ReZone: Disarming TrustZone with TEE Privilege Reduction

David Cerdeira, José Martins, Nuno Santos, Sandro Pinto
TrustZone Is Widely Used in Security Critical Applications
TrustZone Is Widely Used in Security Critical Applications

arm

TECHNOLOGIES

TRUSTZONE FOR CORTEX-A

Biometric Authentication
TrustZone Is Widely Used in Security Critical Applications

Biometric Authentication

Digital Rights Management

NETFLIX
TrustZone Is Widely Used in Security Critical Applications

ARM Technologies

TrustZone for Cortex-A

Biometric Authentication  Digital Rights Management  Electronic Payments
TrustZone TEE Software Architecture (pre Armv8.4)
• REE OS (EL1) and Apps (EL0) in the normal word

TrustZone TEE Software Architecture (pre Armv8.4)
TrustZone TEE Software Architecture (pre Armv8.4)

- REE OS (EL1) and Apps (EL0) in the normal word
- Trusted OS (S.EL1) and TAs (S.EL0) in the secure world

Diagram:

- Normal World (REE)
  - N.EL0: REE Application
  - N.EL0: REE OS

- Secure World (TEE)
  - S.EL0: Trusted Application
  - S.EL1: Trusted OS
TrustZone TEE Software Architecture (pre Armv8.4)

- REE OS (EL1) and Apps (EL0) in the normal word
- Trusted OS (S.EL1) and TAs (S.EL0) in the secure world
- Secure Monitor (EL3) manages world switch
TrustZone TEE Software Architecture (pre Armv8.4)

- REE OS (EL1) and Apps (EL0) in the normal word
- Trusted OS (S.EL1) and TAs (S.EL0) in the secure world
- Secure Monitor (EL3) manages world switch

TrustZone prevents the REE from directly compromising the TEE.
Open Problem: Mitigate Privilege Escalation Attack in Trustzone TEE
Open Problem: Mitigate Privilege Escalation Attack in Trustzone TEE

**Trusted OS has unrestricted access to the full system**
Open Problem: Mitigate Privilege Escalation Attack in Trustzone TEE

Trusted OS has unrestricted access to the full system
Open Problem: Mitigate Privilege Escalation Attack in Trustzone TEE

Trusted OS has unrestricted access to the full system

1. Hijack a user-level TA
Open Problem: Mitigate Privilege Escalation Attack in Trustzone TEE

Trusted OS has unrestricted access to the full system

1. Hijack a user-level TA
2. Hijack the Trusted OS
Open Problem: Mitigate Privilege Escalation Attack in Trustzone TEE

**Trusted OS has unrestricted access to the full system**

1. Hijack a user-level TA
2. Hijack the Trusted OS

A. Control the rich OS
Open Problem: Mitigate Privilege Escalation Attack in Trustzone TEE

Trusted OS has unrestricted access to the full system

1. Hijack a user-level TA
   A. Control the rich OS
2. Hijack the Trusted OS
   B. Control a kernel-level TA
Open Problem: Mitigate Privilege Escalation Attack in Trustzone TEE

Trusted OS has unrestricted access to the full system

1. Hijack a user-level TA
2. Hijack the Trusted OS

A. Control the rich OS
B. Control a kernel-level TA
C. Control the secure Monitor
Solution: Deprivelege the TEE
Solution: Deprivelege the TEE

Deprivileging the TEE increases protection for:

- Application
- Malware
- Rich OS

Diagram:

- Normal World
  - Application
  - Malware
- Secure World
  - TA
  - TOS

El levels:
- EL0
- EL1
- EL3

REZONE Secure Monitor
Solution: Deprivilege the TEE

Deprivilege the TEE increases protection for:

a) Normal World REE

Diagram:
- Normal World
  - Application
  - Malware
- Secure World
  - TAU
  - TOS
  - REZONE Secure Monitor

