IPA

2020 年度 未踏 IT 人材発掘・育成事業 採択案件評価書

1. 担当 PM

竹迫 良範（株式会社リクルート データプロダクトユニット ユニット長）

2. クリエータ氏名

上田 侑真 （慶應義塾大学 総合政策学部）

3. 委託金支払額

2,736,000 円

4. テーマ名

ソフトウェアのインストールを必要としない NIC 型セキュリティ機構

5. 関連 Web サイト

なし

6. テーマ概要

本プロジェクトでネットワークインタフェースコントローラ（NIC）を搭載した PCIe デバイスとサーバからなる、NIC 型セキュリティ機構を開発する。PCIe デバイスは DMA によりメモリダンプを取得、プロセス空間を復元し、計算した特徴量や、不自然な割り込みハンドラやコードの書き換えの有無をサーバに送信する。サーバは受信した特徴量からマルウェアの感染を検出し、それを報告する。これにより、事業者はサーバのメモリ空間を一切閲覧せずにセキュリティサービスを提供できる。プロセス空間を復元するため、ファイルレスマルウェア、パックされたマルウェアの検出、コンテナごとの監視も可能になる。

7. 採択理由

本提案は NIC 型の独自 PCIe デバイスを FPGA で構築し、DMA を用いてメモリ空間全体のダンプを PCIe デバイスに送信し、コンピュータ側ではなくデバイス側でマルウェア検知を実行する野心的なプロジェクトである。ホスト OS でカーネルパニックが発生した場合でもコンピュータ上の DMA 転送機能は有効なため、OS の実行状態に関わらず PCIe デバイスへの常時メモリダンプが可能

である。最初はデータセンターでの応用例で概念実証できるかどうか果敢に挑戦してみるが、技術的には汎用的に展開可能なものであり、特定の用途に拘らず幅広く展開していく未来を期待し採択した。

8. 開発目標

本プロジェクトの具体的な目標は、一切のソフトウェア的変更を加えることなく、物理マシン、その上で動作する仮想マシンのメモリ空間、更に I/O を監視し、高い隠密性、透明性をもったセキュリティ機構を既存の有力オープンソースソフトウェアと連携して手軽に実装できるハードウェアベースのフレームワーク、Bubo の開発である。

Bubo の開発により、ユーザが手軽に高い隠密性、透明性を持ったセキュリティ機構を実装できるようになり、よりセキュアな世界の実現に貢献することを最終的な目的とした。

9. 進捗概要

本プロジェクトでは、監視対象のホスト（Target）で動作する BuboFPGA デバイスを開発し、監視を行うホスト（Monitor）で動作するフレームワーク LibBubo と VolBubo の 3 つを開発した（図 1）。

