ReZone: Disarming TrustZone with TEE Privilege Reduction

David Cerdeira, José Martins,
Nuno Santos, Sandro Pinto

FCT Fundação para a Ciência e a Tecnologia
CENTROALGORITMI
UNIVERSIDADE DO MINHO
TÉCNICO LISBOA

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

arm

TECHNOLOGIES

TRUSTZONE FOR CORTEX-A

NETFLIX

Biometric Authentication

Digital Rights Management

TrustZone Is Widely Used in Security Critical Applications

arm

TECHNOLOGIES

TRUSTZONE FOR CORTEX-A

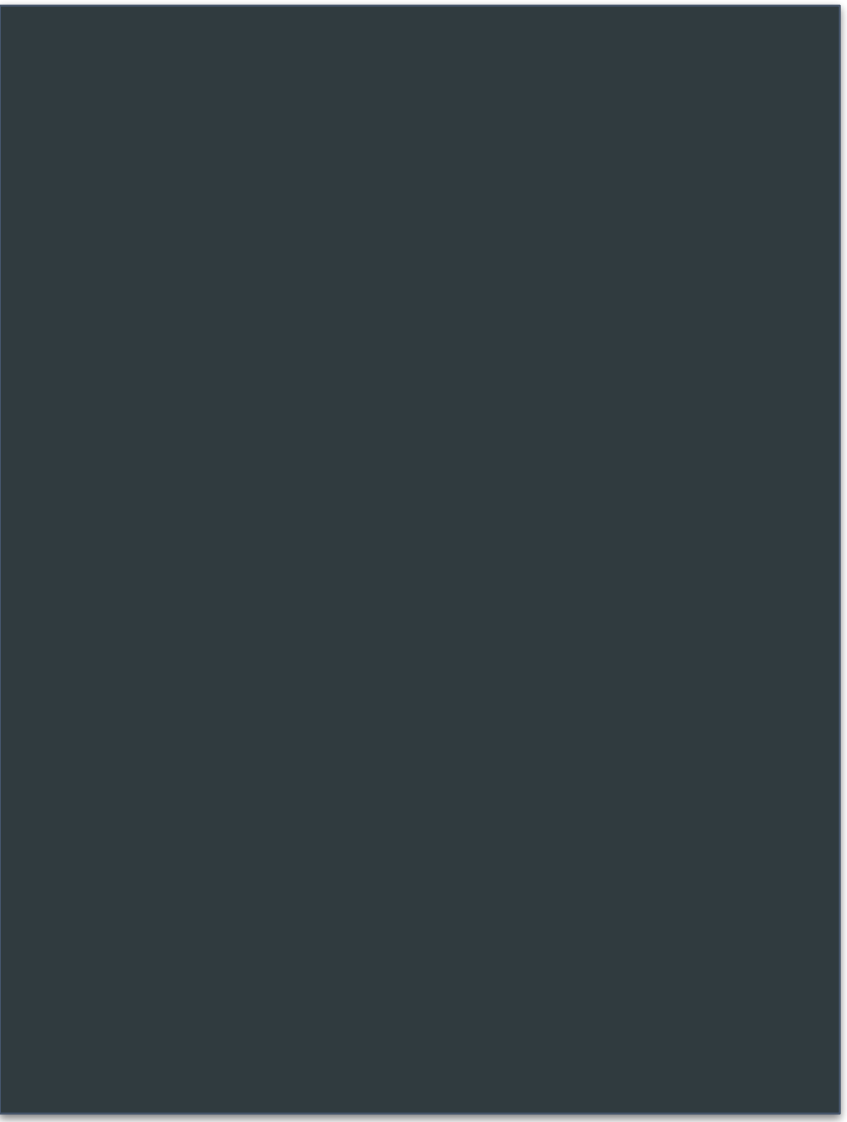
Biometric Authentication

NETFLIX

Digital Rights Management

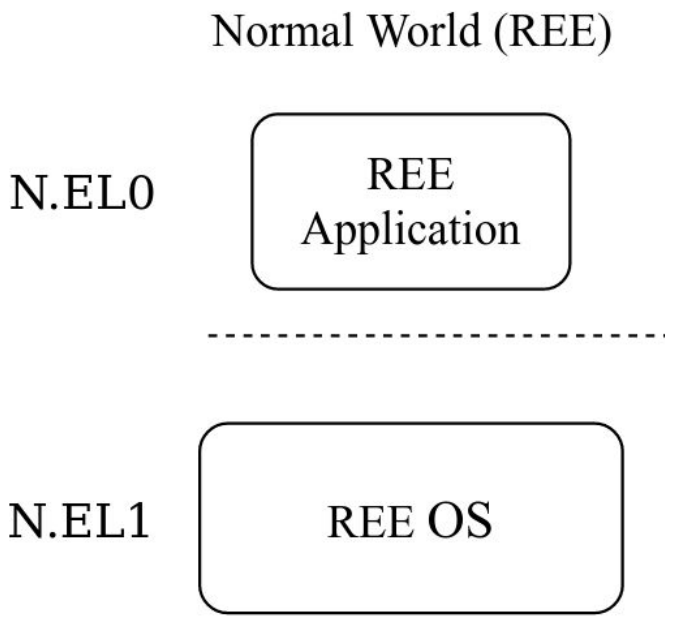
Electronic Payments

TrustZone TEE Software Architecture (pre Armv8.4)



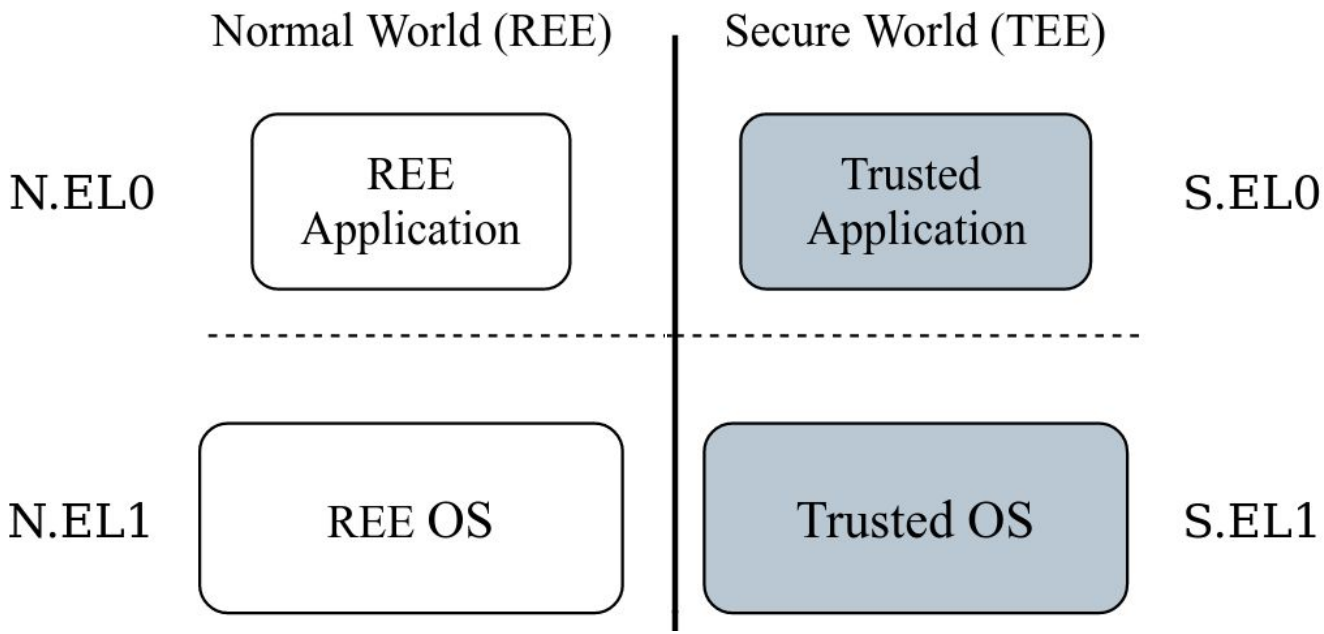
TrustZone TEE Software Architecture (pre Armv8.4)

- REE OS (EL1) and Apps (EL0) in the normal word



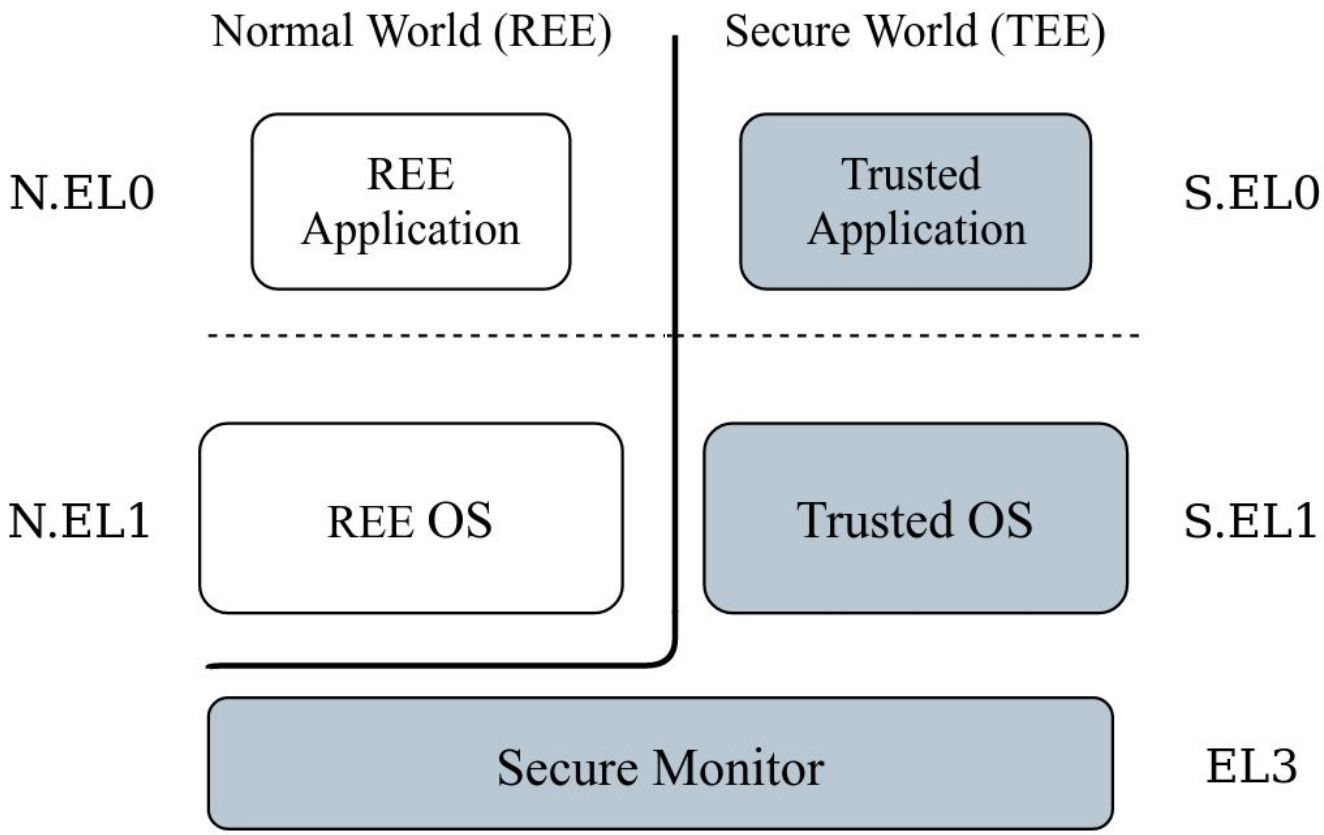
TrustZone TEE Software Architecture (pre Armv8.4)

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



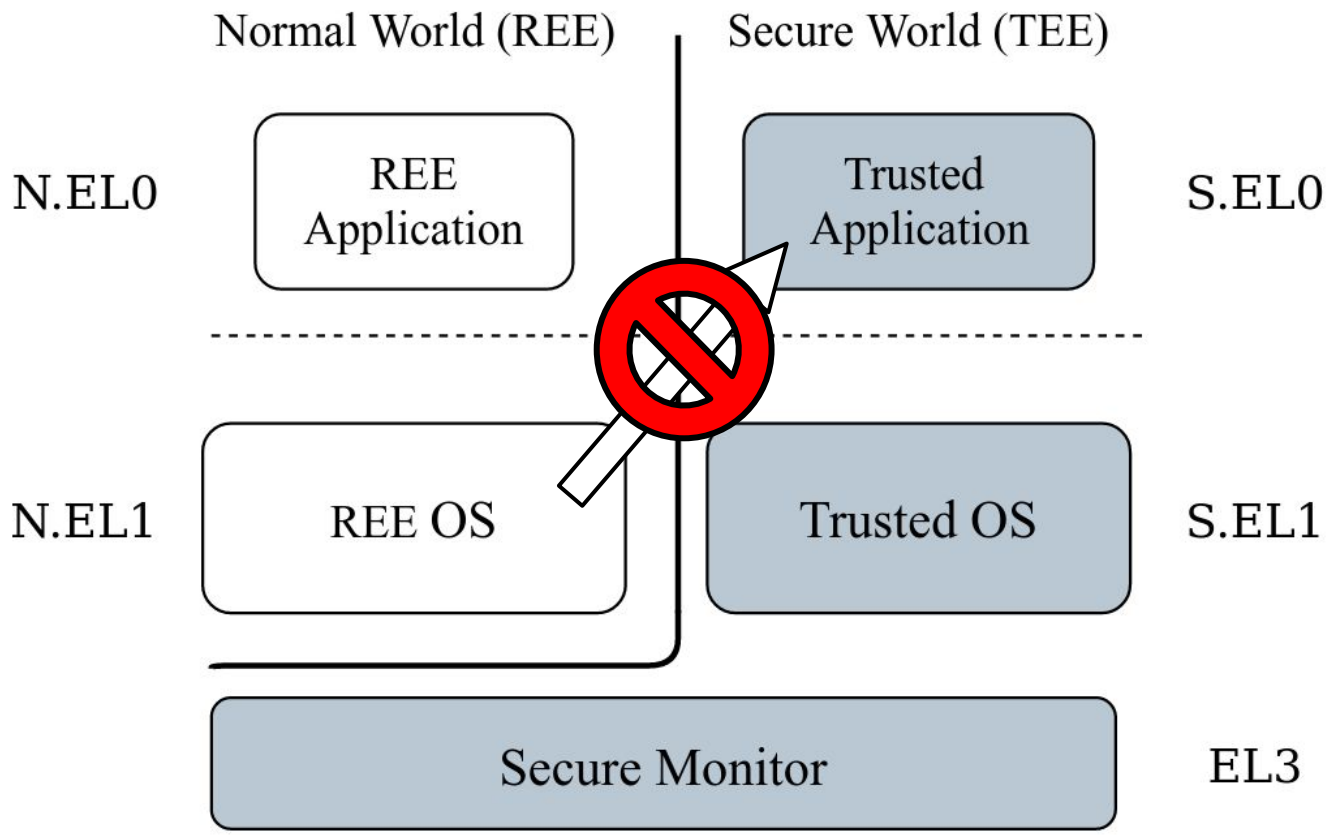
TrustZone TEE Software Architecture (pre Armv8.4)

- 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**.

