Static Analysis, Dynamic Analysis and Symbolic Execution Techniques Applied to Security

Introduction & Case Study

Xinyi Li

May 5, 2020

Overview

- Static Analysis
  - Case 1: Detect PDF Malware

Case 1: Malicious `JavaScript` PDF Extension

sample[1]

[1] Alexander Jordan et al. "Unacceptable Behavior: Robust PDF Malware Detection Using Abstract Interpretation". In: *Proceedings of the 14th ACM SIGSAC Workshop on Programming Languages and Analysis for Security*. 2019, pp. 19–30.

Code

```
while not q.empty():
    p = q.get()
    p_list = os.listdir(p)
    for i in p_list:
        temp_p = os.path.join(p, i)
        if os.path.isdir(temp_p):
            q.put(temp_p)
            continue
        # do something
        print(temp_p)
```