EL0
EL1
EL3
Deprivelege the TEE increases protection for:

a) Normal World REE

b) Other TEEs / Zones

Solution: Deprivelege the TEE
Deprivelege the TEE increases protection for:

a) Normal World REE

b) Other TEEs / Zones

c) Secure Monitor

Solution: Deprivelege the TEE
Solution: Deprivelege the TEE

Deprivelege the TEE increases protection for:

a) Normal World REE
b) Other TEEs / Zones
c) Secure Monitor
We Propose ReZone
We Propose ReZone

- An approach to **deprivilege** the Trusted OS
  - Use TrustZone orthogonal hardware features present in COTS platforms
We Propose ReZone

- An approach to **deprive**lge the Trusted OS
  - Use TrustZone orthogonal hardware features present in COTS platforms
- Implementation in a **real-world platform** and **software**
  - Evaluate ReZone in Embedded Linux and Android software stacks
We Propose ReZone

- An approach to **deprivilege** the Trusted OS
  - Use TrustZone orthogonal hardware features present in COTS platforms
- Implementation in a **real-world platform** and **software**
  - Evaluate ReZone in Embedded Linux and Android software stacks
- Performance penalty does **not degrade UX**
  - Evaluate two use cases: Bitcoin Wallet and DRM
We Propose ReZone

- An approach to **deprivilege** the Trusted OS
  - Use TrustZone orthogonal hardware features present in COTS platforms
- Implementation in a **real-world platform and software**
  - Evaluate ReZone in Embedded Linux and Android software stacks
- Performance penalty does **not degrade UX**
  - Evaluate two use cases: Bitcoin Wallet and DRM
- **Mitigate ~87%** of critical surveyed CVEs (80)
  - Mitigation of most Trusted OS and Trusted Applications vulnerabilities
ReZone Design

Normal World

Secure World

Application
Application

TA
EL0

TOS
EL1

Secure Monitor
EL3

Processor Core

TrustZone Controllers

Memory

Software

Hardware
ReZone Design

![Diagram of ReZone Design](image)

- **Normal World**: Application, Rich OS, Secure Monitor
- **Secure World**: TA, TOS, REZONE Trampoline
- **EL Levels**: EL0, EL1, EL3

- **Processor Core**
- **TrustZone Controllers**
- **Memory**
ReZone Design
By leveraging the PPC and ACU we can deprivilege the Trusted OS.
By leveraging the **PPC and ACU** we can deprivilege the Trusted OS.
Rezone Use of PPC + ACU
ReZone Use of PPC + ACU

- Starting from normal world execution
ReZone Use of PPC + ACU

- Starting from normal world execution
- Normal world can access the normal memory
ReZone Use of PPC + ACU

- Starting from normal world execution
- Normal world can access the normal memory
- TrustZone prevents accesses to secure world
ReZone Use of PPC + ACU

- Trampoline interacts with the Gatekeeper to reconfigure the PPC
ReZone Use of PPC + ACU

- Trampoline interacts with the Gatekeeper to reconfigure the PPC
- To prevent a Zone from undoing access control policy the processor cannot access the PPC Ctl. directly
ReZone Use of PPC + ACU

- Trampoline interacts with the Gatekeeper to reconfigure the PPC.
- To prevent a Zone from undoing access control policy the processor cannot access the PPC Ctl. directly.
- The ACU validates the interaction and performs reconfiguration.
The Zone will execute
- The Zone will execute
- PPC will only allow access to the zone memory
On a Zone exit the PPC is reconfigured again to undo the policy.
Rezone Use of PPC + ACU

- The normal world can resume execution
Implementation Challenges
Implementation Challenges

• Cross-core synchronization
  • Use of synchronization primitives, and core suspension
Implementation Challenges

• Cross-core synchronization
  • Use of synchronization primitives, and core suspension

• Microarchitectural maintenance
  • Cache and TLB Maintenance
Implementation Challenges

