TEE(Trusted Execution Environment)とそれに関する研究開発動向

[1)]産業技術総合研究所 サイバーフィジカルセキュリティ研究センター
[2)]セキュアオープンアーキテクチャ・エッジ基盤技術研究組合
須崎有康[1) 2)]

@デジタルサービス・プラットフォーム技術 特別研究専門委員会, 2021/9/27
(Technical Committee on Digital Service Platform Technology)

AIST CPSEC | Cyber Physical Security Research Center

TRASIO

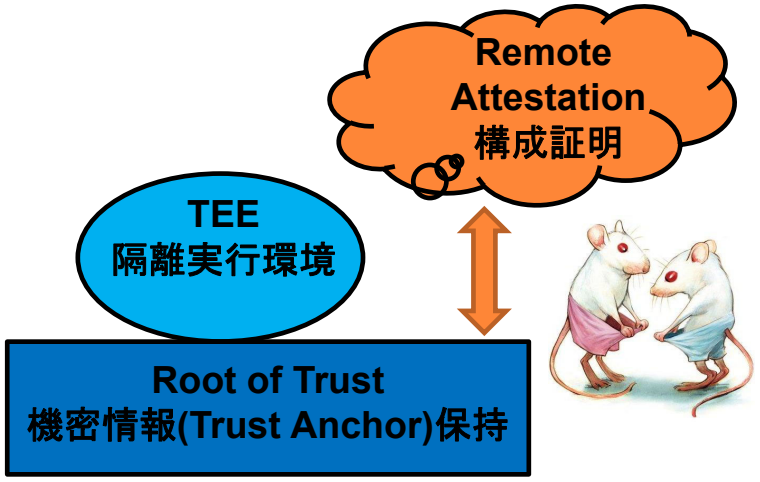
自己紹介

- 名前：須崎有康　Kuniyasu Suzaki
- 所属：産業技術総合研究所サイバーフィジカルセキュリティ研究センター(AIST・CPSEC)
  セキュアオープンアーキテクチャ・エッジ基盤技術研究組合(TRASIO)
- RISC-Vセキュリティの研究に従事。特にTEE関連。
- 2019よりTCG Invited Expert
- 関連書き物
  - Trusted Execution Environmentによるシステムの堅牢化, 情報処理2020/06
    - https://ci.nii.ac.jp/naid/40022255769
  - Trusted Execution Environmentの実装とそれを支える技術,電子情報通信学会基礎・境界ソサイエティ Fundamentals Review, 2020/10
    - https://www.jstage.jst.go.jp/article/essfr/14/2/14_107/_article/-char/ja/
  - IETF111 RATS: Remote Attestation ProcedureS 報告　(IETF111のRATS進捗)
    - https://www.slideshare.net/suzaki/ietf111-rats-remote-attestation-procedures

本日の発表内容

- TEE
  - 多様なハード・ソフトの実装
- Root of Trust
  - 信頼の基点
- Remote Attestation
  - 誰を信頼するか、匿名性ある・なし、スケーラビリティ
- 今後の展開
  - スマホ・PCからクラウドへ、クラウドからIoTへ
  - 関連規格、団体

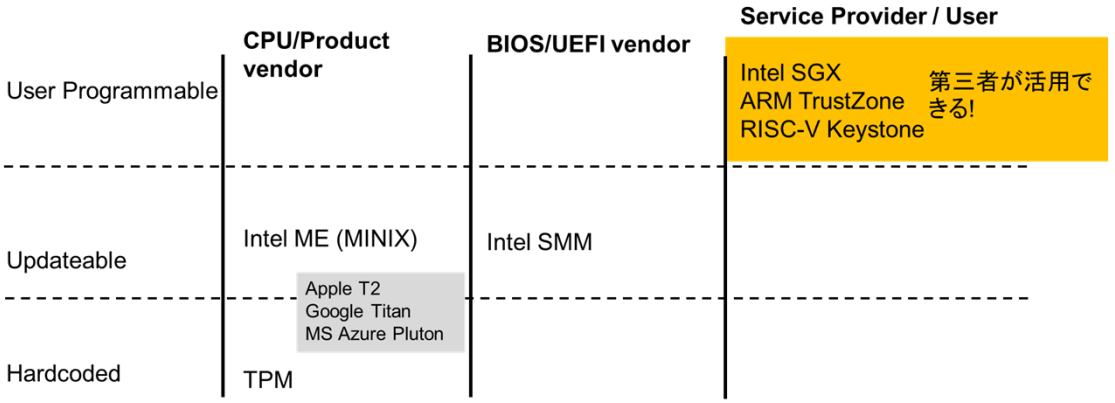
補完する関係だが
それぞれが魑魅魍魎



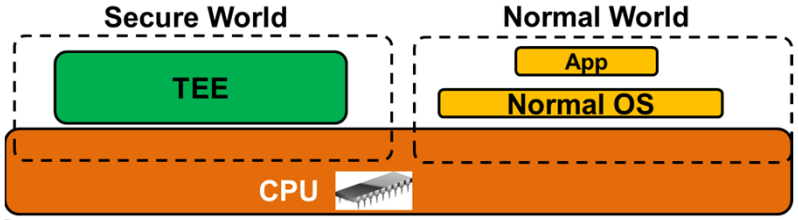
扱わない話題: IDおよびID管理、ソフトウェア更新のOTA: Over the Air

TEEとは

- TEE(Trusted Execution Environment)はHIEE(Hardware-assisted Isolated Execution Environments)の一つ
  - OSから独立してBIOSのみが使うSMM (System Management Mode)などは昔からあった。
  - TEEは第三者がプログラミング可能であることを特徴とする。



- 特徴：(極端に言えば)隔離実行されるのみで、単体ではRoot of Trustになりえない。
  - Root of Trustには安全に鍵・証明書を保存する耐タンパハードウェア(Secure ElementやSecure Coprocessor)が必要
  - **これを信頼の基点に*Remote Attestation*が行われる**
- 利用できるハードウェア
  - Arm TrustZone, Intel SGX, AMD SEV, RISC-V Keystone



この図はあくまでTEEの一例

AIST CPSEC | Cyber Physical Security Research Center

TRASIO

TEEの応用

- 機密情報処理
  - 鍵管理
    - AndroidのKeyMaster
  - DRM処理
    - スマホのWidevine(Google)
  - 個人情報管理
- コード・データの隠蔽
  - 機械学習の重み付けデータ
  - プライバシー保護処理
  - 遺伝子解析
- 暗号処理の前提条件軽減
  - IRON[CCS'17]

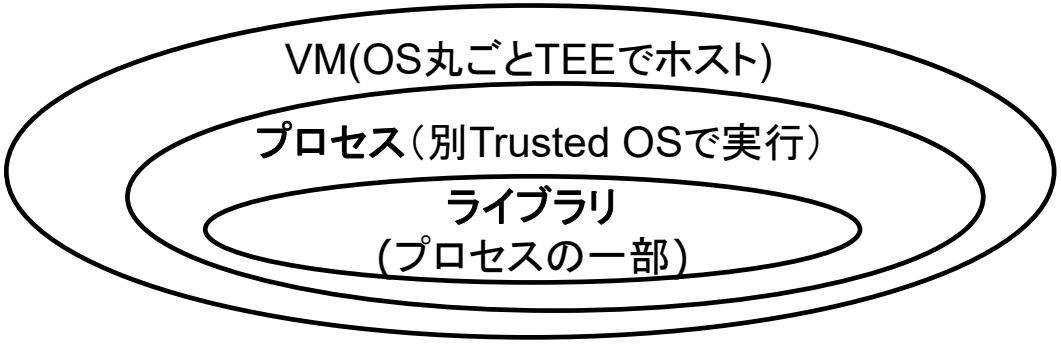
- メモリ消費が少ない
- 要求される機能が少ない
- スマートフォン
- Arm TrustZone向き

- メモリ消費が大きい
- 要求される機能(system call 、ライブラリ)が多い
- サーバ・クラウド
- Intel SGX、AMD SEV, Arm CCA, Amazon EC2 Nitro 向き

- RISC-V?

TEEの分類 (私見)

- Process-based (Intel SGX)
  - **１プロセス内**で**機密処理(ライブラリ相当)**ができる隔離実行環境Enclaveを提供する。
- Device-based (Arm TrustZone, RISC-V Keystone)
  - **デバイスをNormal WorldとSecure Worldに分ける**。２つのWorldがあり、Normal Worldのプロセスが**機密処理のプロセス**をSecure Worldで実行できる。
- VM-based (AMD SEV, Intel TDX, Arm CCA, Amazon EC2 Nitro)
  - TEE内に**機密処理が行えるVM**があり、複数のOSを実行することができる。



TEE内の機密処理単位のイメージ

注：物理的なメモリサイズと必ずしも一致しない。
Arm TrustZoneでは数MBのプロセスしか実行できないのに対して、Intel SGX v1では96MBのライブラリが実行できるなど物理的なサイズとは異なる。

