TEEs and Enclaves

Digital System Integration and Programming
WS 2021/22

Michael Ehrenreich

2021-11-17

Contents

Background

- Runs separate OS/Kernel
- Not dependent on untrusted software
- Implements e.g. GlobalPlatform TEE API
- More functionality than SE
- Implementations:
  - Android: Trusty, QTEE, ...
  - Desktop: Intel CSME, AMD PSP, ...
  - OPTEE
  - iOS Secure Enclave
  - ...

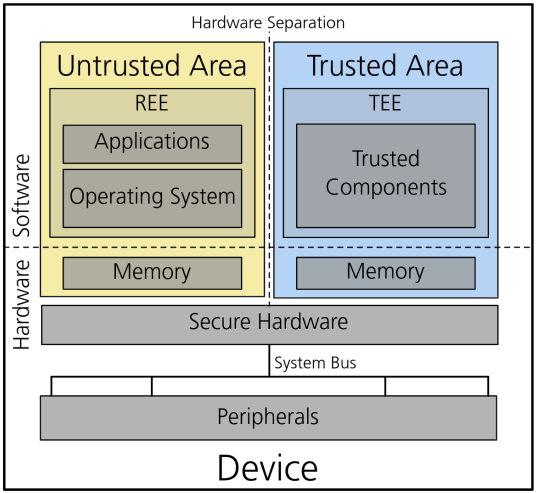
Hardware Separation
Untrusted Area
Trusted Area
REE
TEE
Applications
Operating System
Trusted Components
Software
Hardware
Memory
Memory
Secure Hardware
System Bus
Peripherals
Device

Image: [Gon15]

- TPM/SE usually discrete
- TPM/SE has limited, well-defined functionality

ARM TrustZone

- Cortex-A series
- Splits system in normal/secure world

- Similar name but incompatible
- Lower latency
- For systems without MMU

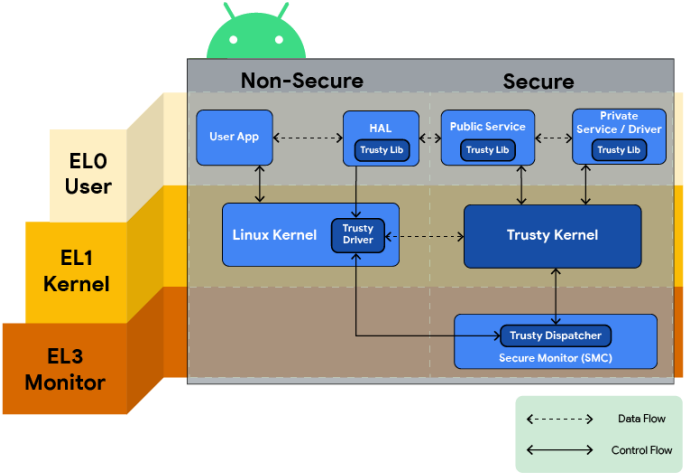

Image: Android OS Documentation

- **AxPROT[0] (P)**: Privileged/unprivileged
- **AxPROT[1] (NS)**: Non-secure/secure
- **AxPROT[2] (I)**: Instruction/data

Intel SGX

- Since Skylake (2015)
- Memory encryption, integrity protection
- Remote attestation
- Trusted time and monotonic counters
- Small enclaves

SGX – Security Model

- Trusted enclave
- Untrusted OS, userspace
- Trusted hardware, firmware (TCB)

- Enclave relies on untrusted OS

- Cache attacks (Prime+Probe [Sch+17])
- Transient execution attacks (SGAxe [Sch+20], MicroScope [Ska+19], ...)
- Software triggered fault attack (PlunderVolt [Mur+20], SGX-Bomb [Jan+17])

AMD SEV

- Since EPYC Naples (2017)
- Secure full system virtualization
- On Naples: Only memory encryption

- Since EPYC Rome (2019)
- Protected register state

- Since EPYC Milan (2021)
- Memory integrity protection
- Support for *non-enlightened* guests

- Trusted Guest
- Untrusted Hypervisor
- Trusted hardware, firmware (TCB)

- VM relies on untrusted Hypervisor
- Before SEV-ES: Register state not protected
- Before SEV-SNP: No memory integrity protection

- CEK extraction through PSP bug [BWS19][Buh+21]
- Exploiting unprotected I/O operations [Li+19]

Thank you!