• Cross-core synchronization
  • Use of synchronization primitives, and core suspension
• Microarchitectural maintenance
  • Cache and TLB Maintenance
• Dynamic PPC reconfiguration
  • PPC reconfiguration optimization
Implementation Challenges

- Cross-core synchronization
  - Use of synchronization primitives, and core suspension
- Microarchitectural maintenance
  - Cache and TLB Maintenance
- Dynamic PPC reconfiguration
  - PPC reconfiguration optimization
- Handling Zone Exits
  - Preventing crashes and cache code injection
ReZone Performance Evaluation
We evaluate ReZone across three vectors
ReZone Performance Evaluation

We evaluate ReZone across three vectors

- Micro-Benchmarks
  - Evaluate overheads of REE-TA interaction
ReZone Performance Evaluation

We evaluate ReZone across three vectors

- Micro-Benchmarks
  - Evaluate overheads of REE-TA interaction
- Performance of Real-World Use Cases
  - Two TAs that implement real workloads
ReZone Performance Evaluation

We evaluate ReZone across three vectors

- Micro-Benchmarks
  - Evaluate overheads of REE-TA interaction
- Performance of Real-World Use Cases
  - Two TAs that implement real workloads
- Impact on REE performance
  - Impact of calls to zones during the execution of an Android benchmark
Performance Evaluation
Performance Evaluation

- Micro benchmarks
  - OPTEE’s xtest
  - GP Client API
Performance Evaluation

- Micro benchmarks
  - OPTEE’s xtest
  - GP Client API

- Real world use cases
  - Bitcoin wallet
  - DRM
Performance Evaluation

- Simple workloads with many world switches → higher overheads

- Micro benchmarks
  - OPTEE’s xtest
  - GP Client API

- Real world use cases
  - Bitcoin wallet
  - DRM
Performance Evaluation

- Simple workloads with many world switches → higher overheads
- UX → not significantly affected

- Micro benchmarks
  - OPTEE’s xtest
  - GP Client API
- Real world use cases
  - Bitcoin wallet
  - DRM

![Graph showing performance comparison under different conditions.](image)
Performance Evaluation
Performance Evaluation

- Normal World Impact
- PCMark 3.0 for Android
Performance Evaluation

- Single-Core interrupt

<table>
<thead>
<tr>
<th>Interval (ms)</th>
<th>Score</th>
<th>Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>4369</td>
<td>12.97%</td>
</tr>
<tr>
<td>100</td>
<td>4776</td>
<td>4.86%</td>
</tr>
<tr>
<td>1000</td>
<td>4983</td>
<td>0.74%</td>
</tr>
</tbody>
</table>

- Normal World Impact
  - PCMark 3.0 for Android
Performance Evaluation

- Single-Core interrupt

<table>
<thead>
<tr>
<th>Interval (ms)</th>
<th>Score</th>
<th>Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>4369</td>
<td>12.97%</td>
</tr>
<tr>
<td>100</td>
<td>4776</td>
<td>4.86%</td>
</tr>
<tr>
<td>1000</td>
<td>4983</td>
<td>0.74%</td>
</tr>
</tbody>
</table>

- Multi-Core interrupt (1s interval)

<table>
<thead>
<tr>
<th># of Cores</th>
<th>Score</th>
<th>Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4983</td>
<td>0.74%</td>
</tr>
<tr>
<td>2</td>
<td>4938</td>
<td>1.63%</td>
</tr>
<tr>
<td>4</td>
<td>4833</td>
<td>3.73%</td>
</tr>
</tbody>
</table>