AIST CPSEC | Cyber Physical Security Research Center

TRASIO

Intel SGX

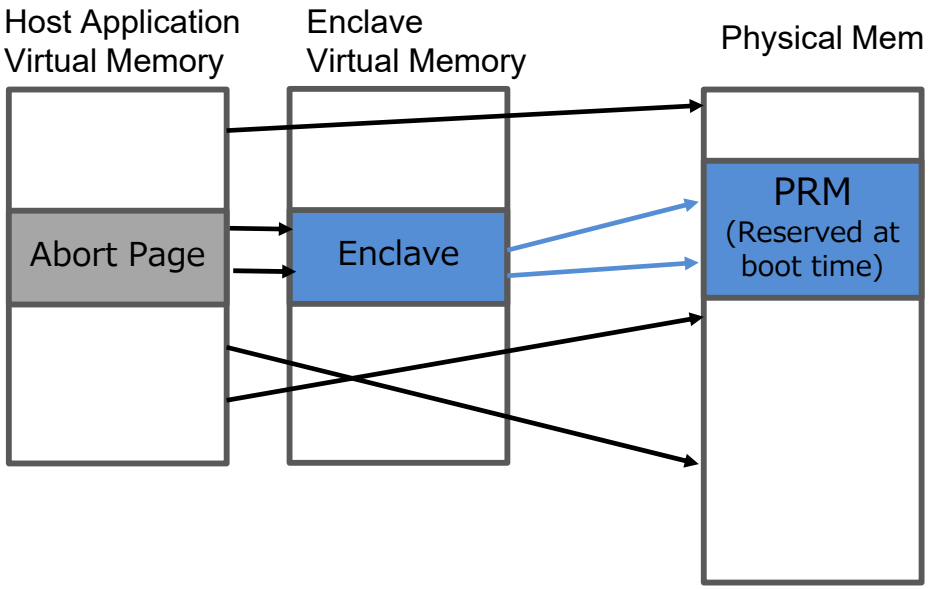
- Intel Skylake (2015)より装備されたTEE
- TEEであるEnclave内はRing3(ユーザモード)のみ。ユーザアプリのみの実行ができる
  - Intel SDKに従えばUntrusted側のプロセスの一部のライブラリ関数として実行される
  - OS相当の機能は単純に入れられない。（苦労して入れている）
- SGX実装の大部分がMicro Code (詳細は特許、講演資料から推測 Secure Processors Part I & II)
  - 追加ハードは PMH(Page Miss Handler)とMEE (Memory Encryption Engine)
  - Miro Codeでは実装が難しい部分には特殊Enclaveがある
    - Provisioning Enclave 鍵管理、Launch Enclave 生成管理、Quoting Enclave リモートアテステーション管理
- 使える暗号メモリはSGXv1の１Enclaveで96MB以下。（BIOSでの確保は128MB以下）
  - 暗号メモリをEnclave外にswap outする仕組みあり。但し、大変遅い。
- キラーアプリは? 4Kブルーレイ再生があるが…

参考資料

1. Intel SGX explained, Victor Costan and Srinivas Devadas, http://css.csail.mit.edu/6.858/2020/readings/costan-sgx.pdf
2. Secure Processors Part I & II, Victor Costan, Ilia Lebedev and Srinivas Devadas **これはバイブル！**
   https://people.csail.mit.edu/devadas/pubs/part_1.pdf https://people.csail.mit.edu/devadas/pubs/part_2.pdf

Intel SGX

- 通常のアプリの一部（ライブラリ関数）としてEnclaveで実行される
- Enclaveのメモリは別仮想空間となる。物理メモリとしてはEnclave用に確保した部分が使われ、暗号化される

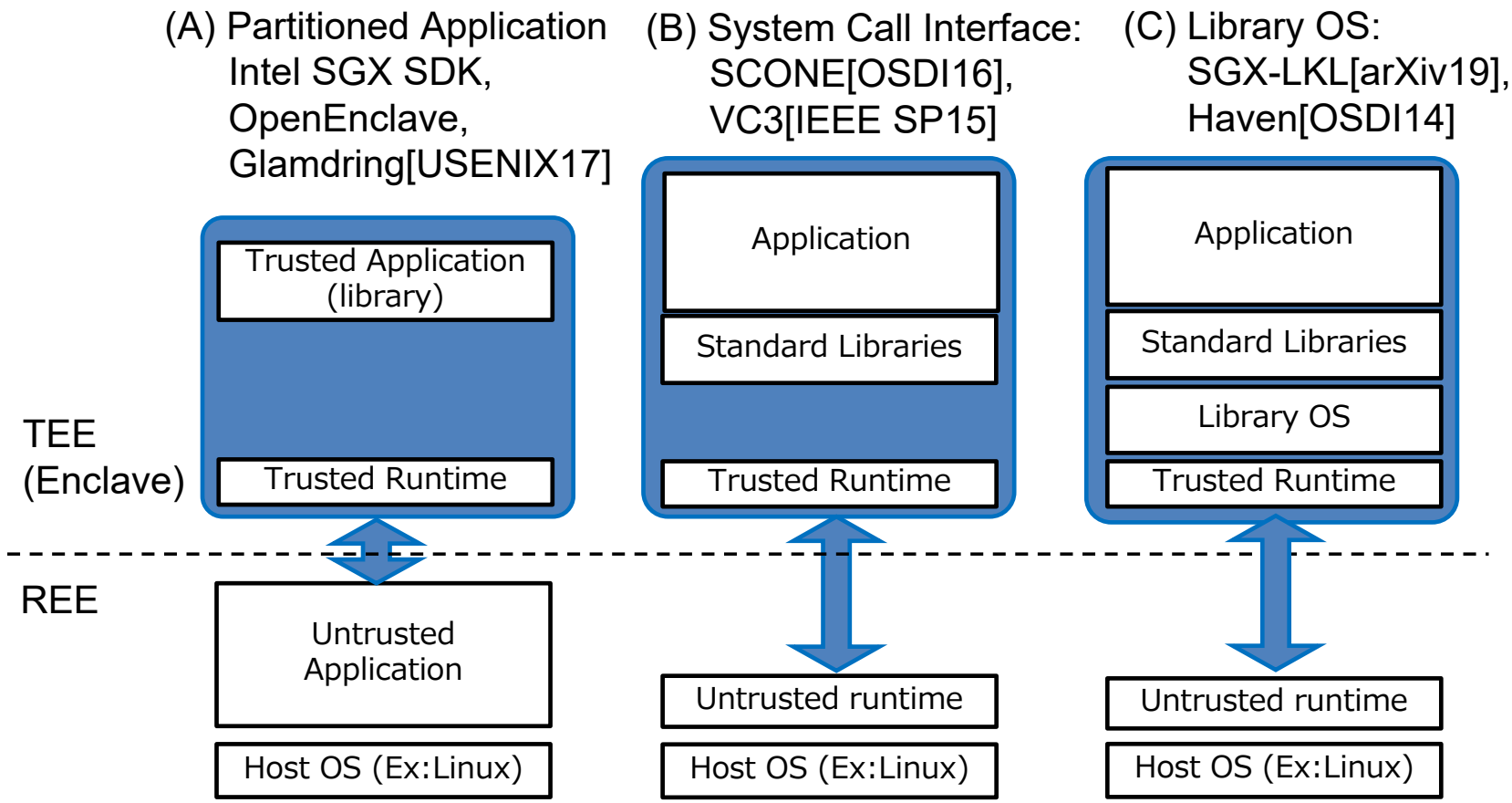


- PRM:　Processor Reserved Memory　　BIOSで確保するメモリ

AIST CPSEC | Cyber Physical Security Research Center

TRASIO

SGX上でのソフトウェア実装



AIST CPSEC | Cyber Physical Security Research Center

TRASIO

Arm TrustZone

- 2004からあるTEE(Cortex-A)だが、広まったのはスマホに入ってから。
  - キラーアプリ：Android Keymaster(鍵管理), WideVine(DRM管理)
- Cortex-A(スマホ)とCortex-M(組み込み用)でアーキテクチャが全く異なる。
  - Cortex-Aは起動時にSecure WorldとNormal Worldで別々のOSを立ちあげ、Secure Monitor経由で切り替える2World View（後スライド）。
    - ペリフェラルもSecure WorldとNormal Worldに分けられる。
    - メモリは暗号化されない。使えるメモリは任意だが通常Secure Worldは数十MB。
  - Cortex-Mは2016のM23/M33から。既存のHandler ModeとThread ModeのSecure/Non-Secureの高速ハードウェア切替をつけたもの。（今回の発表では対象外）