[Buh+21] Robert Buhren, Hans Niklas Jacob, Thilo Krachenfels, and Jean-Pierre Seifert. "One Glitch to Rule Them All: Fault Injection Attacks Against AMD's Secure Encrypted Virtualization". In: *CoRR* abs/2108.04575 (2021). arXiv: 2108.04575. URL: https://arxiv.org/abs/2108.04575.

[BWS19] Robert Buhren, Christian Werling, and Jean-Pierre Seifert. "Insecure Until Proven Updated: Analyzing AMD SEV's Remote Attestation". In: *CoRR* abs/1908.11680 (2019). arXiv: 1908.11680. URL: http://arxiv.org/abs/1908.11680.

[Gon15] Javier González. "Operating System Support for Run-Time Security with a Trusted Execution Environment". PhD thesis. Mar. 2015. DOI: 10.13140/RG.2.1.4827.8161.

[Jan+17] Yeongjin Jang, Jaehyuk Lee, Sangho Lee, and Taesoo Kim. "SGX-Bomb: Locking Down the Processor via Rowhammer Attack". In: *Proceedings of the 2nd Workshop on System Software for Trusted Execution*. SysTEX'17. Shanghai, China: Association for Computing Machinery, 2017. ISBN: 9781450350976. DOI: 10.1145/3152701.3152709. URL: https://doi.org/10.1145/3152701.3152709.

[Li+19] Mengyuan Li, Yinqian Zhang, Zhiqiang Lin, and Yan Solihin. “Exploiting Unprotected I/O Operations in AMD’s Secure Encrypted Virtualization”. In: *28th USENIX Security Symposium (USENIX Security 19)*. Santa Clara, CA: USENIX Association, Aug. 2019, pp. 1257–1272. ISBN: 978-1-939133-06-9. URL: https://www.usenix.org/conference/usenixsecurity19/presentation/li-mengyuan.

[Mur+20] Kit Murdock, David Oswald, Flavio D. Garcia, Jo Van Bulck, Daniel Gruss, and Frank Piessens. “Plundervolt: Software-based Fault Injection Attacks against Intel SGX”. In: *41st IEEE Symposium on Security and Privacy (S&P’20)*. 2020.

[Sch+17] Michael Schwarz, Samuel Weiser, Daniel Gruss, Clémentine Maurice, and Stefan Mangard. "Malware Guard Extension: Using SGX to Conceal Cache Attacks". In: *Detection of Intrusions and Malware, and Vulnerability Assessment*. Ed. by Michalis Polychronakis and Michael Meier. Cham: Springer International Publishing, 2017, pp. 3–24. ISBN: 978-3-319-60876-1.

[Sch+20] Stephan van Schaik, Andrew Kwong, Daniel Genkin, and Yuval Yarom. *SGAxe: How SGX Fails in Practice*. https://sgaxeattack.com/. 2020.

[Ska+19] Dimitrios Skarlatos, Mengjia Yan, Bhargava Gopireddy, Read Sprabery, Josep Torrellas, and Christopher W. Fletcher. "MicroScope: Enabling Microarchitectural Replay Attacks". In: *Proceedings of the 46th International Symposium on Computer Architecture*. ISCA '19. Phoenix, Arizona: Association for Computing Machinery, 2019, pp. 318–331. ISBN: 9781450366694. DOI: 10.1145/3307650.3322228. URL: https://doi.org/10.1145/3307650.3322228.