assembler-disassembler Nyxstone COMING SOON .
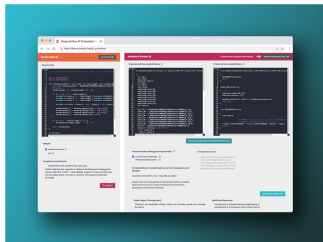
IP Protection Demo

IP Protection is essential for safeguarding your critical algorithms, code, and data from reverse engineering threats. In this demonstration, we will not only show you how Emproof Nyx can robustly protect your binary but also provide insights into the extensive range of techniques available to attackers for analysing binaries. Reverse engineering is easier and happens more frequently than is often perceived, so it is important to protect your binary.

IP PROTECTION DEMO

https://demo.emproof.com/

Conclusion

- often sensitive information in embedded firmware

- anti reverse engineering techniques impede analysis

    Try it yourself:

                    https://demo.emproof.com

                https://github.com/emproof-com/webinars