FreeRTOS meets separation logic

Memory safety, thread safety and functional correctness proofs with VeriFast

Nathan Chong, Principal Applied Scientist

23 July 2020

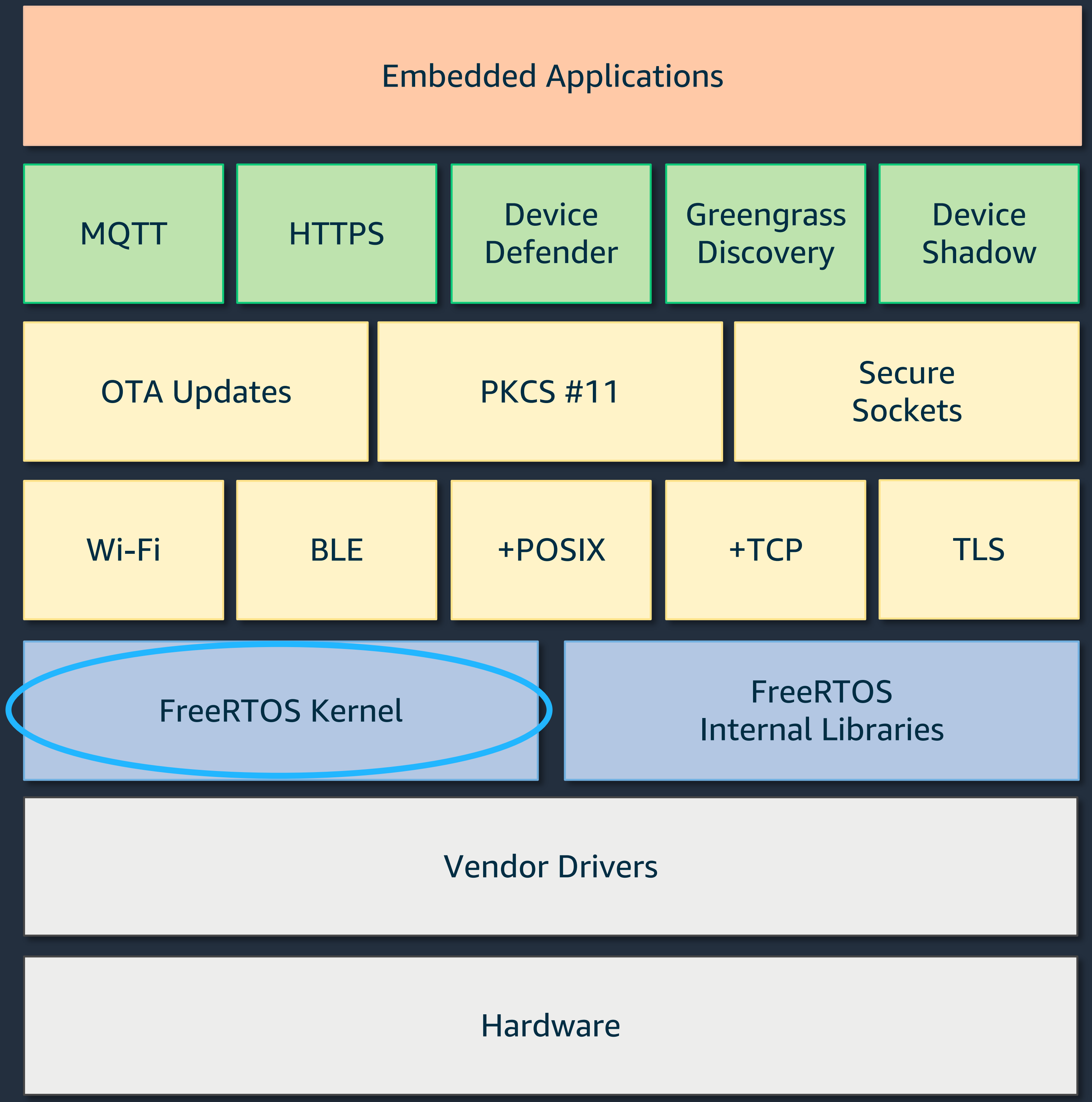
Product photos from Amazon.com

Market-leading real-time operating system (RTOS) for microcontrollers

Downloaded once every 175 seconds

Distributed freely under MIT license

https://freertos.org



Embedded Applications

MQTT | HTTPS | Device Defender | Greengrass Discovery | Device Shadow

