九州工業大学 情報工学部 情報・通信工学科 2024 年度 卒業論文 概要

コース	ソフトウェアデザイン	指導教員	光來 健一
学生番号	23222201	氏　　名	岩野 空仁

論文題目	RISC-V Keystone を用いた IoT 機器の安全なメモリ監視機構

1　はじめに

近年，あらゆるモノがインターネットに接続される Internet of Things (IoT) が急速に普及している．IoT 機器はインターネットからの攻撃を受けやすく，分散サービス妨害 (DDoS) 攻撃などに利用されている．そのため，侵入検知システム (IDS) を動作させて監視を行う必要があるが，IoT 機器内で動作する IDS は無効化されるリスクがある．そこで，Intel 製 CPU が提供する隔離実行環境である SGX を用いて，エンクレイヴと呼ばれる保護領域で IDS を安全に実行する手法 [1] が提案されている．この手法では監視対象システム内で動作する IDS がシステムメモリにアクセスし，メモリ上の OS データを監視する．しかし，エンクレイヴ内からはシステムメモリに直接アクセスできないため，BIOS などを経由してアクセスする必要があり，オーバヘッドが大きい．また，SGX をサポートしているのはサーバ向け CPU のみであり，IoT 機器では利用することができない．

本研究では，RISC-V プロセッサの隔離実行環境である Keystone を用いて IDS を安全に実行し，監視対象システムのメモリデータを効率よく取得することを可能にする Keyspector を提案する．

2　Keyspector

Keyspector は図 1 のように，RISC-V Keystone のエンクレイヴ内で IDS を安全に実行し，IDS が監視対象システムのメモリに格納された OS データを直接取得することを可能にする．RISC-V は近年，注目されているオープンソースの命令セットアーキテクチャであり，今後，IoT 機器での利用が見込まれている．Keystone のエンクレイヴは監視対象システム内ではなく，その下のセキュリティモニタ上で独立に動作する．セキュリティモニタは OS よりも高い権限で実行されるため，IDS をより強固に監視対象システムから隔離することができる．

Keyspector はエンクレイヴが監視対象システム (ホスト) のメモリを共有することを可能にする．Keystone では，セキュリティモニタが PMP と呼ばれるハードウェアを用いてホストとエンクレイヴのメモリを分離している．PMP はアクセス可能なメモリの範囲や権限を細かく制御することができるため，Keyspector はエンクレイヴからホストメモリにアクセスできるように PMP の設定を変更する．さらに，エンクレイヴ内の IDS がホストメモリにアクセスできるようにするために，IDS の下で動作する軽量 OS (ランタイム) がホストメモリを IDS のメモリにマッピングする．

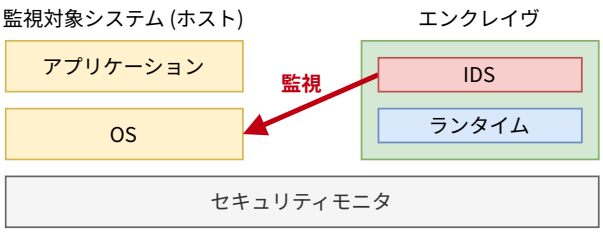

図 1. Keyspector のシステム構成

IDS はマッピングされたホストメモリにアクセスすることで OS データの監視を行う．そのために，ホストメモリ上にあるページテーブルを用いて，OS データの仮想アドレスを物理アドレスに変換する．IDS はランタイム経由でセキュリティモニタを呼び出すことにより，ページテーブルのアドレスが格納されている CPU レジスタの値を取得する．また，LLView [2] を RISC-V に対応させることにより，IDS が OS のソースコードを用いて監視対象システムの OS データに透過的にアクセスすることを可能にしている．

3　実験

Keyspector を用いて監視対象システムの proc ファイルシステムによって提供されるシステム情報の取得時間を測定した．比較のために，監視対象システム内で 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．結果は図 2 に示すようになり，ほとんどの項目において Keyspector での取得時間の方が長くなった．これはアドレス変換をソフトウェアで行うオーバヘッドのためだと考えられる．

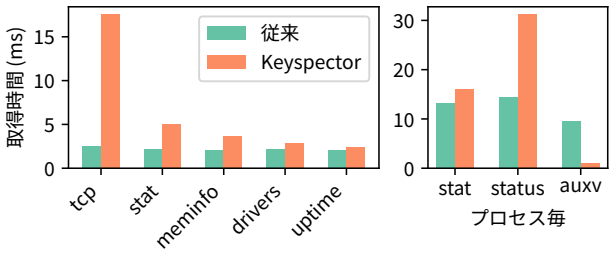

図 2. proc ファイルシステムの情報の取得時間

4　まとめ

本研究では，RISC-V Keystone を用いて IDS を安全に実行し，エンクレイヴ内から監視対象システムのメモリデータを直接取得して監視を行う Keyspector を提案した．今後の課題は，リモートアテステーションを利用して IDS を実行できるエンクレイヴを制限できるようにすることである．

参考文献

[1] Y. Koga et al. SSdetector: Secure and Manageable Host-based IDS with SGX and SMM. TrustCom 2023.
[2] Y. Ozaki et al. Detecting System Failures with GPUs and LLVM. APSys 2019.