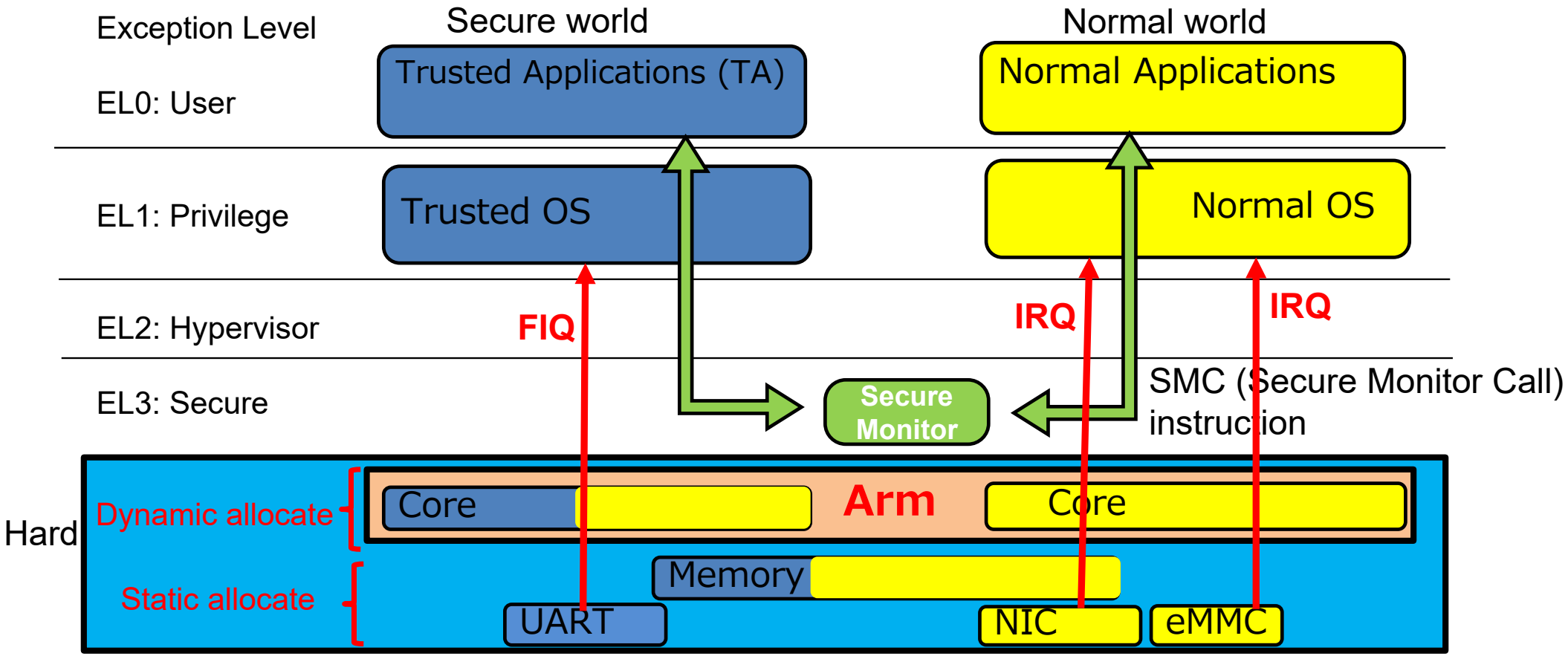
参考資料

1. Demystifying Arm TrustZone: A Comprehensive Survey, Sandro Pinto and Nuno Santos, ACM Comp Survey 2019,
2. SoK: Understanding the Prevailing Security Vulnerabilities in TrustZone-assisted TEE Systems, David Cerdeir, Nuno Santos, Pedro Fonseca, Sandro PintoIEEE S&P 2019

AIST CPSEC | Cyber Physical Security Research Center

TRASIO

Arm Cortex-A TrustZone

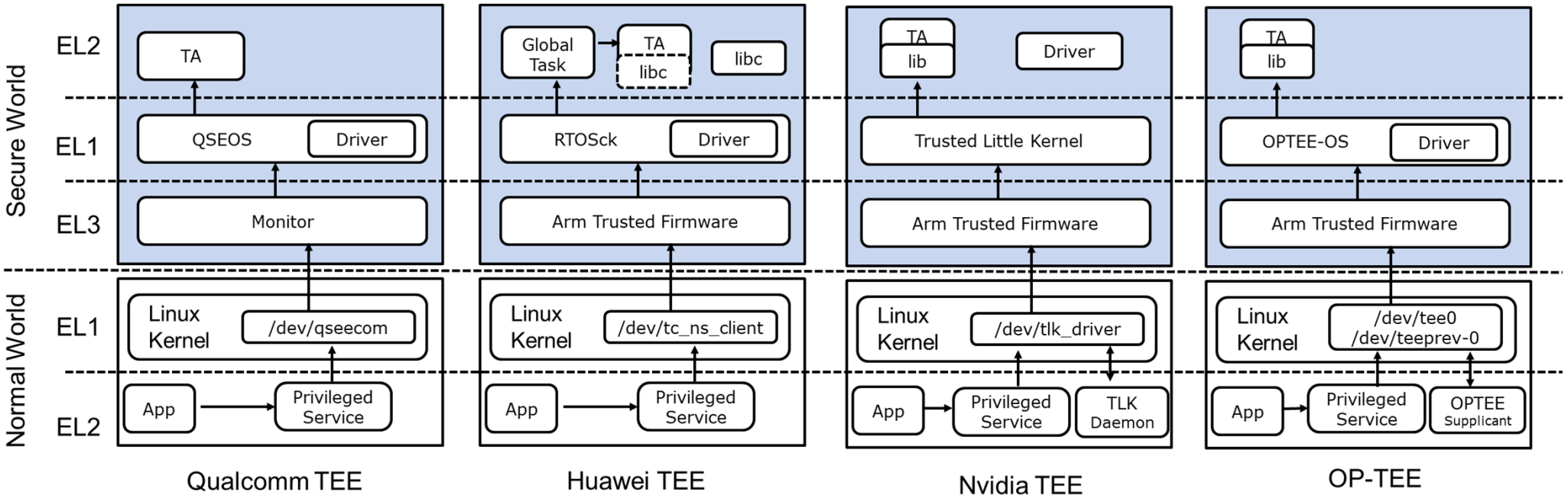


AIST CPSEC | Cyber Physical Security Research Center

TRASIO

Arm Cortex-A TrustZone 上でのソフトウェア実装

- Secure WorldのTAのライブラリ実装(Dynamic/Static),Driverの実装などが異なる。
- Normal WorldのDaemon実装やdeviceインターフェースが異なる。



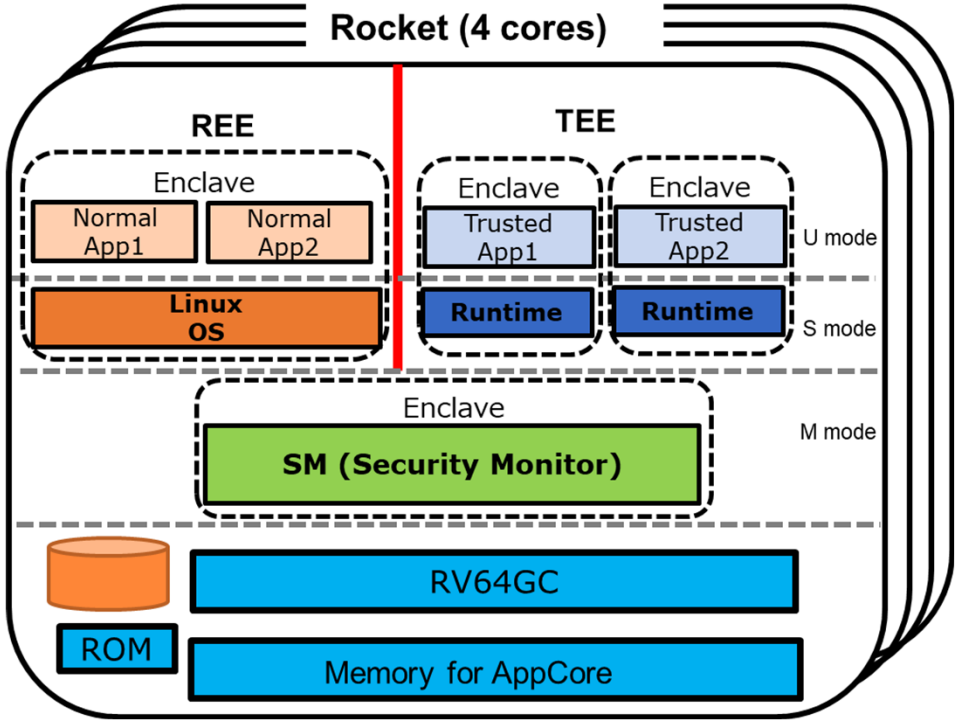
出典：SoK: Understanding the Prevailing Security Vulnerabilities in TrustZone-assisted TEE Systems [IEEE SP20]より

AIST CPSEC | Cyber Physical Security Research Center

RISC-V TEE

TRASIO

- オープンアーキテクチャのためハードのカスタマイズも容易でTEEが多く開発されている
  - Academia
    - Sanctum [MIT,USENIX Sec'16]
    - TIMBER-V [グラーツ工科大学, NDSS'19]
    - MI6 [MIT,MICRO'19]
    - Keystone [UC Berkeley, EuroSys'20]
    - uTango [arXiv'21, ミーニョ大学]
    - Cure [ダルムシュタット工科大学,USENIX Sec'21]
  - Industry
    - MultiZone [HexFive]



右図はKeystone。TRASIOでも活用している。

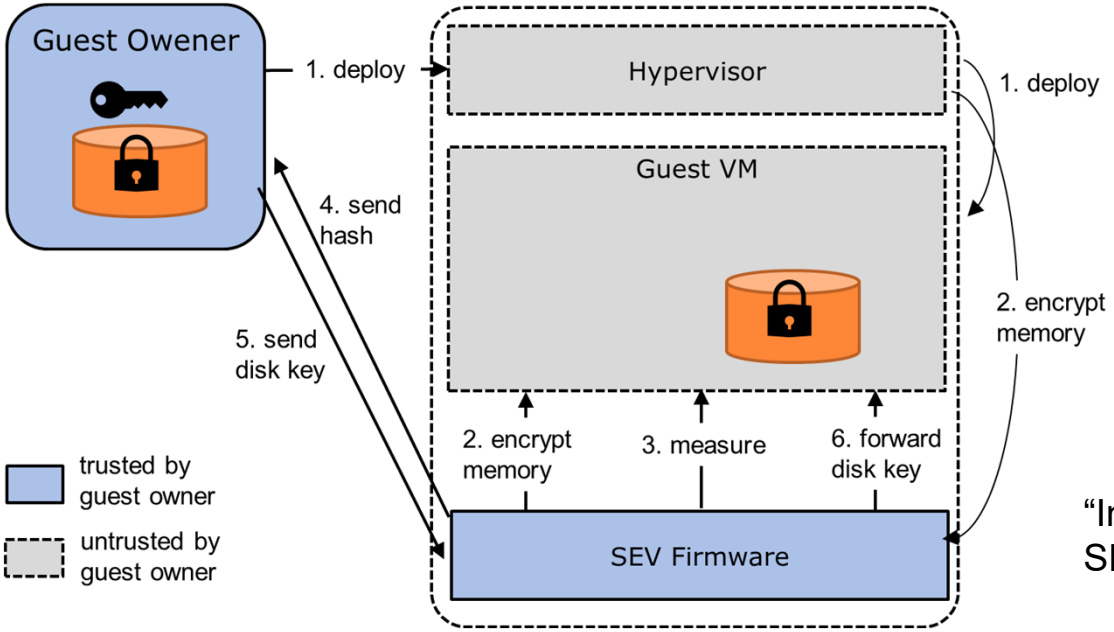
- PMP: Physical Memory Protectionを活用したメモリ分離。
- 図中の点線で囲われているEnclave単位で分離される
- M modeのSMで一つ
- REEのLinuxで一つ
- TEE内に二つ(TEEは動的に作成される。メモリはLinuxから切り出し、終了すればLinuxに戻す。)

