An Integrated Treatment of Ransomware Through Microarchitecture and Software Solutions

UNIVERSITY OF MICHIGAN

Challenge:

- Current ransomware detection solutions are vulnerable to different evasion techniques. Although recovery solutions exist, these solutions leave victims with costly downtimes that stem from long data recovery periods.

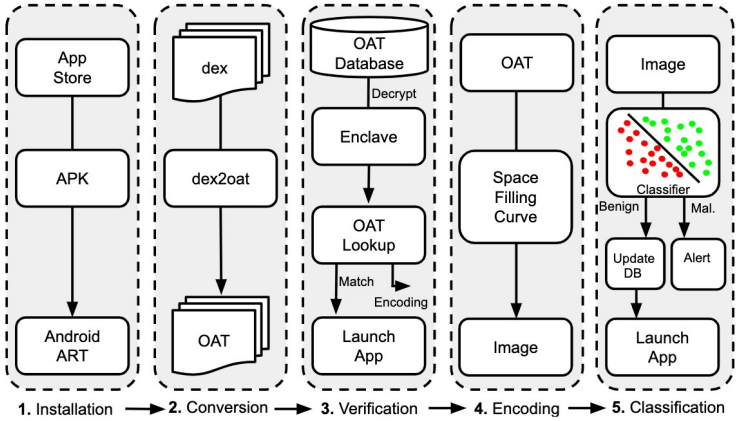

Figure 1: Overview of our mobile ransomware detection system integrated into the Android runtime system.

Scientific Impact:

- Multiple published papers (DSN'20, CAL'20, ESL'20, Access'21). Others under review.
- Resilient malware defenses scale across heterogenous systems (x86 and ARM).
- Seamless, live ransomware recovery system with <2% runtime overhead.

Solution:

- Accurate ransomware detection using visualization techniques (ESL'20)
- Cross stack malware defense system that is robust against evasion techniques (DSN'20, CAL'20)
- Deep learning introspection framework to understand features relevant for ransomware detection (under review).
- Seamless live recovery system to undo the effects of ransomware attacks after data is maliciously encrypted (under review).

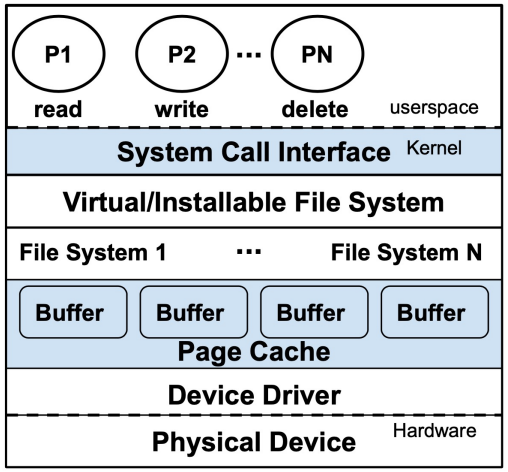

Figure 2: Overview of our live ransomware recovery system that leverages the system call interface and page cache to restore maliciously encrypted data.

Broader Impact:

- Two female PhD students and two undergrad students have been supported and trained.
- Models and dataset integrated into grad and undergrad course offerings
- Dataset for researchers to explore how visualization techniques can be harnessed for malware detection

CNS-1947580, University of Michigan
PI: Anys Bacha