

# 7. SGX Fail

Ao Sakurai

2023年度セキュリティキャンプ全国大会  
L5 - TEEの活用と攻撃実践ゼミ



- **SGXのクソ仕様を痛感する。**
- SGXやTEEを、実世界の様々なシナリオで応用する際に直面するさまざまな困難について解説する。

勘弁してくれSGX

# ECALLによるバッファの転送 (1/4)



- Enclave外のAppで**10MB**のバッファを用意し、ECALLでその**バッファをEnclave内にロードするプログラム**を実装する
  - バッファの型は**uint8\_t\***型が良い
  - バッファはAppにおいてnew演算子等で確保する
  - バッファの内容は**全バイト'A'**とする。**memset**を用いると楽
  - EDLのポインタ方向属性を[in]にしてEnclaveに全バイト読み込む
  - Enclave設定XMLを編集し、**Enclaveヒープサイズを10MB以上** (余裕を見て**20MB程度**) 確保するようにする
- 実行はローカルで良い (RA不要)

# ECALLによるバッファの転送 (2/4)



- このタイミングでわざわざ出しているのだから上手く行くはずがない
- 恐らく **Enclave** が **正体不明の死** を迎え、ゼミで提供しているSGXステータス表示関数を使うと以下のように出るはずである：

```
Execute ECALL.
```

```
=====  
SGX_ERROR_ENCLAVE_CRASHED  
The enclave has crashed.  
=====
```

# ECALLによるバッファの転送 (3/4)



- この事象は、**ECALLやOCALLの際、境界を跨いで引き渡すバッファを一度内部のスタックに格納する**という暗黙の仕様が存在する事により発生する
  - 当然開発者リファレンスに書かれていない
- このスタックは上限が**8MB**であるため、**それを超えるバッファを渡した瞬間にEnclaveが即死**する

# ECALLによるバッファの転送 (4/4)

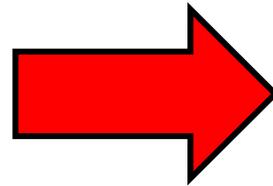


- このスタックサイズは**OSの設定に依存**するため、特権で **ulimit** コマンドを使用する事などで無制限には出来る
  - ただし、自作のSGXアプリを自分だけが使うのであればともかく、例えばサービスとしてSGX依存の機能を提供する場合、**スタックサイズを安易に無制限にするのは潜在的なリスクが大きい**
- 行儀の良い方法で対応するのであれば、**大容量バッファ**を受け渡す際は**8MB未満に分割**して送信するしかない



- この中で整数型 (uint16\_t, uint32\_t, uint64\_t)をtypedefしたものはどれか？

```
sgx_isv_svn_t  
sgx_prod_id_t  
sgx_spinlock_t  
sgx_misc_select_t  
sgx_ra_context_t  
sgx_enclave_id_t  
sgx_time_t
```



**全部**

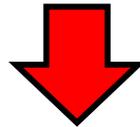


- シーリング (暗号化)を行う関数

```
sgx_seal_data(0, NULL, plain_len, plain,  
sealed_size, sealed_data);
```

- アンシーリング (復号)を行う関数

```
sgx_unseal_data(sealed_data, NULL, 0, plain,  
plain_buf_size);
```



**当たり前のように順序が逆**

# SGXの悪しき文化 (3/4)

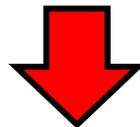


- 様々な機能制約 (Enclave内プログラム)
  - システムコール、一部標準関数、動的ライブラリの禁止
- SGXSDKの煩雑な仕様
  - 使い勝手の悪い独自のAPI・型
  - ある論文「412行の非SGXプログラムをSGX化したら3523行になった」
  - 不親切な公式仕様書、Intelの謎の隠蔽体質
- 「境界管理」の概念
  - 自分が扱おうとしているデータが、Enclave内外のどちらにあるのか
  - 保護境界をまたぐ関数の定義言語の複雑さ



- EDLファイルにおける或る記述

```
public sgx_status_t store_vcf_contexts(sgx_ra_context_t context,  
[in, size=vctx_cipherlen]uint8_t *vctx_cipher,  
size_t vctx_cipherlen, [in, out, size=12]uint8_t *vctx_iv,  
[in, out, size=16]uint8_t *vctx_tag,  
[in, size=ivlen]uint8_t *iv_array, size_t ivlen,  
[in, size=taglen]uint8_t *tag_array, size_t taglen,  
[out, size=msg_len]uint8_t *error_msg_cipher, size_t msg_len,  
[out]size_t *msg_cipher_len);
```



**SGXは罪のない人間向けではない**

# SGXはコード安全性を保証しない



- SGX基本編で議論した通り、SGXは基本的にコードに対する保護や検証は一切行わない
- 何らかの理由でコードを守りたい場合、**SGXElide**[2]という研究成果や、Intel公式の**SGX-PCL**[3]は利用できる
  - しかし、前者はIASとはまた別の**第三者サーバを信頼**しなければならず、かつ**RAによるコード検証が事実上出来ない**
  - SGX-PCLは**RAも出来る**が、**Intelによるメンテナンスが放棄されている**