- Normal World Impact
  - PCMark 3.0 for Android
CVE Mitigation
# CVE Mitigation

<table>
<thead>
<tr>
<th>CVE</th>
<th>C</th>
<th>CVE</th>
<th>C</th>
<th>CVE</th>
<th>C</th>
<th>CVE</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014-9979</td>
<td>TO</td>
<td>2017-11011</td>
<td>TO</td>
<td>2015-9000</td>
<td>TA</td>
<td>2015-8997</td>
<td>TO/TA</td>
</tr>
<tr>
<td>2015-8999</td>
<td>TO</td>
<td>2017-14912</td>
<td>TO</td>
<td>2015-9002</td>
<td>TA</td>
<td>2015-8998</td>
<td>TO/TA</td>
</tr>
<tr>
<td>2015-9070</td>
<td>TO</td>
<td>2017-14916</td>
<td>TO</td>
<td>2015-9162</td>
<td>TA</td>
<td>2015-9005</td>
<td>TO/TA</td>
</tr>
<tr>
<td>2015-9071</td>
<td>TO</td>
<td>2017-14917</td>
<td>TO</td>
<td>2015-9174</td>
<td>TA</td>
<td>2015-9007</td>
<td>TO/TA</td>
</tr>
<tr>
<td>2015-9072</td>
<td>TO</td>
<td>2017-17176</td>
<td>TO</td>
<td>2015-9183</td>
<td>TA</td>
<td>2016-2432</td>
<td>TO/TA</td>
</tr>
<tr>
<td>2015-9073</td>
<td>TO</td>
<td>2017-18071</td>
<td>TO</td>
<td>2017-6293</td>
<td>TA</td>
<td>2016-10297</td>
<td>TO/TA</td>
</tr>
<tr>
<td>2015-9108</td>
<td>TO</td>
<td>2017-18128</td>
<td>TO</td>
<td>2017-18310</td>
<td>TA</td>
<td>2017-6289</td>
<td>TO/TA</td>
</tr>
<tr>
<td>2015-9112</td>
<td>TO</td>
<td>2017-18129</td>
<td>TO</td>
<td>2017-18312</td>
<td>TA</td>
<td>2017-14913</td>
<td>TO/TA</td>
</tr>
<tr>
<td>2015-9113</td>
<td>TO</td>
<td>2017-18132</td>
<td>TO</td>
<td>2017-18317</td>
<td>TA</td>
<td>2017-18293</td>
<td>TO/TA</td>
</tr>
<tr>
<td>2015-9198</td>
<td>TO</td>
<td>2017-18133</td>
<td>TO</td>
<td>2018-5210</td>
<td>TA</td>
<td>2017-18296</td>
<td>TO/TA</td>
</tr>
<tr>
<td>2015-9199</td>
<td>TO</td>
<td>2017-18311</td>
<td>TO</td>
<td>2018-5885</td>
<td>TA</td>
<td>2017-18297</td>
<td>TO/TA</td>
</tr>
<tr>
<td>2015-9200</td>
<td>TO</td>
<td>2017-18314</td>
<td>TO</td>
<td>2014-9932</td>
<td>TO/TA</td>
<td>2017-18298</td>
<td>TO/TA</td>
</tr>
<tr>
<td>2016-2431</td>
<td>TO</td>
<td>2017-18315</td>
<td>TO</td>
<td>2014-9935</td>
<td>TO/TA</td>
<td>2018-5866</td>
<td>TO/TA</td>
</tr>
<tr>
<td>2016-10238</td>
<td>TO</td>
<td>2018-3588</td>
<td>TO</td>
<td>2014-9936</td>
<td>TO/TA</td>
<td>2017-18282</td>
<td>HW</td>
</tr>
<tr>
<td>2016-10432</td>
<td>TO</td>
<td>2018-5870</td>
<td>TO</td>
<td>2014-9937</td>
<td>TO/TA</td>
<td>2015-9003</td>
<td>CI</td>
</tr>
<tr>
<td>2017-6290</td>
<td>TO</td>
<td>2016-10239</td>
<td>TO</td>
<td>2014-9945</td>
<td>TO/TA</td>
<td>2016-10398</td>
<td>CI</td>
</tr>
<tr>
<td>2017-6292</td>
<td>TO</td>
<td>2018-11950</td>
<td>TO</td>
<td>2014-9948</td>
<td>TO/TA</td>
<td>2017-14907</td>
<td>CI</td>
</tr>
<tr>
<td>2017-6294</td>
<td>TO</td>
<td>2015-4422</td>
<td>TA</td>
<td>2014-9949</td>
<td>TO/TA</td>
<td>2017-18146</td>
<td>CI</td>
</tr>
<tr>
<td>2017-8274</td>
<td>TO</td>
<td>2015-6639</td>
<td>TA</td>
<td>2015-8995</td>
<td>TO/TA</td>
<td>2016-10458</td>
<td>BL</td>
</tr>
<tr>
<td>2017-11010</td>
<td>TO</td>
<td>2015-6647</td>
<td>TA</td>
<td>2015-8996</td>
<td>TO/TA</td>
<td>2017-14911</td>
<td>BL</td>
</tr>
</tbody>
</table>
## CVE Mitigation

