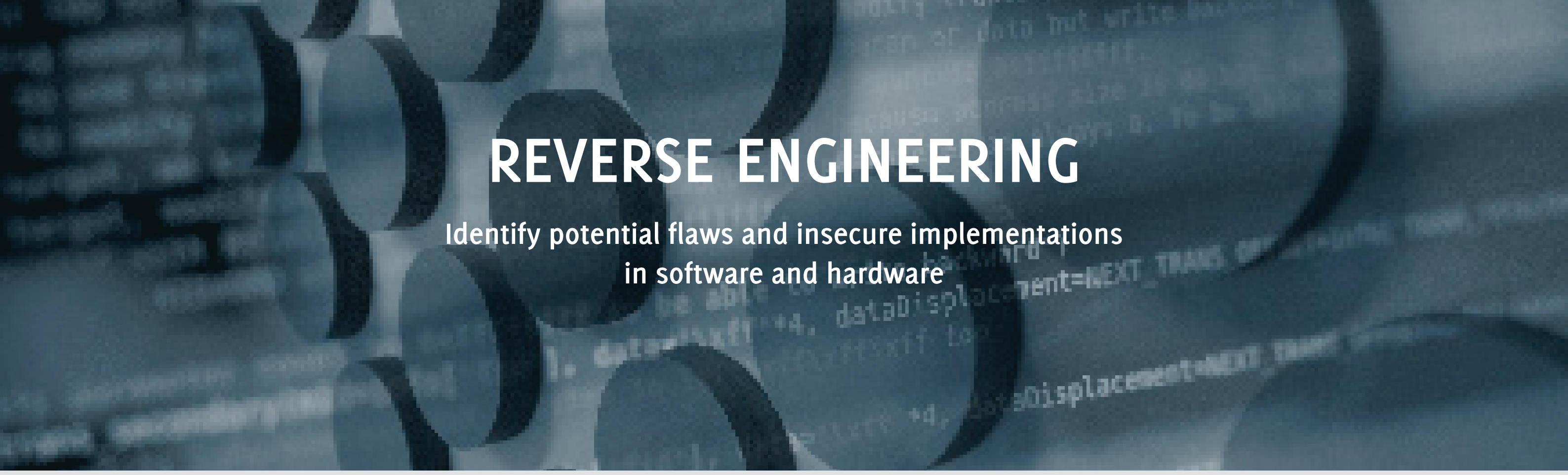

REVERSE ENGINEERING

Identify potential flaws and insecure implementations in software and hardware

Improsec provides a reverse engineering service to establish if the software or hardware in scope contains previously unknown security flaws and potentially insecure implementations – “0-day vulnerabilities”. The focus of the service depends entirely on your needs and will be tailored accordingly.

If a previously unknown vulnerability is identified in a software or hardware product, and you are not the owner of this product, we will engage in direct communication with the vendor in accordance with our Responsible Disclosure policy (https://improsec.com/responsible-disclosure/). The policy is designed to put sufficient pressure on the vendor and thereby eliminate the vulnerability as soon as possible. During this process, we will keep customer confidentiality unless agreed otherwise.

Value

- Evaluate the implemented security of a software or hardware product
- Increase the quality of a software or hardware product by eliminating vulnerabilities
- Obtain concrete recommendations on how to avoid identified product vulnerabilities

Product

The deliverable of the analysis is a written report containing the following:

- A non-technical section with an Executive Summary for management and decision makers
- A technical section including detailed observations and tangible recommendations to improve the security level and hardening of the software or hardware

In most cases, where vulnerabilities are trivial to reproduce, we may also develop a proof-of-concept exploit for a given vulnerability, which can be used to provide a realistic insight into the criticality of the vulnerability.

Method

Our team of dedicated reverse engineers works in a methodical pattern, and will perform the following tasks in the given order:

- A static analysis of the software, in order to map all binary code or functionality that presents a potential risk/exploitability, or otherwise looks suspicious
- A dynamic analysis and active debugging session of the software, to test for unexpected/suspicious behaviour
- A full analysis of all observations from the static and dynamic analysis, and potential attack vectors to identify all exploitable vulnerabilities
- Documentation of vulnerabilities and potential development of various proof-of-concept exploits

Involvement

The delivery requires minimal involvement of your technical staff.

Improsec A/S
www.improsec.com
Telephone: (+45) 5357 5337
Email: info@improsec.com