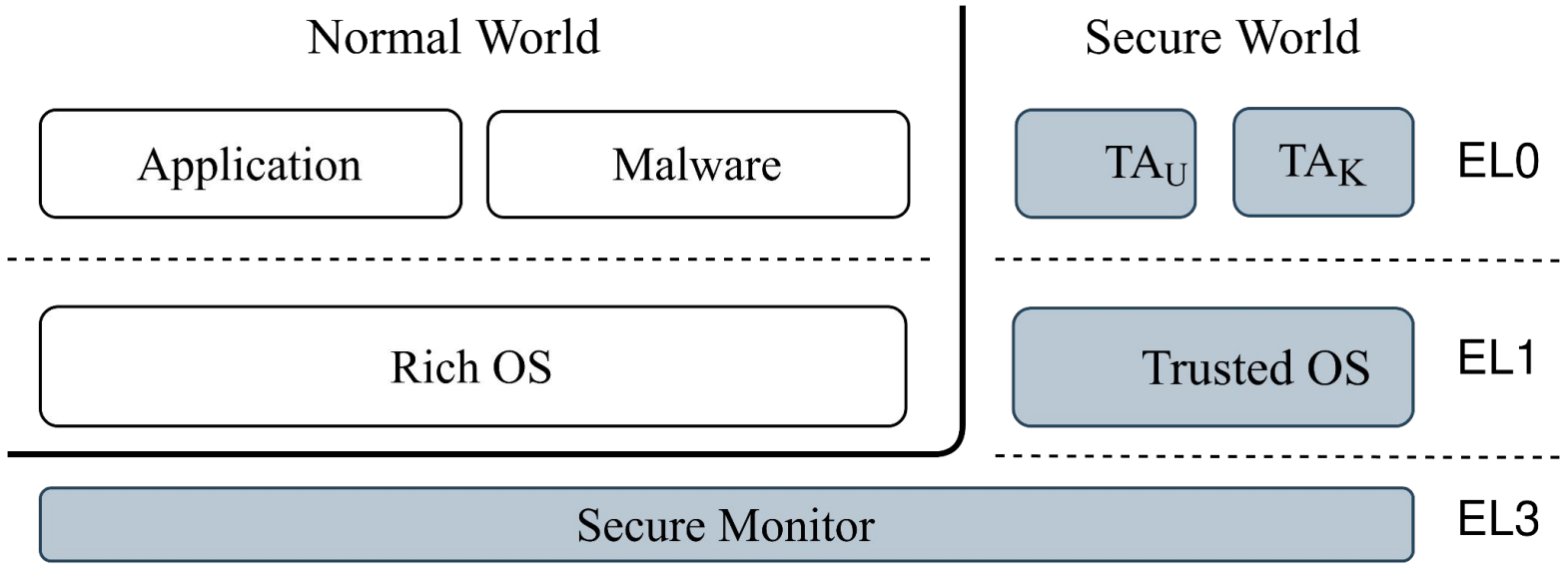
Open Problem: Mitigate Privilege Escalation Attack in Trustzone TEE

Open Problem: Mitigate Privilege Escalation Attack in Trustzone TEE

Trusted OS has unrestricted access to the full system

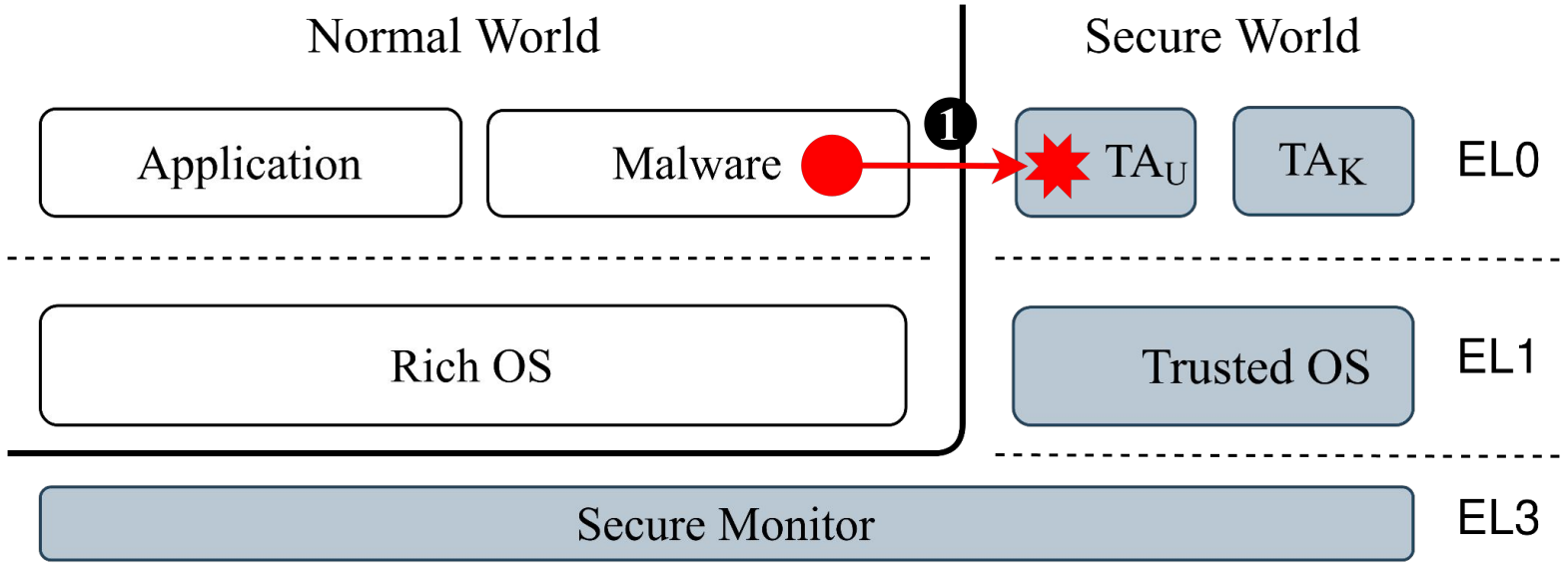
Open Problem: Mitigate Privilege Escalation Attack in Trustzone TEE

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



Open Problem: Mitigate Privilege Escalation Attack in Trustzone TEE

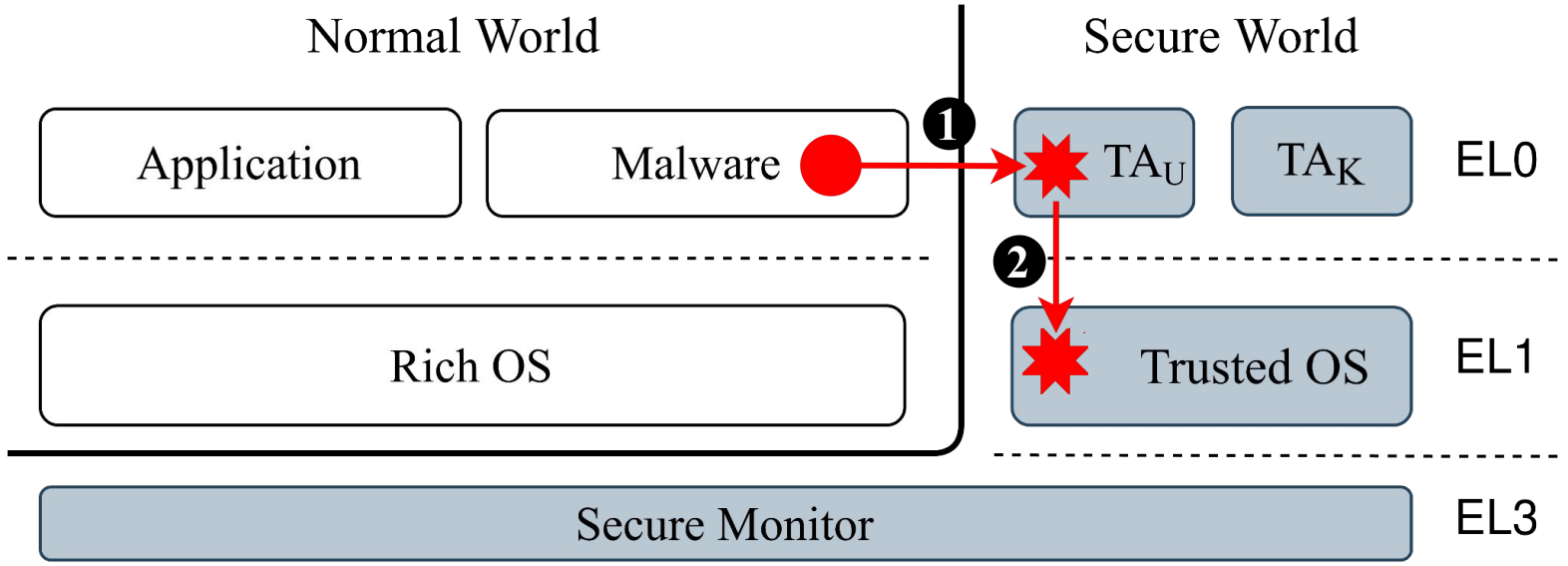
Trusted OS has unrestricted access to the full system



1. Hijack a user-level TA

Open Problem: Mitigate Privilege Escalation Attack in Trustzone TEE

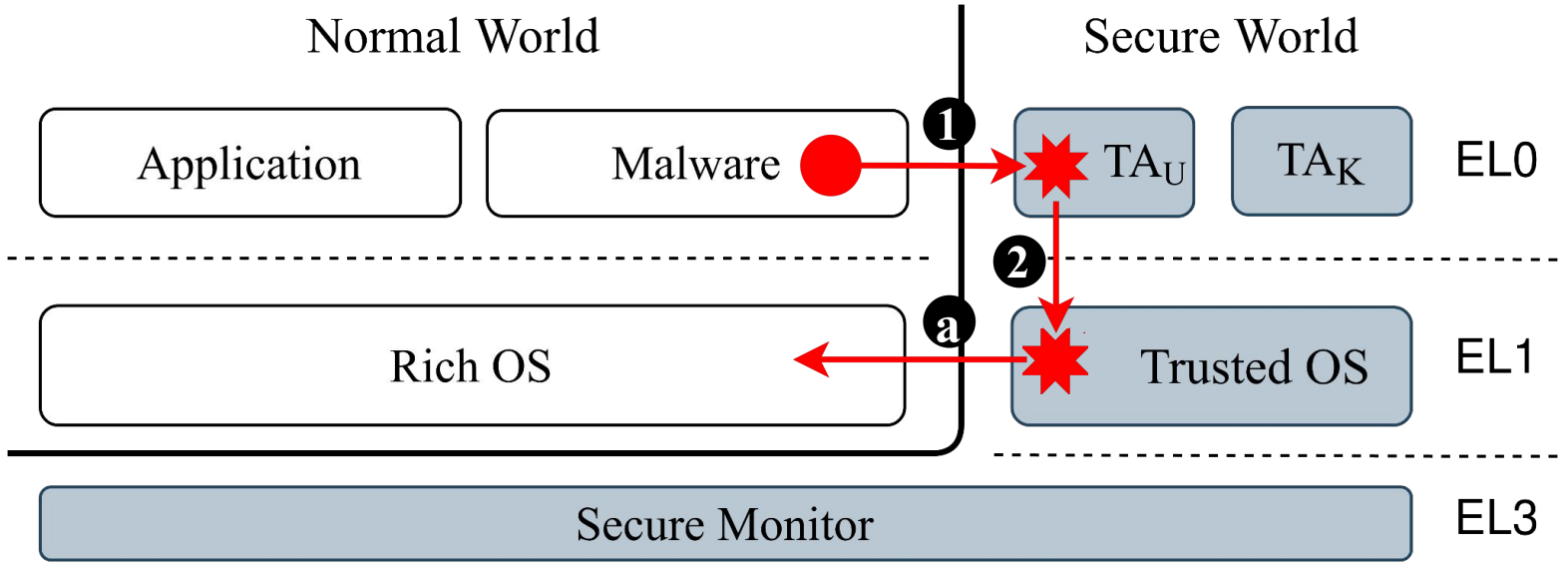
Trusted OS has unrestricted access to the full system



