Demonstrating Post-Quantum Remote Attestation for RISC-V Devices

Maximilian Barger*†, Marco Brohet†, Francesco Regazzoni†‡,
*Vrije Universiteit Amsterdam, The Netherlands, mail@mabarger.at
†University of Amsterdam, The Netherlands, mail@mabarger.at, m.j.a.brohet@uva.nl, f.regazzoni@uva.nl
‡Università della Svizzera italiana, Switzerland, francesco.regazzoni@usi.ch

***Abstract*—The rapid proliferation of Internet of Things (IoT) devices has revolutionized many aspects of modern computing. Experience has shown that these devices often have severe security problems and are common targets for malware. One approach to ensure that only trusted software is executed on these devices is Remote Attestation (RA), which allows a verifier to attest the integrity of software running on such a prover device. As malware is typically not trusted, an infected device will fail to generate a valid signature, which allows the verifier to detect the presence of malware on the prover. To achieve its security guarantees, RA requires a trust anchor, often found in the form of dedicated hardware on the prover. For IoT and embedded devices such hardware has only recently become largely deployed. Current RA protocols rely on classical asymmetric signatures that are vulnerable to quantum attacks, which are expected to become feasible in the near future. In this work we present SPRAV, a software-based RA system that leverages the Physical Memory Protection (PMP) primitive of RISC-V to achieve its security guarantees and employs quantum-safe cryptographic algorithms to ensure resistance against quantum attacks in the future. Our evaluation shows that it is feasible to deploy this solution on RISC-V devices without incurring a prohibitive overhead or the need for additional hardware, paving the way towards quantum-resistant functionalities also in IoT.**

I. Introduction

The swift advancement of technologies in the IoT domain has brought significant security challenges. Due to the lack of resources and widely adopted security measures in the IoT ecosystem, amplified by the short time to market typical for consumer electronics, IoT devices have become attractive targets for malicious actors [1]. A quite recent example for this is the Mirai malware, which turned IoT devices into unwilling participants of the Mirai botnet. This botnet, containing up to 600,000 devices, was used to launch one of the largest Distributed Denial of Service (DDoS) attacks against internet infrastructure and major internet providers [2] [3].

One way to prevent such a scenario is to enhance these devices with Remote Attestation (RA), which allows an external verifier to verify that the device is only executing trusted software. If the proving device is infected with malware, it will fail to generate a valid signature, as the malware is not trusted. This can be detected by the verifier, who can then take corrective actions such as exclusion from the network or sanitization of the device. These RA protocols typically rely on a trust anchor or Root of Trust (RoT), often in the form of a Trusted Platform Module (TPM), to store system measurements and provide an integrity guarantee through attestation. The data's attestation is typically performed with a cryptographic signature, which is created using an attestation key protected by hardware as described by Coker et al. [4].

Most modern RA protocols employ classical cryptographic schemes such as RSA and Elliptic Curve Cryptography, which are vulnerable to quantum attacks such as Shor's algorithm [5]. While quantum computers currently do not possess the resources required to utilize these attacks, it is still necessary to explore the design considerations when implementing post-quantum algorithms to ensure that we are ready to respond to this threat when it arises. Moreover, as the lifetime of an IoT device can extend to multiple decades [6], it is paramount that post-quantum cryptographic primitives can be deployed on these devices well in advance, especially for RA.

This also applies to devices based on the RISC-V instruction set architecture (ISA), which has become increasingly more common in the IoT domain due to its openness and focus on simplicity and efficiency [7]. While many such devices are available, rarely any of them contain a traditional RoT, as they are often considered to be too cumbersome [8].

To address these issues, we propose a software-based post-quantum RA system. Our system utilizes the RISC-V Physical Memory Protection (PMP) primitive and directly-mapped read-only memory as a RoT for RA by marking the memory region containing the attestation code and key as execute-only and preventing further changes to that configuration. It requires no hardware modifications and supports all commodity RISC-V devices that support PMP. Our implementation, SPRAV, is available as open-source software [1].

II. Architecture

Our implementation, which is depicted in Figure 1, targets RISC-V systems and consists of two main components: the prover RA code (*prac*) shown on the left side, which also contains the attestation key, and the verifier RA code (*vrac*) shown on the right side. The figure also shows the main steps of the attestation process in chronological order. The *vrac* is implemented as a self-contained application without dependencies on the software running. However, the *prac* needs a tighter integration with the software, because there needs to be a well-defined interface through which a process can request the computation of an attestation signature. As such, we developed

[1] https://github.com/mabarger/zephyr-sprav/tree/sprav

979-8-3503-4859-0/DATE24/© 2024 EDAA

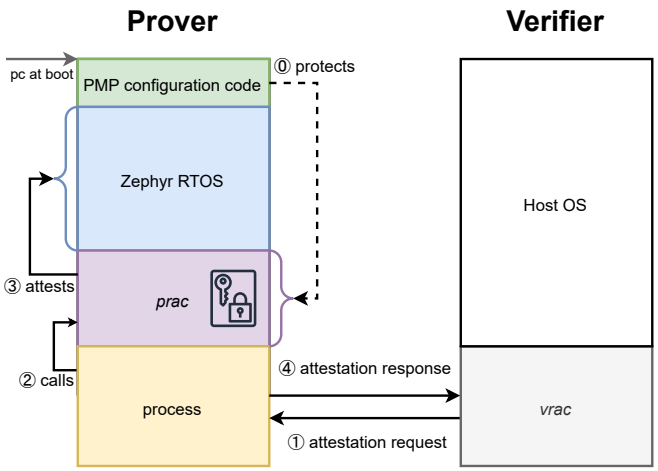

Fig. 1. High-Level view of SPRAV. The numbers ⓪ to ④ mark the attestation steps.

