1W-01

準パススルー型ハイパーバイザーを用いたブロックデバイス監視システムの性能評価

都築卓馬† 岡野兼也‡ 高直我‡ 平野学†

豊田工業高等専門学校 専攻科 情報科学専攻† 豊田工業高等専門学校 情報工学科‡

1. はじめに

現在のサイバー犯罪の捜査手法では、被害にあったコンピュータのブロックストレージやメモリダンプを回収して、それらの電子データから時系列ごとの出来事をまとめたタイムラインを作成するのが一般的である。しかし、手がかりとなるデータの改ざんや、捜査手法を迂回するアンチフォレンジック攻撃が問題になっている。近年、金融や政府・行政サービスなどの重要インフラを管轄する組織では、機密データを保存するコンピュータがサイバー犯罪の被害にあっている。そうした重要なコンピュータについては、データの入出力をあらかじめ監視しておくことによって、犯罪の抑止につながり、万が一被害にあった時でも捜査機関が正確なタイムラインを再現できるようになるはずである。

そこで、本稿ではコンピュータからブロックストレージへの書き込みを監視して、監視記録を自動的に保存してゆくシステムを提案する。提案システムは、クライアントコンピュータを監視対象とし、コンピュータの管理者からは監視についての同意を得ているものとする。本研究の特徴は高速に動作する準パススルー型ハイパーバイザーの BitVisor[1]を用いて書き込みデータを補足して、解析クラスタへ転送保存することである。

2. 準パススルー型ハイパーバイザー

Xen や VMWare といったハイパーバイザーはコンピュータリソースの大部分を仮想化するため、コードサイズが大きくなりコンピュータの動作性能に影響を与えてしまうことがある。加えてコードサイズが大きいほど脆弱性が見つかる可能性は高くなる。品川らはクライアントコンピュータにセキュリティ機能を提供するために BitVisor を開発した[1]。BitVisor は特定のデバイスだけを監視する準パススルー型ハイパーバイザーである。準パススルー型ハイパーバイザーはゲスト OS を一つしか動作させることができないが、高速に動作し、監視するデバイスドライバを限定しているためコードサイズが小さく、BitVisor そのものが攻撃される可能性が低い。BitVisor では準パススルー型のデバイスドライバによって監視を行う。本研究のブロックストレージの書き込み監視は AHCI (Advanced Host Controller Interface)の準パススルードライバで行う。サーバへの転送と書き込み時刻の取得は BitVisor に組み込まれている軽量 TCP/IP スタックである lwip で行う。

3. ブロックデバイス監視システム

小川らは仮想モニタ Xen を使ってブロックデバイスへの書き込みを監視して記録するシステムを開発した[2]。このシステムは、クラウド上のブロックストレージへの 4KiB ブロックごとの書き込みを補足して解析クラスタへ保存するものである。対して、本研究の対象は個人利用のコンピュータである。必要最低限の仮想化でコンピュータへの負荷を減らすことが望ましい。よって、先行研究では Xen を採用していたのに対して、本研究ではクライアントコンピュータのセキュリティを強化する目的で開発された仮想マシンモニタ BitVisor を採用する。提案システムでは、BitVisor で書き込みデータを監視して、記録用のデータ領域に格納し、そのデータを分散ファイルシステムに定期的にアップロードする。保存された監視データは、捜査時に解析システムで利用される。

4. 設計

図 1 に提案システムの設計を示す。書き込みデータの監視は BitVisor の AHCI の準パススルードライバで行う。AHCI の準パススルードライバはブロックストレージへの書き込みを 4KiB ブロックごとに DMA(Direct Memory Access)シャドウバッファにコピーしてセキュリティ処理を施している。本研究では新たに監視記録用のデータ領域を作成し、データ領域に DMA シャドウバッファの一部をコピーして書き込みデータを監

Performance Evaluation of a Surveillance System by Using Parapass-though Hypervisor for Recoding Write Operations

†Takuma Tuzuki, Manabu Hirano, Computer Science Course, Advanced Engineering Course for Bachelor's Degree, National Institute of Technology, Toyota College

‡Kenya Okano, Naoga Taka, Department of Information and Computer Engineering, National Institute of Technology, Toyota College