# ARM TrustZoneにおけるケース



- **コード安全性の保証が対象外**であるのは、SGXだけでなく**TEE全般**に対して言える話である
- 例えば**サムスのスマホ**は、スマホ内のTrustZone内のTEE内で動作する**Keymaster TA**において、**暗号鍵導出時に乱数的**でなければならない所を**決定的に行っていた**ため、攻撃により**暗号鍵を抽出されてしまう**という**脆弱性**を発見されている[12]

# Intelの無責任さ (1/2)



- 基本的にIntelは無責任にも程がある
  - **RAのAPIのバージョンが上がる事** (v2→v3) で、IASリクエストの**旧バージョンとの互換性が喪失**[4]
  - 先程の**SGX-PCL**も、**sgx-ra-sample**も**管理を放棄**している
  - そのくせ**ライセンス**だけは**謎のもの**を使用
- Linux-SGXでは、**モニタックカウンタ**等を使用するための**PSEが突然廃止**されたため、Enclave外のデータとインデックスの対応付けをTrustedに行う事ができなくなった
  - あまりに急な出来事に、**コミュニティも狼狽**[5][6][7]
  - 後の攻撃編でも実践する「**シーリング再生攻撃**」の**対処が困難**となった



- 挙げ句の果てには**第11世代以降CoreシリーズCPUからSGXを削除**
  - 今となっては**第3世代Xeonで継続して搭載されているが、当時は完全に削除されると専らの噂となり、大パニックが起きていた**
- いくら**製品や機能として優秀**であっても、**持続可能性に対する信頼性**を損なうと、**ユーザはその企業のサービスを敬遠する**
  - SDGsという単語はIntelにこそ送り付けてやるべき

# SGX (TEE) の秘密計算利用の難しさ

# RAの登場人物の奇妙なネーミング (1/2)



- ところで、RAでは**非SGX側**が**Service Provider**、**SGX側**が**Independent Software Vendor**と呼ばれていた
- しかし、特に**秘密計算的な文脈**では、SP (**サービス提供者**) の方が**SGX側**なのでは？ という感覚がある
- また、ISV (**独立ソフトウェアベンダ**) というのも、**一体何を意味しているのか釈然としない**

# RAの登場人物の奇妙なネーミング (2/2)



- SGXが本来想定していた利用モデルは、**秘密情報を有するサーバ**が、**SGX対応クライアントにEnclaveを配備**し、それをRAで**検証**してから**Enclaveに秘密情報を送る**というモデルであった
  - PowerDVDでのDRM処理の利用例がまさにこのケース
- つまり、**秘密情報を有する主体 (SP) 自身が、Enclaveイメージを生成してISVに配備**し、「**本当にISVは自分が作ったEnclaveを動かしているか?**」をRAで**検証**している
  - よって、SPは**予め控えておいたMRENCLAVEとQUOTE内のそれを比較**し、何の問題もなく検証する事が出来る

