
RISC-V®
Security HC meeting
March 17, 2022

Only RISC-V Members May Attend

- Non-members are asked to please leave except for Joint Working Groups (JWG).
- Members share IP protection by virtue of their common membership agreement. Non-members being present jeopardizes that protection. Joint working groups (JWG) agree that any IP discussed or worked on is fully open source and unencumbered as per the policy.
- It is easy to become a member. Check out riscv.org/membership
- If you need work done between non-members or or other orgs and RISC-V, please use a joint working group (JWG).
  - used to allow non-members in SIGs but the SIGs purpose has changed.
- Please put your name and company (in parens after your name) as your zoom name. If you are an individual member just use the word "individual" instead of company name.
- Non-member guests may present to the group but should only stay for the presentation. Guests should leave for any follow on discussions.

RISC-V®

Antitrust Policy Notice

RISC-V International meetings involve participation by industry competitors, and it is the intention of RISC-V International to conduct all its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be aware of, and not participate in, any activities that are prohibited under applicable US state, federal or foreign antitrust and competition laws.

Examples of types of actions that are prohibited at RISC-V International meetings and in connection with RISC-V International activities are described in the RISC-V International Regulations Article 7 available here: https://riscv.org/regulations/

If you have questions about these matters, please contact your company counsel.

RISC-V®

Collaborative & Welcoming Community

RISC-V is a free and open ISA enabling a new era of processor innovation through open standard collaboration. Born in academia and research, RISC-V ISA delivers a new level of free, extensible software and hardware freedom on architecture, paving the way for the next 50 years of computing design and innovation.

We are a transparent, collaborative community where all are welcomed, and all members are encouraged to participate. We are a continuous improvement organization. If you see something that can be improved, please tell us. help@riscv.org

We as members, contributors, and leaders pledge to make participation in our community a harassment-free experience for everyone.

https://riscv.org/community/community-code-of-conduct/

RISC-V®

Conventions

- Unless it is a scheduled agenda topic, we don't solve problems or detailed topics in most meetings unless specified in the agenda because we don't often have enough time to do so and it is more efficient to do so offline and/or in email. We identify items and send folks off to do the work and come back with solutions or proposals.
- If some policy, org, extension, etc. can be doing things in a better way, help us make it better. Do not change or not abide by the item unillaterly. Instead let's work together to make it better.
- Please conduct meetings that accommodates the virtual and broad geographical nature of our teams. This includes meeting times, repeating questions before you answer, at appropriate times polling attendees, guide people to interact in a way that has attendees taking turns speaking, …
- Where appropriate and possible, meeting minutes will be added as speaker notes within the slides for the Agenda

Risc-V Security

RISC-V®

Agenda

- Security Model TG
- AP-TEE TG
- Trust Dies in Darkness https://eprint.iacr.org/2022/208.pdf
- iopmp next steps

RISC-V

Security Model TG

- Acting Chair, Vice Chair
- Charter Status

RISC-V

- Manuel volunteered as acting chair to get TG started
- Next step: create charter and request infrastructure

AP-TEE TG

- Update

- Ravi to send latest charter to Security HC reflector
- Will request for TSC meeting slot to discuss & vote on AP-TEE charter
- Ravi to move current doc to its target spec repo

Trust Dies in Darkness

- Lessons ?
- Discussion

Trust Dies in Darkness:
Shedding Light on Samsung's TrustZone Keymaster Design

Alon Shakevsky
shakevsky@mail.tau.ac.il

Eyal Ronen
eyal.ronen@cs.tau.ac.il

Avishai Wool
yash@eng.tau.ac.il

Tel-Aviv University

Abstract

ARM-based Android smartphones rely on the TrustZone hardware support for a Trusted Execution Environment (TEE) to implement security-sensitive functions. The TEE runs a separate, isolated, TrustZone Operating System (TZOS), in parallel to Android. The implementation of the cryptographic functions within the TZOS is left to the device vendors, who create proprietary undocumented designs.

In this work, we expose the cryptographic design and implementation of Android's Hardware-Backed Keystore in Samsung's Galaxy S6, S8, S10, S20, and S21 flagship devices. We reverse-engineered and provide a detailed description of the cryptographic design and code structure, and we unveil severe design flaws. We present an IV reuse attack on AES-GCM that allows an attacker to extract hardware-protected key material, and a downgrade attack that makes even the latest Samsung devices vulnerable to the IV reuse attack. We demonstrate working key extraction attacks on the latest devices. We also show the implications of our attacks on two higher-level cryptographic protocols between the TrustZone and a remote server: we demonstrate a working FIDO2 WebAuthn login bypass and a compromise of Google's Secure Key Import.

We discuss multiple flaws in the design flow of TrustZone based protocols. Although our specific attacks only apply to the >100 million devices made by Samsung, it raises the much more general requirement for open and proven standards for critical cryptographic and security designs.

1 Introduction

Beyond their usage in many and various daily activities, smartphones are increasingly used for many security-critical tasks, such as the protection of sensitive data (messages, images, files), cryptographic key management [20], FIDO2 web authentication [65], Digital Rights Management (DRM), mobile payment services [7] (e.g., Samsung Pay) and enterprise identity management [67].

Simultaneously, smartphones are becoming more and more complex and present an increasingly larger attack surface. The result is that they have become a major target for malware and exploitation attackers. There have been many public exploits that allow an attacker to escalate privileges in the Android OS, gaining execution as root or even as the OS kernel [9, 14, 28, 31, 43]. Ideally, such attacks should not be able to compromise the devices' security-critical tasks.

Trusted Execution Environments (TEEs) are largely used in modern mobile devices to provide an isolated environment for execution of Trusted Applications (TAs) that can securely perform security-critical tasks. They have a relatively small codebase and limited APIs.

In contrast, the Rich Execution Environments (REEs), such as Android OS, cannot be fully audited and trusted (due to their complexity). An isolated TEE can be used alongside the REE to implement security-sensitive functions. This makes it harder for an attacker to compromise these functions, as the attack surface is significantly reduced and is limited to communication with the TEE.

In other words, the goal of the TEE is to withstand attacks from a fully compromised REE, including by privileged adversaries with kernel or root capabilities.

ARM is the most widely used processor in the mobile and embedded markets [70], and it provides TEE hardware support with ARM TrustZone [1, 8]. TrustZone separates the device into two execution environments:

1. A non-secure REE where the "Normal World" operating system runs.
2. A secure TEE where the "Secure World" operating system runs.

The REE and TEE use separate resources (e.g., memory peripherals), and the hardware enforces the protection of Secure World.

In most mobile devices, the Android OS runs the non-secure Normal World. As for the Secure World, there are more choices. Even among Samsung devices, there are at

1

RISC-V

- Need identified for key protection when used crypto operations and during storage ➔ RISC-V isolation requirements ➔ need to decide how to create those and what (existing?) infrastructure to use
- SOC Infra HC has a key role to play in this
- We may need a Platform specification for Secure Element => Ved, Markku, Ravi to create recommendation

IOPMP

- Update and next steps

RISC-V

- Paul to update charter with latest feedback and send to Security HC reflector
- Request for TSC vote