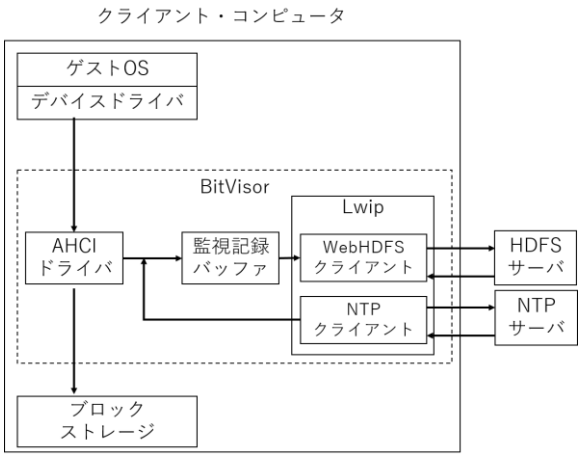

図1　提案システムの設計

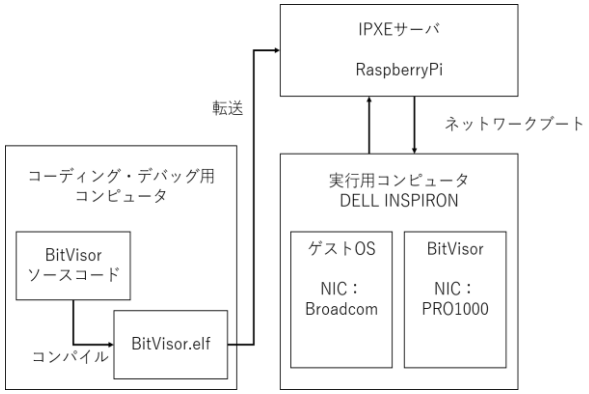

図2　システム構成

表1　実行用コンピュータの仕様

CPU	Samsung SSD 840 256GB
ゲストOS	Debian 8.3.0 amd64
RAM	4GiB
ストレージ	Samsung SSD 840 256GB
NIC	Broadcom BCM57788 (PCIe, オンボード)
	Intel PRO/1000 GT (PCI)
仮想マシン モニタ	BitVisor (BitBucket で 12 月 2 日 時点のソースコードを利用)
分散ファイル システム	Hadoop 2.7.1

視する。書き込み時刻の取得と解析クラスタへの保存は lwip で行う。まず、現在時刻の取得は lwip で NTP クライアントを実装して行う。BitVisor 内部で動作する NTP クライアントは1分間ごとに外部の NTP サーバと時刻同期をして、その時刻をもとに CPU 時間から書き込み時刻を算出する。取得した書き込み時刻は、監視記録に利用する。監視記録データは Hadoop 分散ファイルシステム (Hadoop Distributed File System)へ自動送信させる。WebHDFS は Hadoop 分散ファイルシステムとの通信をするためのプロトコルである。本研究では BitVisor に WebHDFS を用いてファイルを APPEND(追加)していくプロトコルを実装する。

5. 実装

本研究では書き込みデータの監視機能と HDFS への転送機能を実装した。書き込みデータを一時的に保存するデータ領域は 128MB を確保し、0.1 秒ごとに Hadoop 分散ファイルシステムにデータが転送されるよう設定した。書き込みデータが正しく Hadoop 分散ファイルシステムに保存されていることを確認した。開発と評価に用いたシステムの構成を図 2 に示す。提案システムを実行したコンピュータの仕様を表 1 に示す。Broadcom の NIC はゲスト OS 用で、Intel の PRO/1000 の NIC は BitVisor が HDFS 転送に用いるように設定した。

6. まとめ

近年、組織の機密データを扱うコンピュータがサイバー犯罪の標的になることが増える中で、犯罪捜査を迂回するアンチフォレンジック攻撃が問題となっている。その対策として本稿ではコンピュータの入出力をあらかじめ監視するシステムを実装した。先行研究との違いは、監視対象がクライアントコンピュータであることからクライアントコンピュータ用のハイパーバイザーの BitVisor を採用したことである。監視対象はブロックデバイスへの書き込みとその書き込み時刻で、監視データは Hadoop 分散ファイルシステムに自動保存するようにした。また時刻は BitVisor に実装した NTP クライアントが外部サーバから取得するようにした。現段階の実装で、書き込みデータと書き込み時刻を正しく記録できていることを確認できた。今後は本システムを動作させたコンピュータでスループットの計測を行い、システムの有用性について検討する。

参考文献

[1] T. Shinagawa, et al.: BitVisor: a Thin Hypervisor for Enforcing I/O Device Security, In Proc. of the ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments, pp.121-130, 2009.
[2] M. Hirano and H. Ogawa: A Log-structured Block Preservation and Restoration System for Proactive Forensic Data Collection in the Cloud, Proc. of The 11th International Conference on Availability, Reliability and Security (ARES 2016), pp.355-364, 2016.