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**

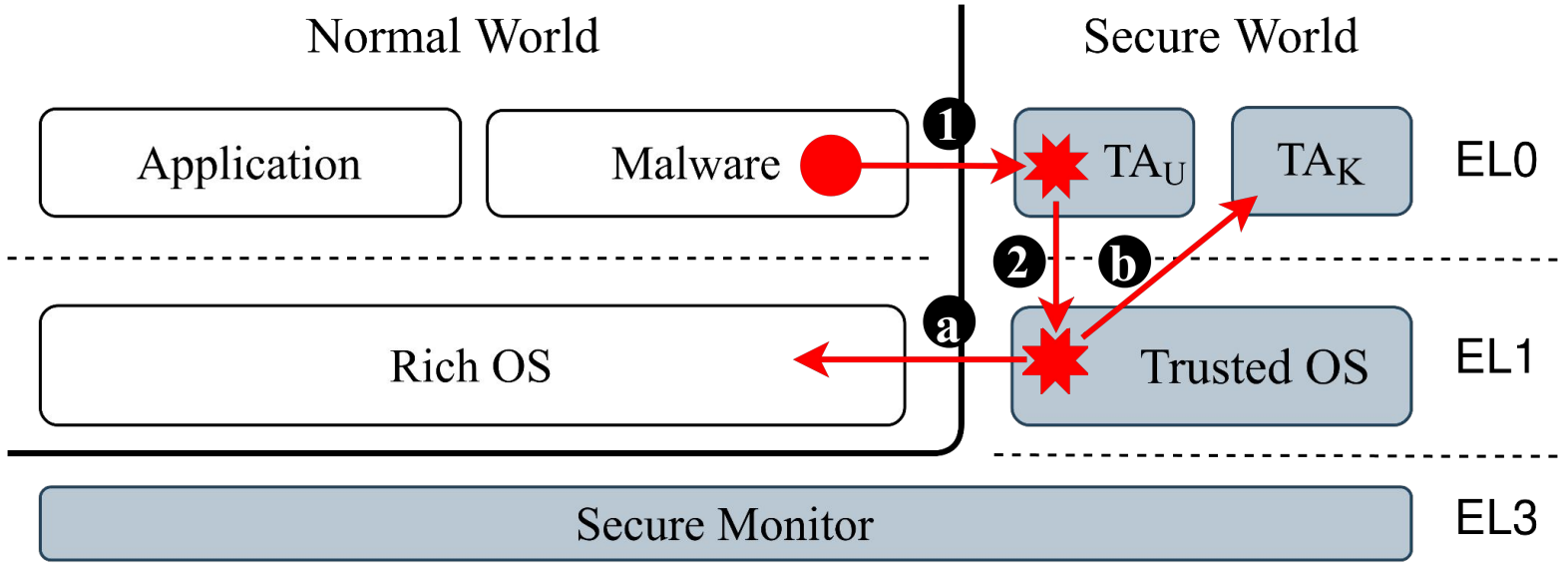


1. Hijack a user-level TA
2. Hijack the Trusted OS

A. Control the rich OS

Open Problem: Mitigate Privilege Escalation Attack in Trustzone TEE

Trusted OS has unrestricted access to the full system

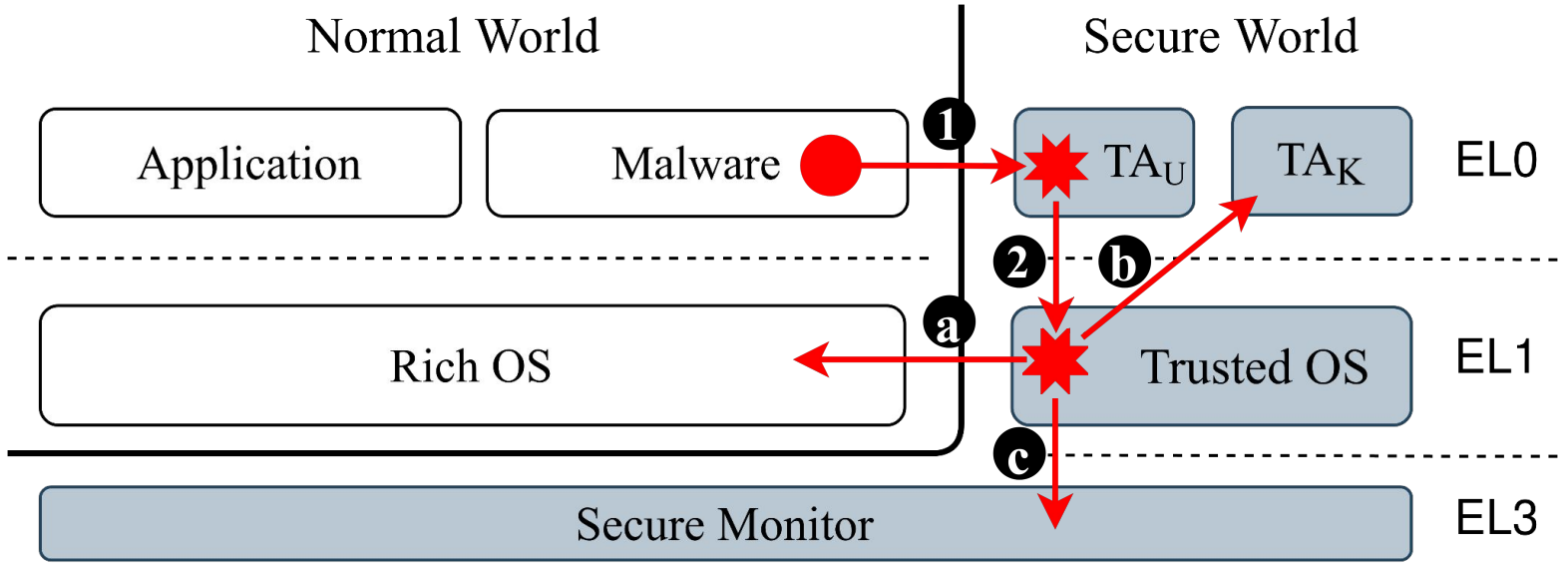


1. Hijack a user-level TA
2. Hijack the Trusted OS

A. Control the rich 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



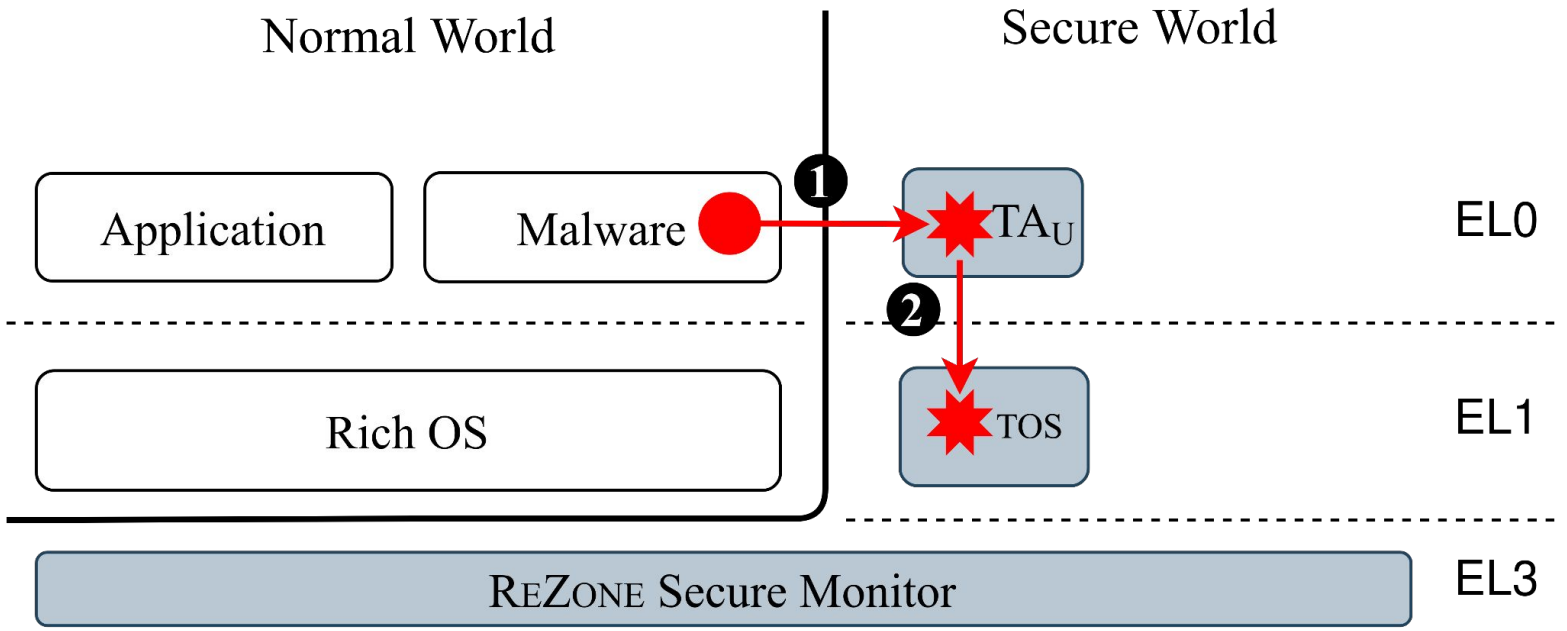
1. Hijack a user-level TA
2. Hijack the Trusted OS

A. Control the rich OS
B. Control a kernel-level TA
C. Control the secure Monitor

Solution: Deprivelege the TEE

Solution: Deprivelege the TEE

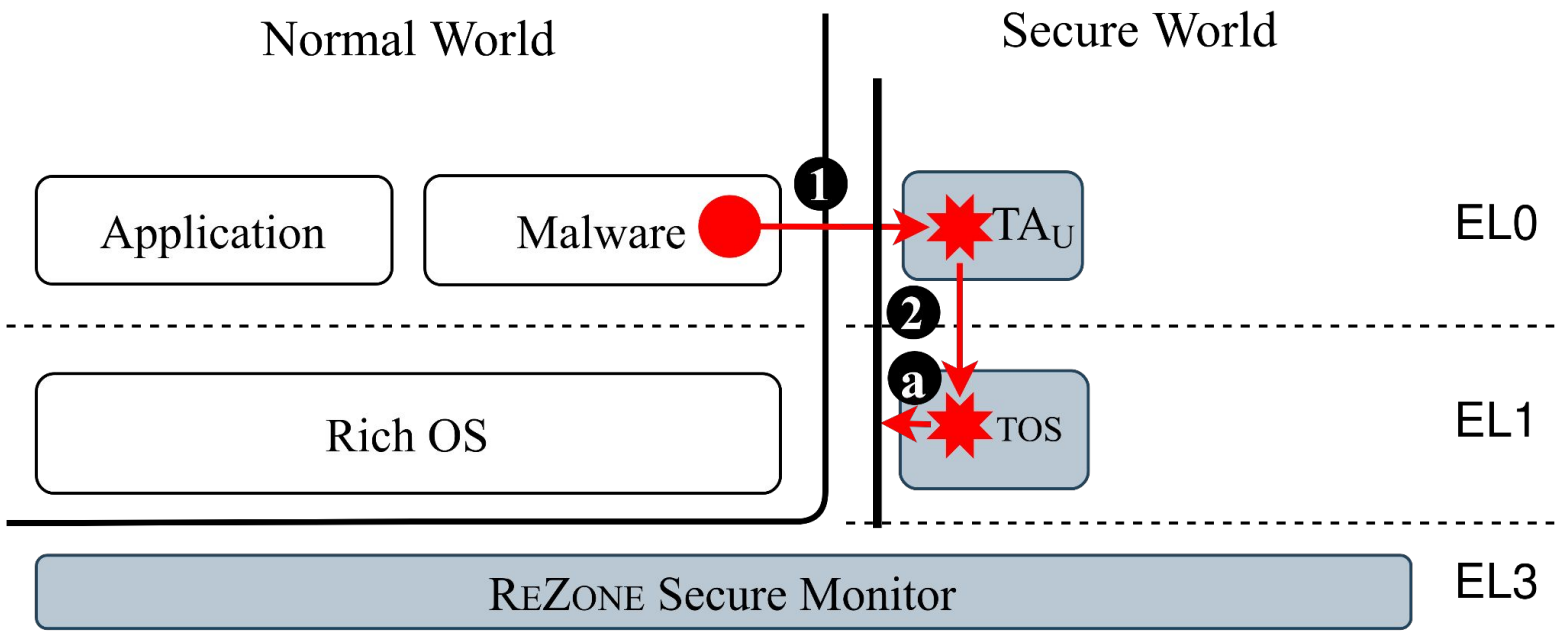
Deprivileging the TEE increases protection for:



Solution: Deprivelege the TEE

Deprivileging the TEE increases protection for:

a) Normal World REE

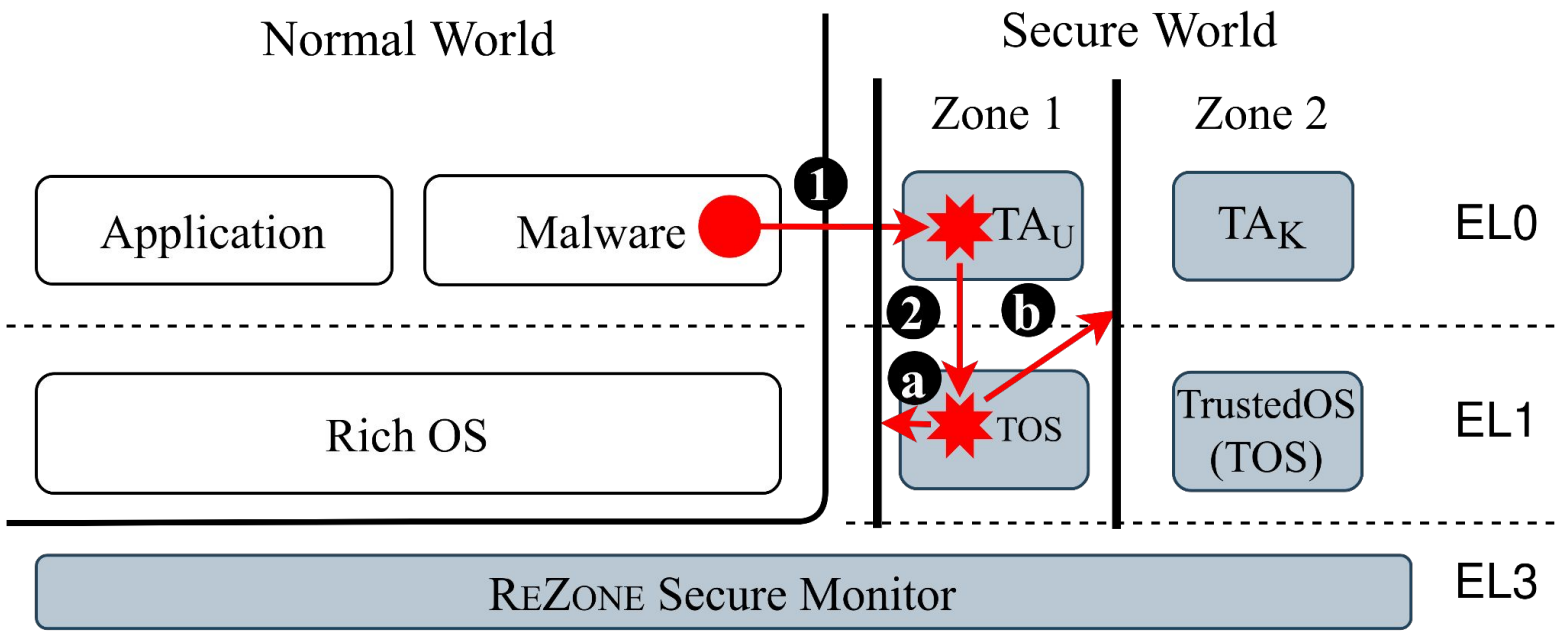


Solution: Deprivelege the TEE

Deprivileging the TEE increases protection for:

a) Normal World REE

b) Other TEEs / Zones



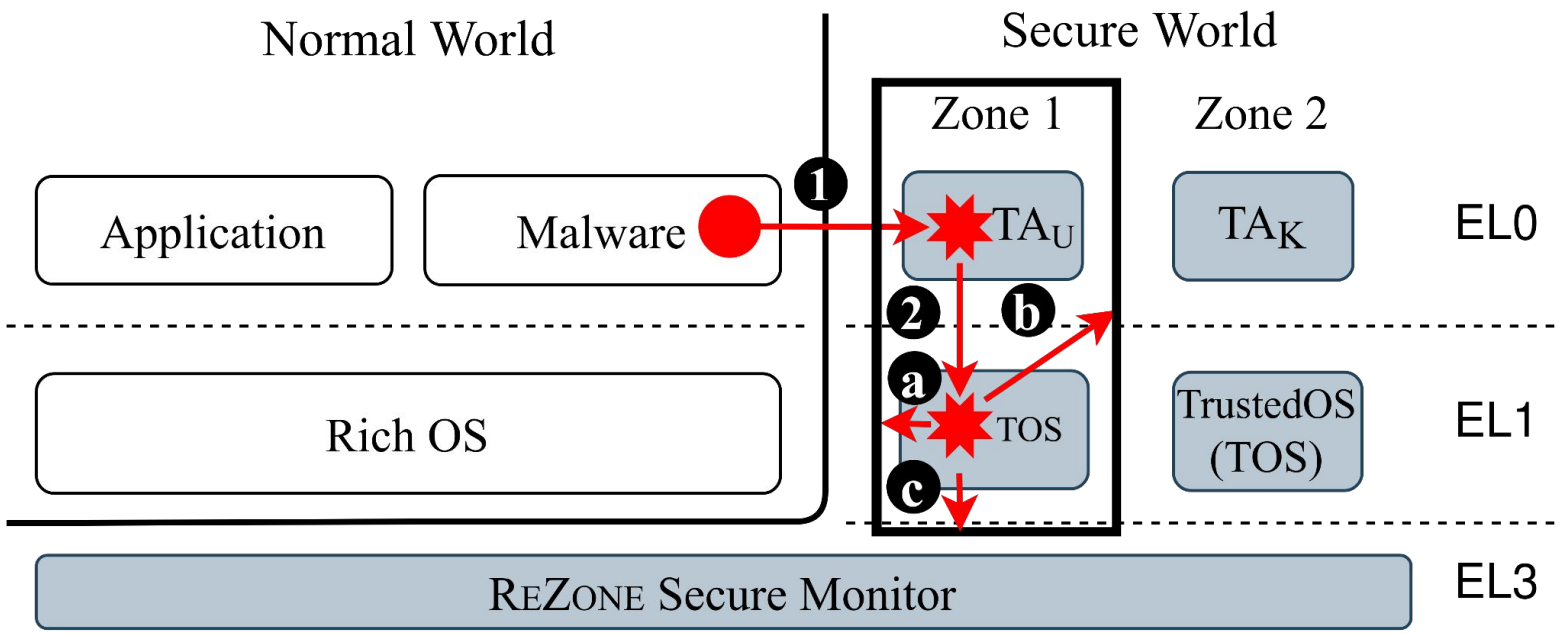
Solution: Deprivelege the TEE

Deprivileging the TEE increases protection for:

