

Secure boot, trusted boot and remote attestation for ARM TrustZone-based IoT Nodes

*Zhen Ling, Huaiyu Yan, Xinhui Shao, Junzhou
Luo, Yiling Xu, Bryan Pearson, Xinwen Fu
Journal of Systems Architecture 119 (2021)*

Oberon Swings

[Lin+21]

Outline

Introduction

Hybrid booting

Process integrity measurement

Evaluation & security analysis

Relevance for thesis

Outline

Introduction

Hybrid booting

Process integrity measurement

Evaluation & security analysis

Relevance for thesis

Goals

- IoT devices
- ARM (TrustZone)
- Assure integrity
- Defend against
 - Hardware attacks
 - OS/Firmware attacks
 - Software attacks

Solutions

- Hybrid booting
 - Secure boot
 - Trusted boot
- Process integrity measurement
 - Pagebased attestation

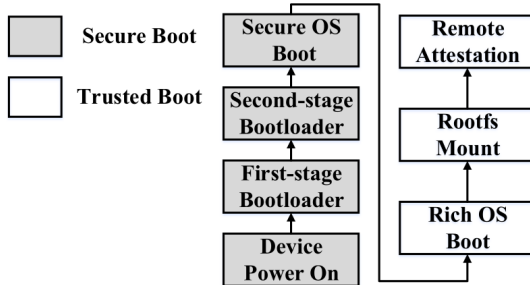


image: [Lin+21]

Outline

Introduction

Hybrid booting

Process integrity measurement

Evaluation & security analysis

Relevance for thesis

Secure boot

- Offline phase
 - Measure image
 - Hash
 - Sign
- Secure boot phase
 - First-stage bootloader trusted base
 - Locate next
 - Verify

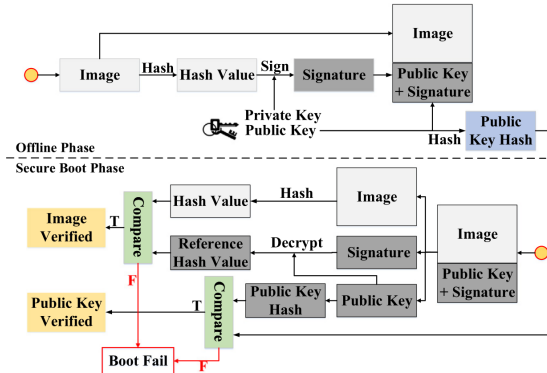
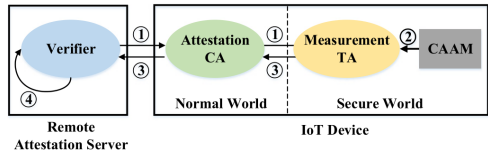
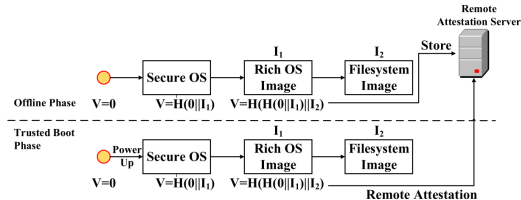


image: [Lin+21]

Trusted boot

- Offline phase
 - Calculate hash
 - Encrypt with symmetric key
 - Store
- Trusted boot phase
 1. TLS connection nonce
 2. Encrypt nonce & hash
 3. Respond
 4. Hash verification (integrity)
Nonce verification (replay)



images: [Lin+21]

Trusted boot encryption

- Symmetric key
- Safe at server
- Storage in IoT device
 - Generate blob key (RNG)
 - Encrypt and MAC
 - Derive BKEK using MK
 - Concatenate parts
 - SNVS for Master Key

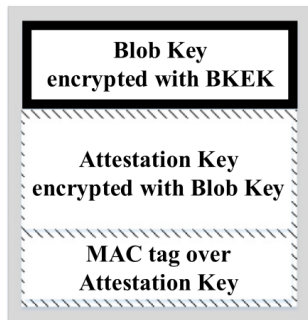


image: [Lin+21]

Outline

Introduction

Hybrid booting

Process integrity measurement

Evaluation & security analysis

Relevance for thesis

Idea

- Secure boot base
- Runtime integrity
- Measure code pages
- Measurement TA
- Remote Attestation Server

Process integrity measurement

1. Map address of init_task
2. Obtain physical address
3. Transform to virtual address
4. Calculate page boundaries
5. Measure each page

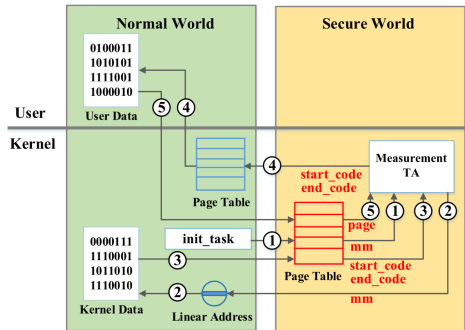


image: [Lin+21]

Process integrity attestation

1. Request nonce
2. Calculate measurement
3. Encrypt attestation info
4. Send cyphertext and repeat 2 or continue
5. Send cyphertext to verifier
6. Verify (new, modified)

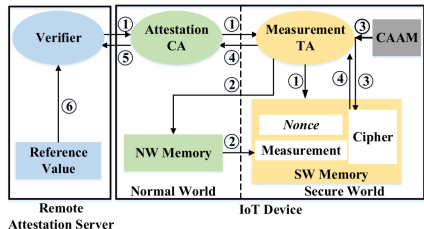


image: [Lin+21]

Outline

Introduction

Hybrid booting

Process integrity measurement

Evaluation & security analysis

Relevance for thesis

Results

Performance

- Secure boot doubles secure OS boot-time
- Trusted boot adds little overhead (0.5%)
- Measurement TA and attestation CA overhead ($-0.5\% \approx +0.5\%$)

Security

- Secure boot gives secure base
- Measurement method relies on NW

Outline

Introduction

Hybrid booting

Process integrity measurement

Evaluation & security analysis

Relevance for thesis

Focus shift

- Secure boot (engineering)
- Attestation
 - Informing user
 - Securing NW
- Reproduction
 - Process measurement
 - Process attestation
- Adjustments
 - Remote server
 - Reliance on NW OS

Differences

Paper

- Secure boot
- Trusted boot
- Remote attestation
- IoT devices

Thesis

- Secure boot assumed
- No Trusted boot
- SW attests NW
- Secure Open platform

Questions?

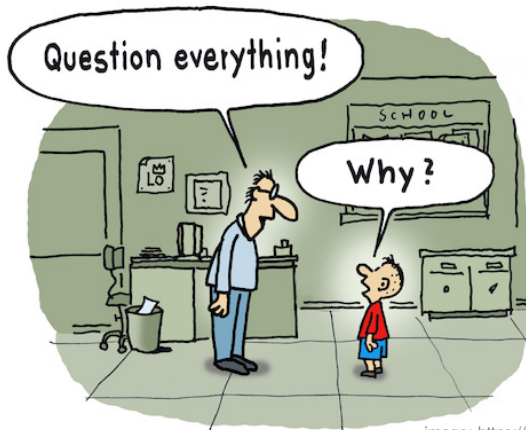


image: https://www.toonpool.com/cartoons/Question_376876

References



Zhen Ling et al. “Secure boot, trusted boot and remote attestation for ARM TrustZone-based IoT Nodes”. In: Journal of Systems Architecture 119 (July 2021), p. 102240. DOI: [10.1016/j.sysarc.2021.102240](https://doi.org/10.1016/j.sysarc.2021.102240).