PLATPAL: Detecting Malicious Documents with Platform Diversity

Meng Xu and Taesoo Kim

Georgia Institute of Technology

**Abstract:**

Due to the **continued exploitation** of Adobe Reader, **malicious document (maldoc)** detection has become a pressing problem. Although many solutions have been proposed, recent works have **highlighted some common drawbacks**, such as **parser-confusion and classifier-evasion attacks**.

In response to this, we propose a new perspective for **maldoc detection**: **platform diversity**. In particular, we identify eight factors in OS design and implementation that could **cause behavioral divergences under attack**, ranging from syscall semantics (more obvious) to heap object metadata structure (more subtle) and further show how they can **thwart attackers from finding bugs**, exploiting bugs, or performing malicious activities.

We further prototype PLATPAL to systematically harvest platform diversity. **PLATPAL hooks into Adobe Reader to trace internal PDF processing** and also uses sandboxed execution to capture a maldoc’s impact on the host system. Execution traces on **different platforms are compared**, and maldoc detection is based on the observation that a benign document behaves the same across platforms, while a **maldoc behaves differently during exploitation**. Evaluations show that PLATPAL raises **no false alarms in benign samples, detects a variety of behavioral discrepancies in malicious samples, and is a scalable and practical solution.**