攻撃手法のリアルタイム可視化

情報工学部 情報工学科 教授 種田　和正

分　　野　サイバーセキュリティ

キーワード　サイバー攻撃、制御フローハイジャック、可視化

研究概要

1. 研究背景

現在、新たなセキュリティ脆弱性が日々発見されている。一方、脆弱性を悪用する新しい攻撃技術の進歩は、バグ報奨金プログラムおよびハッキング競技によって大幅に加速されている。このため、アメリカ労働局の報告によると、情報セキュリティアナリストの需要は、2018年から2028年で32%増加すると予測されている。サイバー技術開発のための仮想環境や隔離されたサンドボックス環境は、攻撃コードで出来ること及び攻撃後の対処の学習に有効である。一方、セキュリティ専門家を目指す学習者が攻撃コードのメモリ上の動作を理解するためには、関連する技術とソースコードを理解するために多くの時間を費やさなければならない。

そこで、本研究はサイバーセキュリティ学習者が攻撃手法を容易に理解できるように、攻撃コードのメモリ上の動作をリアルタイムに可視化するシステムを提案する。

2. 攻撃手法の可視化システムの概要

本システムは、exploitとweb-appの2つのモジュールで構成される（図1）。exploitは脆弱なコードを攻撃すると同時にそのコードのプロセスデータを取得し、Firefoxブラウザに送る。web-appは取得したデータをFirefoxに表示するフォーマット形式等の処理を行う。図1は攻撃に関連するメモリ上のスタック領域の一部を読込み、Firefoxに表示する場合である。図2は、実施されたReturn Oriented Programing (ROP)攻撃が回避策（stack canary）により失敗した直後のFirefoxの内容である。失敗理由とその時のスタック領域が表示される。

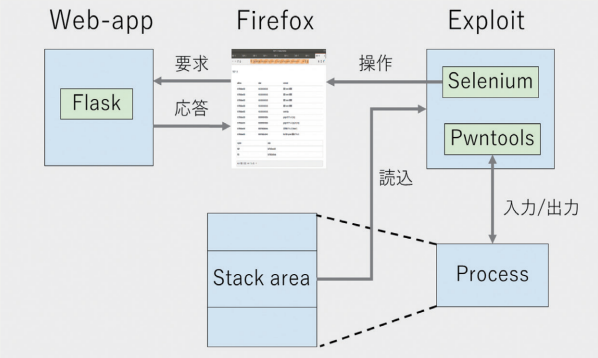

図1：可視化システムの構成

address	value	comment
0x7ffdc8643160	4141414141414141	Address of name[]
0x7ffdc8643168	4141414141414141	Address of name[]
0x7ffdc8643170	4141414141414141	Address of name[]
0x7ffdc8643178	4141414141414141	Address of name[]
0x7ffdc8643180	4141414141414141	
0x7ffdc8643188	4141414141414141	stack canary
0x7ffdc8643190	4141414141414141	saved ebp
0x7ffdc8643198	00007fabb934002b	Return address
0x7ffdc86431a0	0000000000000001	

register	value
RSP	
RDI	

```
The return address is set to the address of function main().
The process terminates and the following statement is displayed:
*** stack smashing detected ***: <unknown>
```

図2：Firefox上のメモリ情報とコメント

利点特徴

本システムは効率的で包括的な学習のための3つの特徴を持つ。(1)攻撃コードの実行環境（シミュレーター／エミュレーターではない）を提供し、学習者は攻撃コードや回避策のon/offを変更しながら学習できる。これにより、より深く攻撃手法を理解できる。(2)攻撃コードに関し、「何が出来るか」ではなく「どのように動作するか」をアセンブリ言語レベルで説明する。(3)攻撃に無関係な情報を除外し学習の効率を高める（実際の攻撃コードは不必要な命令を多く含んでいる）。

応用分野

本システムはセキュリティ専門家の学習用のみならず、攻撃回避策の開発、脆弱性診断、攻撃コードの自動生成の研究としても応用可能である。