a) Normal World REE

b) Other TEEs / Zones

c) Secure Monitor



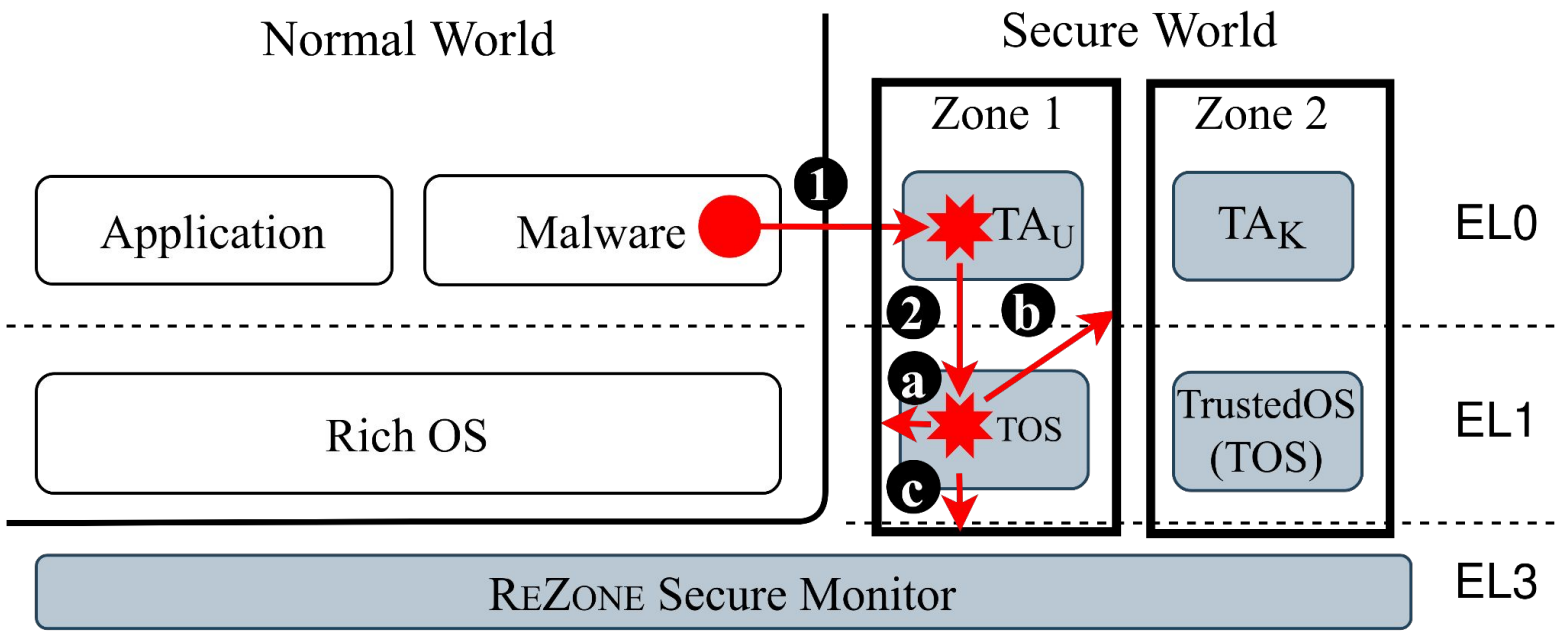
Solution: Deprivelege the TEE

Deprivileging 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 **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

We Propose ReZone

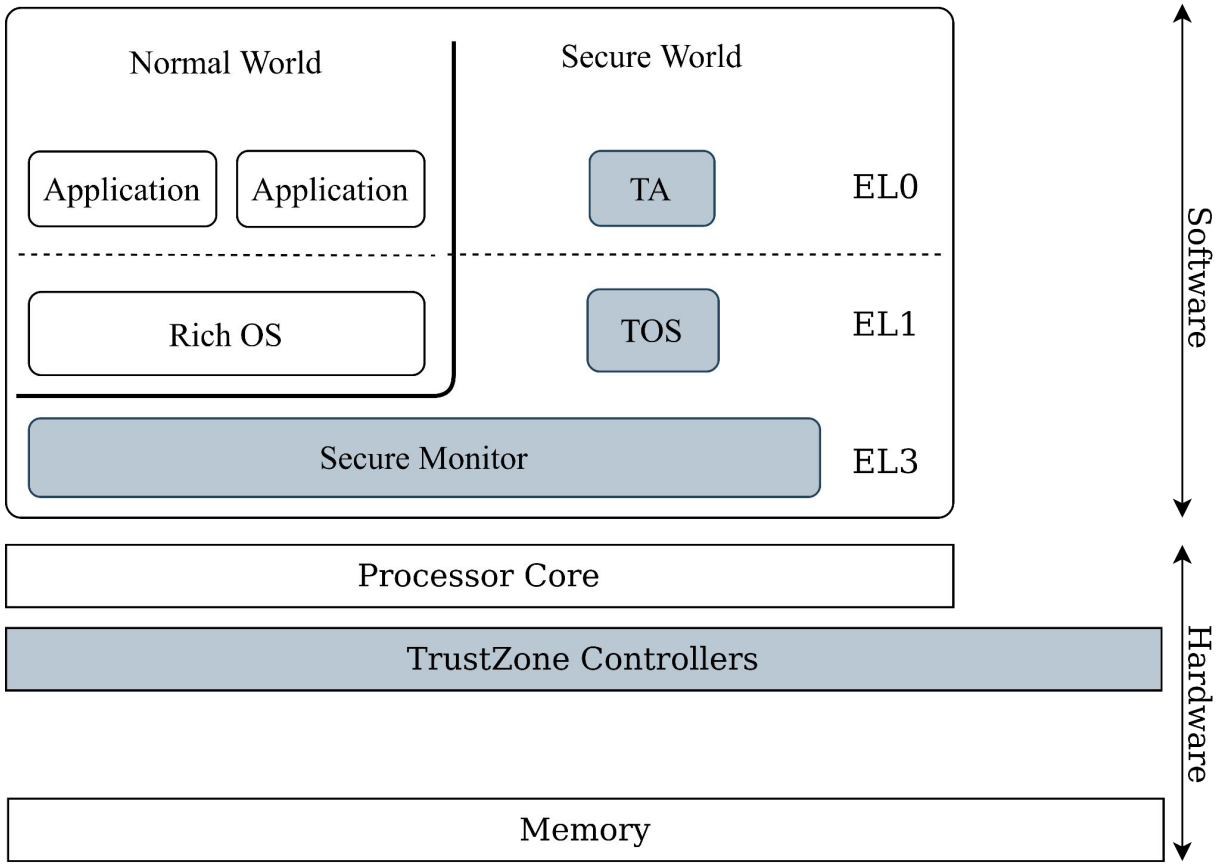
- An approach to **deprivilege** the Trusted OS
  - Use TrustZone orthogonal hardware features present in COTS platforms
- Implementation in a **real-world platform** and **software**
  - Evaluate ReZone in Embedded Linux and Android software stacks
- Performance penalty does **not degrade UX**
  - Evaluate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

We Propose ReZone

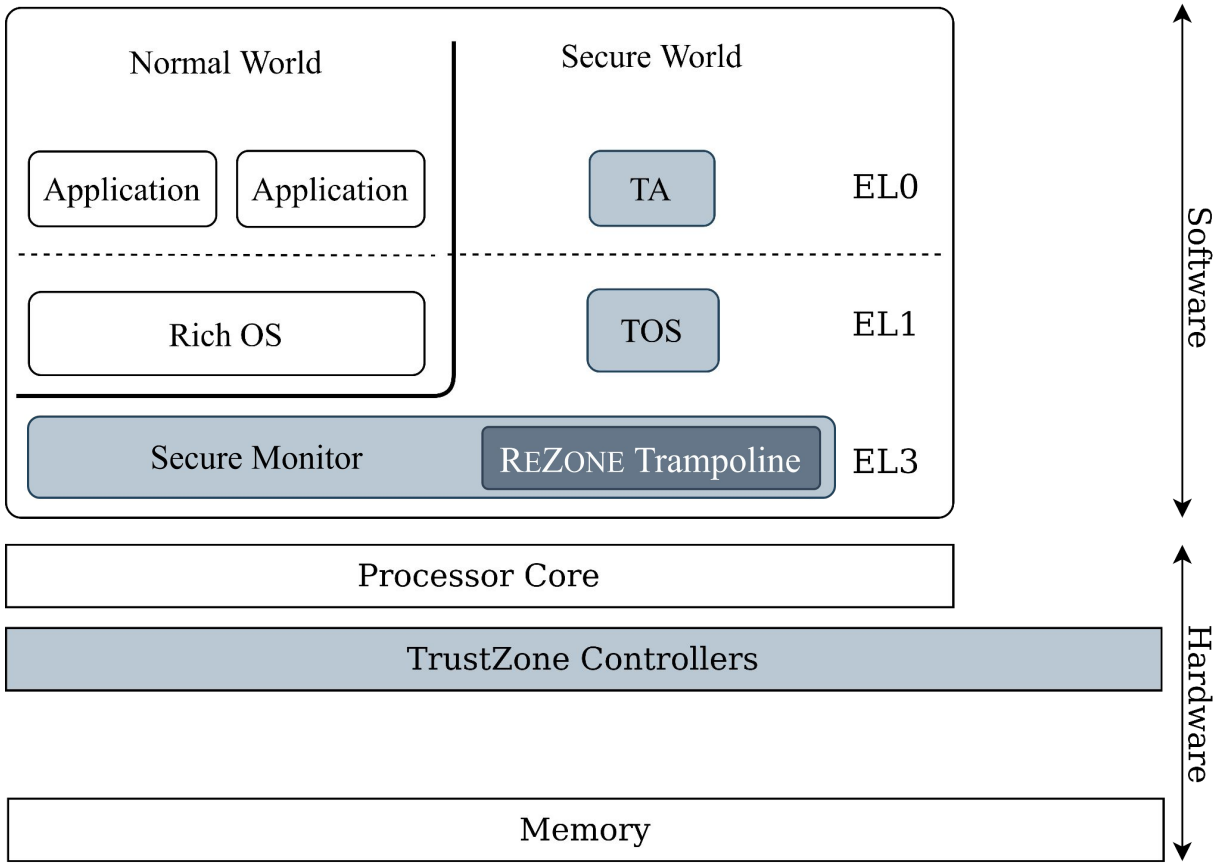
- An approach to **deprivilege** the Trusted OS
  - Use TrustZone orthogonal hardware features present in COTS platforms
- Implementation in a **real-world platform** and **software**
  - Evaluate ReZone in Embedded Linux and Android software stacks
- Performance penalty does **not degrade UX**
  - Evaluate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

