NetReach: Guaranteed Network Availability and Reachability to enable Resilient Networks for Embedded Systems

Tom Van Eyck, Sam Michiels, Xiaojiang Du, Danny Hughes SysTEX 2024



Introduction

- Industrial networks
 - Robots
 - Automated Guided Vehicles
 - •
- Powerful processors
- Worldwide deployment
 - No in person interventions

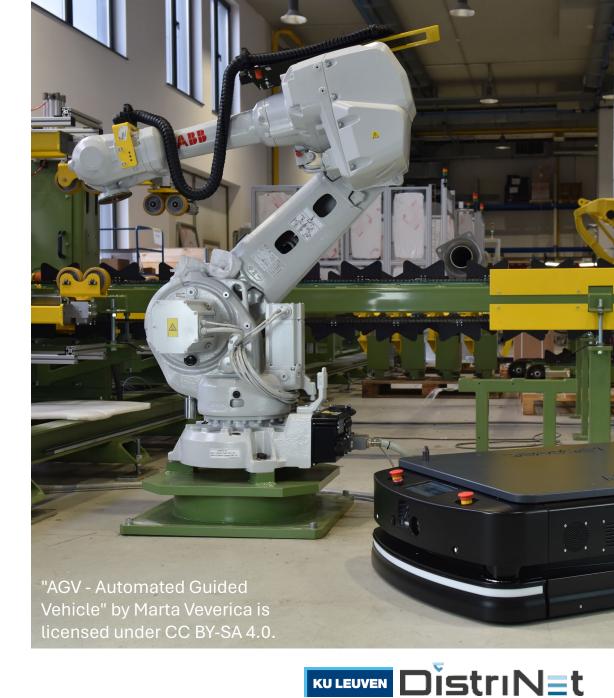




Introduction

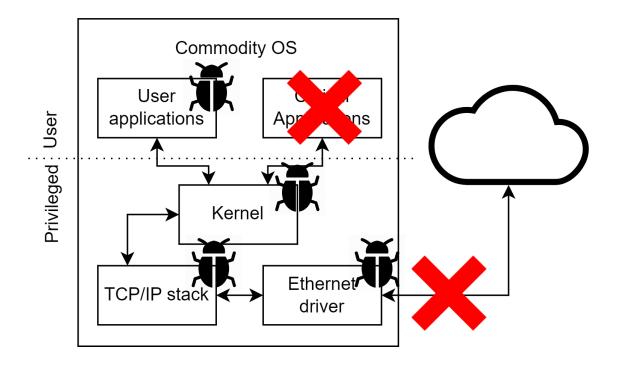
- Commodity OS
 - Networking
 - Remote monitoring
 - Updates
- Real-time control
 - Safety critical!
- Large attack surface

=> Problems



Attacks on Industry

- Strong remote attacker
- Denial of Service
 - Device operation
- Large codebases
 - Ethernet driver alone: ~6k LoC
- Often untested
- Very little separation



