Detection of Malicious Code-Injection Attack Using Two Phase Analysis Technique

Abstract

In today’s world code injection attack is a very big problem. Code injection attacks are to exploit software vulnerabilities and inject malicious code into target program. These malicious codes are normally referred as malware. Systems are vulnerable to the traditional attacks, and attackers continue to find new ways around existing protection mechanisms in order to execute their injected code. Malicious code detection is an obfuscation-deobfuscation game between malicious code writers and researchers working on malicious code detection. Malware writers obfuscate their malicious code to subvert the malicious code detectors, such as anti-virus software. Signature-based detection is the most commonly used method in commercial antivirus software. However, it fails to detect new malware. In this paper, we propose a two phase analysis technique. In first phase a malicious code with obfuscated techniques is detected by means of static analysis of instruction sequence. Phase II involves extracting opcode sequence from the dataset to construct a classification model and compare it to the output of phase I to identify it as malicious or benign.

References

- Govindaraju, A, Faculty, Department of Computer Science, Master Thesis, "Exhaustive Statistical Analysis for Detection of Metamorphic Malware", San Jose State University, San Jose, CA (2010).
- VXheavens http://vx.netlux.org

**Index Terms**

Computer Science

Security

**Keywords**

Obfuscation Techniques Static Analysis Classification Algorithm