OTA Updates | PKCS #11 | Secure Sockets

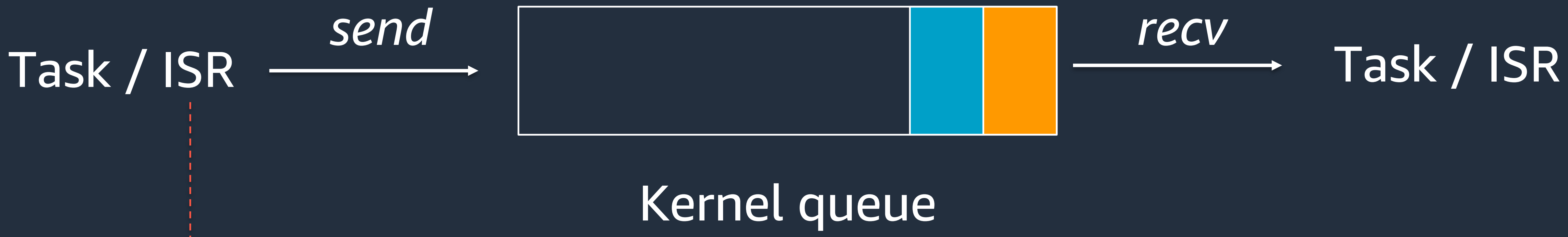
Wi-Fi | BLE | +POSIX | +TCP | TLS

FreeRTOS Kernel | FreeRTOS Internal Libraries

Vendor Drivers

Hardware

This talk:
Memory safety, thread safety and functional correctness proofs with VeriFast



Task / ISR

send

recv

Task / ISR

Kernel queue

Concurrent FIFO data structure

Interrupt Service Routine

Characteristics

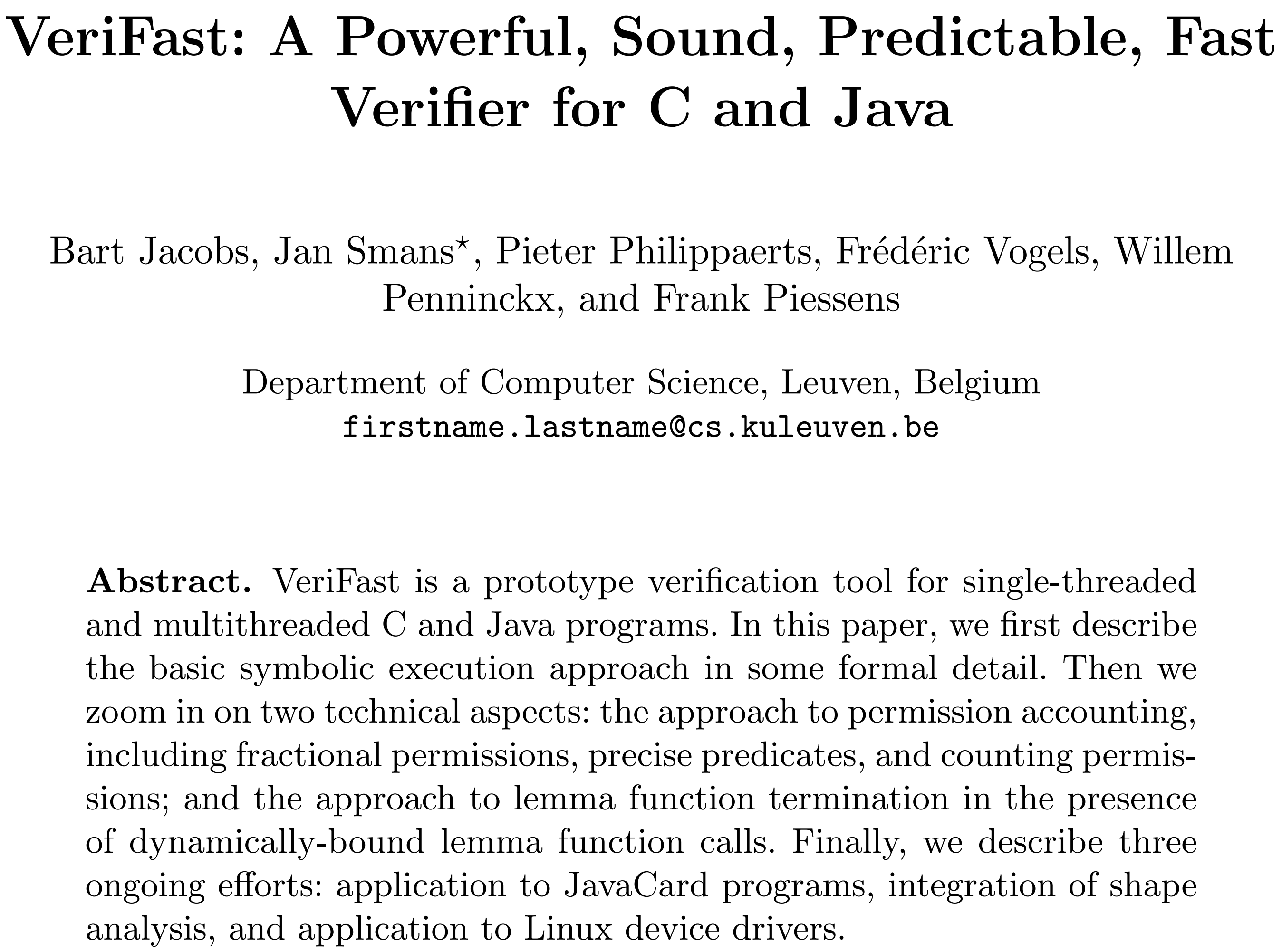
~700 LOC C code designed for resource-constrained environments

