情報セキュリティ・暗号研究の成果を展示中。

松浦研究室

［実行監視によるJIT Spraying 攻撃検知］

生産技術研究所　情報・エレクトロニクス系部門
Department of Informatics and Electronics, IIS
http://kmlab.iis.u-tokyo.ac.jp/

情報理工学系研究科
電子情報学専攻

専門分野：　情報セキュリティ

新たなバッファオーバーフロー攻撃の手法

A New Method for Buffer Overflow Attacks

マルウェアなどをコンピュータに感染させる手段としてよくバッファオーバフロー攻撃が使われる。しかし、近年はデータ領域のコード実行を禁止するDEPやアドレス空間をランダム化するASLRなどのセキュリティ機構が使われるようになり、バッファオーバーフロー攻撃を成功させることは困難になってきている。

一方、リッチになったウェブアプリケーションの高速化のために、主要なウェブブラウザにはJITコンパイラが搭載されるようになってきている。

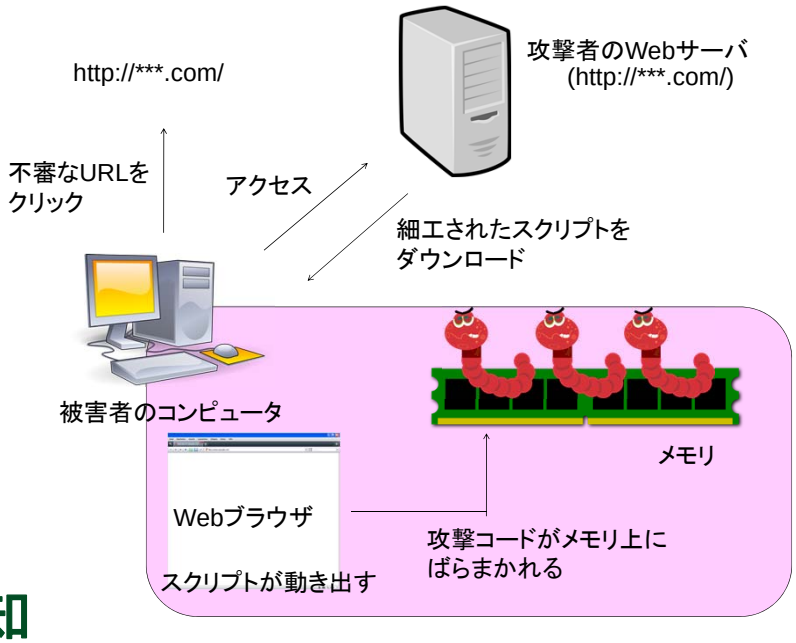
そのような状況の中、JITコンパイラを悪用してDEPとASLRを同時に回避し、バッファオーバーフロー攻撃を成功させる、JIT Spraying という手法が登場し、問題となっている。

JIT Spraying 攻撃の概要

A Summary of JIT Spraying Attacks

攻撃者の用意したウェブサイトにブラウザでアクセスすると、細工されたスクリプトがJITコンパイルされユーザマシンのメモリ上にばらまかれる。ばらまかれたメモリ上のコードは不正なアドレスから実行されることにより攻撃コードとなる。

JITコンパイラがデータ領域に実行可能属性を付加するためDEPは回避され、たくさんのコードがばらまかれることによりASLRも回避される。



JIT Spraying 攻撃検知

Detection of JIT Spraying Attacks

ユーザレベルで実行監視を行う。JITコンパイラがメモリに実行可能属性を付加するときに不正なアドレスを特定し、実行されるアドレスを実行時にチェックする。不正なアドレスの実行を検知したらプログラムを停止させる。

OSやJITエンジンの修正なしに JIT Spraying 攻撃を検知することができる。