SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

Intel SGX における 2 つのリモートアテステーションの利点と欠点の考察
A Discussion of the Advantages and Disadvantages of Two Remote Attestations in Intel SGX

矢川 嵩 *† Yagawa Takashi
照屋 唯紀 † Teruya Tadanori
須崎 有康 † Suzaki Kuniyasu
阿部 洋丈 * Abe Hirotake

キーワード ハードウェアセキュリティ，リモートアテステーション，Intel SGX，TEE

あらまし

リモートアテステーションは，デバイスの管理や操作を目的とした遠隔操作の際にデバイスやデバイス上のソフトウェアの健全性を確認できる仕組みのことである．Intel Software Guard Extensions(SGX) は，隔離実行環境である Enclave で信頼できるアプリケーションを実行する際に，複数のリモートアテステーションに対応している．しかし，それらを比較した際の利点と欠点は明確になっていない．本稿では，この SGX のリモートアテステーションについての比較を行い，それぞれの利点と欠点について考察する．

Intel SGX

Intel SGX は，Intel 第 6 世代 CPU 以降で利用可能な Intel CPU の拡張機能であり，Trusted Execution Environment(TEE) の一種である．SGX を利用することで，Memory Encryption Engine という特別なハードウェアによってメモリの一部を暗号化できる．この暗号化されたメモリ領域は Enclave と呼ばれ，その領域内のデータやプログラムは OS やハイパーバイザ等を利用した特権的な攻撃からも保護される．
SGX はリモートアテステーションに対応しており，ユーザーは遠隔の SGX 対応プラットフォームと Enclave 内のプログラム及びデータの健全性を確認できる．この確認には，SGX 対応プラットフォームが生成する検証用の情報が必要になる．この情報をまとめた構造体は Quote と呼ばれ，SGX 対応プラットフォームに署名される．

2 つのリモートアテステーション

Intel SGX は現在，次の 2 種類のリモートアテステーションをサポートしている．

- Enhanced Privacy ID(EPID) Attestation
- ECDSA Attestation

EPID[1] は Direct anonymous attestation に署名鍵失効についての拡張を加えた暗号化アルゴリズムであり，これによりプラットフォームの匿名性を保ったままでのリモートアテステーションが可能となる．
ECDSA Attestation は，プラットフォームの匿名性を強制する EPID では不都合なデータセンター等での利用を想定されている．サードパーティでの Quote の検証も可能であり，これをサポートするために，Intel は Intel SGX Data Center Attestation Primitives(DCAP) と呼ばれるパッケージを提供している．
本稿ではリモートアテステーションに関するいくつかの項目についてこれらの比較を行うことで，それぞれの利点と欠点を明確にする．

参考文献

[1] Simon Johnson, Vinnie Scarlata, et al. ,“Intel Software Guard Extensions: EPID Provisioning and Attestation Services”， INTELCORP，March 2016.

* 筑波大学, 茨城県つくば市天王台 1-1-1, University of Tsukuba, 1-1-1 Tennodai, Tsukuba City, Ibaraki Prefecture
† 産業技術総合研究所, 東京都江東区青海 2-3-26, National Institute of Advanced Industrial Science and Technology, 2-3-26 Aomi, Koto-ku, Tokyo