VRIJE UNIVERSITEIT BRUSSEL

The faculty of Engineering of the Vrije Universiteit Brussel invites you to attend the public defense leading to the degree of

DOCTOR OF ENGINEERING SCIENCES

of **Thibaut Vandervelden**

The public defense will take place on **Monday 22nd September 2025 at 4 pm** in room **I.2.01** (Building I, VUB Main Campus)

To join the digital defense, please click here

RUST-BASED IOT NETWORKS: A NETWORK PROTOCOL AND SECURITY PERSPECTIVE

BOARD OF EXAMINERS

Prof. dr. ir. Gerd Vandersteen

Prof. dr. ir. Wendy Meulebroeck

Dr. ir. Ruben De Smet

Prof. dr. Lesley De Cruz

Prof. dr. Bruno Quoitin

Prof. dr. ir. Stijn Volckaert

PROMOTORS

Prof. dr. ir. Kris Steenhaut

Prof. dr. An Braeken

VRIJE UNIVERSITEIT BRUSSEL

Abstract of the PhD research

The Internet of Things (IoT) continues to transform our interconnected world. Its rapid growth raises significant concerns about privacy and security. In recent years, numerous IoT botnets have exploited vulnerabilities in embedded devices to launch large-scale Distributed Denial of Service attacks. These attacks have caused significant disruption to internet services worldwide.

Many of these security vulnerabilities come from the use of memory-unsafe programming languages, such as C and C++. Programming languages with built-in safety features can mitigate these vulnerabilities. Since its first stable release in 2015, Rust has emerged as a popular choice for system programming, gaining popularity due to its unique combination of memory safety guarantees while keeping its performance comparable to the one obtained with traditional programming languages. Developers have successfully deployed Rust across diverse domains, including Operating Systems (OSs), web services, and embedded devices.

For IoT devices, two software components are particularly important: the OS and the network stack enabling communication. We provide an evaluation of OSs and frameworks for embedded devices available in Rust and examine their suitability for various IoT applications. We also investigate the feasibility and advantages of implementing a complete network stack in Rust for resource-constrained embedded devices. We built on the smoltcp library and extended it with a Rust implementation of IPv6 over Low-power Wireless Personal Area Networks (6LoWPAN). We studied and implemented the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL). We developed and applied an evaluation methodology to check compliance with the standard and to verify interoperability with existing implementations. Doing so, we solved several issues of the current RPL implementation in Contiki-NG. Our research also evaluates the effectiveness of 6LoWPAN generic header compression for use in RPL networks. The results demonstrate that this compression format significantly reduces energy consumption for IEEE 802.15.4-based networks that offer low data rates. For higher data rates, the benefit of this compression format diminishes.

Alongside contributing to networking components in Rust, we also explored security primitives. We evaluated the performance of different Keccak sponge constructions, cryptographic primitives that can serve as building blocks for various security protocols. Our findings reveal that Keccak sponge constructions with lower capacity parameters achieve significantly better efficiency on 32-bit microcontrollers commonly used in IoT devices. Building on these insights, we design and implement two novel symmetric-key-based authentication protocols. One tailored for wireless sensor networks and the other for fog based networks. We demonstrate that our protocol provides robust protection against known attacks while maintaining low computational and communication overhead.