Twitter-Enhanced Android Malware Detection

Jordan DeLoach Doina Caragea

Microsoft[1] Kansas State University

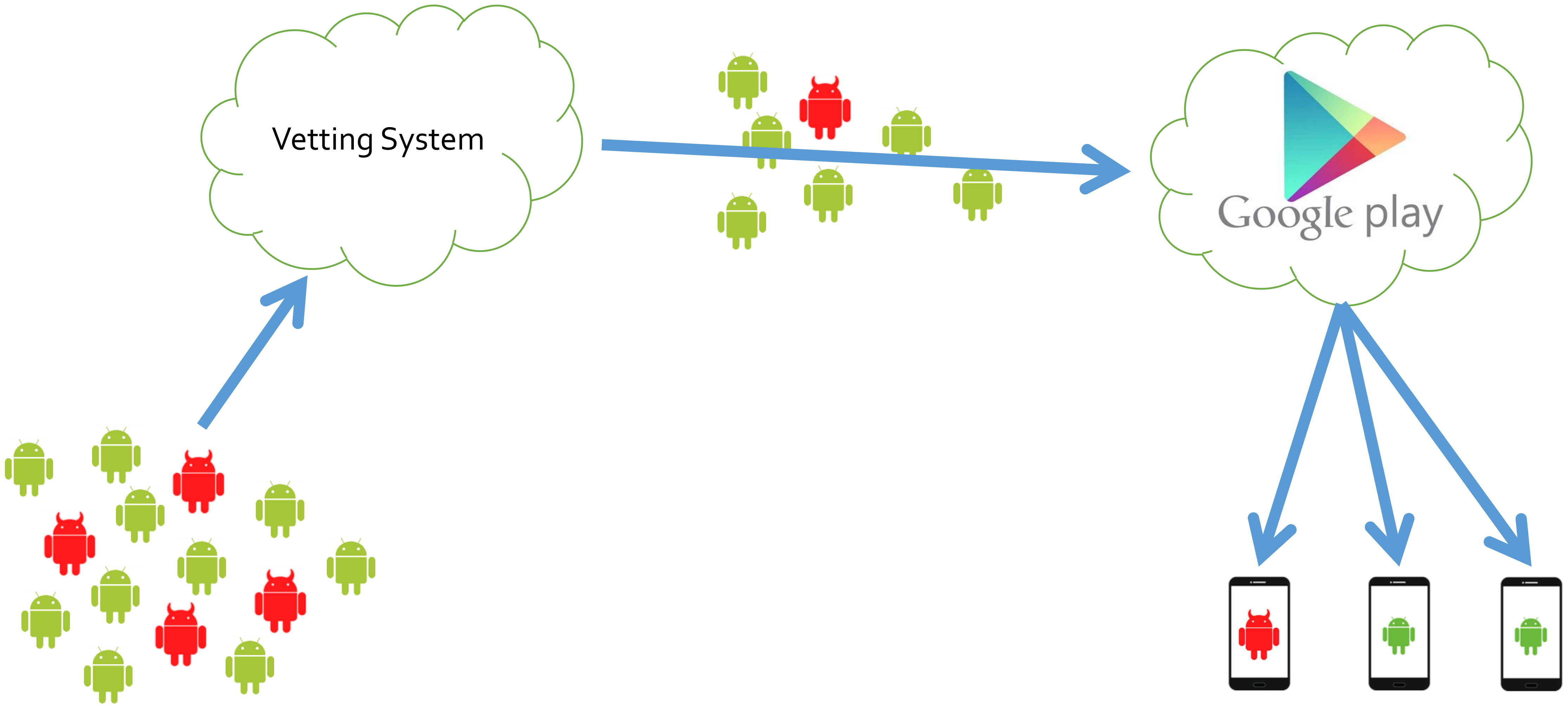
[1] Work performed while at Kansas State University