=> High chance of failure or successfull attack

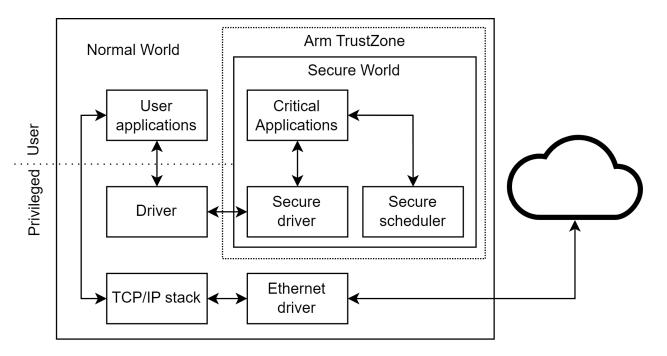


State of the art: Availabilty with TEE

Session 5A: Control System Security CCS '21. November 15-19, 2021. Virtual Event, Republic of Kores AION: Enabling Open Systems through Strong Availability Guarantees for Enclaves Fritz Alder Io Van Bulc imec-Distri? Leuven 2022 IEEE Symposium on Security and Privacy (SP) Frank I frank.piessens RT-TEE: Real-time System Availability for imec-DistriN Leuwen Cyber-physical Systems using ARM TrustZone ABSTRACT Embedded Trusted Execution Er strong security for software in the Approaches to combine this secur marantees are currently missing. I onfigurable security architect anteed real-time execution for dy Abstract-Embedded devi implement preemptive multitaski vasive in safety-critical syster world. While trusted executi ARM TrustZone, have been w top of strong enclave software is proach allows the hardware to enfo protections, while a decoupled sm little attention has been given physical systems, which prese pared to mobile applications Mr-TEE: Practical Trusted Execution of Mixed-Criticality Code of a bounded number of protected Tom Van Eyck Hamdi Trimech Sam Michiels systems, such as autonomous TEE deployment paradigm, and integrity, is insufficient. Danny Hughes ily introducing a notion of priorit We implement a prototype on a provide a case study. Our imple tom vanevck@kuleuven.be danny hughes@kuleuyen.b ditrimech@kuleuven.bamichiels@kuleuven.b DistriNet, KU Leuven DistriNet, KU Leuven DistriNet, KU Leuven DistriNet, KU Leuver needs to be completed in a th Leuven, Belgium Leuven, Belgium tected applications can handle inte Leuven, Belgium Leuven, Belgium a pedestrian), putting a muc deterministic activation latencies. To bridge this gap, we p Majid Salehi Hassan lanjuaa Thanh-Liem Ta adversary with arbitrary code e majid.salehi@nokia-bell-labs.com Nokia Bell Labs ta.thanh-liem.sup@hotmail.com execution environment. There First, RI-TEE bootstraps the a minimal set of hardware ded platforms. Second, to ha scheduler complexity, we desi hierarchical scheduler. Third, device drivers in the secure CCS CONCEPTS DistriNet, KU Leuven Polytech Sorbonne Antwerp, Belgium Leuven, Belgium Paris, France - Security and privacy \rightarrow Trust tems security; Embedded system ABSTRACT 1 INTRODUCTION organization → Real-times ust Industry 4.0 is increasingly using commodity hardware and soft-Until recently, industrial control was implemented using reliable ware in place of dedicated control systems to lower costs and in crease flexibility. However, this means that critical control code yet inflexible Programmable Logic Controllers (PLCs), which were rarely connected to the Internet. However, this approach is being reference monitor that lever KEY WORDS reterence monitor that levera debioating to provide fine-gr while minimizing the trusted We implemented prototype platforms. The system is teste life CPS applications. We eval and quadcopter both in simu trusted computing, avail must compete for resources with an increasingly complex soft challenged by Industry 4.0, which connects industrial assets such ware stack that exposes a new attack surface. The Mixed Criticality Trusted Execution Environment (Mr-TEE) tackles this problem at as machines, robots, and production lines with real-time analytics and control to improve efficiency, safety and quality. Additionally, ACM Reference Format Nr. M. Reference Form at Fritz Alder, Jo Van Bulck, Frank Pies Aron: Enabling Open Systems throug Enclaves. In Proceedings of the 2021 A its root, by delivering availability for safety-critical control code. these assets are inherently a Cyber Physical System (CPS), which while running untrusted applications in a minimally modified Linux interacts continuously with the physical world and are hence bound stack. This is achieved by providing a real-time scheduler and nove y stringent timing and safety requirements. This makes it crucial I IN peripheral sharing system in the Secure World. Mr-TEE hence prothat all required system resources are made available to critical The software of modern vides the best of both worlds for Industry 