<table>
<thead>
<tr>
<th>CVE</th>
<th>C</th>
<th>CVE</th>
<th>C</th>
<th>CVE</th>
<th>C</th>
<th>CVE</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014-9979</td>
<td>TO</td>
<td>2017-11011</td>
<td>TO</td>
<td>2015-9000</td>
<td>TA</td>
<td>2015-8997</td>
<td>TO/TA</td>
</tr>
<tr>
<td>2015-8999</td>
<td>TO</td>
<td>2017-14912</td>
<td>TO</td>
<td>2015-9002</td>
<td>TA</td>
<td>2015-8998</td>
<td>TO/TA</td>
</tr>
<tr>
<td>2015-9070</td>
<td>TO</td>
<td>2017-14916</td>
<td>TO</td>
<td>2015-9162</td>
<td>TA</td>
<td>2015-9005</td>
<td>TO/TA</td>
</tr>
<tr>
<td>2015-9071</td>
<td>TO</td>
<td>2017-14917</td>
<td>TO</td>
<td>2015-9174</td>
<td>TA</td>
<td>2015-9007</td>
<td>TO/TA</td>
</tr>
<tr>
<td>2015-9072</td>
<td>TO</td>
<td>2017-17176</td>
<td>TO</td>
<td>2015-9183</td>
<td>TA</td>
<td>2016-2432</td>
<td>TO/TA</td>
</tr>
<tr>
<td>2015-9073</td>
<td>TO</td>
<td>2017-18071</td>
<td>TO</td>
<td>2017-6293</td>
<td>TA</td>
<td>2016-10297</td>
<td>TO/TA</td>
</tr>
<tr>
<td>2015-9108</td>
<td>TO</td>
<td>2017-18128</td>
<td>TO</td>
<td>2017-18310</td>
<td>TA</td>
<td>2017-6289</td>
<td>TO/TA</td>
</tr>
<tr>
<td>2015-9112</td>
<td>TO</td>
<td>2017-18129</td>
<td>TO</td>
<td>2017-18312</td>
<td>TA</td>
<td>2017-14913</td>
<td>TO/TA</td>
</tr>
<tr>
<td>2015-9113</td>
<td>TO</td>
<td>2017-18132</td>
<td>TO</td>
<td>2017-18317</td>
<td>TA</td>
<td>2017-18293</td>
<td>TO/TA</td>
</tr>
<tr>
<td>2015-9198</td>
<td>TO</td>
<td>2017-18133</td>
<td>TO</td>
<td>2018-5210</td>
<td>TA</td>
<td>2017-18296</td>
<td>TO/TA</td>
</tr>
<tr>
<td>2015-9199</td>
<td>TO</td>
<td>2017-18311</td>
<td>TO</td>
<td>2018-5885</td>
<td>TA</td>
<td>2017-18297</td>
<td>TO/TA</td>
</tr>
<tr>
<td>2015-9200</td>
<td>TO</td>
<td>2017-18314</td>
<td>TO</td>
<td>2014-9932</td>
<td>TO/TA</td>
<td>2017-18298</td>
<td>TO/TA</td>
</tr>
<tr>
<td>2016-2431</td>
<td>TO</td>
<td>2017-18315</td>
<td>TO</td>
<td>2014-9935</td>
<td>TO/TA</td>
<td>2018-5866</td>
<td>TO/TA</td>
</tr>
<tr>
<td>2016-10238</td>
<td>TO</td>
<td>2018-3588</td>
<td>TO</td>
<td>2014-9936</td>
<td>TO/TA</td>
<td>2017-18282</td>
<td>HW</td>
</tr>
<tr>
<td>2016-10432</td>
<td>TO</td>
<td>2018-5870</td>
<td>TO</td>
<td>2014-9937</td>
<td>TO/TA</td>
<td>2015-9003</td>
<td>CI</td>
</tr>
<tr>
<td>2017-6290</td>
<td>TO</td>
<td>2016-10239</td>
<td>TO</td>
<td>2014-9945</td>
<td>TO/TA</td>
<td>2016-10398</td>
<td>CI</td>
</tr>
<tr>
<td>2017-6292</td>
<td>TO</td>
<td>2018-11950</td>
<td>TO</td>
<td>2014-9948</td>
<td>TO/TA</td>
<td>2017-14907</td>
<td>CI</td>
</tr>
<tr>
<td>2017-6294</td>
<td>TO</td>
<td>2015-4422</td>
<td>TA</td>
<td>2014-9949</td>
<td>TO/TA</td>
<td>2017-18146</td>
<td>CI</td>
</tr>
<tr>
<td>2017-8274</td>
<td>TO</td>
<td>2015-6639</td>
<td>TA</td>
<td>2015-8995</td>
<td>TO/TA</td>
<td>2016-10458</td>
<td>BL</td>
</tr>
<tr>
<td>2017-11010</td>
<td>TO</td>
<td>2015-6647</td>
<td>TA</td>
<td>2015-8996</td>
<td>TO/TA</td>
<td>2017-14911</td>
<td>BL</td>
</tr>
</tbody>
</table>
• Assuming multiple Zones with one TA per zone

