コンピュータ間におけるデータ移動の機密実行環境を用いた実装の提案

石黒 淳[†1]　新城 靖[†1]

1. 序論

近年，機密実行環境 (Trusted Execution Environment, TEE) の機能を提供するプロセッサが普及し始めている．機密実行環境とは，OS・ハイパーバイザを含む他のすべてのソフトウェアから隔離された実行環境である．クラウド環境において管理者を信頼せずに個人情報や機密情報を安全に処理したり，個人が所有する PC において著作物の不正利用を防ぐなど，機密実行環境には様々な用途が考えられる．

著作物の例のように，データには複製を避けなければならないものがある．同時に，著作物を譲渡したり貸し出す機能を実現しようとする場合などには，原子的に移動したいという要求がある．しかし，このようなデータの移動は容易ではない．ユーザはコンピュータ上のソフトウェアや永続記憶を改ざんしたり任意の時点でプログラムの実行を止めることができるからである．

そこで本研究では，機密実行環境を用いて複製を許さずコンピュータ間でデータを移動するための手法を提案する．本研究では機密実行環境が動作するコンピュータ上のシステムソフトウェアを自由に操作できる攻撃者を想定する．この想定の元で，永続記憶の改ざん，通信に用いるメッセージの複製・破棄，任意のタイミングのプログラムの実行停止といった攻撃を考慮する．さらに提案する手法を用いて，著作物をユーザ間で譲渡できる著作権管理を実装し，提案手法の評価を行う．

2. 目標

本研究では以下の要件を満たすデータの移動を実現することを目標とする．

複製不可能　データの移動は原子的に行われ，移動元と移動先で同時に利用できる状態にならない．

エラーからの回復　通信中にエラーが発生した場合であっても，移動元もしくは移動先において利用可能な状態に回復できる．

†1 筑波大学
Uniersity of Tsukuba

3. 前提条件

本研究では以下を満たす機密実行環境を想定する．

- 機密実行環境毎に固有の鍵を利用できること
- 機密実行環境の内部で動作するプログラムをリモートアテステーションによって外部から検証できること
- リモートアテステーションの際に，機密実行環境と検証者の間で共通の鍵を共有できること

本研究ではこの条件を満たす機密実行環境を，Intel SGX を利用して構築する．また，データを移動する各々の機密実行環境で以下の機能を利用できるものとする．

- 信頼性のあるモノトニックカウンタ
- (信頼性のない) 永続記憶

4. 脅威モデル

本研究では次のような攻撃者を想定する．攻撃者は機密実行環境をホストするコンピュータに対して，OS・ハイパーバイザなどを含む任意のソフトウェアを改変できる．攻撃者は永続記憶を操作して，過去に記録された状態を復元したり，記録された内容を改変することができる．また，コンピュータの電源を意図的に切断したりシステムソフトウェアのスケジューラを変更することによって，機密実行環境で動作するプログラムを任意のタイミングで停止することができる．

5. 提案手法

5.1 概要

本研究では機密実行環境の内部でデータに対して**表 1** に示したような利用可能かどうかを表す状態を紐づける．状態 *0* はデータが利用不可能なことを表す．状態 *1* はデータが利用可能であり，別の機密実行環境へと移動可能なことを表す．その他の状態は移動中の中間状態を表す．データが要求されたとき，状態 *1* の時だけ出力する．

本研究では，機密実行環境の間におけるデータの移動を次のような 2 つの部分に分けて扱う．

データ本体の転送　データの本体を暗号化して送信する．移動先では受信したデータを永続化する．ただし，転

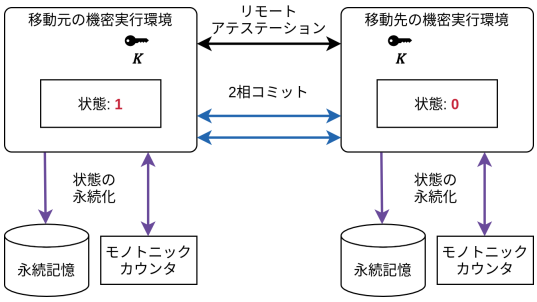

図 1 利用可能状態の変更

送されたデータに対して状態 *0* を紐づけて利用不可能な状態にしておく．

利用可能状態の原子的な変更 各機密実行環境で利用可能状態を変更する．移動先では利用可能な状態へ，移動元では利用不可能な状態へ原子的に変更する．

データの本体を転送する部分については，成功・失敗にかかわらず移動先ではデータは利用不可能になっている．そのため，エラーが起きたときには回復も中止も簡単である．従って，データの移動を実現するための本質的な部分は，利用可能状態を変更する部分である．