参考資料

1. A Survey on RISC-V Security: Hardware and Architecture, TAO LU (Marvell), arXiv21

仮想マシンのTEE化 1/4

- AMD Secure Encrypted Virtualization(SEV)
  - 暗号化されたDisk ImageがSEV Firmwareで検証される。
  - VM用メモリも暗号化されHypervisorはVMの内容に関知できない。



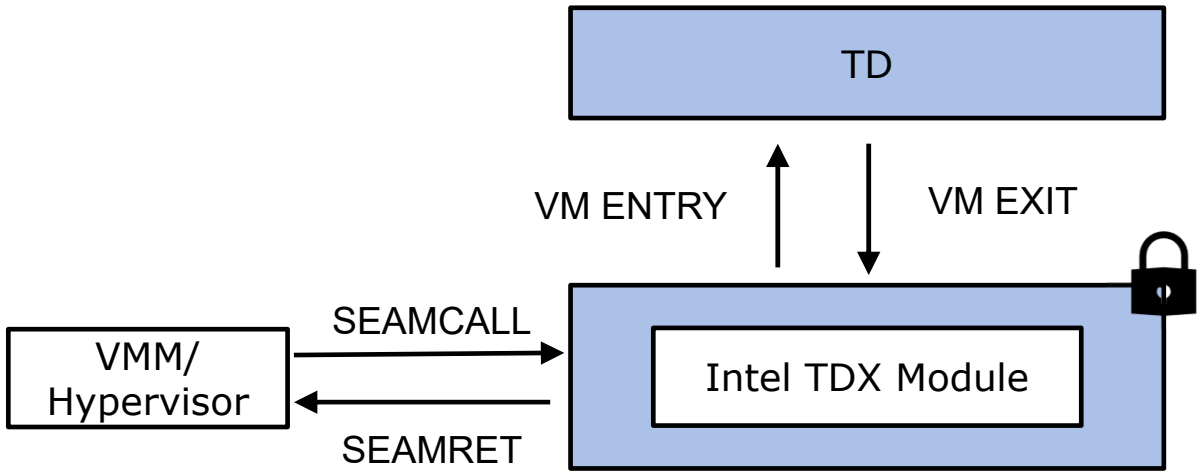
“Insecure Until Proven Updated: Analyzing AMD SEV‘s Remote Attestation”CCS19より

仮想マシンのTEE化 2/4

- Intel Trusted Domain Extensions (TDX) (実機はまだない)
  - Intel VT, TXT, SGXを組み合わせてTD (Trusted Domain)の保護
  - Secure Arbitration Mode (SEAM)を通して通信

Trusted by TD
- Intel TDC module
- Intel authenticated code (ACM)
- TD Quoting Enclave
- CPU hardware

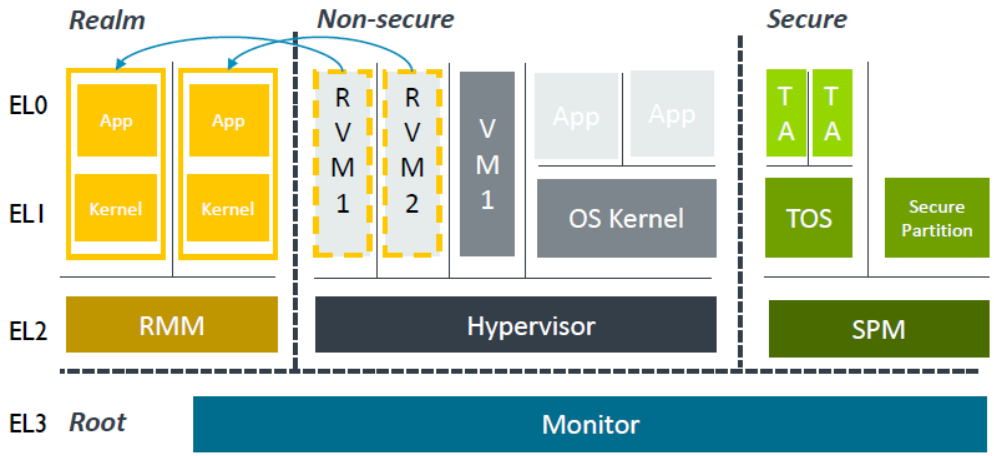
Untrusted by TD
- Platform Admin
- Devices
- All other software
- Platform Firmware
- Host-OS/VMM
- BIOS/SMM



Intel White Paper “Intel Trusted Domain Extensions”より

仮想マシンのTEE化 3/4

- Arm CCA: Confidential Computing Architecture (実機はまだない)
  - realmの概念の導入
    - メモリ隔離を施したRealmにVMのイメージを預けることができる。
    - RMM: Realm Management Monitorで管理
  - 今までのSecure World(TrustZone)も残す
    - SPM: Secure Partition Managerで複数のSecure Worldも設定可能

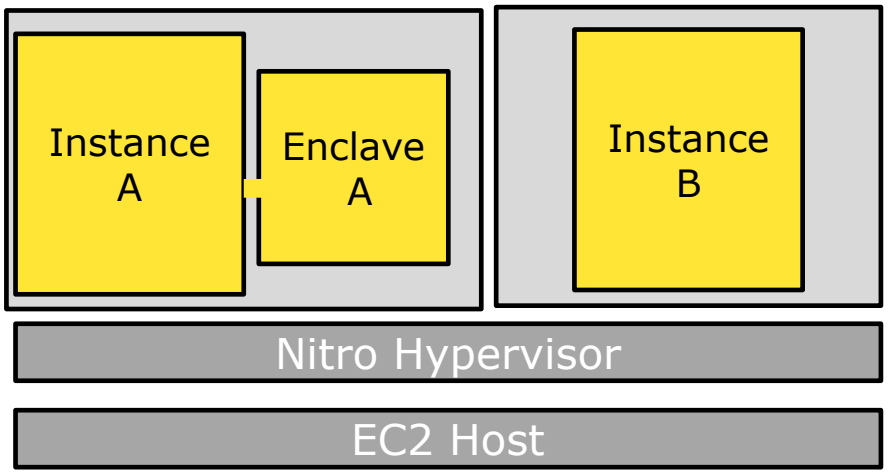


Security State/PA space	Non-Secure PA	Secure PA	Realm PA	Root PA
Non-secure	Allow	Block	Block	Block
Secure	Allow	Allow	Block	Block
Realm	Allow	Block	Allow	Block
Root	Allow	Allow	Allow	Allow

Linaro Connect発表資料より
https://static.linaro.org/connect/armcca/presentations/CCATechEvent-210623-CGT-2.pdf

仮想マシンのTEE化 4/4

- Amazon EC2 Nitro
- EC2インスタンスのみに繋がる隔離実行(Enclave)
  - 外部ネットワーク接続も永続的なストレージもない。ローカル仮想ソケット (vsock) のみで通信。
  - Nitro Hypervisor はEnclave を作成する際に構成証明ドキュメント(適切はブート処理の測定値)を作成および署名。これにより改竄検知。
    - https://aws.amazon.com/jp/ec2/nitro/nitro-enclaves/
    - https://aws.amazon.com/jp/blogs/news/aws-nitro-enclaves-isolated-ec2-environments-to-process-confidential-data/



AIST CPSEC | Cyber Physical Security Research Center

TRASIO

TEEへの攻撃

- Intel SGXへの脆弱性・攻撃
  - Spectreタイプ：Foreshadow[USENIX Sec18]、SgxSpectre[EuroS&P19]
  - 電源制御を使った攻撃: Plundervolt[IEEE S&P20], V0LTpwn[USENIX Sec20], Voltpillager[USENIX Sec21], PLATYPUS [IEEE S&P21]
  - レジスタのサニタイズ（クリア）をしていない脆弱性：Faulty Point Unit: ABI Poisoning Attacks on Intel SGX[ACSAC20]
  - Memory RowHammerを使った攻撃：SGX-Bomb[SysTex'17]
- Arm TrustZoneへの脆弱性・攻撃
  - TEE内からREE内のメモリにアクセスできることを悪用して、OSが持つ機密情報を盗む：boomerang attack[NDSS17]
  - Trusted OSの脆弱性を利用する：QSEEのbuffer overflow脆弱性[BlackHat USA14]