# 秘密計算モデルでのRAの致命的な欠点 (1/3)

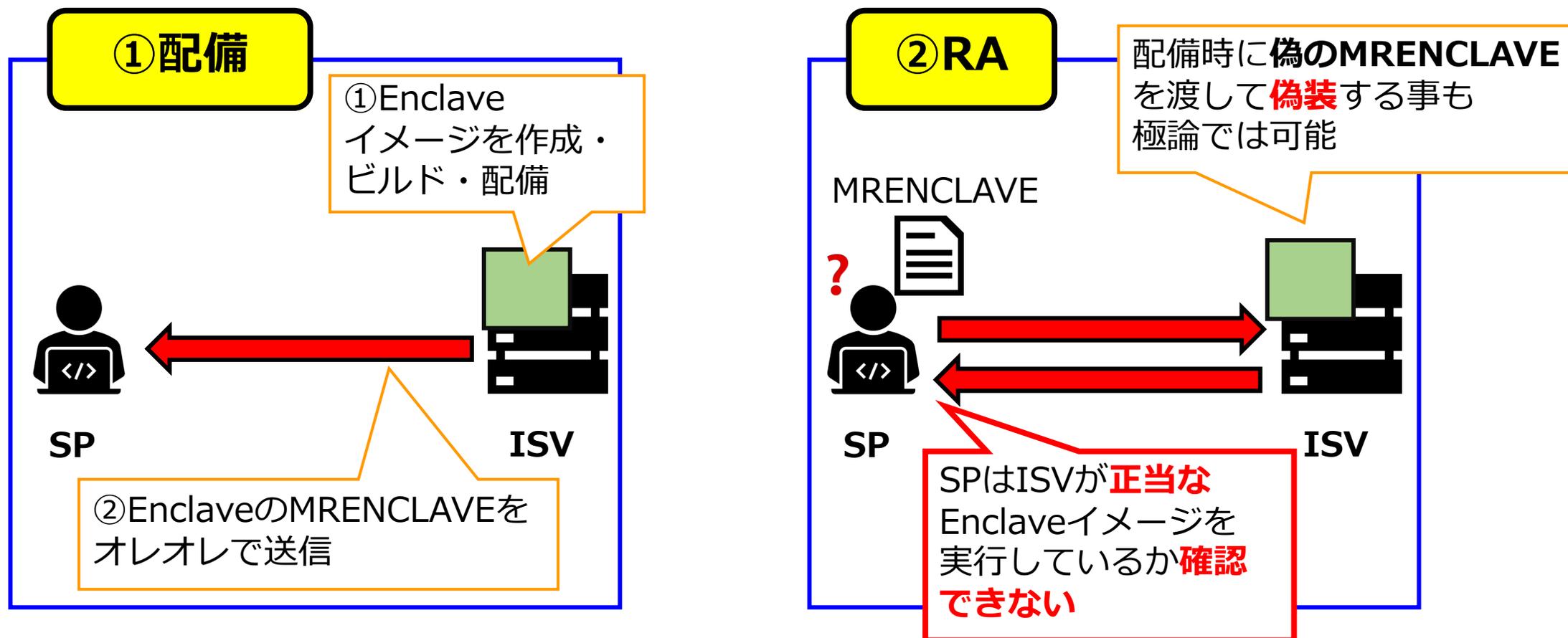


- しかし、サーバ側がSGX機能を提供する秘密計算モデルの場合、このRAは致命的な欠陥を抱えている
- SGXサーバ (**ISV**) 側が**Enclaveコードを作成**し、それに基づくEnclaveを**ISV自身に配備**する場合、**SP**はどうやってそのEnclaveの**MRENCLAVEを検証**するのか？
- **作成・ビルド・配備全てがISVで完結してしまっている**ため、例え**ISVからMRENCLAVEを受け取り**それに基づいてRAをしても、そのMRENCLAVEは**オレオレMRENCLAVE**でしかない

# 秘密計算モデルでのRAの致命的な欠点 (2/3)



- つまり、秘密計算モデルでは例えRAを使っても、**相手のEnclaveの同一性を検証しようがない**という**致命的な欠点**を抱えている



# 秘密計算モデルでのRAの致命的な欠点 (3/3)



- 一見、**SP側でもSGX環境を用意し**、そこでEnclaveイメージを**ビルドしてMRENCLAVEを検証**するという手も考えられる
- しかし、MRENCLAVEは署名前**Enclaveイメージ (=コードだけでなくコンパイラ等にも依存)** や**SGXSDK**等にわずかでも差があれば**値が変わる**ため、ISVと**同一のものを導出出来ない事も多い**



## ■ SPがEnclaveを作成し、ISVに配備する

- この方法であれば本来の利用モデルと合致し、RAで検証できる
- しかし、Azure等で自分で勝手にSGXアプリを作って動かす（PaaS的運用）ならともかく、クライアントにやらせている時点で**SaaSとしての運用が成立しない**
- そもそも、**この地獄のSGXプログラミングをユーザに強制するのはですか？**
  - **そのような非人道的な真似は私が許さん**



## ■ 運用で改善する

- ユーザにEnclaveを開発させるのは非人道的なので、**ユーザにSGX環境を用意させ、EnclaveのビルドだけSPに行わせる**
  - コードは**サービス提供側**（紛らわしいが**ISV**）が**提供する**か、**OSSから持ってくる**などをする
- これであれば、ユーザである**SP**は少なくとも**コーディングはしなくて良い**運用になる
- しかし、結局SPはその**コードの正当性**を**目視で確認**しなければ、その**Enclaveを信頼する事は出来ない**
  - **Enclaveコードを目視検証しなければならぬ時点で地獄**



## ■ ISVでビルドされたEnclaveイメージを逆アセンブルする

- **正気か？**
- 例え署名済みEnclaveイメージでもコードは前述の通り**保護**されないため、**逆アセンブルで動作定義を検証**する事は**理論上は可能**である
- 誰かしらに課す**拷問として利用**するのであればおすすめ



## ■ CAからコード一式のデジタル証明書をもらう

- ソースコードやEnclaveイメージ、MRENCLAVE等の一式に対する**コードサイニング証明書**を**CA（認証局）**からもらう方法
- 公開鍵基盤という**脆弱な神話に甘える**方法なので、そもそもTEE的には**思想面でも好ましいとは言えない**
- さらに、このようなCAによる電子証明書は一般的に**年単位のスパン**である事が多いので、比較的**頻繁に更新の入る**Enclave周りの要素とは**絶望的に相性が悪い**



## ■コンテナで検証する

- ISVと全く同じ環境を**コンテナ**で**SP**に提供し、そこでビルドして**MRENCLAVE**を検証するアプローチ
- コードは勿論、**コンパイラ**や**OS**レベルで**統一**できるので、  
解決策候補の中では**最も現実的**
- コンテナが**そもそもSGXSDKを偽装していないか**等の検証は  
**別個必要**になる