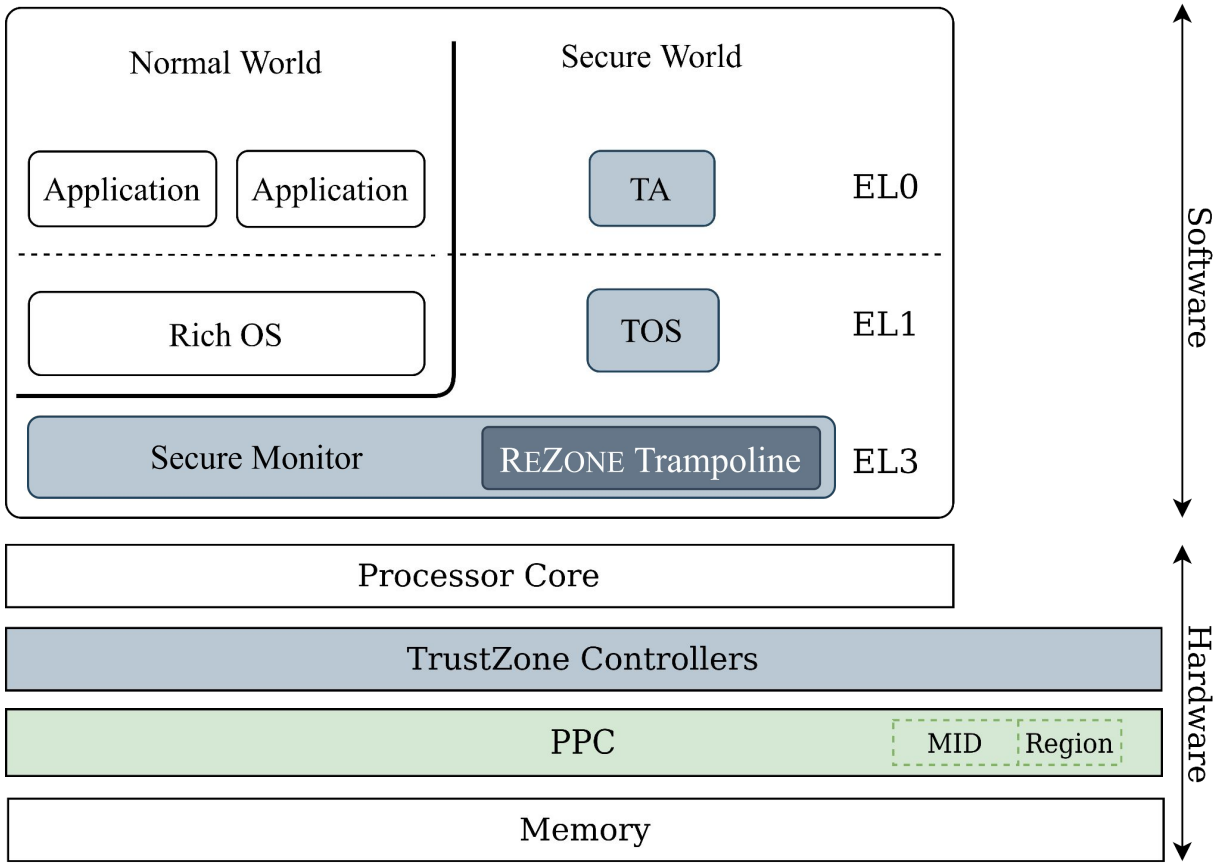
ReZone Design



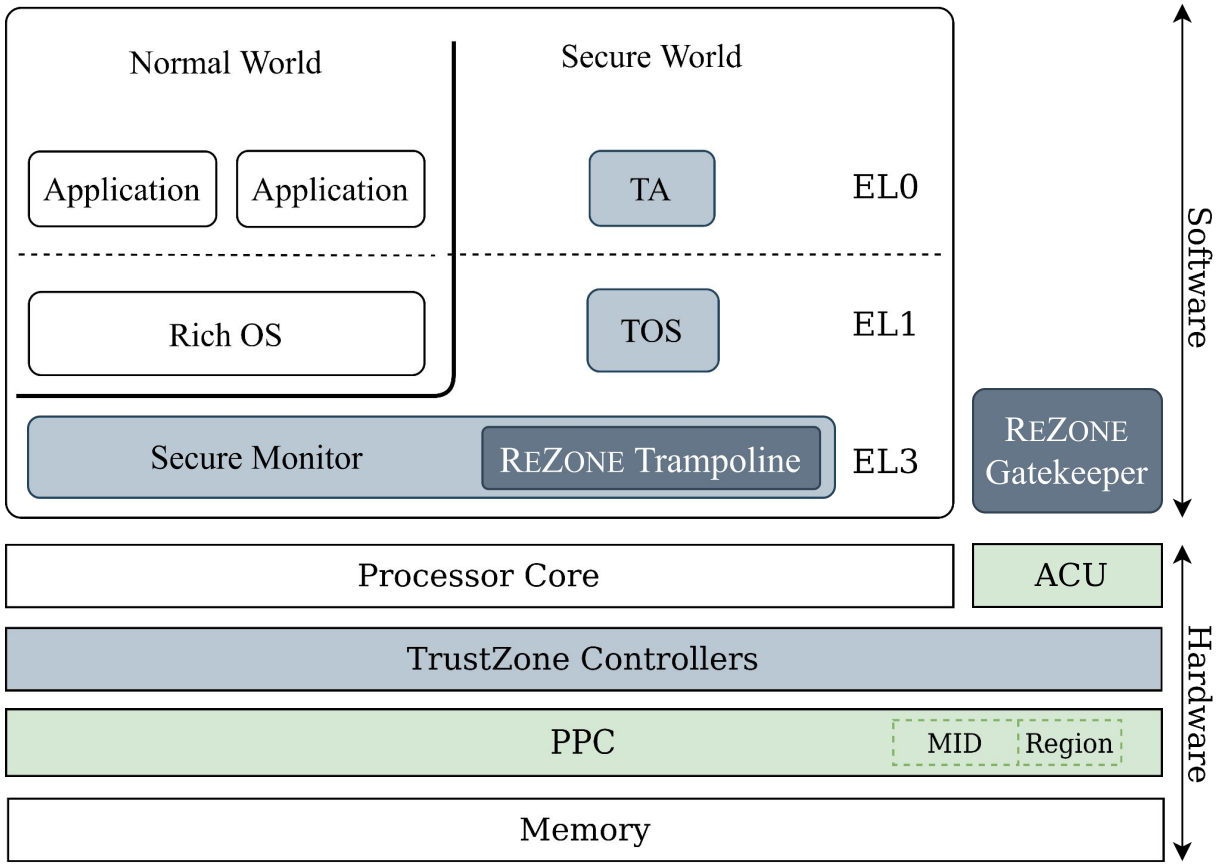
ReZone Design



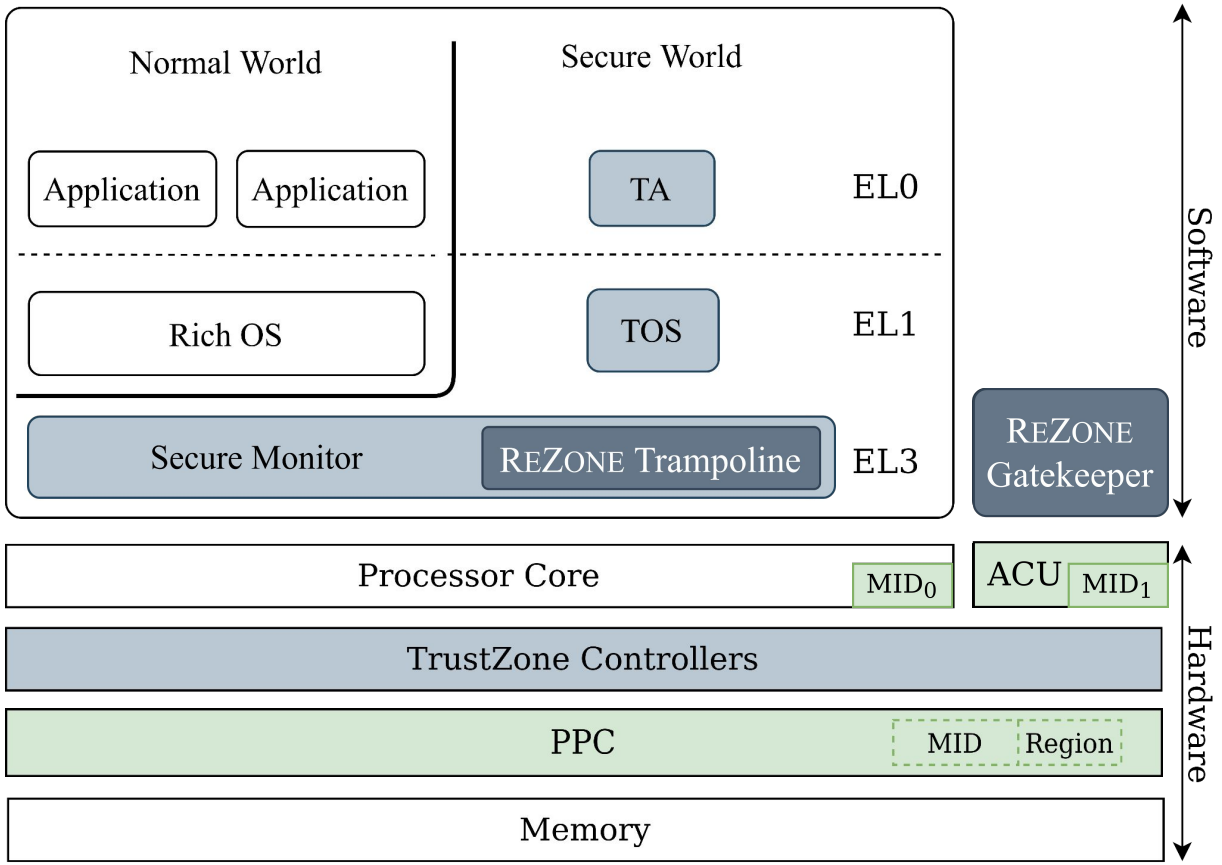
ReZone Design



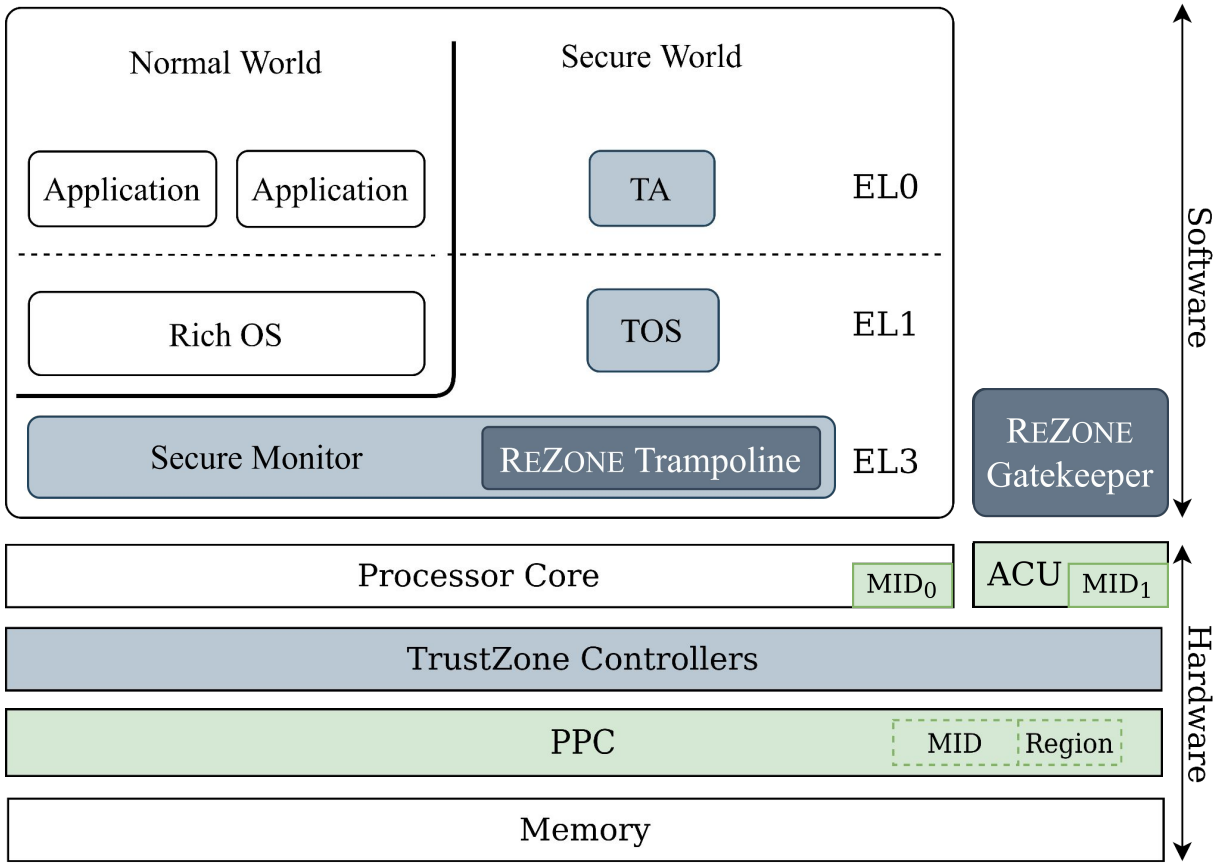
ReZone Design



ReZone Design

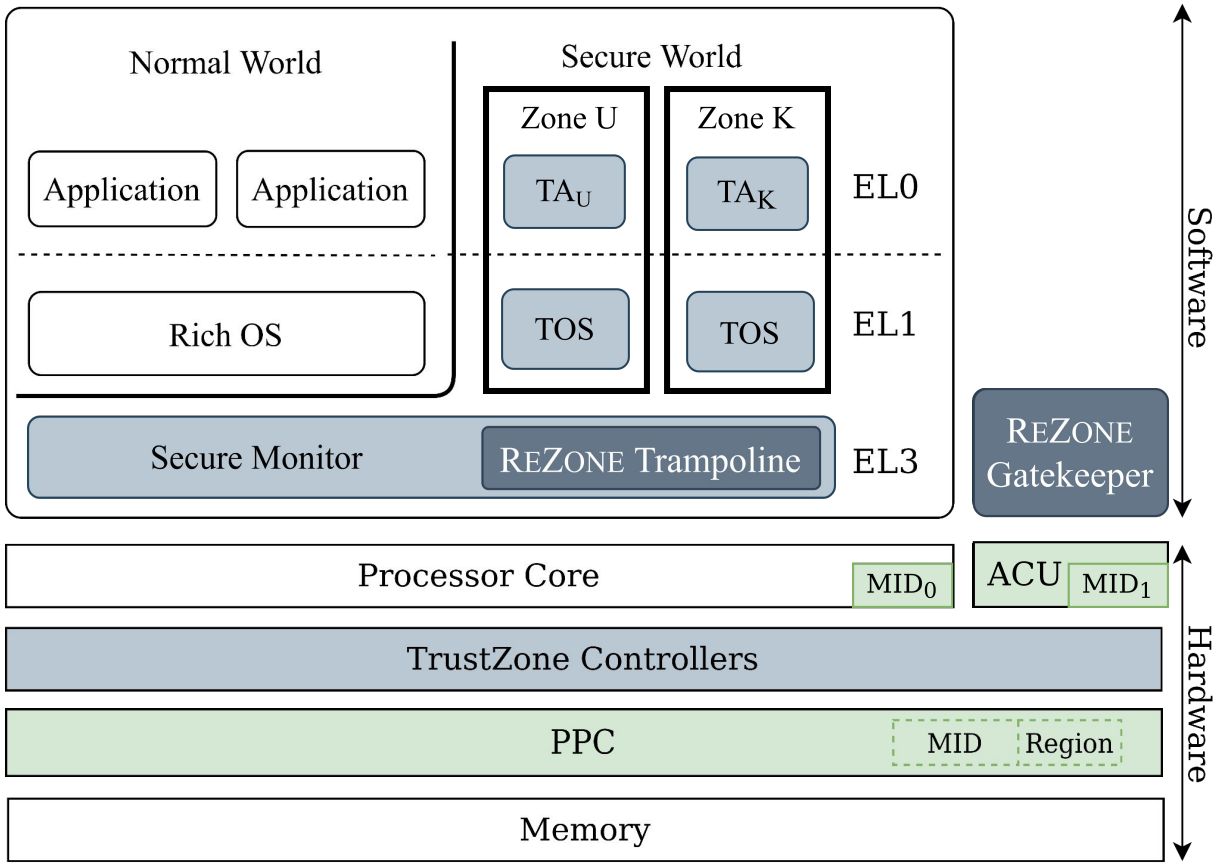


ReZone Design



By leveraging the **PPC and ACU** we can deprivilege the Trusted OS.

ReZone Design

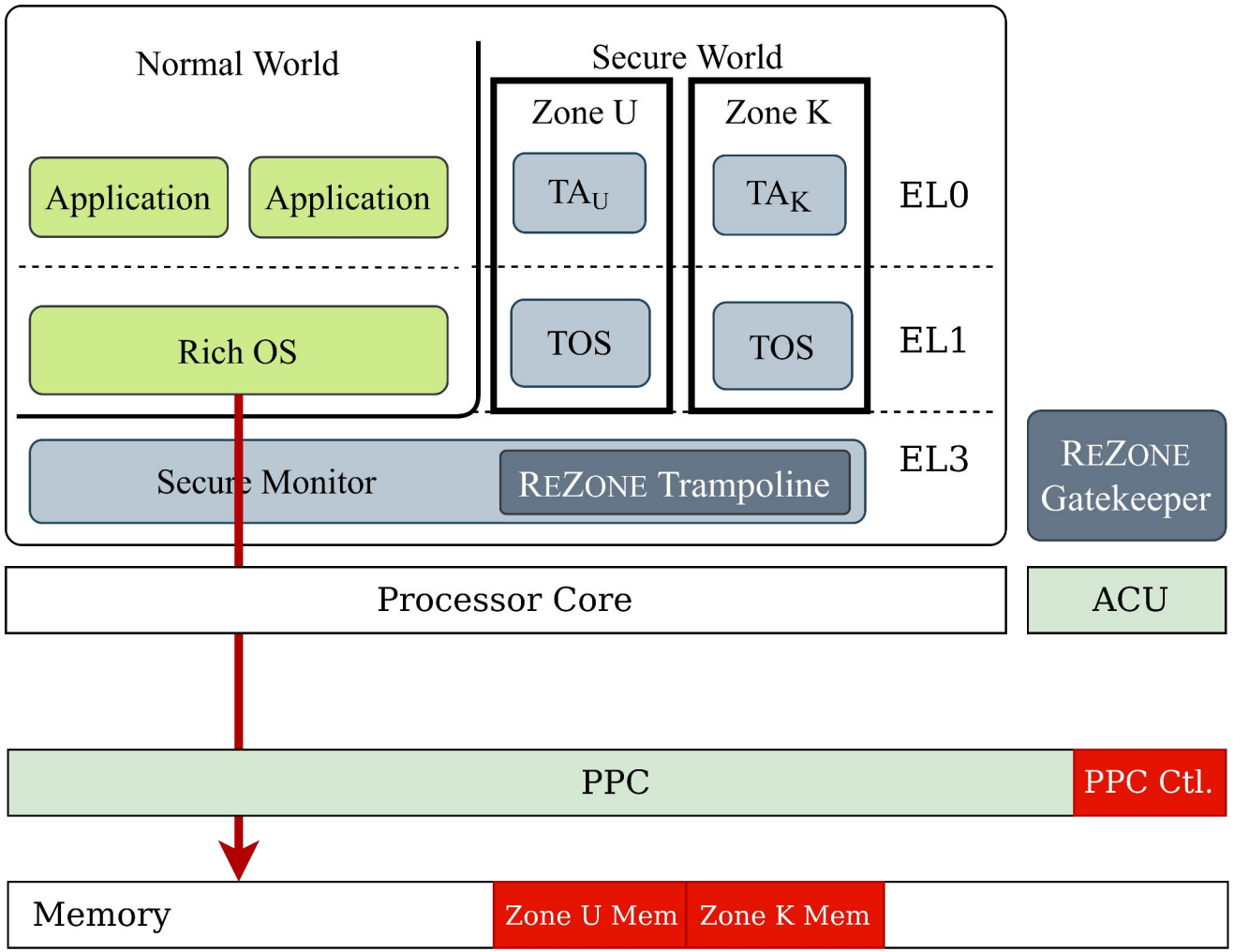


By leveraging the **PPC and ACU** we can deprivilege the Trusted OS.

