

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

sample¹

¹Alexander 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

```
1 while not q.empty():
2     p = q.get()
3     p_list = os.listdir(p)
4     for i in p_list:
5         temp_p = os.path.join(p, i)
6         if os.path.isdir(temp_p):
7             q.put(temp_p)
8             continue
9         # do something
10        print(temp_p)
```