<table>
<thead>
<tr>
<th>CVE</th>
<th>C</th>
<th>CVE</th>
<th>C</th>
<th>CVE</th>
<th>C</th>
<th>CVE</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014-9979</td>
<td>TO</td>
<td>2017-11011</td>
<td>TO</td>
<td>2015-9000</td>
<td>TA</td>
<td>2015-8997</td>
<td>TO/TA</td>
</tr>
<tr>
<td>2015-8999</td>
<td>TO</td>
<td>2017-14912</td>
<td>TO</td>
<td>2015-9002</td>
<td>TA</td>
<td>2015-8998</td>
<td>TO/TA</td>
</tr>
<tr>
<td>2015-9070</td>
<td>TO</td>
<td>2017-14916</td>
<td>TO</td>
<td>2015-9162</td>
<td>TA</td>
<td>2015-9005</td>
<td>TO/TA</td>
</tr>
<tr>
<td>2015-9071</td>
<td>TO</td>
<td>2017-14917</td>
<td>TO</td>
<td>2015-9174</td>
<td>TA</td>
<td>2015-9007</td>
<td>TO/TA</td>
</tr>
<tr>
<td>2015-9072</td>
<td>TO</td>
<td>2017-17176</td>
<td>TO</td>
<td>2015-9183</td>
<td>TA</td>
<td>2016-2432</td>
<td>TO/TA</td>
</tr>
<tr>
<td>2015-9073</td>
<td>TO</td>
<td>2017-18071</td>
<td>TO</td>
<td>2017-6293</td>
<td>TA</td>
<td>2016-10297</td>
<td>TO/TA</td>
</tr>
<tr>
<td>2015-9108</td>
<td>TO</td>
<td>2017-18128</td>
<td>TO</td>
<td>2017-18310</td>
<td>TA</td>
<td>2017-6289</td>
<td>TO/TA</td>
</tr>
<tr>
<td>2015-9112</td>
<td>TO</td>
<td>2017-18129</td>
<td>TO</td>
<td>2017-18312</td>
<td>TA</td>
<td>2017-14913</td>
<td>TO/TA</td>
</tr>
<tr>
<td>2015-9113</td>
<td>TO</td>
<td>2017-18132</td>
<td>TO</td>
<td>2017-18317</td>
<td>TA</td>
<td>2017-18293</td>
<td>TO/TA</td>
</tr>
<tr>
<td>2015-9198</td>
<td>TO</td>
<td>2017-18133</td>
<td>TO</td>
<td>2018-5210</td>
<td>TA</td>
<td>2017-18296</td>
<td>TO/TA</td>
</tr>
<tr>
<td>2015-9199</td>
<td>TO</td>
<td>2017-18311</td>
<td>TO</td>
<td>2018-5885</td>
<td>TA</td>
<td>2017-18297</td>
<td>TO/TA</td>
</tr>
<tr>
<td>2015-9200</td>
<td>TO</td>
<td>2017-18314</td>
<td>TO</td>
<td>2014-9932</td>
<td>TO/TA</td>
<td>2017-18298</td>
<td>TO/TA</td>
</tr>
<tr>
<td>2016-2431</td>
<td>TO</td>
<td>2017-18315</td>
<td>TO</td>
<td>2014-9935</td>
<td>TO/TA</td>
<td>2018-5866</td>
<td>TO/TA</td>
</tr>
<tr>
<td>2016-10238</td>
<td>TO</td>
<td>2018-3588</td>
<td>TO</td>
<td>2014-9936</td>
<td>TO/TA</td>
<td>2017-18282</td>
<td>HW</td>
</tr>
<tr>
<td>2016-10432</td>
<td>TO</td>
<td>2018-5870</td>