Rezone Use of PPC + ACU

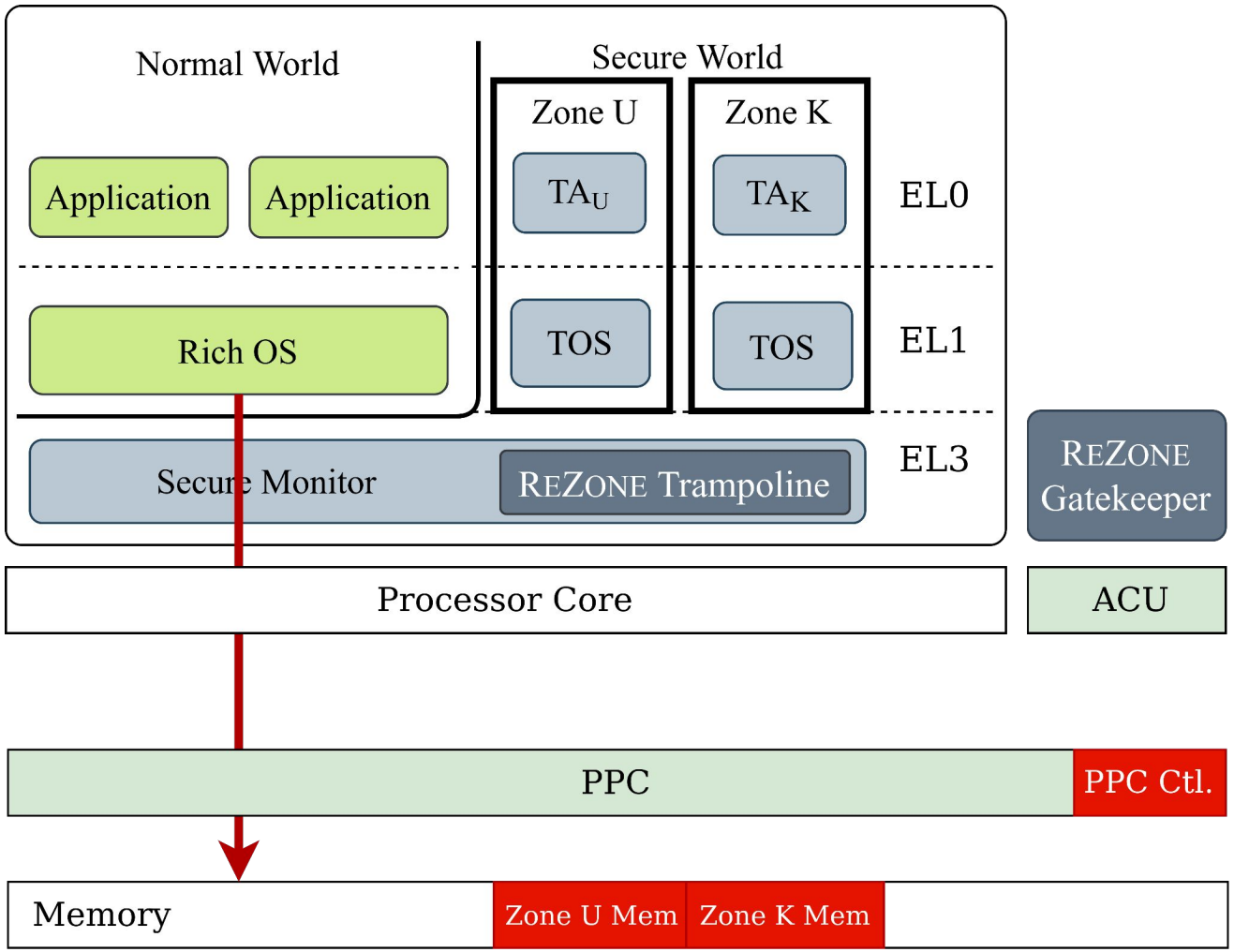
ReZone Use of PPC + ACU

- Starting from normal world execution



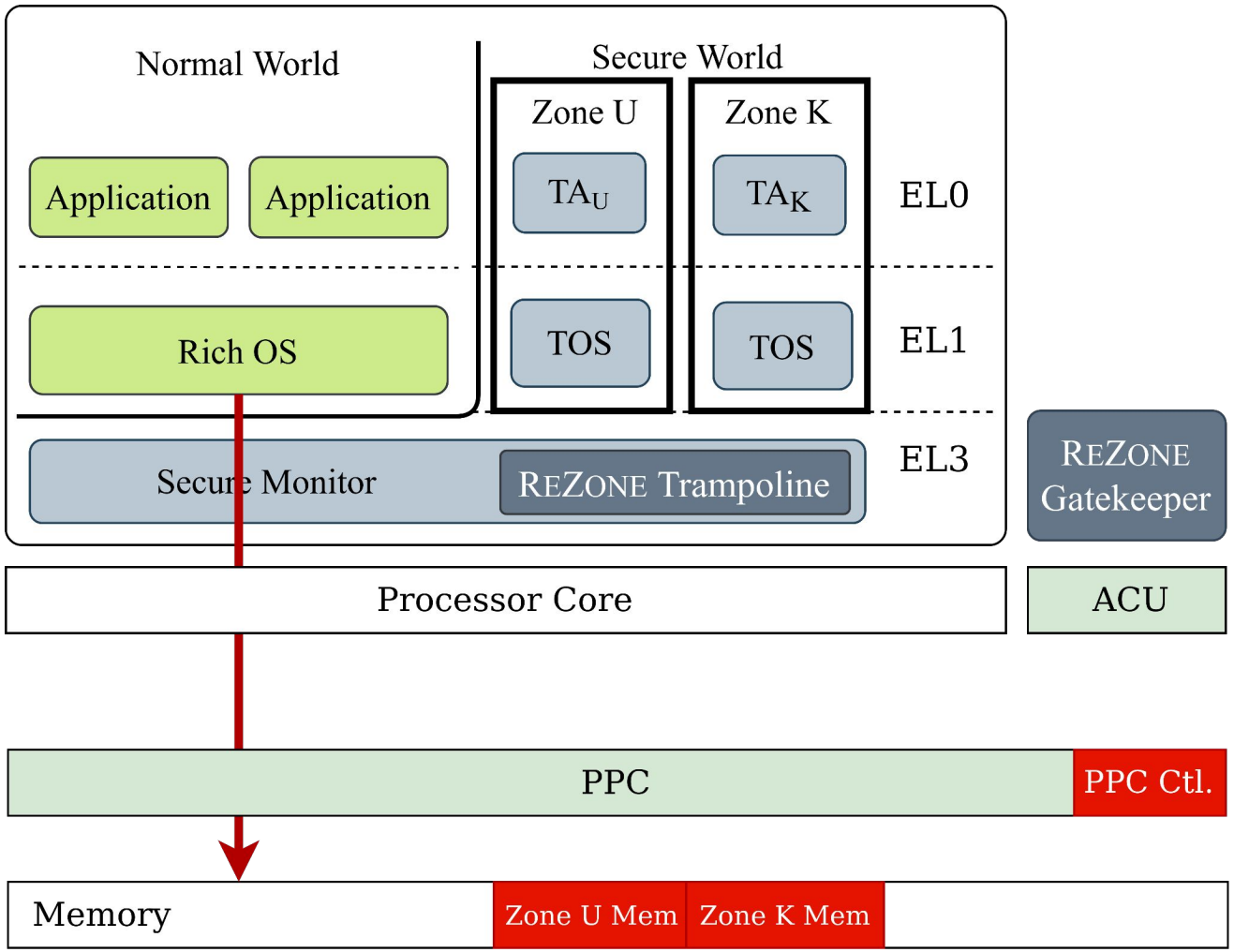
ReZone Use of PPC + ACU

- Starting from normal world execution
- Normal world can access the normal memory



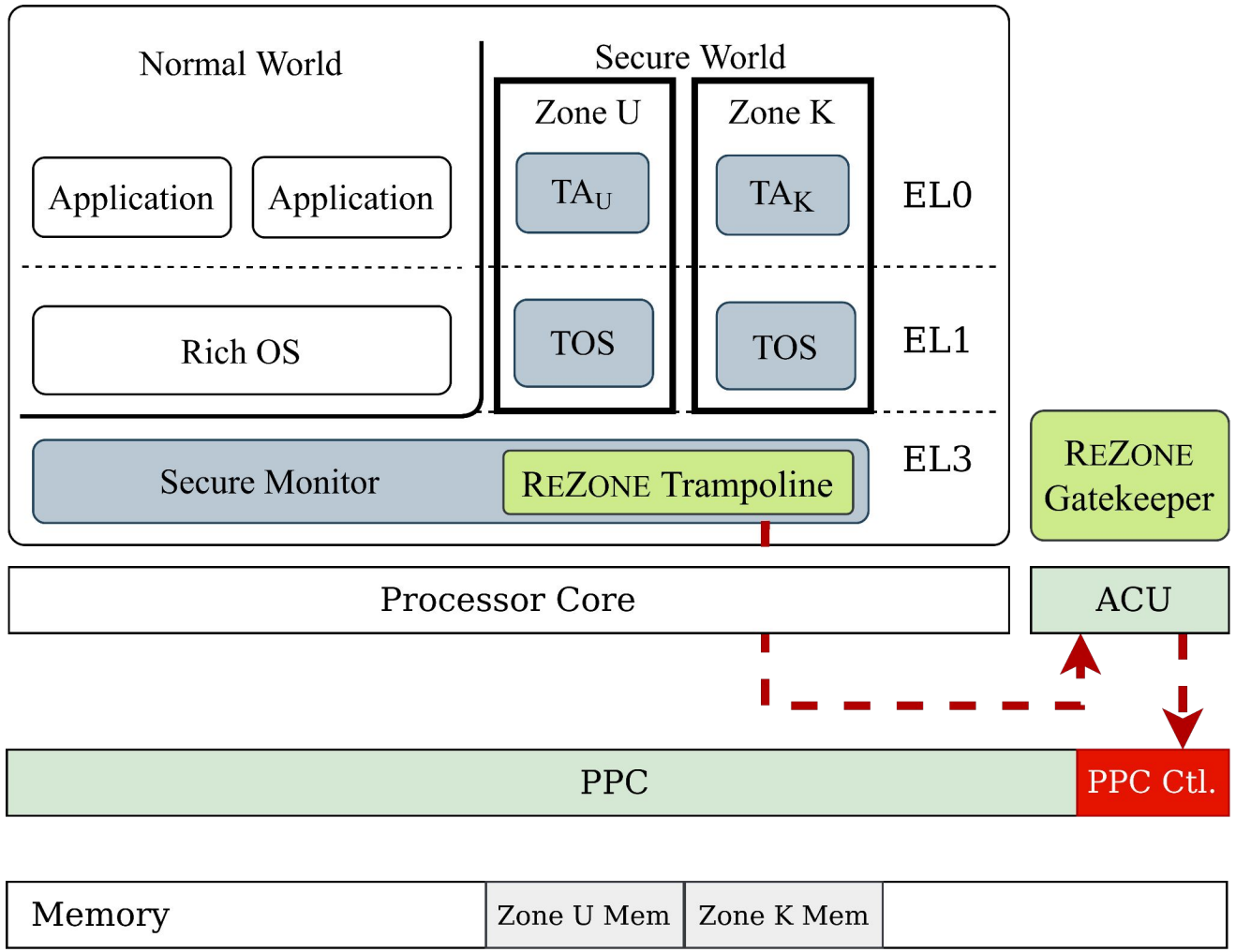
ReZone Use of PPC + ACU

- Starting from normal world execution
- Normal world can access the normal memory
- TrustZone prevents accesses to secure world



