Build Security Collaboratively

Matteo Carlini & Shebu V. Kuriakose
Privilege Escalation Attacks and The SaaS Cloud

The CPU catastrophe will hit hardest in the cloud

Security alert: Millions of cars vulnerable to key cloning

Consumers urged to secure internet connected cameras

IoT Device Security Concerns Could Limit IoT Growth

HUGE NUMBER OF ANDROID PHONES VULNERABLE TO CRITICAL TRUSTZONE BUG
Firmware is increasingly becoming the preferred target for attacks in every system

Firmware vulnerabilities recorded in the NIST National Vulnerability Database

https://nvd.nist.gov/vuln/search/statistics?form_type=Basic&results_type=statistics&query=Firmware&search_type=all
But there’s hope...a new hope!
Security: we win when we collaborate!
Trusted Firmware: Build Security Collaboratively

Open Governance Community Project

Reference open source implementation of Secure world software for Arm processors across all market segments

Membership open to all

Board

Technical Steering Committee
A success story: from 0% to infinity...and beyond!

Ecosystem contributions trend over years

- Arm Trusted Firmware (now TF-A)
- CLA → DCO
- TrustedFirmware.org
- OP-TEE.org
- TF-M Launch


TF-A & TF-M combined - 2020 projections

+120% in 2yrs
And the family is expanding!
And the family is expanding!

Welcome

Hafnium

to the Trusted Firmware family
Google is transferring Hafnium to Trusted Firmware

- Reference **Secure Partition Manager (SPM)** for **Armv8.4-A Secure EL2** extension
- Minimal codebase → reduced attack surface
- Enforces principle of least privilege and defence in-depth
- Enables isolation of one or multiple TEE instances

[Diagram showing the integration of Hafnium into Trusted Firmware]

[Link to Hafnium repository: http://git.trustedfirmware.org/hafnium]
Comprehensive open source reference implementation of Secure world software

**Isolation through virtualization** in the Secure world

**Standardization of interfaces** between Normal and Secure world through Arm PSA FF-A (SPCI) compliance

**Defragmentation** of the generic Secure Firmware space (EL3 & S-EL2)

Ease integration, testing, updatability and auditing

**Increased Security & Transparency**

**Reduced TTM & costs for all ecosystem!**
Trusted Firmware-M v1.0

Just the beginning, Not the End

- Implements Platform Security Architecture (PSA) v1.0 Specifications except PSA Crypto
- Meets PSA Level2 Protection Profile Requirements
- Root of Trust (RoT) for IoT Ecosystem to Meet PSA L1, L2 and Functional API certification
Mbed TLS Joins Trusted Firmware
To Build a Vibrant Community For A World Leading TLS/SSL Library

• Arm donating

• Distributed under Apache2.0 License

• Subscribe to Mbed TLS Mailing List to Start Collaborating
  https://www.trustedfirmware.org/contact/
PSA Crypto Steadfast Under Trusted Firmware

Normal World (REE/NSPE)
- Mbed TLS
- Network Stack
- Applications
- Operating System
- Hardware

Secure World (TEE/SPE)
- PSA Crypto
- PSA Driver APIs
- Secure Element OR Accelerators
Building Security Collaboratively

TF-A
OP-TEE
Hafnium

TF-M
Mbed TLS
PSA Crypto
How Do We Operate

BOARD

Technical Steering Committee

Maintainers

Sub Group1

Sub Group2
Members

arm

Data iO

FUTURE WEI Technologies

CYPRESS Embedded in Tomorrow

Google

Linaro

Texas Instruments

life.augmented
Welcome to Trusted Firmware Family
The Virtuous Circle Of Collaboration!

- Mailing Lists
- Open CI
- Open Source
- Open Reviews
- Tech Forums
- Workshop

https://www.trustedfirmware.org/meetings/

https://git.trustedfirmware.org/

https://review.trustedfirmware.org/

https://ci.trustedfirmware.org/
A Case For Collaborative Security Software

- To Solve Increasing Complexity, Skills Gaps, Vulnerability and Attacks

“63% of companies have experienced a data compromise or breach within the past 12 months due to an exploited vulnerability in hardware- or silicon-level security” - Forrester
Stay Safe & Secure
Thank you

Accelerating deployment in the Arm Ecosystem