5.2 利用可能状態の変更

本研究では，**図 1** に示すように，2 相コミットプロトコルに基づく通信によって利用可能状態の変更を行う．2 相コミットを行う際には，まず相互にリモートアテステーションを行う．これにより攻撃者によって改ざんされたプログラムと通信することを防ぐ．以降の通信はリモートアテステーションの際に交換した鍵による TLS コネクションを通じて行う[*1]．その後，移動元における利用可能状態が状態 *1* であり，移動先における利用可能状態が状態 *0* であることをことを確認した上で 2 相コミットを開始する．

任意の時点でプログラムが停止する可能性を考慮し中間状態を永続化しながら 2 相コミットを行う．一般的な 2 相コミットでは永続記憶は安定であり，永続記憶への攻撃は想定されていないが，本研究で想定する永続記憶は信頼できず，ロールバック攻撃が行われることが考えられる．従って，状態を変更する際には Ariadne[2] の手法に従ってモノトニックカウンタを操作し，カウンタ値を含めて状態を永続化する．

表 1 データに紐づく状態の一覧

状態	説明
0	利用不可能・移動不可能
1	利用可能・移動可能
S-prepared *D-prepared* *Commit*	2 相コミットの中間状態 (利用不可能)

[*1] https://github.com/cloud-security-research/sgx-ra-tls

5.3 攻撃への対応

リモートアテステーションにより機密実行環境のコードの完全性が保証されるため，コードを改ざんしてアクセス制御を避けるような攻撃は検出される．同様に，機密実行環境のデータの機密性・完全性が保証されるので，利用可能状態を変更する攻撃は検出される．

永続記憶に記録される情報は，機密実行環境に固有な鍵を用いて暗号化されるため，これを改ざんする攻撃は検出される．永続化する際にはモノトニックカウンタのカウンタ値を含め，復号時に現在のカウンタ値と一致していることを検証するため，ロールバック攻撃は検出される．

通信に用いるメッセージは TLS によって保護されるため，攻撃者がメッセージを再送したり改ざんや捏造を行うと，それを検出することができる．

6. 関連研究

Strackx らの研究 [3] では本研究と同様の問題を扱っているが，状態の永続化およびエラー発生時の回復に関する具体的な手順が示されていない．Alder らの研究 [1] では，クラウド環境における Intel SGX enclave のマイグレーション手法を提案している．データセンターという安定した通信環境を想定しているため，通信中のエラーに対応する方法は示されていない．

7. まとめ

本研究では，機密実行環境を用いてコンピュータ間でデータを移動する手法を提案する．具体的には，2 つの機密実行環境間でモノトニックカウンタを使いながら，2 相コミットで双方の状態を変更することによって移動を実現する．

現在までに，状態の永続化方法と通信手順を設計した．今後，提案手法が実際に要件を満たしていることを形式的に確認する．また，本研究の手法を用いて貸し借りや譲渡が可能な著作権管理を実現する．

参考文献

[1] Alder, F., Kurnikov, A., Paverd, A. and Asokan, N.: Migrating SGX Enclaves with Persistent State, *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pp. 195–206 (online), DOI: 10.1109/DSN.2018.00031 (2018).

[2] Strackx, R. and Piessens, F.: Ariadne: A Minimal Approach to State Continuity, *25th USENIX Security Symposium (USENIX Security 16)*, pp. 875–892 (2016).

[3] Strackx, Raoul and Lambrigts, Niels: Idea: State-Continuous Transfer of State in Protected-Module Architectures, *Engineering Secure Software and Systems*, pp. 43–50 (2015).