開発テーマ名

Super Creator

高速なVMI機構を実装したバイナリ解析基盤

森　瑞穂
もり　みずほ

《略歴》

2015年4月　電気通信大学 情報理工学部 情報・通信工学科 入学

2019年3月　電気通信大学 情報理工学部 情報・通信工学科 卒業

2019年4月　電気通信大学大学院 情報理工学研究科 情報・ネットワーク工学専攻 入学

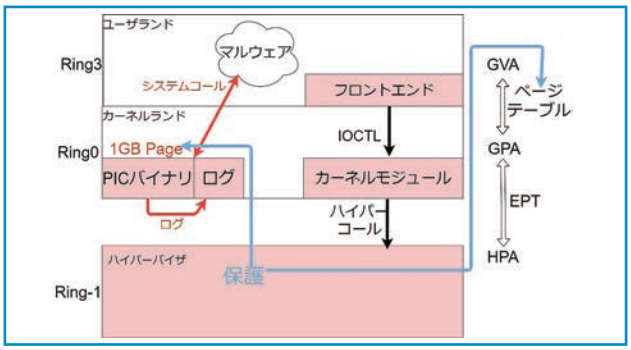
《所属》※ 2020年5月現在

電気通信大学 大学院 情報理工学研究科 情報・ネットワーク 工学専攻 本多研究室

テーマ概要

OSSのハイパーバイザ「BitVisor」をベースとしたバイナリ解析基盤「FastVMIX」を開発した。本プロジェクト「FastVMIX」は、BitVisorベースのハイパーバイザ、これを操作するカーネルモジュール、カーネルモジュールを操作するフロントエンドコマンド、特殊なメモリ空間1GB Huge Pageで動作するPICバイナリの大きく4つで構成されている。本プロジェクトでは高速性とマルウェアの解析耐性機能の迂回機構を実装することを目標に掲げた。高速性はコンテキストスイッチをなるべく配したデザインを一貫させ、実際に先行プロジェクトである「drakvuf」の約306倍高速化を達成することができた。

また「FastVMIX」への攻撃を防ぐために、ページテーブル保護、動的メモリマップの変更機能を実装した。動的メモリマップの変更にはEPTP Switchingを用いてコンテキストスイッチなしでメモリマップを変更させることができる。また1GB HugePageを用いて、解析用のコードを当領域へ格納させることにより、保護するべきページエントリ数を大幅に削減し、大きな高速化を達成した。また、解析コードのモジュール化を行い、開発が容易に進むようにデザインした。解析耐性機能の迂回として、タイミング解析の迂回機能を簡易的であるが実装し、それの有効性が確認できた。



田中 PM の評価

元々のプログラミング能力が非常に高く、加えてプロジェクト期間においては先行する研究室から学び、自らのやりたいことを実現し、自信を持って発表をする事ができた。フィードバックをもとにプロジェクトを真正面から見つめ、自らの高い技術力を持ってプロジェクトを完遂させたことは、大いに評価できる。

近況メッセージ

・開発成果の近況、展開方針、今後の目的など

開発は一段落し、ソースコードのリファクタリングを行っている最中である。また、関連した技術の論文を提出する予定で、それに向けても開発と論文執筆を継続して行っている。

今後の目標として「FastVMIX」のOSS化、リファクタリングの完成、論文投稿、さらにマルウェアの動的解析耐性への対応、対応OSを増やすことなどを考えている。

・近況

「FastVMIX」以外に、様々なプロジェクトを同時進行で行っている。最近ではRustにはまり、インタプリタを書いた。未踏終了後も低レイヤーでやりたいことを探し、手を動かすことを継続して行っている。またアルバイトでセキュリティ関連会社に入社し、Linux向けのアンチマルウェアソフトウェアを作るプロジェクトに参加して継続して実務的な現実に通用するアンチマルウェア技術を磨いている。

関連 URL

https://morimolymoly.com