<td>TO</td>
<td>2014-9937</td>
<td>TO/TA</td>
<td>2015-9003</td>
<td>CI</td>
</tr>
<tr>
<td>2017-6290</td>
<td>TO</td>
<td>2016-10239</td>
<td>TO</td>
<td>2014-9945</td>
<td>TO/TA</td>
<td>2016-10398</td>
<td>CI</td>
</tr>
<tr>
<td>2017-6292</td>
<td>TO</td>
<td>2018-11950</td>
<td>TO</td>
<td>2014-9948</td>
<td>TO/TA</td>
<td>2017-14907</td>
<td>CI</td>
</tr>
<tr>
<td>2017-6294</td>
<td>TO</td>
<td>2015-4422</td>
<td>TA</td>
<td>2014-9949</td>
<td>TO/TA</td>
<td>2017-18146</td>
<td>CI</td>
</tr>
<tr>
<td>2017-8274</td>
<td>TO</td>
<td>2015-6639</td>
<td>TA</td>
<td>2015-8995</td>
<td>TO/TA</td>
<td>2016-10458</td>
<td>BL</td>
</tr>
<tr>
<td>2017-11010</td>
<td>TO</td>
<td>2015-6647</td>
<td>TA</td>
<td>2015-8996</td>
<td>TO/TA</td>
<td>2017-14911</td>
<td>BL</td>
</tr>
</tbody>
</table>
• Assuming multiple Zones with one TA per zone
• Mitigates ~87% CVEs:
  • Most TOS and TA vulnerabilities
• Assuming multiple Zones with one TA per zone
• Mitigates ~87% CVEs:
  • Most TOS and TA vulnerabilities
• Doesn’t Mitigate against:
  • Secret disclosures, Hardware attacks, Cryptographic flaws, Bootloader flaws
<table>
<thead>
<tr>
<th>Vendor</th>
<th>SoC Platform</th>
<th>PPC</th>
<th>ACU</th>
<th>RZ?</th>
</tr>
</thead>
<tbody>
<tr>
<td>NXP</td>
<td>iMX8MQ, iMX8QM</td>
<td>RDC, xRDC</td>
<td>Cortex-M4 SCU</td>
<td>YES</td>
</tr>
<tr>
<td>Xilinx</td>
<td>Ultrascale+ MPSoC, Versal ACAP</td>
<td>XMPU, XPPU, (SMMU)</td>
<td>PMU</td>
<td>YES</td>
</tr>
<tr>
<td>Nvidia</td>
<td>Tegra X1/X2, Xavier</td>
<td>SMMU</td>
<td>BPMP</td>
<td>YES</td>
</tr>
<tr>
<td>Socionext</td>
<td>SC2A11</td>
<td>SMMU</td>
<td>SCP</td>
<td>YES</td>
</tr>
<tr>
<td>Qualcomm</td>
<td>Snapdragon 845, 855, 865, 888, 8gen1</td>
<td>SMMU, XPU*</td>
<td>SPU</td>
<td>YES</td>
</tr>
<tr>
<td>Broadcom</td>
<td>Stingray</td>
<td>SMMU</td>
<td>SCP</td>
<td>YES</td>
</tr>
<tr>
<td>Samsung</td>
<td>Exynos 990, Exynos 2100</td>
<td>Periph. MMUs</td>
<td>iSE eSE</td>
<td>N/A</td>
</tr>
<tr>
<td>Mediatek</td>
<td>Dimensity 1200</td>
<td>x</td>
<td>x</td>
<td>No</td>
</tr>
<tr>
<td>HiSilicon</td>
<td>Kirin 9000</td>
<td>x</td>
<td>PMU</td>
<td>No</td>
</tr>
</tbody>
</table>
In Summary

