











## **Experiences of Landing Machine Learning onto** Market-Scale Mobile Malware Detection

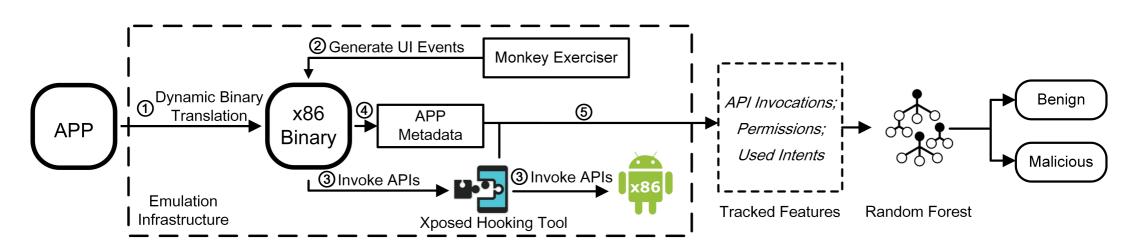
Hao Lin, Liangyi Gong, Zhenhua Li, Feng Qian, Zifan Zhang, Qi Alfred Chen, Zhiyun Qian, Yunhao Liu

## APICHECKER has been vetting 10K apps per day at

Tencent App Market since 03/2018! **260 APIs** Checking Hidden and Correlated to malware permissions internal APIs 70 APIs **112 APIs** IPC through Checking Restrictive Sensitive intents intents permission operation **Feature Selection: Feature Engineering:** Principled, data-driven Adversary's perspective Benign Malicious 430 Number of Key APIs 426 427 425 426 1.3 minutes per-app scan time, with 98% precision & 96% recall 7 Month **Analysis Speed: Model Evolution:** Efficient app emulation **Developer Engagement:** Monthly update with on powerful x86 servers Active & complete avoidance of false positives

## **APICHECKER: No Wooden Barrel Effect!**

vs. Passive mitigation of false negatives



novel apps & SDK APIs