4.0 developers, ensu tasks in a real-time manner and protected from any undue inter emission to make digital or hard copies incroom use is granted without feeprovid often highly complex. Fo ing the trusted execution of time-sensitive control applications ference. Extensive conversations with our industry partners in the automobile such as the Che while minimizing design effort and restrictions for untrusted ap ontext of industrial/applied research projects (TACOS1, TRUSTI2 in the first page. Copyrights for component athony) must be honored. Abstracting with flight software of the Boe nlications Evaluation on an Arm TrustZone-enabled Cortex MCU and ERATOSTHENES3) identified support for deterministic 1 ms pressure to include more fe ead of 1.88% to support real-tim strol loops as a key requirem cost, weight, and testing, (scheduling in the TEE. Connecting CPS to the Internet is best achieved by reusing rep-CCS '21, Nevember 15-19, 2021, Virtual utable commodity OS components and applications because of their dating more and more fu ease of implementation and well-tested nature. Unfortunately, these significantly increase the attack surface due to their large code base, CCS CONCEPTS chip (SoC) [2], [3], Nume been discovered on moder Computer systems organization → Embedded systems; Real prosing vulnerabilities [5, 15, 19] which range from musances [20] drones [4]. [5] and autor time operating systems; Availability; - Security and privacy to life-threatening malfunctions [18]. This poses the urgent ques-tion: How can strong trust in time-sensitive cyber-physical control vulnerabilities are only nu ating syst to escalate into system priv functionality be preserved when using a commodity Linux OS? KEY WORDS life or death implications As prior research has shown, attackers can cause a catastrophic accident by delaying or altering sensorroadings [27]. The end goal is thus to prevent attackers from tampering with the schedule of real-Lack of availability prote Cyber-Physical Systems, Mixed-Criticality, Trusted Execution Enognizing the importance of has been significant interest vironments, Arm TrustZone time tasks or overloading resources. To achieve this, it is necessary ACM Reference Format to prevent unauthorized reconfiguration of the system, and to deny unauthorized tasks from accessing certain critical peripherals. This security mechanisms, such Tom Van Evek, Handi Trimech, Sam Michiels, Danny Hushes, Maiid Salehi Haisan Janjaaa, and Thanh Liem Ta. 2023. Mr-TEE: Practical Troated Ere-cation of Mixed-Criticality Code. In Middleware Industrial Track '23: Pro-rendmin of the 20th International Middleware Industrial Track '23: Prominimization, specialized r must be achieved while preserving access to standard peripherals [12], [13]. Common to all s on a trusted OS. However, rom the non-secure OS in order to prevent extensive re-engineering edings of the 24th International Middleware Conference Industrial Track fiddleware '29), December 11–15, 2023, Bologna, Italy. ACM, New York, NY, efforts microcontrollers in particul This paper proposes Mr-TEE, which guarantees using a hard USA, 7 pages. https://doi.org/10.1145/363 enabled Trusted Execution Environment (TEE) (specifically Arm TrustZone) to host and schedule safety-critical code, while maintaining a strong separation from the Linux OS, which executes outside © 2022, Jinwen Wang. Under lice DOI 10.1109/SP46214.2022.0014 mnission to molee digital or hand copies of sill or part of this work for personal on succosm use is generated without for provided that copies are not rude or distributed profil or commercial advantage and that copies loss this native and the fall entation whe first page. Capyrights for components of this work seemed by others than 400 or the honored. Altoristing with containing and the provided seemed by others than 400 or the honored. Altoristing with containing and the provided seemed are republished of the TEE. Mr-TEE also provides mediated access to peripherals via a Shared Secure Peripheral Framework. This prevents untrusted applications from performing Denial of Service (DoS) attacks. In antrast to prior research in this area [29], Mr-TEE does not require