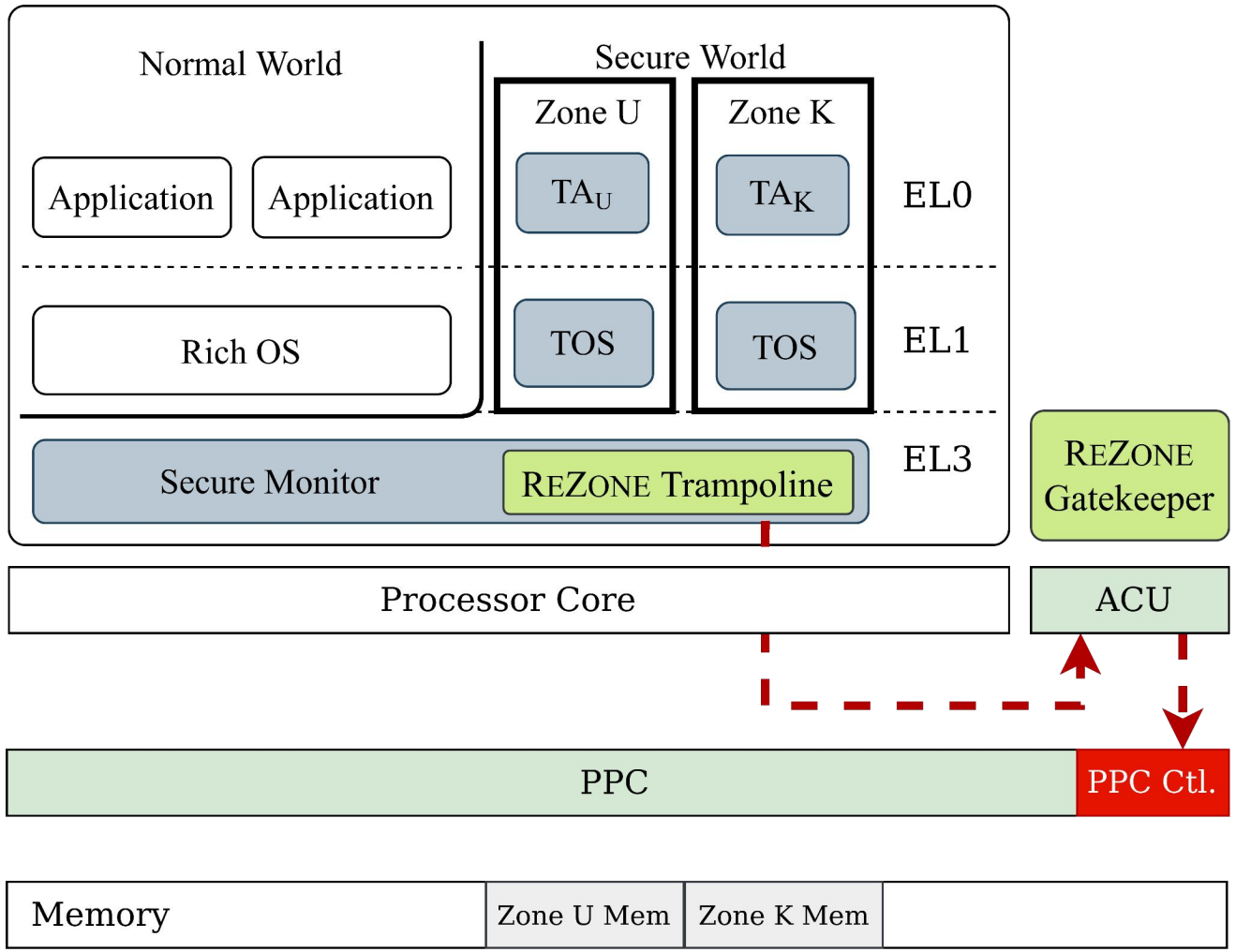
ReZone Use of PPC + ACU

- Trampoline interacts with the Gatekeeper to reconfigure the PPC



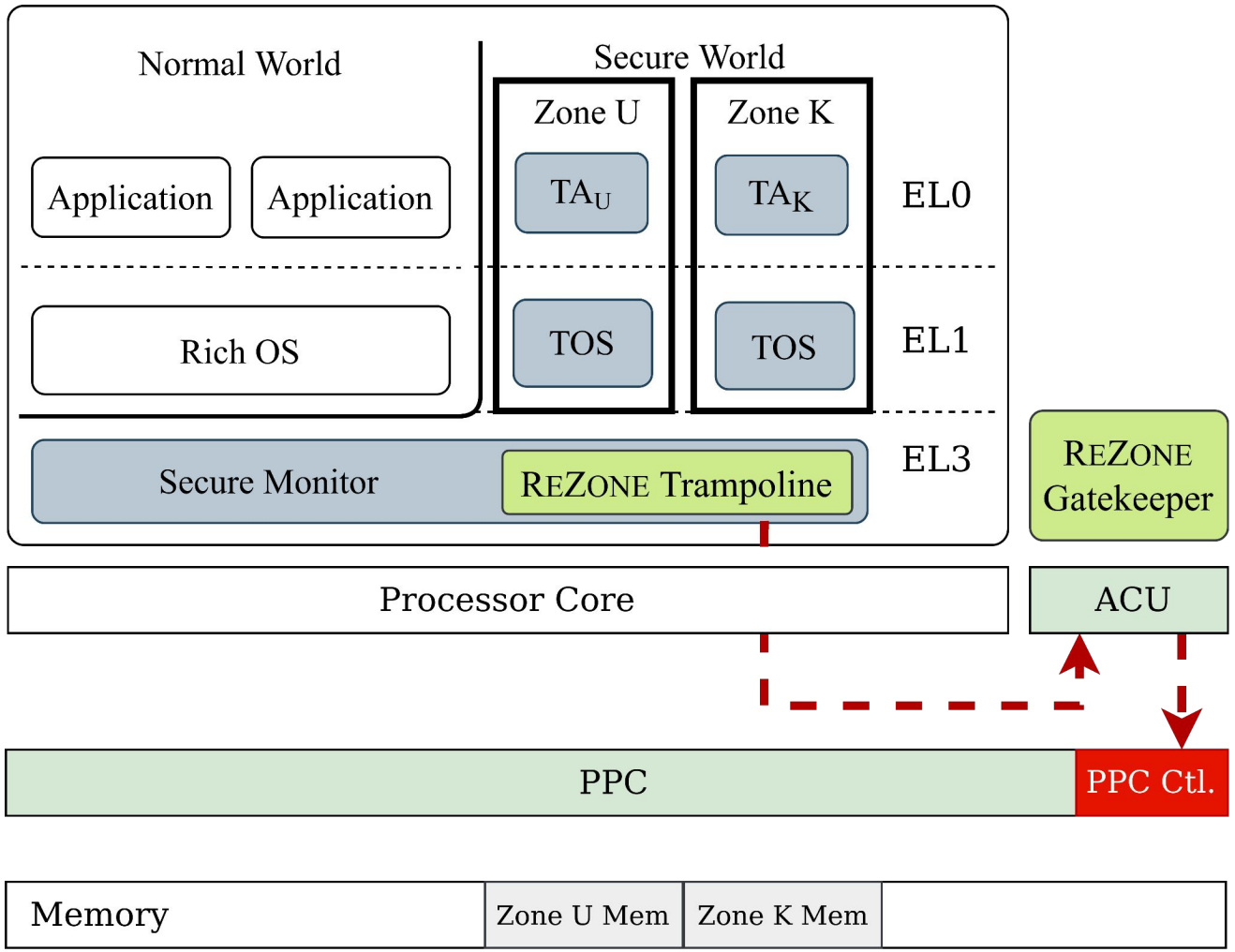
ReZone Use of PPC + ACU

- 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



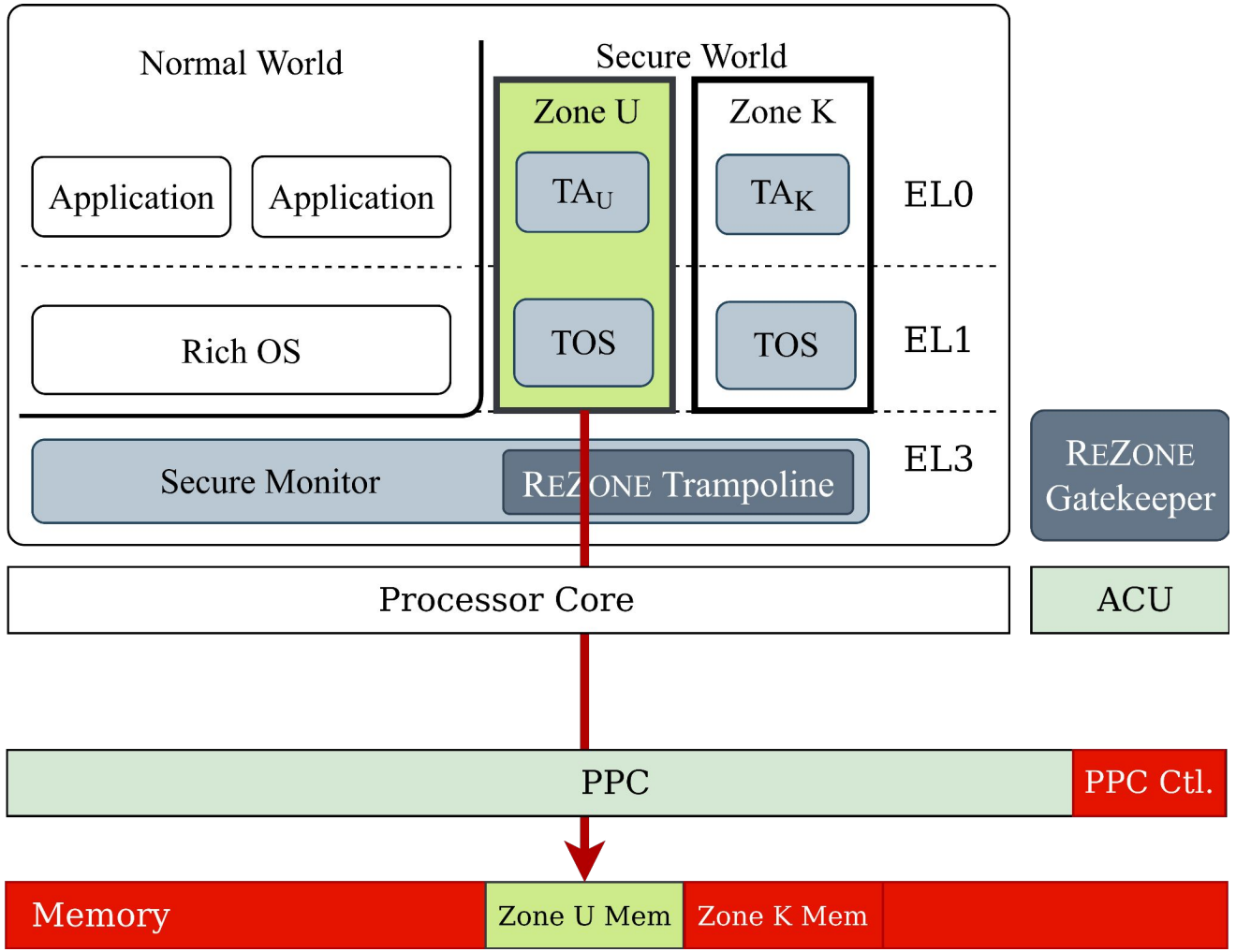
ReZone Use of PPC + ACU

- 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



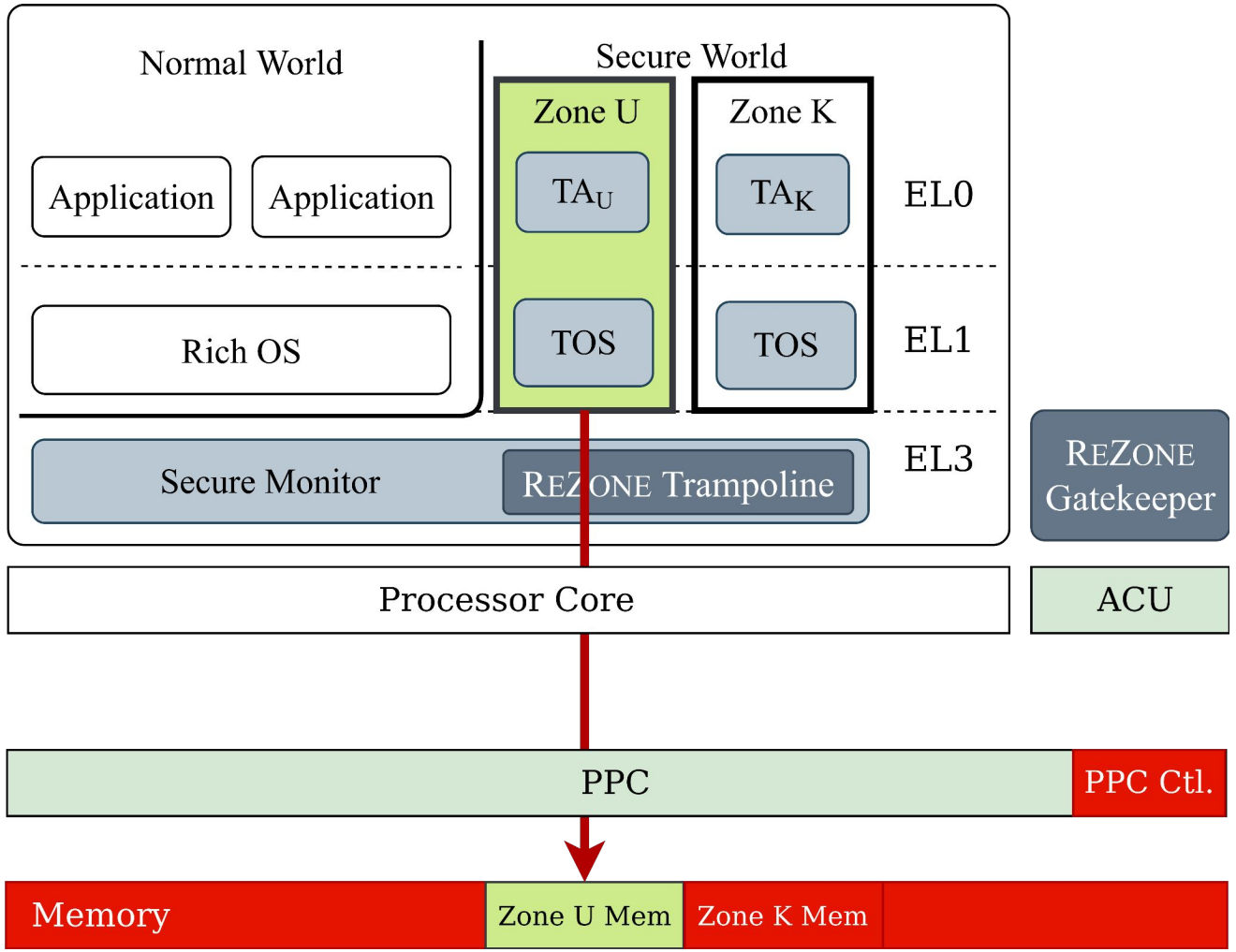
ReZone Use of PPC + ACU

- The Zone will execute



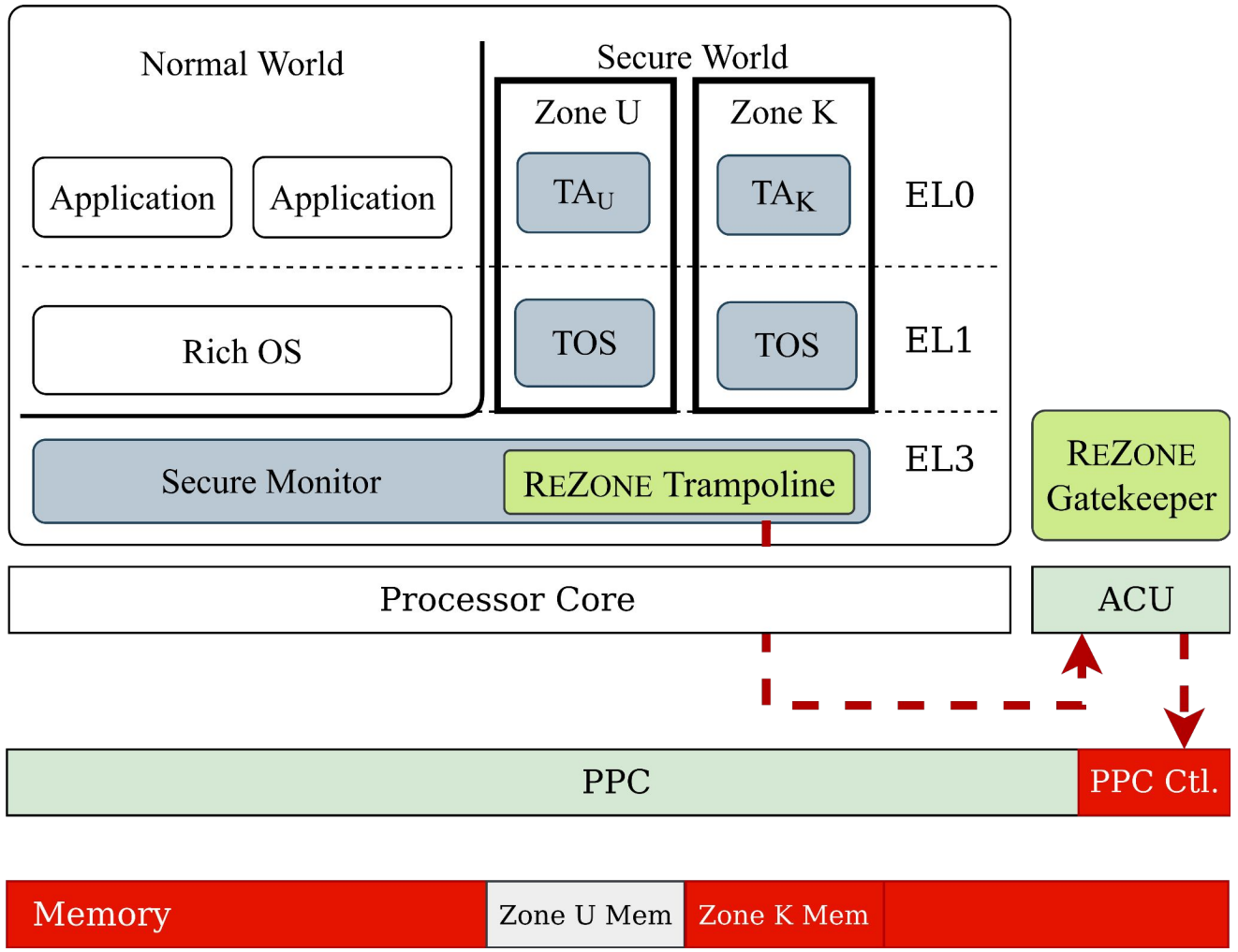
ReZone Use of PPC + ACU

- The Zone will execute
- PPC will only allow access to the zone memory



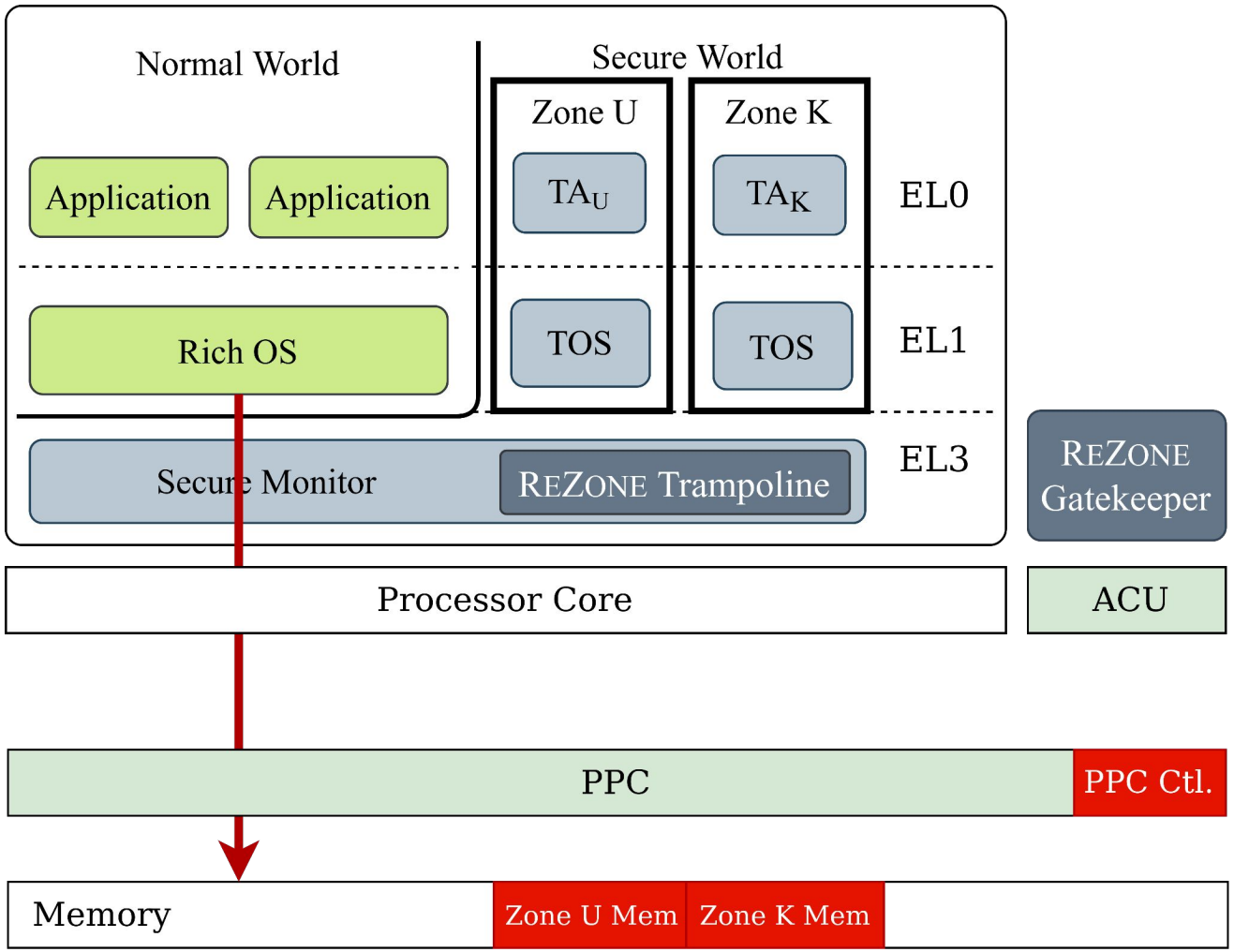
ReZone Use of PPC + ACU

- 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

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

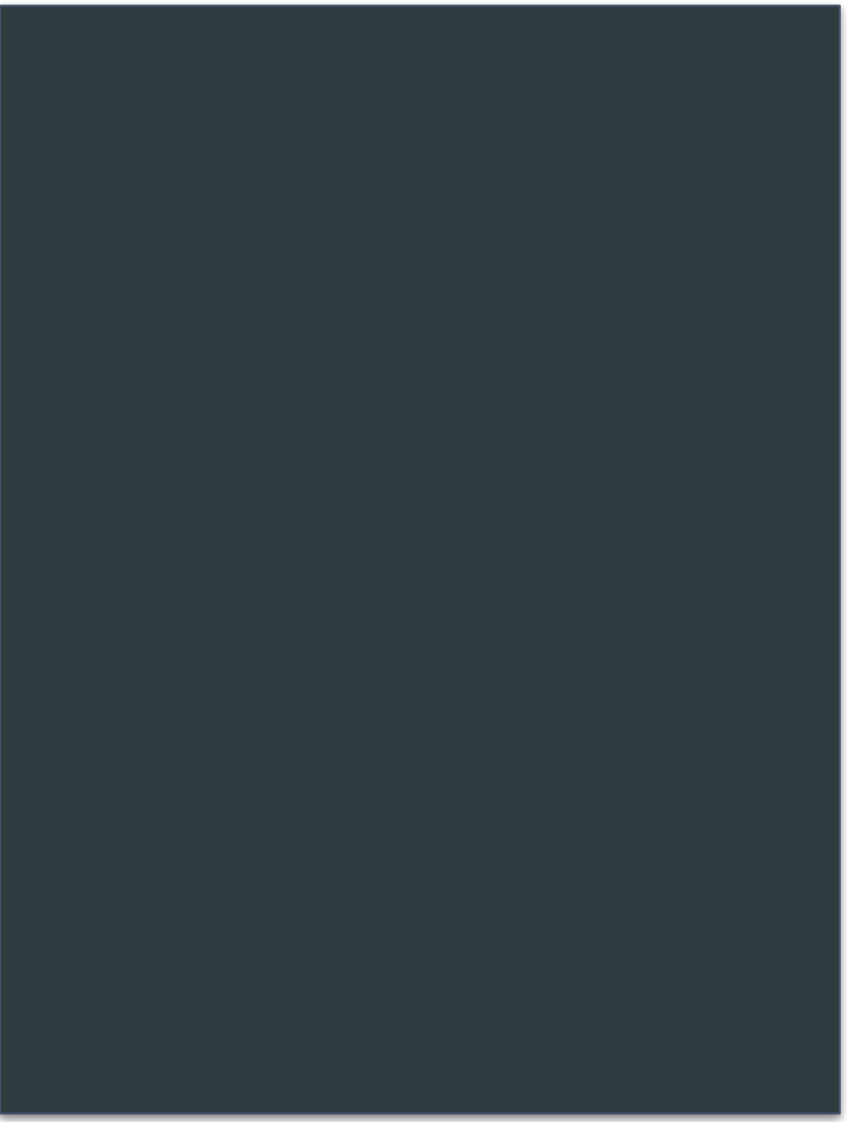
- Micro-Benchmarks
  - Evaluate overheads of **REE-TA interaction**
- Performance of Real-World Use Cases
  - **Two TAs** that implement real workloads

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

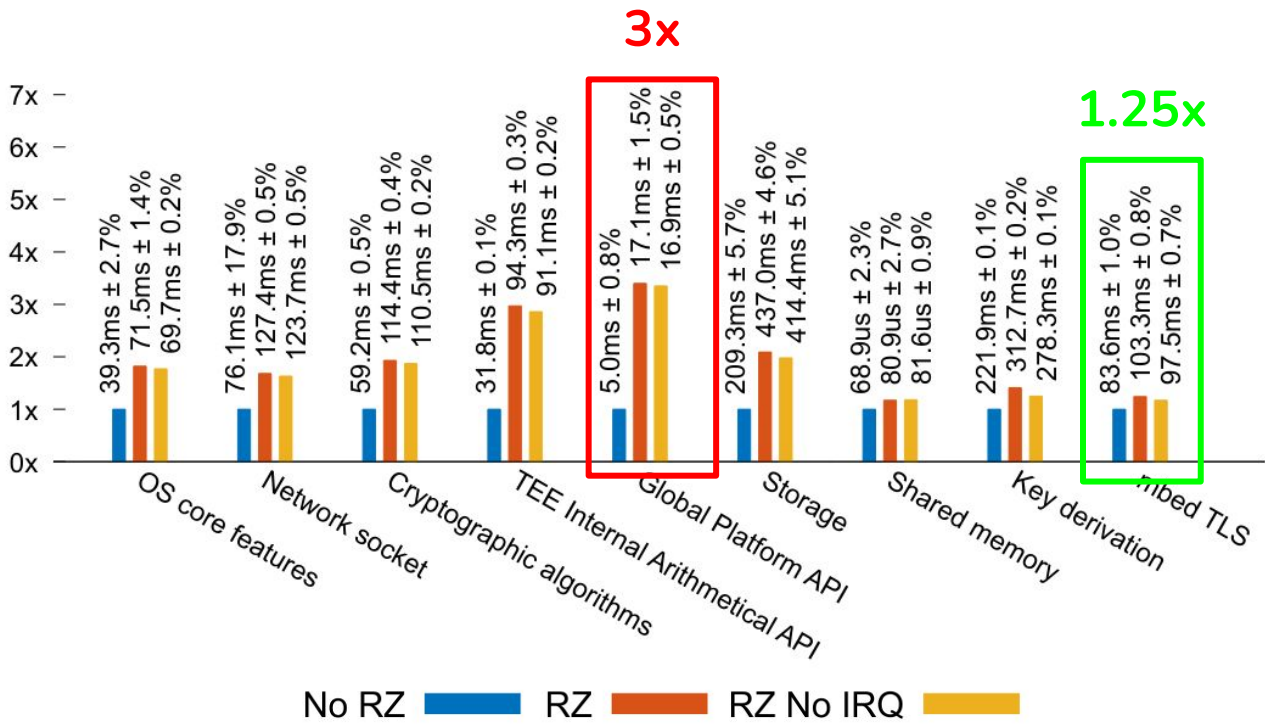
Performance Evaluation

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

Performance Evaluation

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

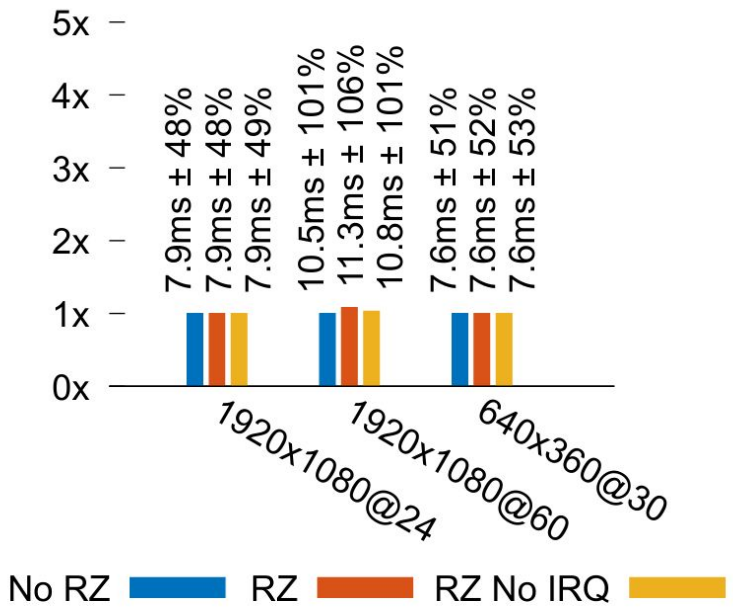
- Simple workloads with many world switches → higher overheads



Performance Evaluation

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

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



Performance Evaluation

Performance Evaluation

- Normal World Impact
  - PCMark 3.0 for Android

Performance Evaluation

- Normal World Impact
  - PCMark 3.0 for Android

- Single-Core interrupt

Interval (ms)	Score	Penalty
10	4369	12.97%
100	4776	4.86%
1000	4983	0.74%

Performance Evaluation

- **Normal World Impact**
  - **PCMark 3.0 for Android**

- Single-Core interrupt

Interval (ms)	Score	Penalty
10	4369	12.97%
100	4776	4.86%
1000	4983	0.74%