International Workshop on Big Data Analytics for Cyber Intelligence and Defense

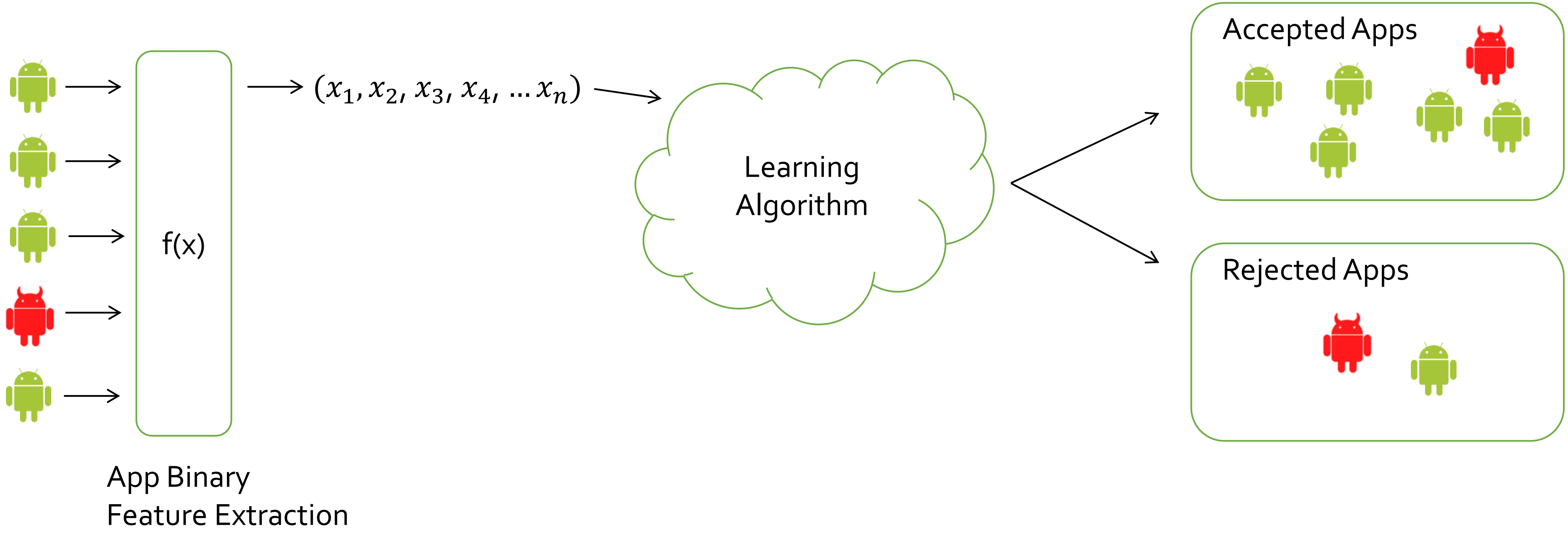
Android Malware

- Android dominates market share world wide
- Common malware behavior:
  - Leaking personal data
  - GPS tracking
  - SMS messages to premium numbers
- Reported levels of malware in the Google Play Store vary anywhere from Google's self-reported less than 1% to 7% or higher.
- Machine learning has been proposed as a way to take old apps that are malware or benign, and learn classifiers from them.

Vetting Process



Standard ML-Approach to Vetting



f(x)