参考文献

1. Security Vulnerabilities of SGX and Countermeasures: A Survey, ACM Comp Survey 21

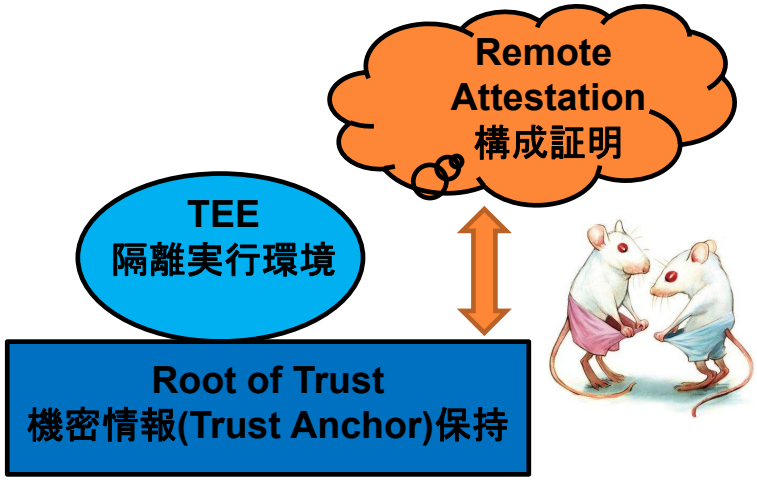
AIST CPSEC | Cyber Physical Security Research Center

TRASIO

本日の発表内容

- TEE
  - 多様なハード・ソフトの実装
- Root of Trust
  - 信頼の基点
- Remote Attestation
  - 誰を信頼するか、匿名性ある・なし、スケーラビリティ
- 今後の展開
  - スマホ・PCからクラウドへ、クラウドからIoTへ
  - 関連規格、団体

補完する関係だが
それぞれが魑魅魍魎



扱わない話題: IDおよびID管理、ソフトウェア更新のOTA: Over the Air

AIST CPSEC | Cyber Physical Security Research Center

Root of Trust

TRASIO

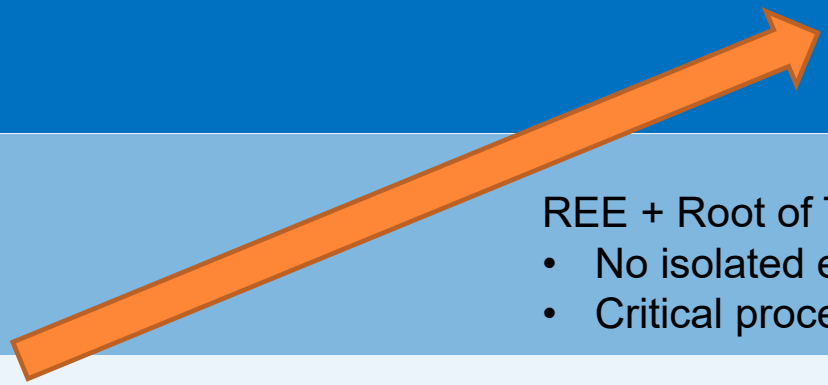
- 秘密鍵や証明書などの機密情報(Trust Anchor)を持続的に保持し、信頼の基点となるハードウェア
- Root of Trustの例
  - Intel SGXではIntel ME(Management Engine)。実装はIntel Quark x86-based (32bit)
  - AMD SEVではPSP(Platform Security Processor)。実装はArm Cortex-A5 (32bit)
  - Arm TrustZoneではIPの購入が必要。CryptCell(旧Discretix、現Arm)、CryptoManager (Rambus)
  - iPhoneのSecure Enclave
  - Apple MacのT2
  - GoogleのTitan (on Google Pixel, GCP: Google Compute Platform), Open Titan
  - AWS Nitro Security Chip
  - Secure Element 多くのスマホ
  - Microsoft のPluton (実態はArm Cortex-M: MediaTek MT3620) Azure Sphereで管理するIoT用
  - TPM
  - Secure Element

スマホ
クラウド
IoT

AIST CPSEC | Cyber Physical Security Research Center

TRASIO

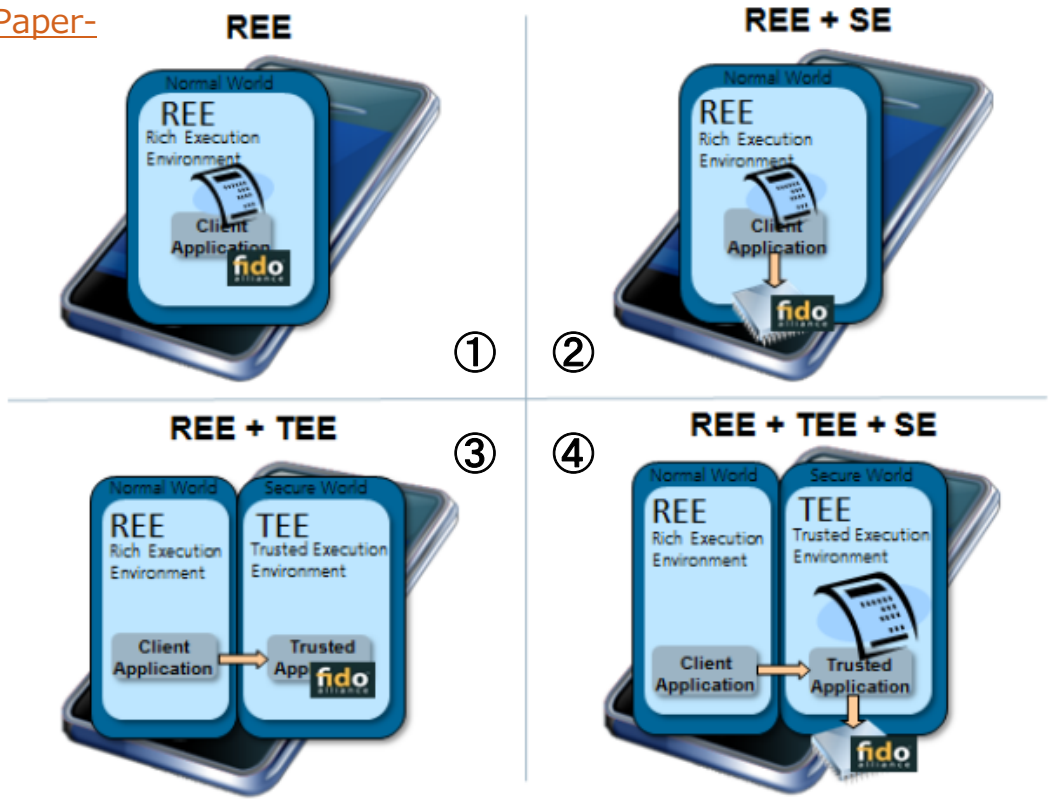
TEEとRoot of Trustの構成



2 layers	REE + TEE + Root of Trust • **The order is important** • **REE -> TEE -> Root of Trust**		
1 layer	REE + Root of Trust • No isolated environment • Critical processing is not protected	REE + TEE • No hardware tamper-proof • Critical data is not protected	
0 layer	REE only • No isolated environment • No hardware tamper-proof • Critical data and processing are not protected		

TEEとRoot of Trustの構成例(FIDO Authenticator)

- Realizing FIDO Authentication Solutions with GlobalPlatform Technologies, 2018
  - https://globalplatform.org/wp-content/uploads/2018/04/White-Paper-Technical-FIDO-Auth-using-GlobalPlatform-Jan2018.pdf
  - FIDO Authenticatorの実装パターン
    - ① REE直接
    - ② REE+SE(RoT)
    - ③ REE+TEE
    - ④ REE+TEE+SE



GLOBALPLATFORM
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

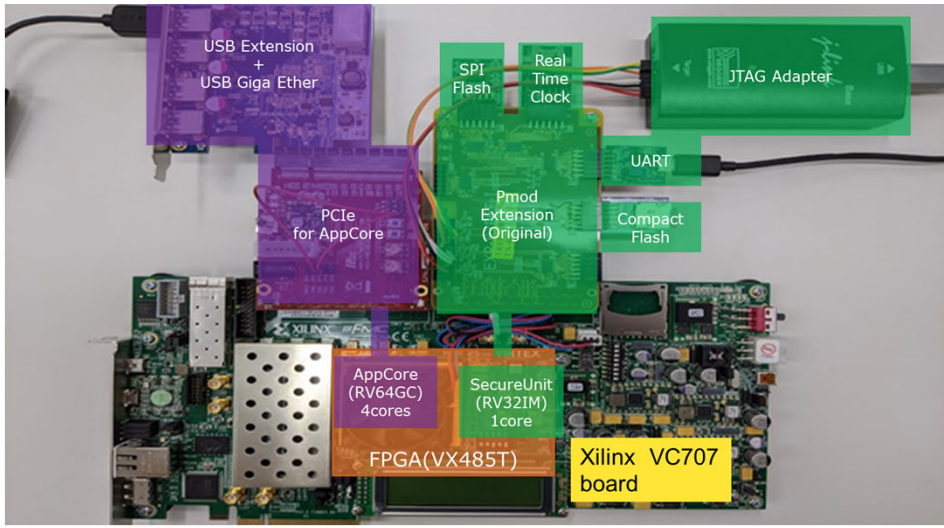
Practical Considerations: Technical Overview

