Matsuura LAB.

Research results on information security and cryptography are on display.

[Detecting JIT Spraying Attacks by Monitoring Execution]

Department of Informatics and Electronics, IIS

Graduate School of Information Science and Technology
Department of Information & Communication Engineering

http://kmlab.iis.u-tokyo.ac.jp/

Information Security

A New Method for Buffer Overflow Attacks

A Background of JIT Spraying Attacks

Buffer overflow attacks are often used for a means that infect malware to computers. However, major operating systems become equipped security structures such as DEP which forbids code execution in data area and ASLR which randomizes address space in recent years, then making a success of buffer overflow attacks is getting difficult.

Meanwhile major web browsers are getting to use JIT compiler for speed-up rich web applications.

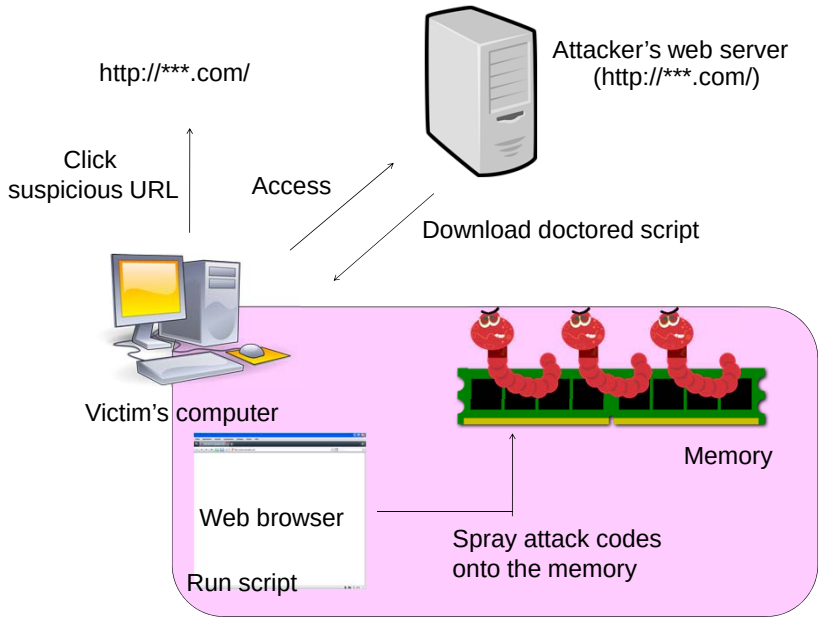
Under these conditions, the method called JIT Spraying which can bypass DEP and ASLR simultaneously abusing JIT compiler appears and becomes a big issue.

A Summary of JIT Spraying Attacks

How to be performed JIT Spraying Attacks

If users access attackers website, doctored script is JIT compiled and sprayed onto the memory of user's machine. Sprayed on-memory code becomes attack code by executing from invalid address.

This bypasses DEP because JIT compiler adds executable attribute to data area and also bypass ASLR because many codes are sprayed.



Detection of JIT Spraying Attacks

Detection of JIT Spraying Attacks

Our method monitors execution at user-level. It identifies invalid addresses when JIT compiler adds executable attribute to the memory and checks addresses which are executed on run-time. If it detects executing invalid addresses then it stops the program.

This can detect JIT Spraying Attacks without fixing OSes and JIT engines.