$(x_1, x_2, x_3, x_4, \ldots x_n)$

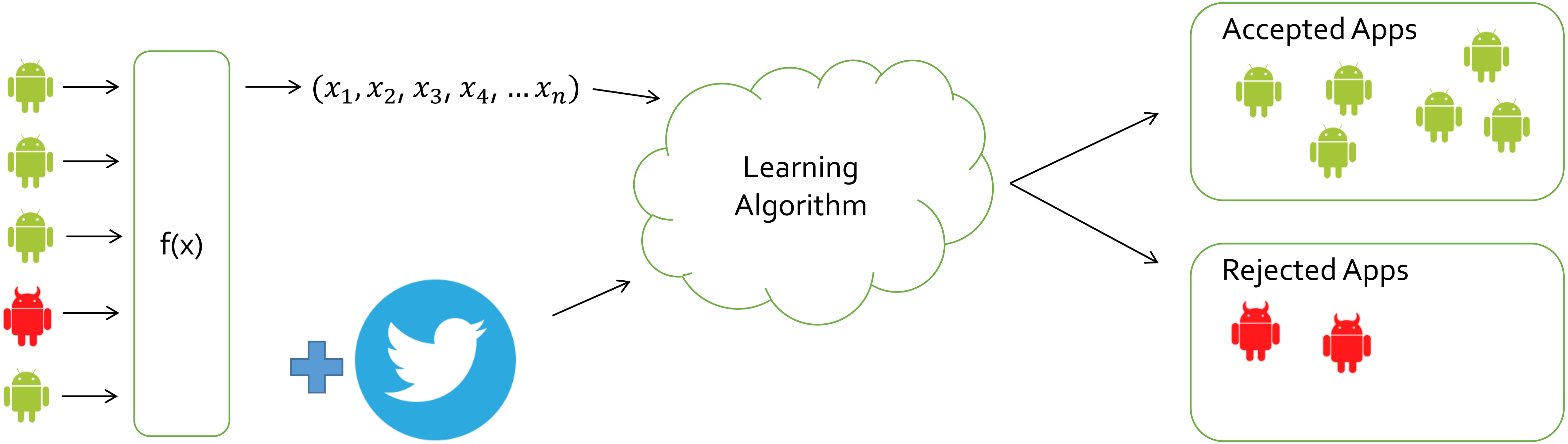
Learning Algorithm

Accepted Apps

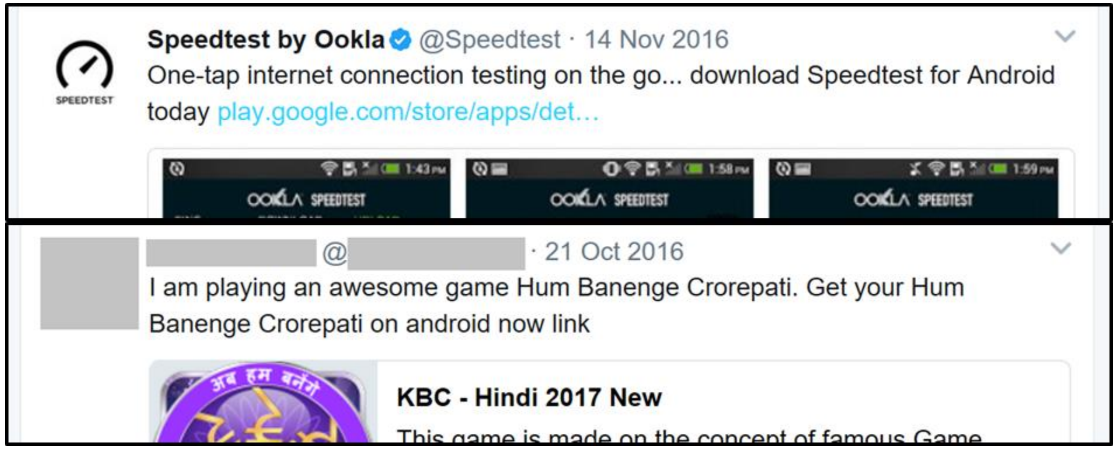
Rejected Apps

App Binary Feature Extraction

Standard ML-Approach to Vetting + Social?



App Binary
Feature Extraction



Speedtest by Ookla @Speedtest · 14 Nov 2016

One-tap internet connection testing on the go... download Speedtest for Android today play.google.com/store/apps/det...

[redacted] @[redacted] · 21 Oct 2016

I am playing an awesome game Hum Banenge Crorepati. Get your Hum Banenge Crorepati on android now link