# TEEの秘密計算利用の難しさ



- このように、秘密計算モデルにおいてTEEをSaaS的に応用する場合、RAの根本的な設計に由来する困難がつきまとう
- これはAWS Nitro Enclaves等の**他のTEEにも共通する議論**であり、以下のように**何かしらの妥協の線引**を行わないと運用は難しい
  - ISVの提示するMRENCLAVEを全面的に信用する
  - 前述のようにSPがコードを受け取りビルドし、そのEnclaveイメージをISVに配備する、PaaSとSaaSの間のような運用を行う
  - コンテナを検証するか無条件で信頼する前提で、コンテナによるMRENCLAVEの検証の手法を行う

SGX Fail



- **SGXの運用**における、Intelの想定とユーザの実態、言い換えれば**理想と現実の乖離**に伴う**致命的な破綻**を糾弾している論文
  - 2022年に発表された、比較的新しい論文である
- 以下のような、**SGXの運用に伴うジレンマ**やそれに由来する**実世界での破綻例**を紹介している
  - マイクロコードアップデート (TCB Recovery) のタイムライン
  - Enclave開発者のジレンマ
  - **実世界での破綻例** (PowerDVD、SECRET Network)
  - IASに対するSigRLを悪用した潜在的なDoS攻撃

# マイクロコードアップデートのTL (1/5)



- **TCB Recovery**には通常マイクロコードアップデートが伴うが、これは**BIOS (UEFI) アップデート**の形を取る
  - ちなみに、マイクロコードアップデートは恒久的に適用されるのではなく、マシンの起動の度にパッチを当てる方式になっている[8]
- BIOSアップデートはその**マザーボードのベンダ**から**配布される**ため、**ベンダが提供してくれないとユーザはマイクロコードアップデートによる修正を一切受けられない**

# マイクロコードアップデートのTL (2/5)



- SGX Failは、6つのHWベンダについて、**Intel**によりマイクロコードアップデートが公開されてから**何日でBIOSアップデートを提供**しているかを調査している
  - ASRock、Dell、HP、Lenovo、MSI、Gigabyte
- **SGXの脆弱性に対応**するような**BIOSアップデート**については、最短で**中央値25日** (HP)、最長で**中央値125日** (Lenovo) と、リリースまでに**非常に時間がかかっている**事が判明した

# マイクロコードアップデートのTL (3/5)



引用 : SGX Fail[8]

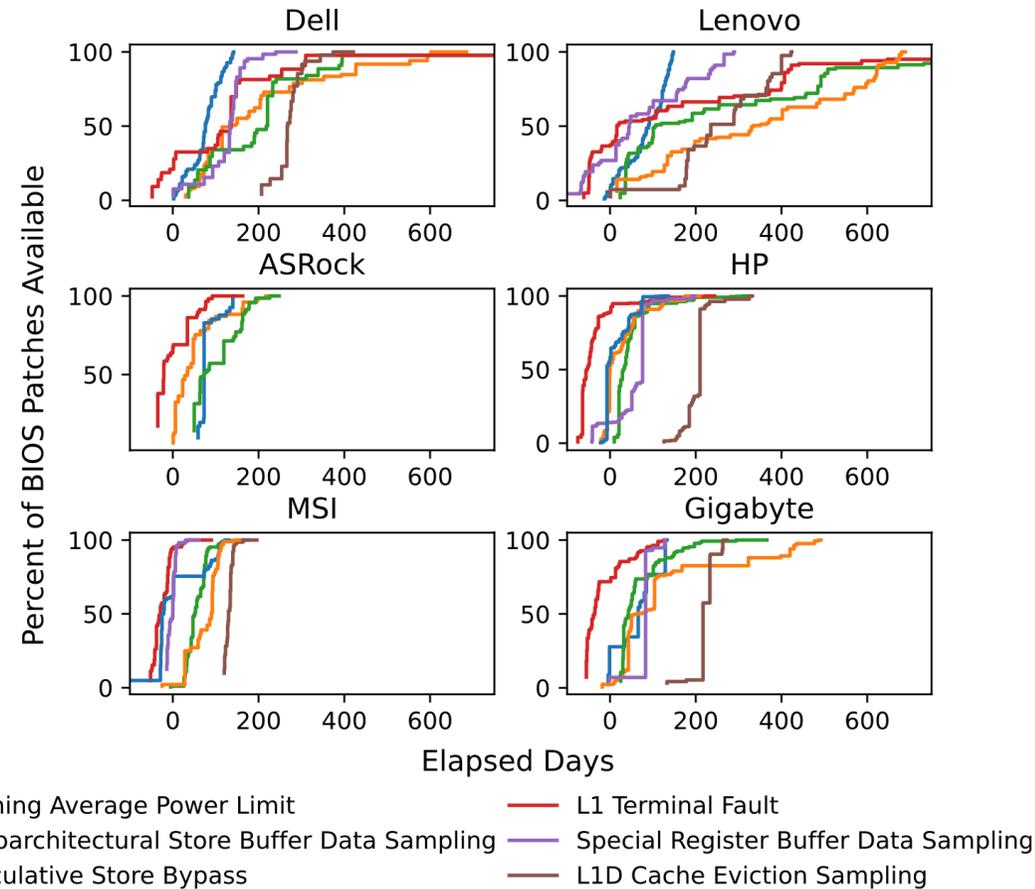


Figure 2: Time Taken To BIOS-Patch Major SGX Vulnerabilities After They Are Made Public