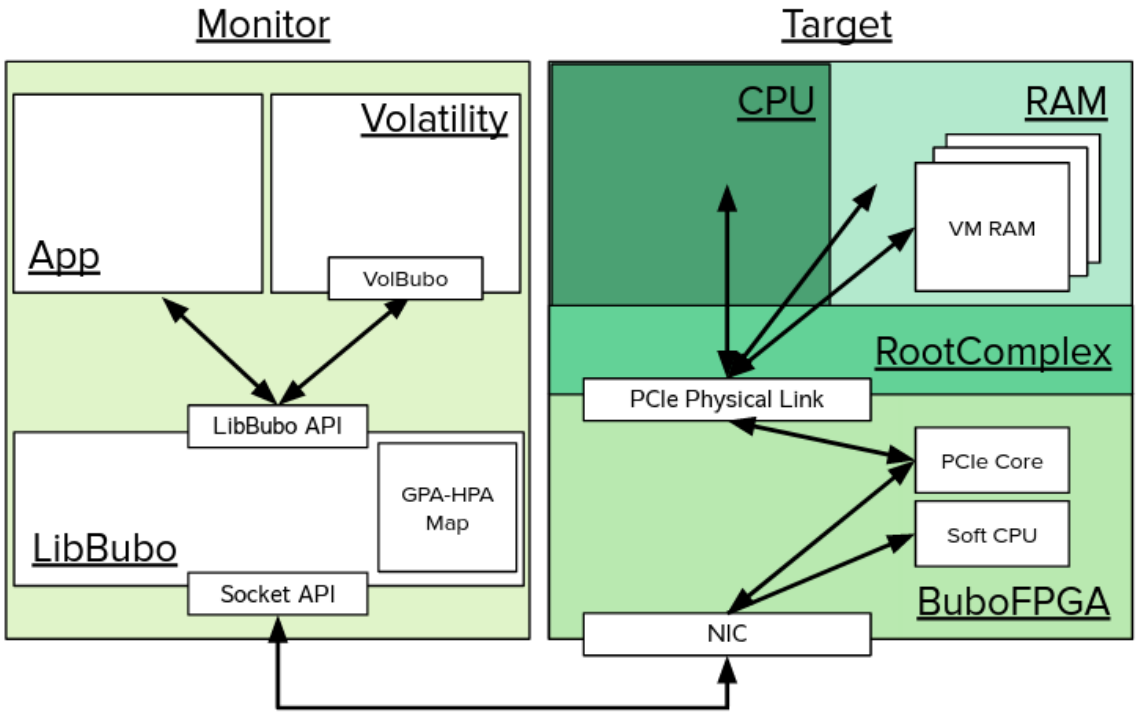

図 1　開発した Bubo フレームワークのシステム構成図

(1) BuboFPGA

BuboFPGA は Target のメモリ空間の取得と、PCI Express デバイスのエミュレーションを実現するためのハードウェアである。NIC を通じて Monitor から受信した UDP パケットで制御される。Xilinx Kintex-7 KC705 FPGA 評価ボード上に PCI Express デバイスとして実装された。

メモリ空間の取得は、BuboFPGA が NIC を通じて受信した UDP にカプセリングされた Transaction Layer Packet をそのまま Target のルートコンプレックスまで中継し、DMA を行い、返されたメモリ上のデータを含む Transaction Layer Packet をそのまま Monitor まで UDP にカプセリングして返すことで実現した。

PCI Express デバイスのエミュレーションは、後述する LibBubo との連携により実現されている。BuboFPGA はこのために、自身の PCI コンフィグレーション空間を Monitor から UDP パケットで読み書きできる仕様となっている。また、自身の PCI コンフィグレーション空間、特定の BAR がマップするデバイスメモリ空間への Target からの Transaction Layer Packet による読み書きを、全て Monitor に Transaction Layer Packet を UDP にカプセリングし、送信することで中継している。これにより PCI Express デバイスの Monitor 側でのソフトウェアによるエミュレーションが可能となる。

(2) LibBubo

LibBubo は BuboFPGA を通じて物理マシン、その上で動作する仮想マシンそれぞれのメモリ空間の取得、PCI Express デバイスのエミュレーションを実現するためのソフトウェアライブラリである。BuboFPGA は UDP パケットで制御できる。物理マシンのメモリ空間を取得するためには、Socket API のラッパーを用意し、TLP を UDP 上にカプセリングして BuboFPGA の NIC へ送信するのみで良い。仮想マシンのメモリ空間の取得は、はじめに物理マシンのメモリ空間を取得し、ゲスト物理アドレスからホスト物理アドレスへの変換を担うページテーブルである EPT（Extended Page Table）を復元することで実現される。これにより、ゲスト物理アドレスを用いた透過的なメモリ取得が可能となる。

(3) VolBubo

VolBubo は LibBubo、BuboFPGA を通じて取得できる、物理マシン、その上で動作する仮想マシンのメモリ空間上のデータを、Volatility への入力として提供するための Address Space Plugin である。これにより、Volatility プラグインを Target の物理メモリ空間や仮想メモリ空間にそのまま使用することが出来、ユーザがセキュリティ機構の実装を行うコストが大幅に低下する。

10. プロジェクト評価

本プロジェクトの開発成果により、ユーザは非常に高い隠密性、透明性を持ったマルウェア検知、解析にはじまるセキュリティ機構を Volatility プラグインとして素早く実装することが可能となった。Bubo は監視対象のホストの CPU リソースを一切消費しないため、従来のセキュリティ機構とも競合しない。よって、この成果を単体で、あるいは従来のセキュリティ機構と併せて用いることで、より信頼性の高いセキュリティ機構を実現できる。また、この成果をきっかけに、セキュリティ機構のトラストモデルという課題により注目が集まり、更なる研究が実施され、その成果が社会に還元されることで、よりセキュアな世界が実現されることも期待している。

11. 今後の課題

BuboFPGA に実装された PCI Express デバイスエミュレーション機能は、現状、PCI Express デバイスの全ての機能をソフトウェアでエミュレートすることができない。具体的には PCI Express コンフィギュレーション空間のいくつかのフィールドの値を論理合成時にハードコードする必要がある。これをソフトウェアでエミュレートできるようにすることが直近の課題である。

また、BuboFPGA はプロジェクト後半でオープンソース版が実装されたが PCI Express デバイスエミュレーション機能の一部、ソフト CPU へのメモリ取得、解析のオフロード、ドキュメントの整備などのタスクが残っている。

本プロジェクトの成果を周知するためにも学会発表を行い、実用化に向けた検討を進めることが今後の発展的な課題である。