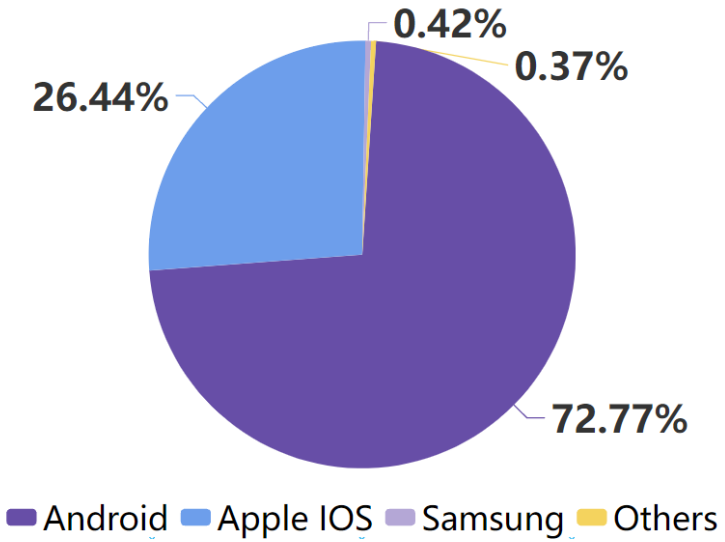
Visualizing Android Malware Feature Drift Through Time

Michael Tegegn

Intro: Android

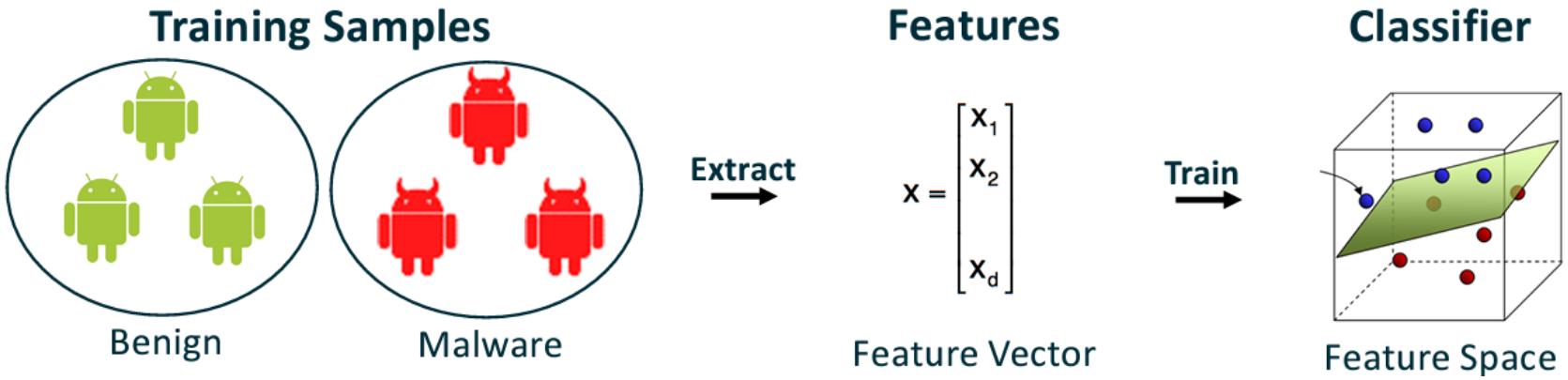
- Most widely used Mobile OS



- 12,000 new android malware instances every day. unb

Android Malware detection

- Machine learning based methods work great



- *Features more common in Malware applications should matter more.*

  On Benign Features in Malware Detection (Michael Cao et al. 2020)

Diagram above taken from Michael Cao's presentation slides

Problem

- Malware applications evolve over time
  - Evasion mechanisms exist

- Questions:
  1. Do malware application features change over time?
  2. Which features can boost Malware Detectors' robustness?

Project Tasks

- Goal: 2010 – 2020
- Compile datasets on the internet.
- Do we need both benign and malware apps or both?

- ❑ Which features to focus on?
- ❑ Effect of feature updates?

- ✓ Malware app feature drift over the years

- ✓ Any feature trend
- ✓ Which features are consistent?
- ✓ Which malware groups rely on which features?
- ✓ How can we make detectors robust?

Visualizing Android Malware Feature Drift Through Time

Interested?

Email: michaelwalelegn11@gmail.com