Tightly integrated with task scheduler

Low-level, coarse-grain concurrency

Memory safety, thread safety, functional correctness requirements

NFM 2011



VeriFast: A Powerful, Sound, Predictable, Fast Verifier for C and Java

Bart Jacobs, Jan Smans*, Pieter Philippaerts, Frédéric Vogels, Willem Penninckx, and Frank Piessens

Department of Computer Science, Leuven, Belgium
firstname.lastname@cs.kuleuven.be

Abstract. VeriFast is a prototype verification tool for single-threaded and multithreaded C and Java programs. In this paper, we first describe the basic symbolic execution approach in some formal detail. Then we zoom in on two technical aspects: the approach to permission accounting, including fractional permissions, precise predicates, and counting permissions; and the approach to lemma function termination in the presence of dynamically-bound lemma function calls. Finally, we describe three ongoing efforts: application to JavaCard programs, integration of shape analysis, and application to Linux device drivers.

https://people.cs.kuleuven.be/~bart.jacobs/verifast/

> “Demonstrating due diligence through the use of these state-of-the-art best practices is essential to maintain the confidence and trust of our user base”
>
> – Richard Barry, Founder of FreeRTOS and Senior Principal Engineer, AWS

References

- Amazon, FreeRTOS User Guide, 2020
  https://docs.aws.amazon.com/freertos/latest/userguide/

- Jacobs et al., VeriFast: A Powerful, Sound, Predictable, Fast Verifier for C and Java, NFM 2011

- Vogels et al., Featherweight VeriFast, Logical Methods in Computer Science 2015

https://github.com/FreeRTOS/FreeRTOS/tree/master/FreeRTOS/Test/VeriFast

Related work

- Andronick et al., Proof of OS scheduling behavior in the presence of interrupt-induced concurrency, ITP 2016

- Ferreira et al., Automated Verification of the FreeRTOS Scheduler in HIP/SLEEK, STTT 2014

- Xu et al., A Practical Verification Framework for Preemptive OS Kernels, CAV 2016

Thank you

Nathan Chong

Get started at freertos.org