Availability of Critical Code

• Mr-TEE [1] on Arm TrustZone:



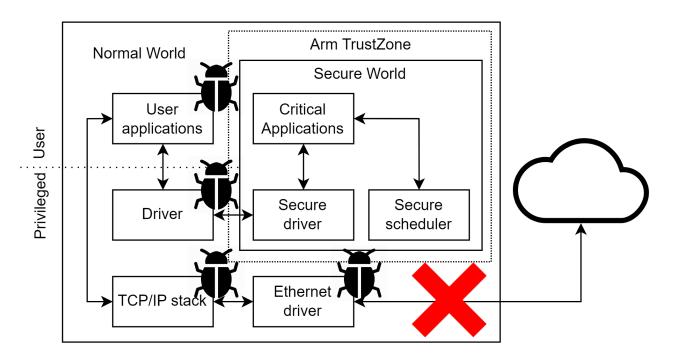
[1] T. Van Eyck et al., Mr-TEE: Practical Trusted Execution of Mixed-Criticality Code. 2023. doi: 10.1145/3626562.3626831.



.

Mr-TEE: Practical Mixed-Criticality

- Real-time scheduler in TEE
 - Minimal implementation
- Secure sharing of peripherals
 - Interrupt passing
- Reboot of Linux
- No network availability
 => Costly manual intervention





NetReach

Guaranteed Network Availability and Reachability



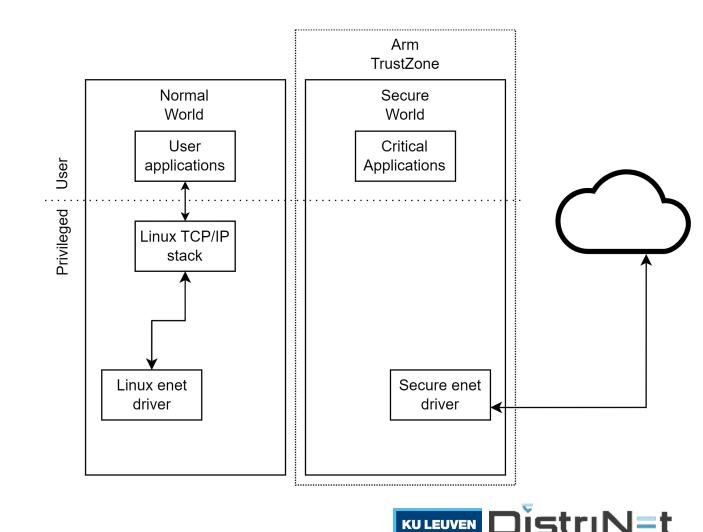
NetReach

- First step towards resilient networks
 - 1. Always available network peripheral
 - 2. Always reachable backup network
- Requirements
 - 1. Protect peripheral from DoS by NW
 - 2. Provide backup network
 - 3. Minimize TCB



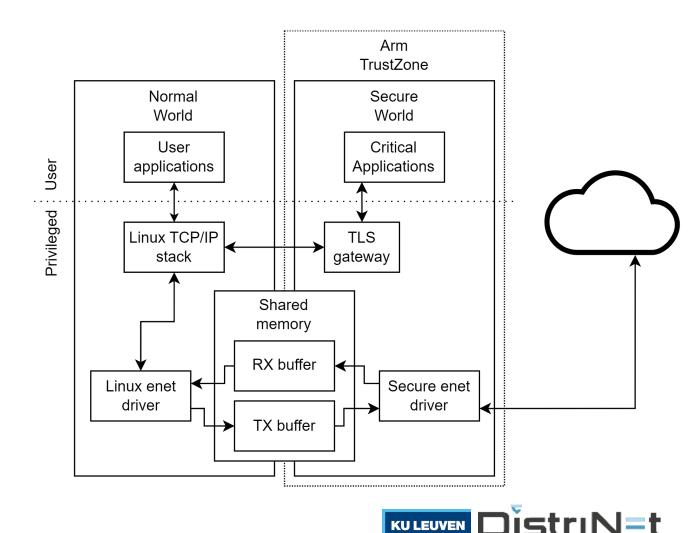
The network peripheral

- Availability
 - Assign memory to SW
 - Assign interrupts to SW
 - Minimal driver in SW



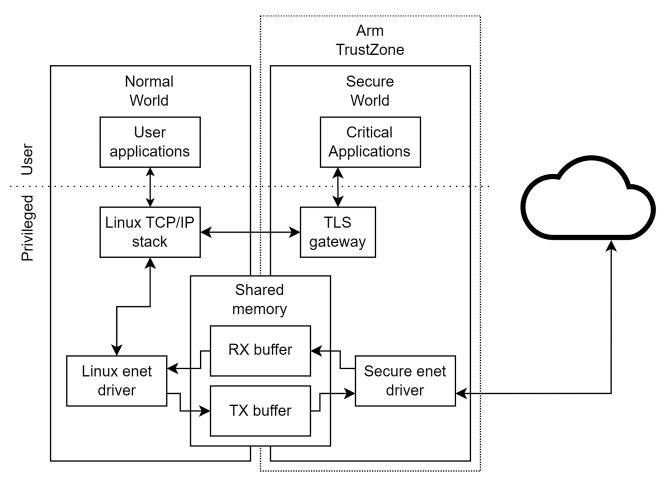
The network peripheral

- Availability
 - Assign memory to SW
 - Assign interrupts to SW
 - Minimal driver in SW
- Sharing access with NW
 - Buffers in shared memory
 - Using Linux network stack