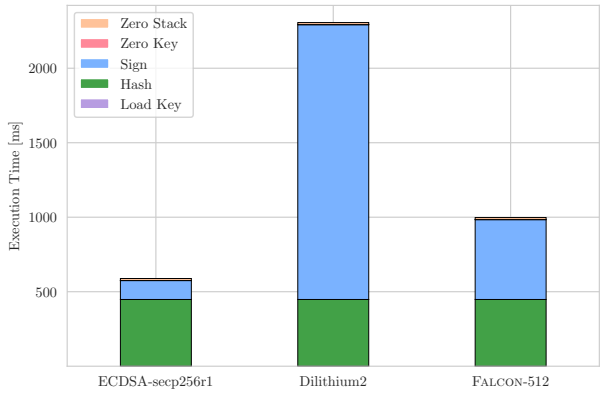

Fig. 2. Execution time breakdown for the attestation of 8KiB of memory.

the *prac* on top of Zephyr, an open-source real-time operating system tailored for embedded systems.

Nonetheless, we emphasize that the underlying concept of the *prac* does not depend on Zephyr and it can easily be extended to other OSes. Our implementation employs the lattice-based schemes CRYSTALS-Dilithium and Falcon to protect against quantum attacks, because of their low signature size compared to that of the hash-based scheme Sphincs+ [9].

While the attestation key itself must be protected from being read by an attacker, it has to be readable for the implementation of the signature algorithm in the *prac*, as otherwise it is not possible to compute a signature. We achieve both goals at the same time with our key loading code, which, when executed, stores the attestation key at a predefined memory location. After the signature has been computed, the temporary key will be zeroed out.

III. Evaluation

For the evaluation of our work we focus on the *prac*, as the prover device is typically constrained, while the verifier can be a high-performance system. We evaluate our implementation on the ESP32-C3-DevKitM-1, which contains a single RISC-V core implementing RV32IMC and operating at 160 MHz. Our implementation was compiled for this CPU with gcc v12.2.0 using `-Os` as optimization level.

We measure the execution time of loading the key, hashing the memory contents, signing the data, key zeroing and stack zeroing to determine the impact of security measures and potential overheads of the attestation procedure. Figure 2 shows the execution time of the attestation procedure of each algorithm for the attestation of 8 KiB of memory. We compare the two post-quantum algorithms with ECDSA, which is the current de facto standard.

The results show that while the post-quantum algorithms do take significantly longer to perform the attestation compared to ECDSA, most of that time is spent on the creation of the signature, which does not depend on the amount of memory attested. With an increasing amount of memory that is being attested, only the hashing time will increase and the relative overhead imposed by the signature algorithm itself will decrease.

IV. Conclusion

In this work we designed and implemented a post-quantum RA system, demonstrating its suitability for resource constrained devices. Further we showed that it is possible to retrofit existing RISC-V devices with the ability to perform post-quantum RA without requiring specialized hardware or incurring additional costs despite the overhead imposed by the post-quantum algorithms. We demonstrate this with our implementation SPRAV, which does not require dedicated security hardware and relies solely on the RISC-V PMP primitive as well as directly mapped ROM to provide a RoT. Since the inclusion of PMP is prevalent, when more than one privilege level is implemented in a RISC-V system, many current and future devices will be able to benefit from this research.

References

[1] B. Schneier, "IoT Security: What's Plan B?," *IEEE Security & Privacy*, vol. 15, no. 5, pp. 96–96, 2017.

[2] H. Griffioen and C. Doerr, "Examining Mirai's Battle over the Internet of Things," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS)*, p. 743–756, 2020.

[3] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou, "Understanding the Mirai Botnet," in *26th USENIX Security Symposium*, pp. 1093–1110, 2017.

[4] G. Coker, J. Guttman, P. Loscocco, A. Herzog, J. Millen, B. O'Hanlon, J. Ramsdell, A. Segall, J. Sheehy, and B. Sniffen, "Principles of remote attestation," *Int. J. Inf. Sec.*, vol. 10, pp. 63–81, 06 2011.

[5] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997.

[6] H. Jayakumar, A. Raha, Y. Kim, S. Sutar, W. S. Lee, and V. Raghunathan, "Energy-efficient system design for iot devices," in *2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC)*, 2016.

[7] S. Greengard, "Will RISC-V revolutionize computing?," *Communications of the ACM*, vol. 63, pp. 30–32, 2020.

[8] F. Brasser, B. El Mahjoub, A.-R. Sadeghi, C. Wachsmann, and P. Koeberl, "TyTAN: Tiny trust anchor for tiny devices," in *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, pp. 1–6, 2015.

[9] A. P. Fournaris, G. Tasopoulos, M. Brohet, and F. Regazzoni, "Running Longer To Slim Down: Post-Quantum Cryptography on Memory-Constrained Devices," in *2023 IEEE International Conference on Omni-layer Intelligent Systems (COINS)*, pp. 1–6, 2023.