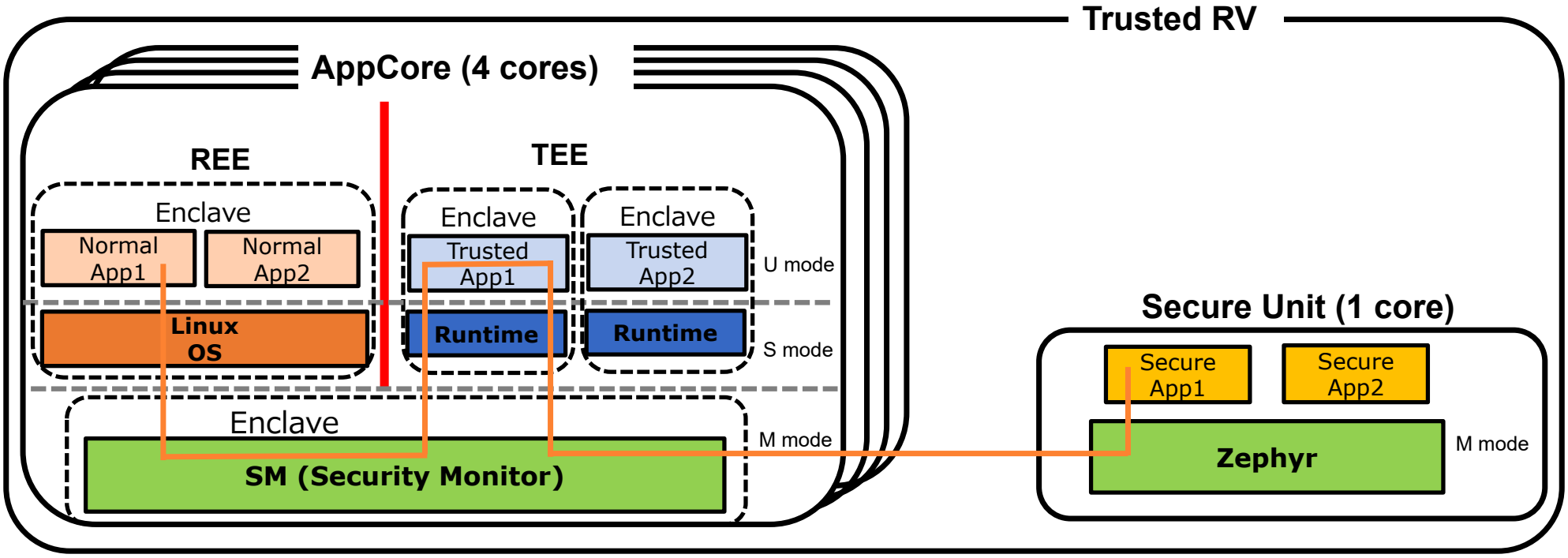
Realizing FIDO Authentication Solutions with GlobalPlatform Technologies

AIST CPSEC | Cyber Physical Security Research Center

TRASIOで開発するRISC-V TEEとRoT

- RoT(Secure Unit)で鍵管理、セキュアブート管理
- 限定された通信
  - FOSDEM 2021やRISC-V Forum Securityで発表





AIST CPSEC | Cyber Physical Security Research Center

TRASIO

Root of Trustへの攻撃

- Intel MEの脆弱性・攻撃
  - マスクROMの脆弱性：CVE-2019-0090として登録
  - EPIDに対する攻撃：SGAxe[Real World Crypto 2021]
- Apple Secure Enclaveの脆弱性・攻撃
  - Demystifying the Secure Enclave Processor [black Hat USA 2016]
  - iOS 14 JailBreak by Pangu[Mosec 2020]
- Apple T2の脆弱性・攻撃
  - By Pangu [2020]

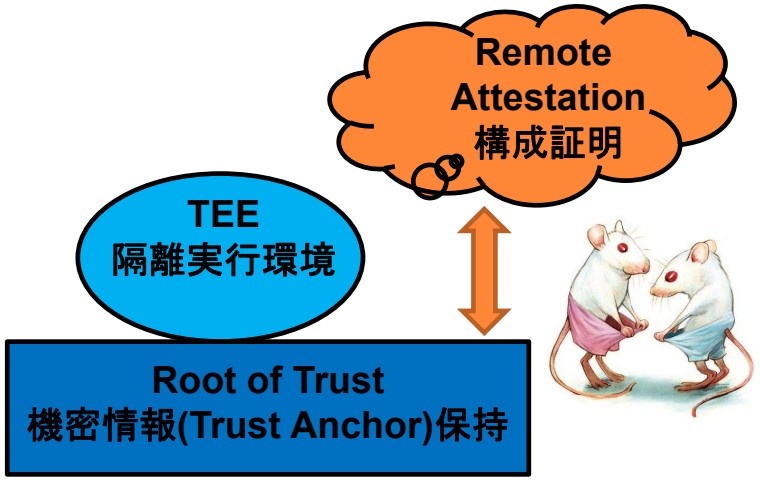
AIST CPSEC | Cyber Physical Security Research Center

TRASIO

本日の発表内容

- TEE
  - 多様なハード・ソフトの実装
- Root of Trust
  - 信頼の基点
- **Remote Attestation**
  - **誰を信頼するか、匿名性ある・なし、スケーラビリティ**
- 今後の展開
  - スマホ・PCからクラウドへ、クラウドからIoTへ
  - 関連規格、団体

補完する関係だが
それぞれが魑魅魍魎



扱わない話題: IDおよびID管理、ソフトウェア更新のOTA: Over the Air

Remote Attestation

- リモートの第三者がデバイスの認証、および意図したバイナリが実行されることを確認する手段
  - TEE以外でも使われる

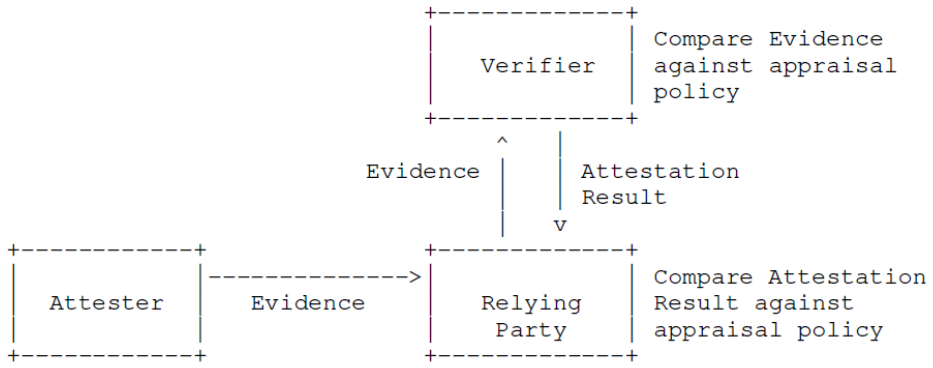


Figure 6: Background-Check Model

IETF RATS Architectureより

- Attesterが自分が真正のラットフォームであることのEvidenceをサービスやデータを提供するRelying Partyに提出する。
- Relying Partyは信頼できるVerifierに正しいことを検証依頼する。
- 正しければサービス・データを提供。

- 現在、IETFのRemote Attestationに関するプロトコルRTAS(Remote Attestation ProcedureS)が議論されている。
  - TPM-style、EAT-styleなど議論が分かれている。
  - 認証するためのクレームが多岐に渡る。実行状態、時間、位置までクレームがある
  - FIDO、Arm Platform Security Architecture (PSA)なども関係してきており、まとめるのが大変。

AIST CPSEC | Cyber Physical Security Research Center

TRASIO

既存のRA: Remote Attestation

青字はAttesterカテゴリの分類

- Intel SGX: Software Guard Extensions (process-based)
  - EPID: Enhanced Privacy ID, Intel提供のプライバシーを考慮したRA
  - DCAP: Data Centric Audit Protection, プライバシーを考慮しないRA
- Intel TXT: Trusted Execution Technology. 実行途中で信頼基点を作るDynamic Root of Trust
- AMD SEV: Secure Encrypted Virtualization (VM-based)
- RISC-V
  - Keystone
- Arm TrustZone (本体にはRemote Attestationの機能はない)
  - Android Key Attestation https://github.com/google/android-key-attestation
  - Samsung Knox Attestation https://docs.samsungknox.com/dev/knox-attestation/index.htm
  - PSA Attestation API
- TPM: Trusted Platform Module 通常のWindows PCには標準準拠 (HSM-based)
- DICE: Device Identifier Composition Engine
- FIDO
  - FIDO ECDAA Algorithm
    - https://fidoalliance.org/specs/fido-uaf-v1.2-rd-20171128/fido-ecdaa-algorithm-v1.2-rd-20171128.html
- Android 7以降
- iOS 14以降
- Azure IoT、TPM、Intel SGXなどに対応
  - https://docs.microsoft.com/ja-jp/azure/attestation/overview

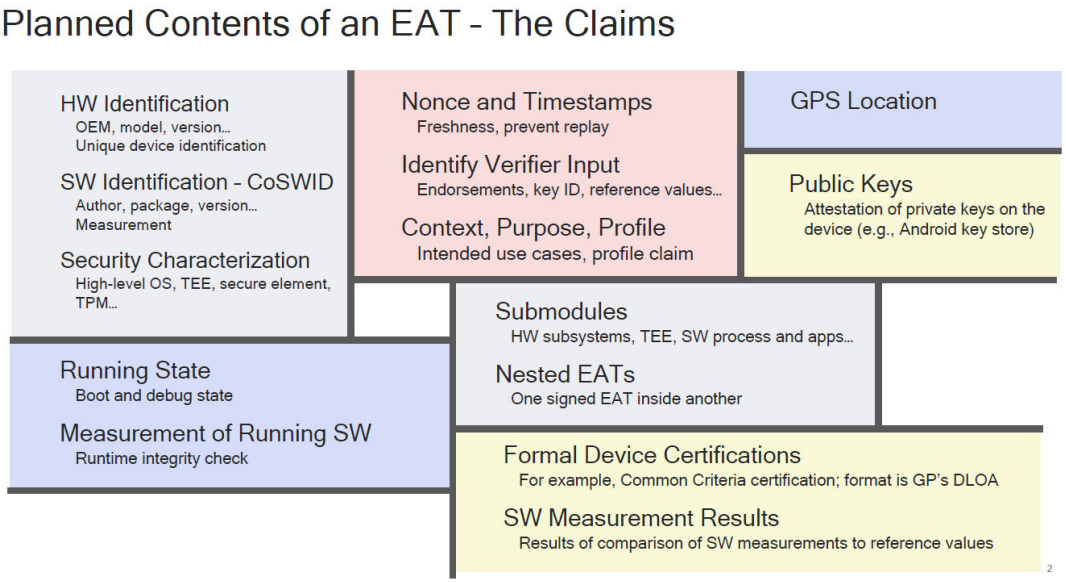
Arm
SPA
TCG
FIDO Alliance

AIST CPSEC | Cyber Physical Security Research Center

TRASIO

Remote Attestationの現状

- 既存のものが多岐に渡る
  - 全スライド参考
- IETFではRATS: Remote Attestation ProcedureSの策定
  - TPM(Trusted Platform Module)タイプ
    - ネットワーク装置/サーバなどが対象
  - EAT(Entity Authentication Token)タイプ
    - スマホ・IoTなどが対象
  - 検査する項目(Claim)が多岐に渡る。(右図)
- 課題
  - 誰を信頼するか
  - プライバシーを考慮した匿名性
    - Direct Anonymous Attestation
  - スケーラビリティ
    - Swarm/Collective Attestation



