Arm CCAのRealm VMを用いたノーマルワールドの監視

高巣 雄大[1]　光来 健一[1]

1. はじめに

近年，クラウドやIoT，エッジデバイスなど，様々なシステムがインターネットに接続されるようになっている．それに伴い，インターネット経由でのシステムへの攻撃も増加しているが，システムへの侵入を完全に防ぐことは難しい．そのため，侵入後の異常を早期に検知し，被害を最小限に抑えるために，侵入検知システム（IDS）による監視が重要となる．従来のIDSでは，年々巧妙になる攻撃を完全に防ぐことは難しいため，機械学習を用いた高度なIDSが用いられるようになっている．しかし，監視対象システム内でIDSを動作させると，侵入者によって無力化される恐れがある．

そこで，プロセッサが提供する隔離実行環境（TEE）を用いてIDSを安全に実行し，監視対象システムのメモリ上にあるOSデータを監視する手法が提案されている．例えば，Intel SGXのエンクレイヴ内でIDSを実行したり，Arm TrustZoneのセキュアワールドでで IDSを実行したりすることができる．しかし，エンクレイヴ内では一つの小さなアプリケーションだけを動かすことが想定されているため，複数のプロセスや多数のライブラリを用いる高度なIDSを動かすのには向いていない．セキュアワールドでは複数のプロセスを動かすことができるが，IDSが攻撃を受けるとシステム全体の権限を奪われる恐れがある．

本研究では，Arm CCAで導入されたRealmワールドを用いてRealm仮想マシン（VM）上でIDSを安全に実行し，ノーマルワールドのメモリを直接参照してシステムを監視するCCAmonitorを提案する．

2. CCAmonitor

CCAmonitorは，図1のように，Arm CCAのRealmワールド内で動作するRealm VM上でIDSを実行し，ノーマルワールドで動作するシステムを監視する．Realm VMでは既存のOSやアプリケーションを動作させることができるため，高度なIDSを実行するのに適している．Realm VMはノーマルワールドから隔離されているため，ノーマルワールド内の侵入者からIDSへの攻撃を防ぐことができる．また，IDSはRealm VMに隔離されるため，IDSが攻撃を受けたとしても任意のメモリやデバイスにアクセスすることはできない．

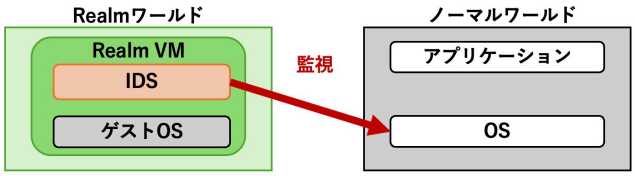


図 1　CCAmonitorのシステム構成

CCAmonitorでは，Realm VMの下で動作するRealm Management Monitor（RMM）を用いて，ノーマルワールドのメモリをRealm VMから参照できるようにする．RMMはRealm VMの作成時に，Realm VM内で物理アドレスとして用いられる中間物理アドレス（IPA）からノーマルワールドの物理アドレスへの対応をRealm Translation Table（RTT）に設定し，読み出しのみを許可する．

IDSは初期化時に，ゲストOS経由でRealm Service Interface（RSI）を用いてRMMを呼び出し，マッピングするノーマルワールドのメモリの範囲を取得する．そして，IDSはそのメモリ領域をIDSの仮想アドレス空間にマップする．このマッピングによって，IDSの仮想アドレスからIPAへの対応が作成される．IDSへのマッピングも読み出し専用とし，書き込みと実行を許可しない．そのため，IDSが攻撃を受けたとしても，このマッピングを用いてノーマルワールドのメモリを改ざんすることはできない．

IDSはノーマルワールドのOSデータにアクセスするために，OSの仮想アドレスを物理アドレスに変換する．そのために，マップしたノーマルワールドのメモリ上のページテーブルを参照してアドレス変換を行う．ページテーブルのアドレスや変換方式などの情報は，初期化時にRMM

[1] 九州工業大学
Kyushu Institute of Technology

© 2026 Information Processing Society of Japan

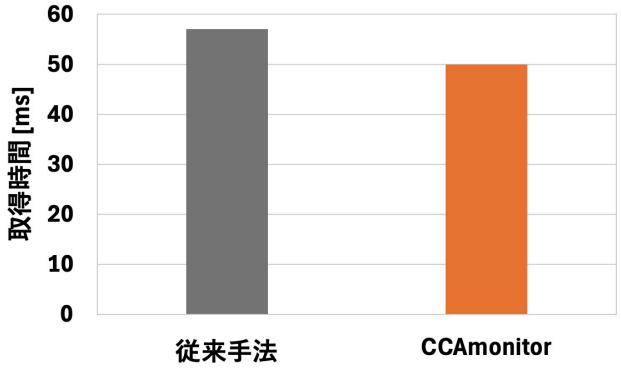


図 2 proc ファイルシステムの情報の取得時間

から取得する．変換した物理アドレスに対応するマッピング先のアドレスを求めることで，目的の OS データを取得する．

3. 実験

LLView [1] を用いて，ノーマルワールドの proc ファイルシステムによって提供されるシステム情報を取得する IDS を開発した．LLView は OS のソースコードを利用して監視対象の OS データに透過的にアクセスすることを可能にするフレームワークである．この IDS を CCAmonitor を用いて実行し，システム情報を取得する時間を測定した．比較のために，ノーマルワールド内で proc ファイルシステムを読み出す従来手法についても取得時間を調べた．Arm CCA に対応した実機がまだないため，エミュレーション環境で実験を行った．結果は図 2 に示すようになり，Realm VM での取得時間は従来手法よりも短くなった．これは，従来手法ではファイルシステムへのアクセスに時間がかかっているためである．

4. まとめ

本研究では，Realm VM 上で IDS を安全に実行し，ノーマルワールドのメモリを直接参照してシステムを監視する CCAmonitor を提案した．CCAmonitor は IDS にノーマルワールドのメモリを読み出し専用で直接マッピングし，IDS 内でアドレス変換とデータ取得を行う．今後の課題は，取得した情報を用いる高度な IDS を Realm VM 内で実行できるようにすることと，Realm VM が正常に動作しているかを確認できる仕組みを実現することである．

謝辞 本研究は，JST 経済安全保障重要技術育成プログラム【JPMJKP24U4】の支援を受けたものである．

参考文献

[1] Ozaki, Y. et al.: Detecting System Failures with GPUs and LLVM, Proc. APSys, pp. 47–53 (2019).

© 2026 Information Processing Society of Japan