PlatPal: Detecting Malicious Documents

**with Platform Diversity**

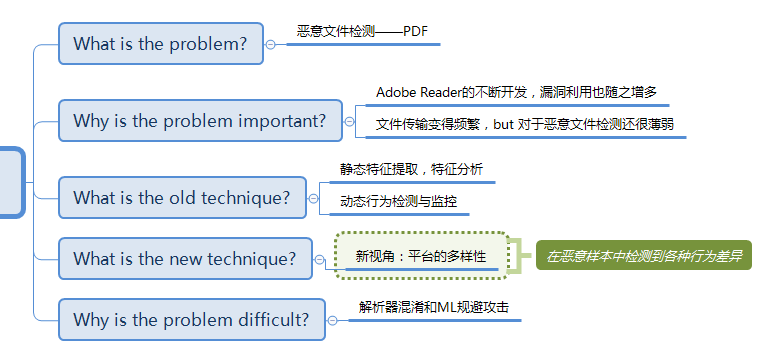
Meng Xu and Taesoo Kim, *Georgia Institute of Technology*

<https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/xu-meng>

## 中文标题：

P LAT P AL ：检测与平台多样性恶意文件

## Questions:



## 一句话概述：

基于动态分析，有大量的领域知识，但此论文并没有直接使用机器学习的方法。对于好样本，在跨平台的运行过程中，行为一致；而对于恶意样本，跨平台行为会不同。如 此恶意软件只在WinXP下的某个版本的PDF Reader下执行

## 中文摘要：

由于Adobe Reader的不断开发，恶意文件（maldoc）检测已经成为一个紧迫的问题。尽管已经提出了许多解决方案，但最近的作品突出了一些常见的缺陷，例如解析器混淆和分类器规避攻击。

针对这一点，我们提出了一个新的视角maldoc检测：平台的多样性。具体来说，我们确定了操作系统设计和实现中可能导致行为分歧的八个因素，从系统调用语义（更明显）到堆对象元数据结构（更加微妙），并进一步展示如何阻止攻击者发现错误，利用错误或执行恶意活动。

我们进一步对P LAT P AL 进行原型系统收集平台多样性。P LAT P AL 挂接到Adobe Reader以跟踪内部PDF处理，并使用沙箱执行来捕获maldoc对主机系统的影响。比较不同平台上的执行跟踪，并且maldoc检测基于良性文档在不同平台上表现相同的观察结果，而maldoc在开发过程中表现不同。评估表明，P LAT P AL 在良性样本中不会产生虚假警报，在恶意样本中检测到各种行为差异，是一个可扩展和实用的解决方案。

## 主要贡献

•    我们建议跨不同平台执行文档，并使用行为差异作为maldoc检测的指标。

•    我们对平台多样性进行深入分析和分类，并展示它们如何用于检测Maldoc攻击。

•    我们基于这些见解对P LAT P AL进行了原型设计。评估证明P LAT P AL 是可扩展的，不会引起虚假警报，并检测恶意样本中的各种行为差异。

我们计划开源P LAT P AL，以提示使用平台多样性进行Maldoc检测，并启动一个PDF maldoc扫描服务供公众使用。

## 亮点解读

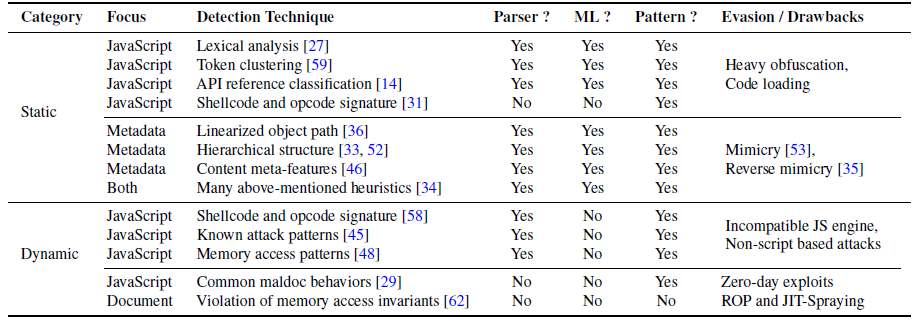
1. Dataset

Ben 1000 from Google

Mal cve 标签样本 34 个

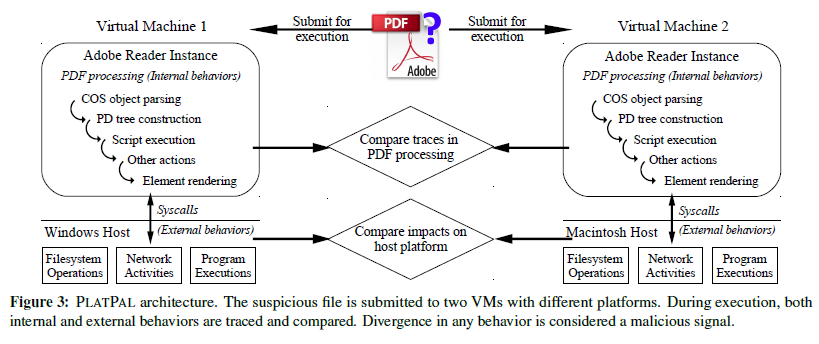
1. 动静结合分析检测恶意文件。主要针对动态分析时PDF内部的调用和外部系统调用
2. 如下图是现有检测技术的一个大致分类

现有的maldoc检测方法可以大致分为两类：1）动态分析，在特定的仪器环境中执行和检测恶意代码; 和2）静态分析，其中执行检测而不执行代码。表1 列出了现有方法的总结。



1. 通过几个具体详细的CVE病毒漏洞做内部与外部双层跟踪

如下图是内部跟踪的一些差异性比较



几乎所有的maldocs都会注册任何可能在OpenAction中**触发其恶意负载的东西**，以便在文档打开时立即利用。

## 论文总结

由于AAR的持续开发，maldoc检测已经成为一个紧迫的问题。对现有技术的调查显示，他们很容易受到最近的攻击，如解析器混淆和ML规避攻击。针对这一点，我们提出了一个新的视角：平台多样性，以及用于maldoc检测的原型P LAT P AL。P LAT P AL挂钩到AAR以跟踪内部PDF处理，还使用全面的动态分析来捕获maldoc对主机系统的外部影响。内部和外部的痕迹都进行了比较，唯一的启发式检测maldoc是基于这样的观察：良性文档在不同平台上表现相同，而maldoc在开发过程中表现不同，因为系统调用，内存管理等的多样化实现跨平台。这样的启发式算法不需要已知的maldoc样本来导出区分maldoc和良性文档的模式，这也使得P LAT P AL 能够在事先不知道攻击的情况下检测到零日攻击。评估显示P LAT P AL在良性样本中不会产生虚假警报，在恶意样本中检测到各种行为差异，是一个可扩展和实用的解决方案。