# マイクロコードアップデートのTL (4/5)



- SGX向けでない**一般的なBIOSアップデート**の場合、最短で**中央値37日** (HP、MSI)、最長で**中央値329日** (Lenovo) となっている
  - AMDでのBIOSアップデートの場合、**Lenovoの中央値は1043日**
- そもそもBIOSアップデートはOSアップデートのように**頻繁に行う前提**とはいいがたく、しかも**マザーボードを損傷させるリスク**もあるため、SGX脆弱性対応のような**迅速な修正**との**相性が致命的に悪い**

# マイクロコードアップデートのTL (5/5)



- さらに、Azure含むクラウドベンダが提供しているSGX対応VMの場合、HWベンダから配布された**BIOSアップデートをクラウドベンダが適用**するまでにも**また時間がかかる**



- 実はこのゼミのRAの実装でも**既にこのジレンマに遭遇している**
- Humane-RAFWのデフォルトの実装では、IASからの応答の内 **SW\_HARDENING\_NEEDED** については**看過するようにしている**
  - Azureがパッチを当てていないため
- このように、RAの受理条件を決める上で、**どこまで許すかにより発生するトレードオフにEnclave開発者は苛まれる**

# Enclave開発者のジレンマ (2/3)



- IASからの応答が**OKである場合のみ受理**するのが理想ではあるが、**現実問題**としてそのように**丁寧に最新化しているマシンは少ない**
  - 先程の**BIOSアップデートの危険性**や**適用頻度**の議論も関連する
  - 例えば**9割のマシンがRAで弾かれてしまっ**ては、製品として**UXが最悪**となり、**お話にならない**
- かと言って、**条件を緩くしすぎるとその分膨大な量の脆弱性を看過**する事になり、結果として**SGXシステムの致命的な破綻に直結**してしまう
  - **PowerDVDの破綻例**がまさにこのケース



- マイクロコードアップデートに限らず、例えば**SGXSDK**についても、**平然と互換性を喪失させる**ようなアップデートをねじ込んでくる**Intelの無責任さ**も看過できない
  - **PSEの突然の削除**による**モニタリングカウンタ**や**信頼可能時間ソースの剥奪**が顕著な例



- **SECRET Network** : スマートコントラクトの実行をSGXのEnclave内で行い、**トランザクションも暗号化する事**を特長としている**ブロックチェーン**の1つ
  - **スマートコントラクト** : ブロックチェーン上での**処理・取引**を行うに当たって**自動実行されるプログラム**。例えばスマートコントラクトによる**検証の結果、特定の条件**を満たし**取引が許可された場合のみ**実際に自動的に取引が行われる、等の運用が出来る
  - **トランザクション** : そのブロックチェーン上における**取引履歴**の事。ブロックの中身そのものでもある



# SECRET Networkの破綻例 (2/9)



- SECRETでは、前述の様々な保護機能で使用する鍵は、全て親玉（**マスター秘密鍵**）である**コンセンサスシード**から導出される
- スマートコントラクトへのメッセージ送信時は、ユーザは**コンセンサスシード**から導出した**公開鍵**を用いて**暗号化**し、その**暗号文**を**トランザクション**に含める
  - 一方、**秘密鍵**は**MRSIGNERポリシーのシーリングデータ**として、チェーン全体に複製（デプロイ）される
- また、口座残高等の現在の状態を暗号化する鍵もまた**コンセンサスシード**から導出される



- 当然、この**コンセンサスシード**が**万が一にも漏洩**すると、SECRETが売りにしている**あらゆる保護機能が無力化**される
- さらに、このコンセンサスシードは原則として**永続的かつ不変**のものであるため、もし漏洩すると**極めて面倒な事になる**
  - **ブロックチェーンそのものを分裂**させなければならない**ハードフォーク**でのみ対応する事が出来る



- コンセンサスシードは、独自に用意した鍵により **Intel Protected File System Library** (以下、IPFSL) を用いて128bit AES/GCMで暗号化され**Enclave外にストア**される
- **IPFSL : SGX\_FILE**型という**Enclave内**で直接扱えるようなFILE構造体に基づき、**暗号化した状態でのファイル入出力** (sgx\_fopen等) を提供する機能
  - Enclave内から**直接Enclave外に保存**できる、**暗号化鍵を指定**できる等の部分でシーリングと異なる
  - 本ゼミでは使用していないが、includeとリンクさえ行えば普通に**デフォルトのSGXSDKで利用可能**