- **TrustZone TEEs** have architectural **flaws**
In Summary

- **TrustZone TEEs** have architectural **flaws**
- **ReZone** is a novel security architecture that **reduces TEE privileges**
In Summary

- **TrustZone TEEs** have architectural **flaws**
- **ReZone** is a novel security architecture that **reduces TEE privileges**
- **ReZone** leverages **TrustZone-agnostic** hardware primitives
In Summary

- **TrustZone TEEs** have architectural **flaws**
- **ReZone** is a novel security architecture that **reduces TEE privileges**
- **ReZone** leverages **TrustZone-agnostic** hardware primitives
- **ReZone** was **implemented** and **evaluated** in a real-world **platform**
In Summary

• **TrustZone TEEs** have architectural **flaws**

• **ReZone** is a novel security architecture that **reduces TEE privileges**

• **ReZone** leverages **TrustZone-agnostic** hardware primitives

• **ReZone** was **implemented** and **evaluated** in a real-world **platform**

• **Performance** of real-world **TAs** (e.g., DRM) is **not** significantly **affected**
In Summary

- **TrustZone TEEs** have architectural **flaws**
- **ReZone** is a novel security architecture that **reduces TEE privileges**
- **ReZone** leverages **TrustZone-agnostic** hardware primitives
- **ReZone** was **implemented** and **evaluated** in a real-world **platform**
- **Performance** of real-world **TAs** (e.g., DRM) is **not** significantly **affected**
- **ReZone** could help **mitigate** many high severity **vulnerabilities**
QUESTIONS?

david.cerdeira@dei.uminho.pt
ReZone in Perspective

Armv8.4 S.EL2

Normal World (REE)
- N-EL0: App
- N-EL1: REE OS

Secure World (TEE)
- S-EL0: Trusted App
- S-EL1: Trusted OS

EL2: Hypervisor
- S-EL2: Partition Manager

Armv9 CCA

Realm World
- Re-EL0: App
- Re-EL1: OS
- Re-EL2: Realm Manager

Normal World (REE)
- N-EL0: App
- N-EL1: REE OS

Secure World (TEE)
- S-EL0: Trusted App
- S-EL1: Trusted OS

EL2: Hypervisor
- S-EL2: Partition Manager

EL3: Secure Monitor
- Root World