Keyspector：RISC-V Keystoneを用いたIoT機器の安全な監視

岩野 空仁[1]　光来 健一[1]

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) が急速に普及しており，今後も増加すると見込まれている．Wi-Fi ルータ，プリンタ，テレビ，自動車といった IoT 機器はインターネットを介してサーバや他のデバイスと接続されるため，外部から攻撃を受けるリスクが高く，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，監視対象システム内で動作する IDS は侵入者に無効化されるリスクがある．

そこで，最近のプロセッサが提供している隔離実行環境 (TEE) を用いて，IDS を安全に実行する手法が提案されている．例えば，Intel SGX のエンクレイヴと呼ばれる保護領域で IDS を実行する手法 [1] では，IDS が監視対象システムのメモリにアクセスしてメモリ上の 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，メモリデータを取得するオーバヘッドが大きい．一方，Arm TrustZone のセキュアワールドで IDS を実行する手法 [2] では，IDS がシステムメモリに直接アクセスすることができる．しかし，セキュアワールドは IDS が必要とするよりも高い権限を持つため，IDS の実行にはリスクが伴う．

本稿では, RISC-V プロセッサの TEE である Keystone [3] 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直接アクセスすることを可能にする．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．

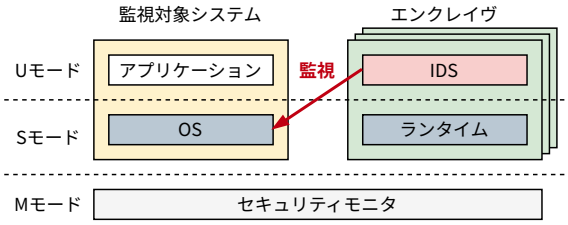

図 1　Keyspector のシステム構成

Keyspector はエンクレイヴが監視対象システム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 はアクセス可能な物理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の読み出しのみできるように PMP の設定を変更する．侵入者が作成したエンクレイヴによる盗聴を防ぐために，エンクレイヴ内の IDS のハッシュ値が事前に登録されたものと一致する場合にのみ，ホストメモリへのアクセスを許可する．IDS は，エンクレイヴ内で動作する軽量 OS であるランタイムを呼び出して，ホストメモリを IDS のアドレス空間にマッピングすることで，IDS からホストメモリへのアクセスを実現する．

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

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

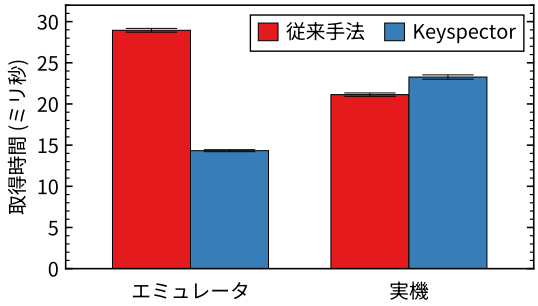

図 2 システム情報の取得時間

する．また，LLView [4] 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．実験には RISC-V エミュレータと，SiFive 社製の HiFive Unmatched Rev B を用いた．結果は**図 2** に示すようになり，エミュレータでは Keyspector での情報取得時間が従来手法の約半分まで短くなったが，実機では約 10% 長くなった．エミュレータで Keyspector での取得時間が短くなった原因について調査したところ，実機に比べて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ことがわかった．実機においては，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に取得時間が長くなった．

4. まとめ

本稿では，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から直接 OS データを取得することを可能にする Keyspector を提案した．今後の課題は，セキュリティモニタで IDS が動作するエンクレイヴの停止を検知できるようにすることである．

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] Koga, Y. and Kourai, K.: SSdetector: Secure and Manageable Host-based IDS with SGX and SMM, *Proc. 22nd IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications*, pp. 539–548 (2023).
[2] Guerra, M., Taubmann, B., Reiser, H. P., Yalew, S. and Correia, M.: Introspection for ARM TrustZone with the ITZ Library, *Proc. 18th IEEE Int. Conf. on Software Security and Reliability*, pp. 123–134 (2018).
[3] Lee, D., Kohlbrenner, D., Shinde, S., Asanovic, K. and Song, D.: Keystone: An Open Framework for Architecting Trusted Execution Environments, *Proc. 15th European Conf. Computer Systems* (2020).
[4] Ozaki, Y., Kanamoto, S., Yamamoto, H. and Kourai, K.: Detecting System Failures with GPUs and LLVM, *Proc. 10th ACM SIGOPS Asia-Pacific Workshop on Systems*, p. 47–53 (2019).