- IPFSLでコンセンサスシードを暗号化する際に使用した鍵は  
**シーリングでストア**される
  - 鍵自体はAESで使う普通の128bitの共通鍵
- SGX Failでは、この**IPFSL用の鍵**がEnclave内で**コンセンサスシードの暗号化及び復号**に**使用されている最中**に**攻撃を仕掛け**、IPFSL用鍵を抽出する手法を選択した
  - **IPFSL鍵が漏れる**と簡単に**コンセンサスシードが復号**出来てしまい、**SECRET上のあらゆる秘密情報が究極的には暴かれてしまう**



- ノード初期化関数でコンセンサスシードを復号し初期化する際に発生する、IPFSL鍵の**AES鍵伸長処理**に対し、**ÆPIC Leak**攻撃を仕掛けた
  - ÆPIC Leakの詳細は攻撃編セクションで解説
  - 鍵伸長処理への到達の特定には、これまた攻撃編で解説する**Controlled-Channel Attacks**で提案された手法を用いている
- ÆPIC Leakにより得られた**IPFSL鍵の断片情報**から、一般的かつ容易な手法で**IPFSL鍵を完全に復元**し、**コンセンサスシードを復号し取得**する事に成功している
  - 断片情報からの復元方法についてはここでは割愛。SGX特有の要素は一切存在しない一般的なものである



- コンセンサスシードが漏洩してしまうと、所有する個人だけで閲覧し楽しむNFTである**プライベートNFT**まで**暴露出来てしまう**
  - 画像はSGX Failより引用



Figure 5: Example NFT that we created and then decrypted.



- 同様の方法により、ÆPIC Leakによってそのノードの **Attestationキーの抽出**にも成功している
- SGX Failの論文執筆時点で、前述した**唯一の回復策**である **ハードフォークの実施**をSECRETは計画している
- **応急措置**として**危険なノードからのコンセンサスシードの削除**等が行われている
- しかし、**ゼロデイ的かつステルスに世界の誰かが既にこの攻撃を仕掛けたかも知れない**という、非常に**疑心暗鬼的かつ苦しい状況**に **SECRETを陥れる結果**となっている



- SECRETの事例は、**Intelが脆弱性を開示**してから、実際に**マイクロコードアップデートを頒布**するまでに**ラグがある**という**運用上の問題を浮き彫りにしている**
  - **ÆPIC Leak脆弱性開示**が2022/8で、論文執筆が2022/10周辺であり、**TCB Recovery**は2022/11末
  - 元々は**TCB Recovery**は2023/3予定であったため、**SGX Fail**の報告を受けて早回しにした形となっている
  - 仮に**TCB Recovery**が展開されても、前述の**ベンダ**による**展開速度の問題**や**ユーザがそれを適用するか**という**問題**が依然つきまとう



- **PowerDVD** : Cyberlinkが提供している動画再生PCソフト。  
Ultra HD Blu-ray Disk (**UHD-BD**) の再生時に、**SGX**によって**デジタル著作権管理**を行っている事で知られている
- UHD-BDディスクの内容は**AACS2鍵**という**専用のAES鍵**で暗号化されており、**AACS2**というアルゴリズムに従って内容を復号し再生する
  - AACS2は**ディスクの内容を暗号化**するための**コピーガード**であって、再生処理中の**メモリ上の映像データを保護**するものではない点に注意



- UHD-BDを再生するSGXマシンは、PowerDVDの提供する**CLKDE** (CyberLink Key Downloader Enclave) を起動し、Cyberlinkの**AACS2鍵プロビジョニングサーバ**により、**CLKDEを検証するRA**が実行される
  - 鍵を提供する**サーバがSP**、再生する**クライアントがISV**である、SGXの元々の利用モデルに見事に合致している運用例である
- **RAに成功**すると、Cyberlinkの**プロビジョニングサーバ**は**AACS2鍵**を**CLKDEにデプロイ**し、CLKDEは**MRSIGNERポリシー**で**AACS2鍵をシーリングし保存**する
- UHD-BD再生時は、この**AACS2鍵で内容を復号し再生**する



- 逆に言えば、AACCS2鍵はこの世のあらゆるUHD-BDを復号できる鍵であるため、これが漏洩するとどのマシンだろうが**全てのUHD-BDの内容を復号**出来てしまう
  - これに対応するにはその鍵を**失効**させなければならないが、**既存のUHD-BDのセキュリティを回復させる事はできず**、漏洩した鍵の**失効後に製造されるUHD-BDでセキュリティ保証を回復させる事**しかできない
- にも関わらず、PowerDVDはIASからのRA応答でも**一番許してはいけない類のステータスであるGROUP\_OUT\_OF\_DATEをも許容する実装**となっている