AIST CPSEC | Cyber Physical Security Research Center

TRASIO

Remote Attestationの課題：誰を信頼するか

- Intel SGX、AMD SEVにもRemote Attestationの機能があるが、Intel/AMDがて提供するサービスを信頼しなければならない。
  - 第三者機関を置けるようする提案はあり。
    - DCAP: Data Center Attestation Primitives
    - OPERA (OPEn Remote Attestation) [CCS19,オハイオ州立大学]

Remote Attestationの課題：匿名化

- DAA: Direct Anonymous Attestation
  - デバイスの識別IDで特定されないようにグループ署名などを使う。
  - Intel SGXのデフォルトのRemote AttestationはEPID (Enhanced Privacy ID, ISO/IEC 20008/20009)
- IETF RATSではRATSアーキテクチャにGroup keyを扱うDAA Issuerを付加する話がある。(右図)
  - Draftにもあるが Revocationが難しくなる。
- 但し、単独企業によるデバイス管理など、利用によっては匿名性がないものも求められている。

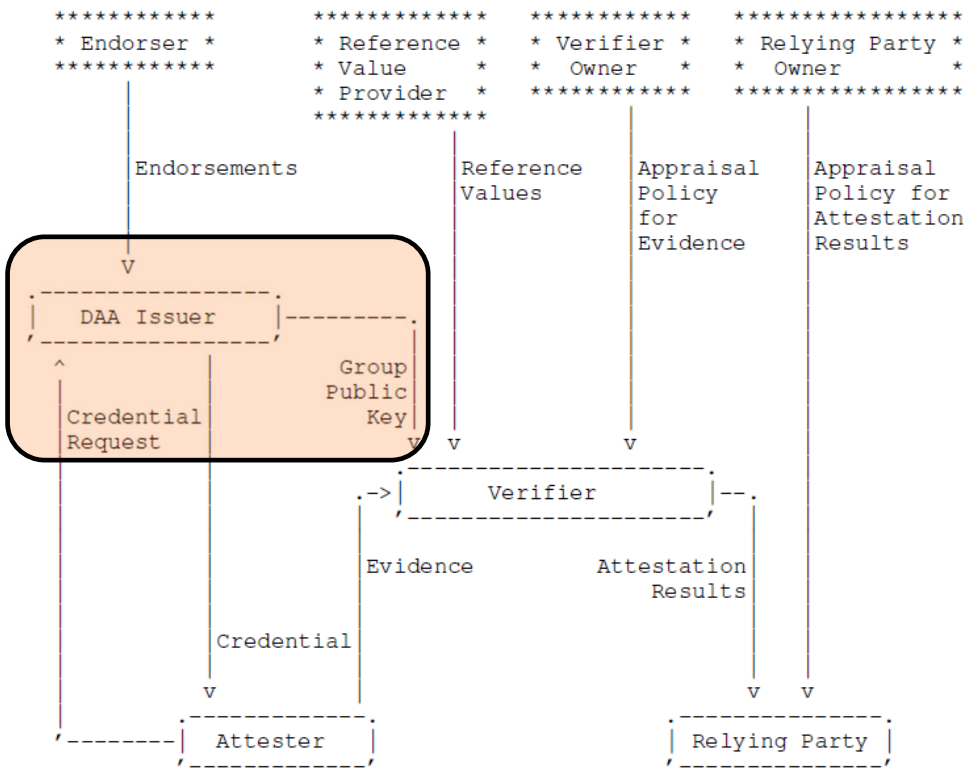


Figure 1: DAA data flows

raft-birkholz-rats-daa-01より

AIST CPSEC | Cyber Physical Security Research Center

TRASIO

Remote Attestationの課題：スケーラブル

- 多量のデバイス・サービスに対してRAを行うのは大変。
- Swarm or Collective Attestation[1,2] と呼ばれている技術の提案。
  - 多量のAttesterに対するAttestationの方式拡張。１つ１つではなく、あるかたまりでのAttestation。
  - IETFのRATSでもスケーラビリティに対処する提案があるが、プロトコル的に大きな変更あるか心配。

2. 論文より
多量のデバイスを経由する際にまとめでRAを行う。

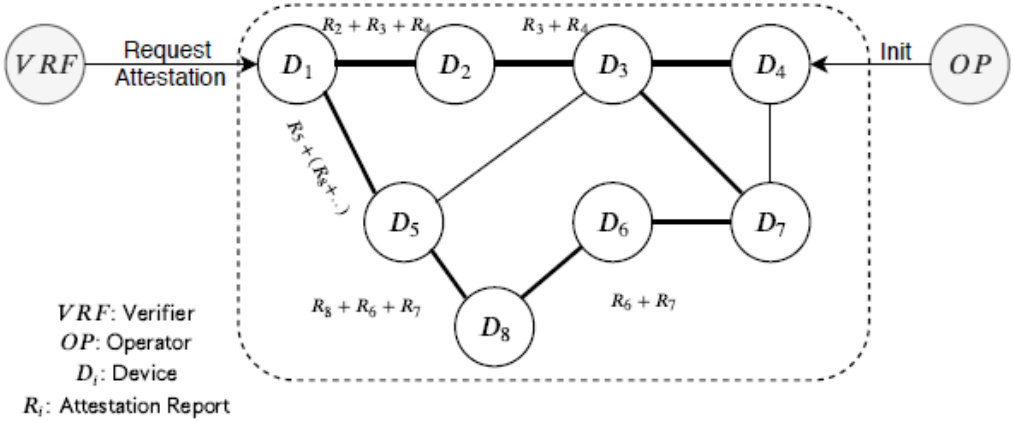


Fig. 4. SEDA collective attestation in a swarm of 8 devices [7]

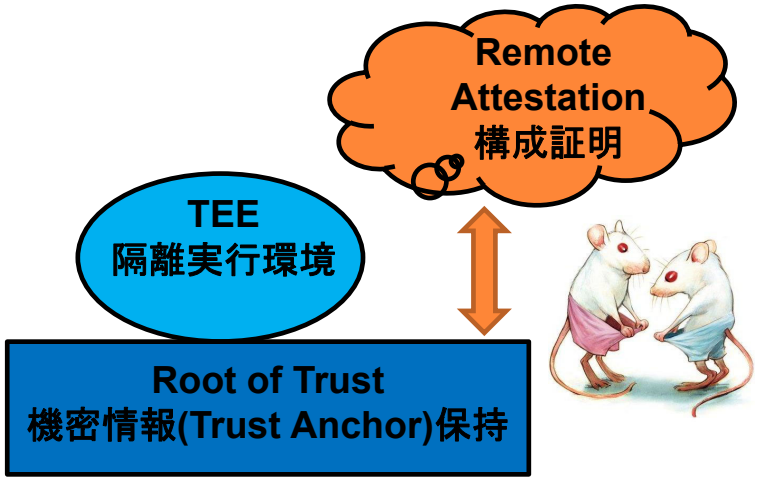
1. Alexander Sprogø Banks, Marek Kisiel, and Philip Korsholm, Remote Attestation: A Literature Review, arXiv21
2. Ioannis Sfyrakis, Thomas Gross, A Survey on Hardware Approaches for Remote Attestation in Network Infrastructures, arXiv21

本日の発表内容

- TEE
  - 多様なハード・ソフトの実装
- Root of Trust
  - 信頼の基点
- Remote Attestation
  - 誰を信頼するか、匿名性ある・なし、スケーラビリティ

補完する関係だが
それぞれが魑魅魍魎

- 今後の展開
  - スマホ・PCからクラウドへ、クラウドからIoTへ
  - 関連規格、団体



扱わない話題: IDおよびID管理、ソフトウェア更新のOTA: Over the Air

今後の展開(1/2)

- スマホ・PCからクラウドへ
  - クラウドで必要な仮想化対応は先に説明したように既にCPUレベルで始まっている
  - Amazon EC2 Nitroは既に運用
  - ブロックチェーン、電子投票(右図)
  - Confidential Computing
    - CCC: Confidential Computing Consortiumの方向性

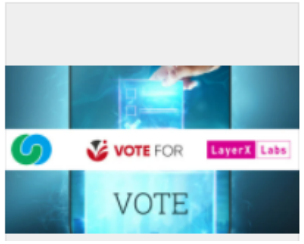
電子投票にTEEが使われた記事

LayerX、つくば市らネット投票の実証研究実施へ。プライバシー保護技術「Anonify」活用

9/21(火) 17:16 配信 0

あたらしい経済

つくば市で「インターネット投票システムの実証的共同研究」実施へ



株式会社LayerX（レイヤーエックス）が、株式会社VOTE FOR（ボートフォー）および茨城県つくば市と共に「インターネット投票システムの実証的共同研究」を実施することが9月21日分かった。研究の期間は2022年3月31日までとのこと。