- Multi-Core interrupt (1s interval)

# of Cores	Score	Penalty
1	4983	0.74%
2	4938	1.63%
4	4833	3.73%

CVE Mitigation

CVE Mitigation

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

CVE Mitigation

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

CVE Mitigation

- Assuming multiple Zones with one TA per zone

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

CVE Mitigation

- Assuming multiple Zones with one TA per zone
- Mitigates ~87% CVEs:
  - Most TOS and TA vulnerabilities

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

In Scope?	TO/TA	TO	TA	HW	CI	BL	Total	Percentage
Y	21	34	11				66	86.84%

CVE Mitigation

- 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

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

In Scope?	TO/TA	TO	TA	HW	CI	BL	Total	Percentage
Y	21	34	11				66	86.84%
N		2	1	1	4	2	10	13.16%
Total	21	36	12	1	4	2	76	

Availability of PPC/ACU primitives on COTS platforms

Vendor	SoC Platform	PPC	ACU	RZ?
NXP	**iMX8MQ** iMX8QM	**RDC** xRDC	**Cortex-M4** SCU	**YES** **YES**
Xilinx	Ultrascale+ MPSoC Versal ACAP	XMPU, XPPU, (SMMU)	PMU	**YES** **YES**
Nvidia	Tegra X1/X2 Xavier	SMMU	BPMP	**YES** **YES**
Socionext	SC2A11	SMMU	SCP	**YES**
Qualcomm	Snapdragon 845, 855, 865, 888, 8gen1	SMMU, XPU*	SPU	**YES**
Broadcom	Stingray	SMMU	SCP	**YES**
Samsung	Exynos 990 Exynos 2100	Periph. MMUs Periph. MMUs	iSE eSE	**N/A** **N/A**
Mediatek	Dimensity 1200	x	x	**No**
HiSilicon	Kirin 9000	x	PMU	**No**

In Summary

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

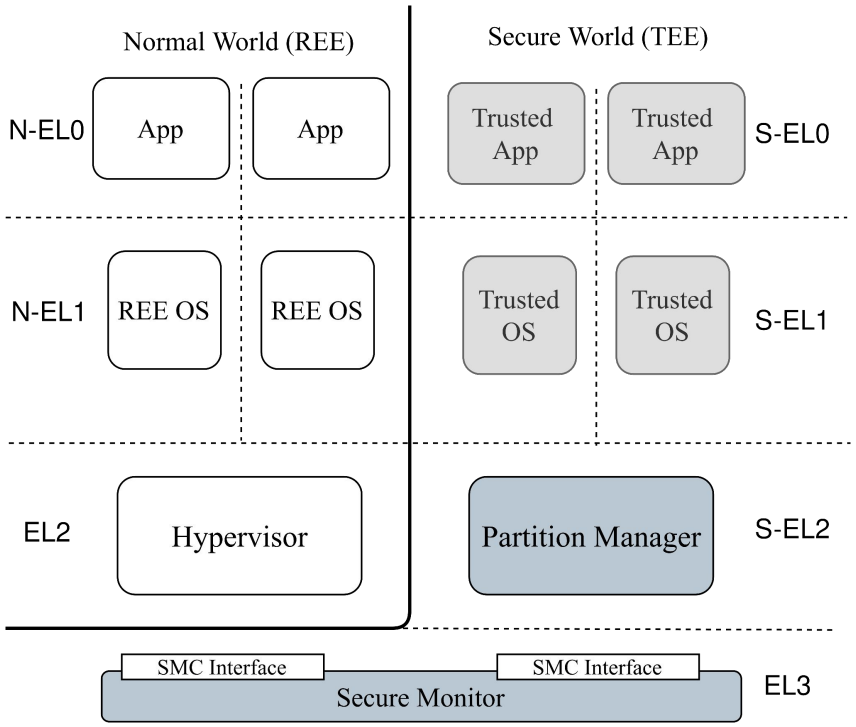
- **TrustZone TEEs** have architectural **flaws**
- **ReZone** is a novel security architecture that **reduces TEE privileges**
- **ReZone** leverages **TrustZone-agnostic** hardware primitives
- **ReZone** was **implemented** and **evaluated** in a real-world **platform**
- **Performance** of real-world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



Armv9 CCA