The network peripheral

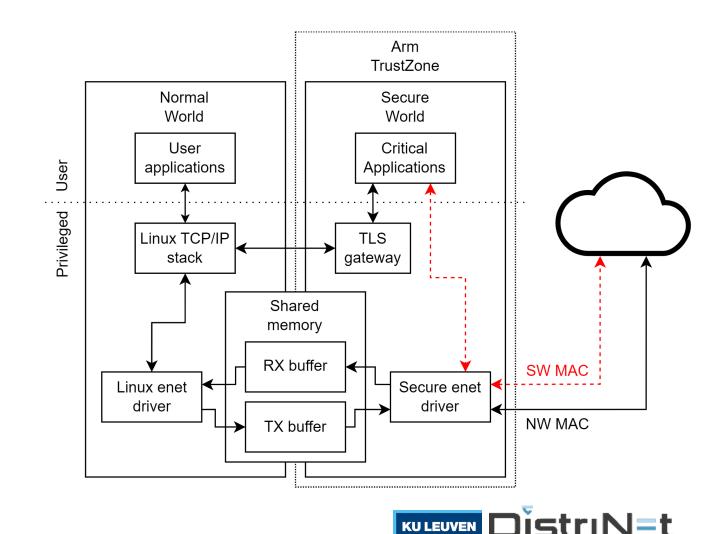
- Availability
 - Assign memory to SW
 - Assign interrupts to SW
 - Minimal driver in SW
- Sharing access with NW
 - Buffers in shared memory
 - Using Linux network stack
- Interrupt driven operation
 - Avoids overhead
 - Intelligent priorities





The backup network

- Separate ip & mac address
 => Ensures reachability
- Reduced capabilities
 - Smaller attack surface
 - Local network only
 - ~400 LoC



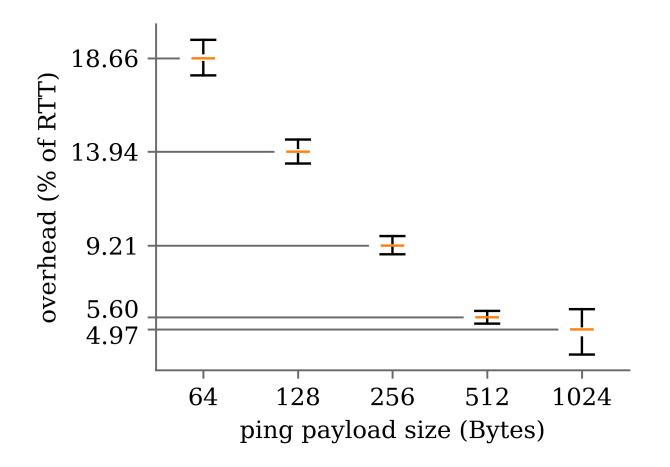
Evaluation

- Proof of Concept
 - BD-SL-i.MX6
 - SPI Ethernet controller
 - Mr-TEE & OP-TEE OS
- Measured RTT using ping



Evaluation

- Overhead
 - 64 bytes: 18,66%
 - 1024 bytes: 4,97%
 - Typical packet size: ~100B and ~2kB
- TCB size Driver
 - 418 LoC (0,1% of OP-TEE OS)
 <-> ~6k LoC Linux driver





What's next?

- Monitoring the state of the device remotely
- Controlling the device
- Recovering the device in case of attack
- Formal verification



NetReach: Guaranteed Network Availability and Reachability to enable Resilient Networks for Embedded Systems

Tom Van Eyck, Sam Michiels, Xiaojiang Du, Danny Hughes



Contact

tom.vaneyck@kuleuven.be

Source code

https://gitlab.com/distrinetnetreach/documentation





With the support of VLAIO. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020416.