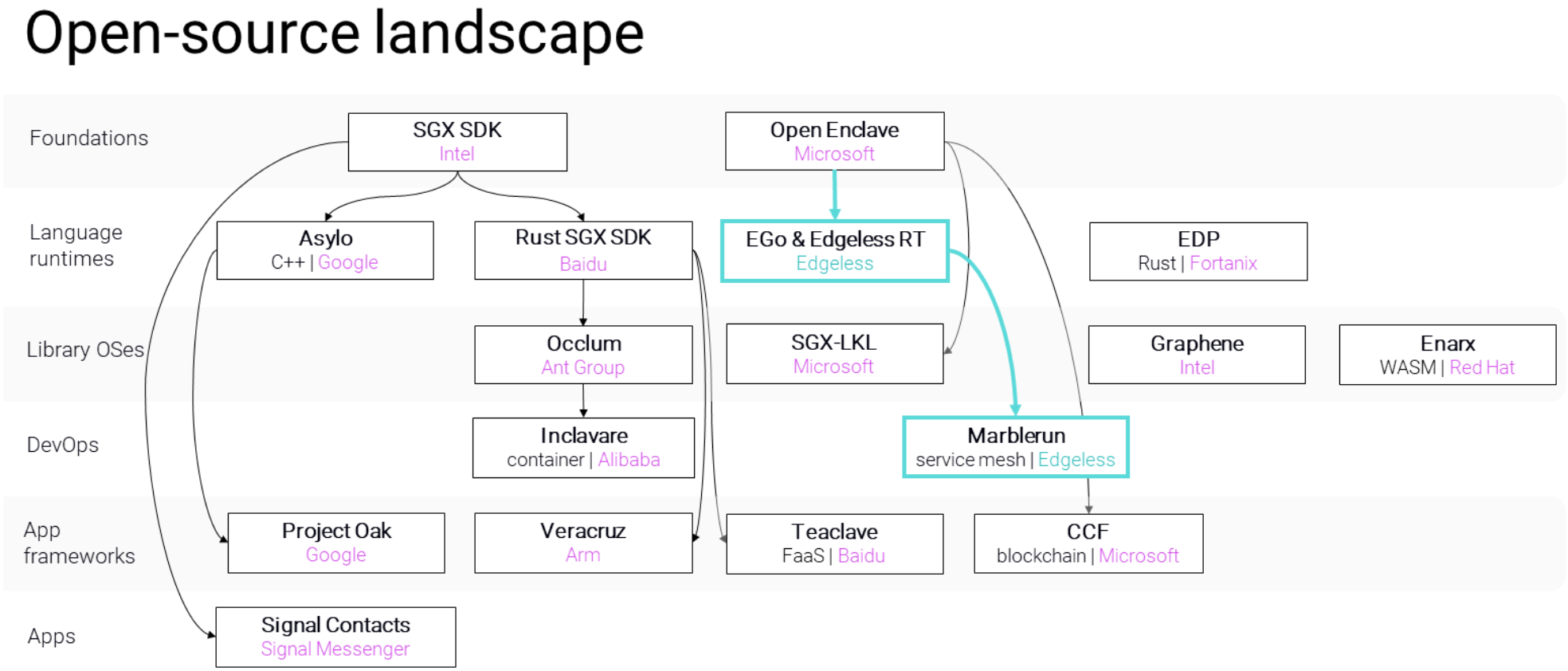
Anonifyはプライバシーを保護した上で、ブロックチェーンを改ざん不可能なデータ共有基盤として用いることを可能にするシステムで、通常のブロックチェーンのように、状態遷移の履歴を平文のまま記録するのではなく、TEE（Trusted Execution Environment）を通して、暗号化された命令データをブロックチェーンに記録していくとのことだ。

AIST CPSEC | Cyber Physical Security Research Center

TRASIO

今後の方向性予想(Confidential Computing のプロジェクト)

- The open-source landscape of confidential computing in 2021より
  - https://medium.com/edgelesssystems/the-open-source-landscape-of-confidential-computing-in-2021-7f847ebfc0a9



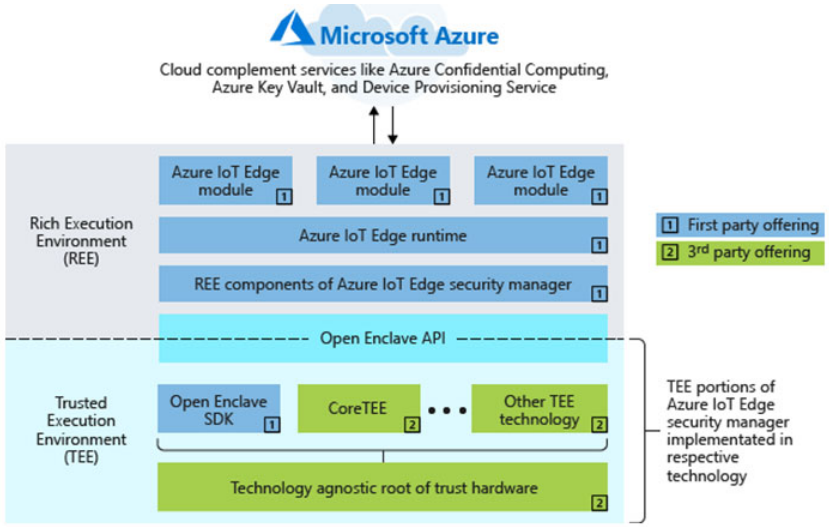
今後の展開(2/2)

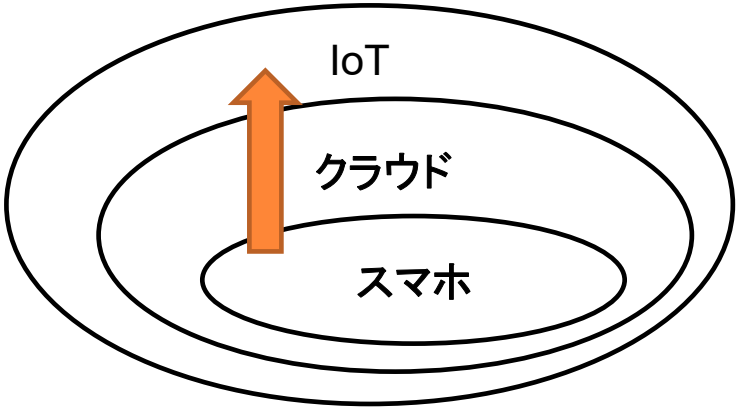
- クラウドからIoTへ
  - ルネサスのR-CarではArm TrustZoneを使うことを宣言している。
  - Arm PSA: Platform Security Architecture はコントローラ(Cortex-M)志向?
  - Microsoft Azure IoT, Azure Sphere
    - https://azure.microsoft.com/en-in/blog/simplifying-confidential-computing-azure-iot-edge-security-with-enclaves-public-preview/ より

Simplifying confidential computing: Azure IoT Edge security with enclaves – Public preview

Posted on 19 November, 2018

Eustace Asanghanwa, Principal Program Manager, Azure IoT





TEEの広がり

TEE関連組織・規格

- GlobalPlatform
  - TEE関係のAPI規格。スマートフォンで採用が多い。
  - SESIP: Security Evaluation Standard for IoT Platforms
- CCC: Confidential Computing Consortium
  - Linux Foundationプロジェクト
- TCG: Trusted Computing Group
  - TPMの仕様を作成している組織。
- Arm PSA(Platform Security Architecture) Certificate
- IETF Protocol
  - TEEP: Trusted Execution Environment Provisioning
  - RATS: Remote Attestation Procedures
  - SUIT: Software Updates for Internet of Things

- 規格争い
- 主導権争い

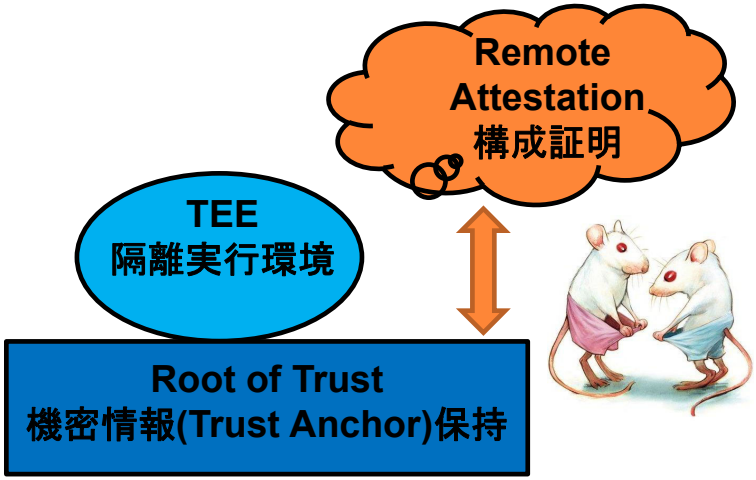
AIST CPSEC | Cyber Physical Security Research Center

TRASIO

まとめ

- TEEとは
  - 隔離実行環境
- Root of Trustとは
  - 信頼の基点で機密情報保持
- Remote Attestationとは
  - 構成証明

- 現状は色々な実装があって相互運用が難しい。しかし、実用化は多方面で進んでいる。



謝辞:この成果は国立研究開発法人新エネルギー・産業技術総合開発機構（ＮＥＤＯ）の委託業務（JPNP16007）の結果得られたものです。