- SGX Failでは、GROUP\_OUT\_OF\_DATEであるようなマシンに対し**Foreshadow**攻撃を仕掛けて**Attestationキーを抽出**した
  - Foreshadowの詳細は攻撃編で解説
- 抽出したAttestationキーを用いて、**REPORTの検証をスキップ**し**任意のMRENCLAVE/MRSIGNERで差し替えた偽造REPORT**に対し**EPID署名**する、**偽造QE**を実装している
- これを中心に、SGXの**Enclaveの動作を全てEnclave外でエミュレート**する、Emulated Guard Extensions (**EGX**) ということんでもない**SGXエミュレータ**まで実装している



- EGXにおける**偽造QE**で偽造されたQuoteは、Cyberlinkによる**正規のMRENCLAVE/MRSIGNER**を含むように**改竄**しているため、CyberlinkのAACCS2プロビジョニングサーバはそれが**正当**であると誤認して**AACCS2鍵を送信**する
- しかし、EGXは実際には**Enclave外で動作**するため、**全く保護**されていないメモリ上に**AACCS2鍵が提供されてしまう**事になる
  - AACCS2鍵が手に入れば、**SGX**どころか**Intel CPU**ですらないマシンでも**UHD-BDの内容を任意に復号**出来てしまう
- そして、本来公開されてはならないAACCS2アルゴリズム自体も論文中の攻撃により**解読され暴露**されてしまっている



- 言うまでもなく、**GROUP\_OUT\_OF\_DATE**を許容していた事が原因
  - RAから返ってくる応答の中でも**最も許可してはならない**類の応答
- しかし、一般的に製品の**ユーザの殆ど**は**非技術者層**であり、**安全性**よりも**有用性を圧倒的に重視**する
  - 何なら、ユーザからしてみれば**コピーガード**含む**DRM**はユーザからしたら**邪魔**でしか無い



- **有用性が落ちるとユーザはPowerDVDを購入してくれなくなる**ので、**非常に条件の厳しいOK応答だけを通す**設定にするのは、**商業的には論外**である
- このように、**安全性と有用性のトレードオフ**の末に、本来のSGXの安全性を損なってしまう (**how Stuff Gets eXposed**) 極めて**苦しい選択**を、**大衆向け商用展開**では迫られてしまう
  - その意味では、前述の通り本来SGXの想定していない**秘密計算モデル**の方が、こういったトレードオフ問題は**サービス提供側** (サーバ) で**対処できる**ので解決しやすい

# SGXキー漏洩時の対応



- **SGXの安全性は、Enclave内で導出される様々な鍵が漏洩しない前提のもとに成り立っている**
- しかし、2023年現在となっては数多くの攻撃により、例えば **レポートキー** や **Attestationキー** が抽出されている

# SGXキー漏洩時の対応 (2/3)



- レポートキーが漏洩すると、**SECS**によって保証されていない**任意のMRENCLAVE等**に対する**REPORT**を**Enclave外で偽造**出来るようになってしまう (**EREPORTの迂回**)
  - **LA及びRAの検証者を騙す**のに悪用可能
- Attestationキーが漏洩すると、**任意のREPORT**に対して署名して**偽造QUOTE**を生成し、あたかも正当なEnclaveであるかのように**IASを騙す事**が出来てしまう (**QEの迂回**)
  - IASは**気付かずにQUOTEは改竄されていない**という応答を返してしまう
  - **RAの検証者を騙す**のに悪用可能



- これらは、**TCB Recovery**を行う事でいずれも対処できる
  - レポートキーは**CPUSVN**（マイクロコードバージョン等を材料に導出）に依存して生成される[9]ため、TCB Recoveryで**マイクロコード更新**を行えば**鍵が変わり偽造不可**となる
  - TCB Recoveryの際は、**再プロビジョニング**によりAttestationキーを更新するため、QUOTEも**偽造不可**となる
- では、**上記の鍵が漏洩**しているにも関わらず「**TCB Recoveryを実施しない**」という選択を取る**悪性のSGXマシン**をどのように識別しているのか？

# レポートキーのみ漏洩した場合



- レポートキーのみの漏洩の場合、そのマシンの**AttestationキーによるEPID署名**を**SigRL**に登録してもらう事で対処可能
  - これらの鍵漏洩時のどのシナリオにも共通するが、基本的に**Intelに頼んで失効リストに登録してもらう**しか無い
- **QUOTE**には**REPORT**の他に**EPID-GID**も含まれており、かつ**SigRL**はこの**GID**に紐づいているので、仮に**SigRLを無視して署名チャレンジを無視**すると**一発でバレる**
- ISVが**正常にSigRLを処理**（**Basename**に対する**EPID署名**）した場合、その**EPID署名がSigRLのブラックリスト**に引っかかり**検知**できる

# Attestationキーのみ漏洩した場合



- Intelに依頼し漏洩したAttestationキーをPrivRLに登録させる事で対処可能
- PrivRL上の鍵による署名とQUOTEの署名を比較し、一致したら失効済みなので、IASはRA応答としてKEY\_REVOKEDをSPに返却する[10]
- こうなるとISVはTCB Recoveryを行う以外にSPを信頼させる手段が存在しなくなる

