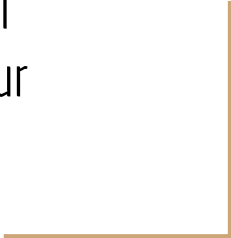




Detecting Malware in Android

Professor Fu
Hani Alshahrani
Harrison Mansour
Seaver Thorn



Outline

- Network info
- Intents and components
-
- This week
- Questions

(Day 1) Network Info

This week we worked on fixing the network information from apps to use as a feature. We are collecting:

- Number of bytes sent/received.
- Number of packets sent/received.

This is done through the Android API and will work on all tablets after Android 6.0.

This information will be put through our feature selection algorithms to determine if it is a useful feature or not.

(Day 2-4) App Components and Intents

- As mentioned last week, we are expanding our feature set.
- This week we focused on finalizing programs to extract all these new features.
- On Friday we started our programs and features for 2,000 benign apps were collected over the weekend.
- Yesterday we started running our program on a set of 2,000 malicious apps.

This week

- Draft research paper.
- Run tablets with new features collected.

Questions?