# レポートキーとAttestationキー双方が漏洩した場合



- この場合も漏洩した**Attestationキー**を**PrivRLに登録**する事で対処可能である
- この場合レポートキーは、**Attestationキー**を**再プロビジョニング**すると**TCB Recovery**で**マイクロコードも更新**されている事になるので、**CPUSVNの変更**により**漏洩したものは使用不可**になる
- 全てのシナリオにおいて起こりうる議論であるが、**收拾がつかないレベル**で**多発的に侵害が発生**した場合、**GroupRL**による**グループ全体の失効**が行われる

# Linkable v.s. Unlinkable

# Unlinkableは万能なのか？



- QUOTEタイプが**Unlinkable**だと、各**Attestation**キーを**特定する事が出来ない**ため、**EPIDの本来の匿名化機能**の恩恵にも預かれて**安全そうな印象**がある
- しかし、実は**Unlinkable**はメリットよりも**デメリットの方が大きい**

# Unlinkableの欠点 (1/3)



- そもそも、**Attestationキーが匿名性を持つ事で得をする状況はSGXではあまり存在しない**
  - **DRMモデルの場合**：同一Attestationキーの署名だとバレても、QUOTE同士の識別以外に**漏れる情報が存在しない**
  - **秘密計算モデルの場合**：**SGXサーバが匿名性を持つ事によるメリットがほぼ存在しない**（強いて挙げててもライセンス剥奪対策くらい）
- その上、**Unlinkable**ではその性質上、**同一EPIDグループ内の鍵による署名がただ1つでもSigRLに登録されると、そのEPIDグループ内のAttestationキーによるUnlinkableなQUOTEは全て巻き添えで拒絶**させられてしまう

# Unlinkableの欠点 (2/3)



- SigRLで**無実のUnlinkableなAttestationキー**が**巻き添えを食らう**のは、**署名からでは鍵を識別できない**が故に、**その署名を生成し得るUnlinkableな鍵全てを失効させなければならない**ため
  - 事実上GroupRLによる失効なみの大惨事である
- PrivRLの場合、**固定値**（同一のBasenameに同一の乱数を足したもの）**に対する署名を検証**するため、**事実上Linkableな検証**となり、**無実なUnlinkable鍵は巻き添えにならない**

# Unlinkableの欠点 (3/3)



- この事から、デフォルトでは**SGXにおいてはLinkable**とする事が**Intel**によっても**推奨されている**[11]
- Unlinkableによる匿名性を明確な利点の宣言無しに標榜して非技術者層を誘導したいわけでもなければ、**原則としてLinkable**とする方が、**システム運用面では安全**である
  - **巻き添えで失効**させられてサービスが止まっては**可用性が壊滅**するため

# 本セクションのまとめ



- 様々な観点及びレイヤから、SGXやTEEの抱える数々の難しさについてある程度詳細に議論した
- このセクションの内容は直接コーディングスキルに紐づくものではないが、SGXやTEEを用いたシステムのセキュリティ設計を行う上では極めて重要なものとなっている



[1]“Segfault While passing a big data through an Ocall #376”, GitHub, <https://github.com/intel/linux-sgx/issues/376>

[2]“SgxElide: Enabling Enclave Code Secrecy via Self-Modification” by Erick Bauman et al., <https://web.cse.ohio-state.edu/~lin.3021/file/CGO18.pdf>

[3]“linux-sgx-pcl”, GitHub, <https://github.com/intel/linux-sgx-pcl>

[4]“Error 400 from IAS for Quote Attestation Request #27”, GitHub, <https://github.com/intel/sgx-ra-sample/issues/27>

[5]“SealedData example missing Platform Service capability”, GitHub, <https://github.com/intel/linux-sgx/issues/541>

[6]“The delay attack towards the trusted time”, Intel, <https://community.intel.com/t5/Intel-Software-Guard-Extensions/The-delay-attack-towards-the-trusted-time/m-p/1343497#M5056>

[7]“No longer compatible with SGXSDK v2.8 or newer version #48”, GitHub, <https://github.com/intel/sgx-ra-sample/issues/48>



[8]“SoK: SGX.Fail: How Stuff Gets eXposed, by Stephan van Schaik et al.,  
<https://sgx.fail/files/sgx.fail.pdf>

[9]“SgxPectre Attacks: Stealing Intel Secrets from SGX Enclaves via Speculative Execution”,  
Guoxing Chen et al., <https://arxiv.org/pdf/1802.09085.pdf>

[10]“Attestation Service for Intel® Software Guard Extensions (Intel® SGX): API Documentation”,  
Intel, <https://api.trustedservices.intel.com/documents/sgx-attestation-api-spec.pdf>

[11]“SGAxe: How SGX Fails in Practice”, Stephan van Schaik et al.,  
<https://sgaxe.com/files/SGAxe.pdf>

[12]“Trust Dies in Darkness: Shedding Light on Samsung’s TrustZone Keymaster Design”, Alon  
Shakevsky et al., <https://eprint.iacr.org/2022/208.pdf>