KBC - Hindi 2017 New

This game is made on the concept of famous Game

Datasets

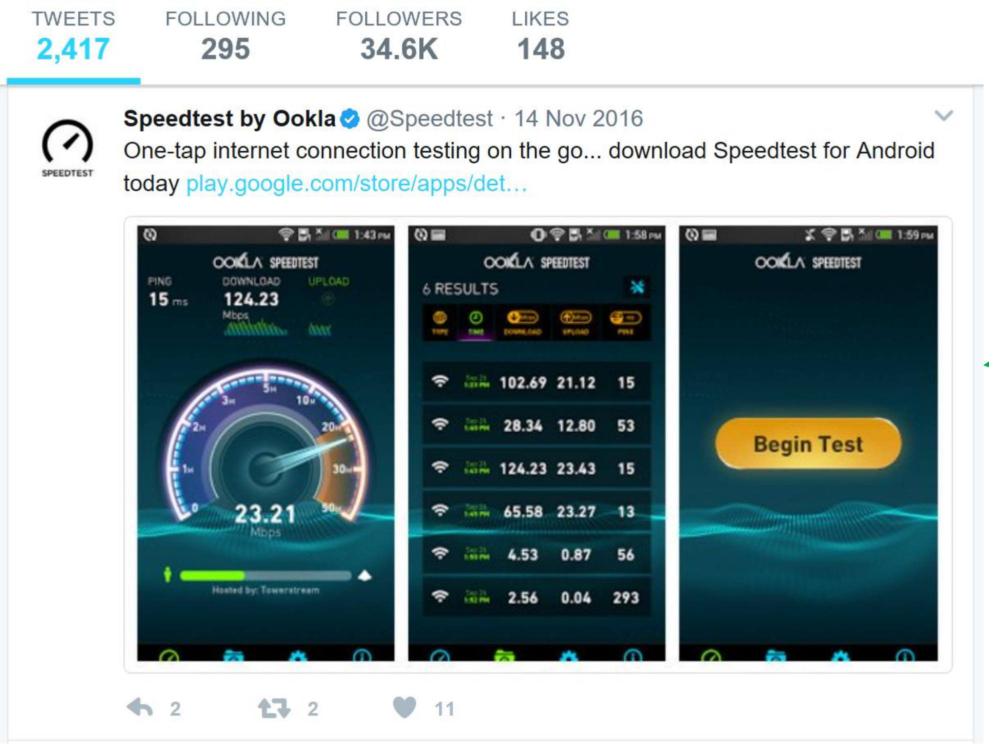
- Android Apps: PlayDrone and AndroZoo datasets
  - 1.38 million apps, of which 158k were considered malicious (based on at least 3 VirusTotal scanners), and 939k were benign
  - We do not use all of these apps, we use only those for which we have a linked tweet
- Twitter Dataset
  - Used Twitter Firehose API, and listened for keywords such as “Android,” “app,” “mobile,” and “malware”
  - Crawled 50 million tweets over November & December 2016

Two Key Challenges

1. How to relate a tweet with an app?
2. How to effectively use tweets to aid malware detection?

Two Key Challenges

1. How to relate a tweet with an app?
2. How to effectively use tweets to aid malware detection?

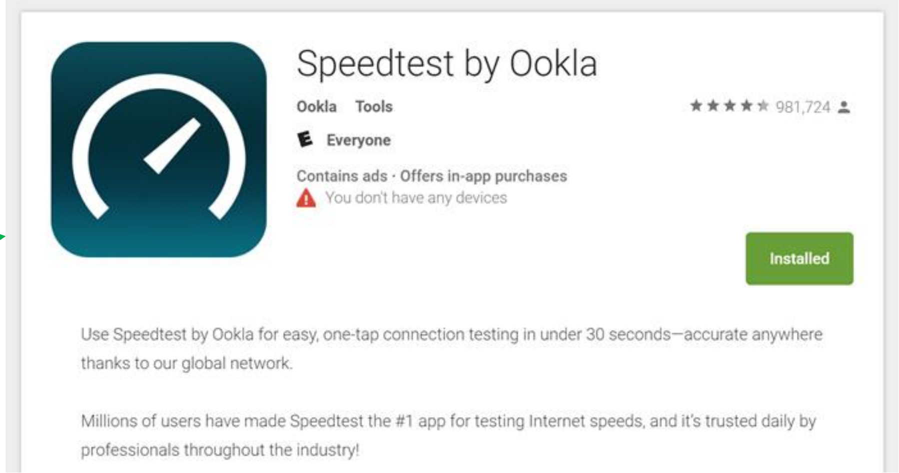


TWEETS	FOLLOWING	FOLLOWERS	LIKES
2,417	295	34.6K	148

Speedtest by Ookla @Speedtest · 14 Nov 2016

One-tap internet connection testing on the go... download Speedtest for Android today play.google.com/store/apps/det…

TYPE	TIME	DOWNLOAD	UPLOAD	PING
	[illegible]	102.69	21.12	15
	[illegible]	28.34	12.80	53
	[illegible]	124.23	23.43	15
	[illegible]	65.58	23.27	13
	[illegible]	4.53	0.87	56
	[illegible]	2.56	0.04	293



Speedtest by Ookla

Ookla Tools

★★★★★ 981,724

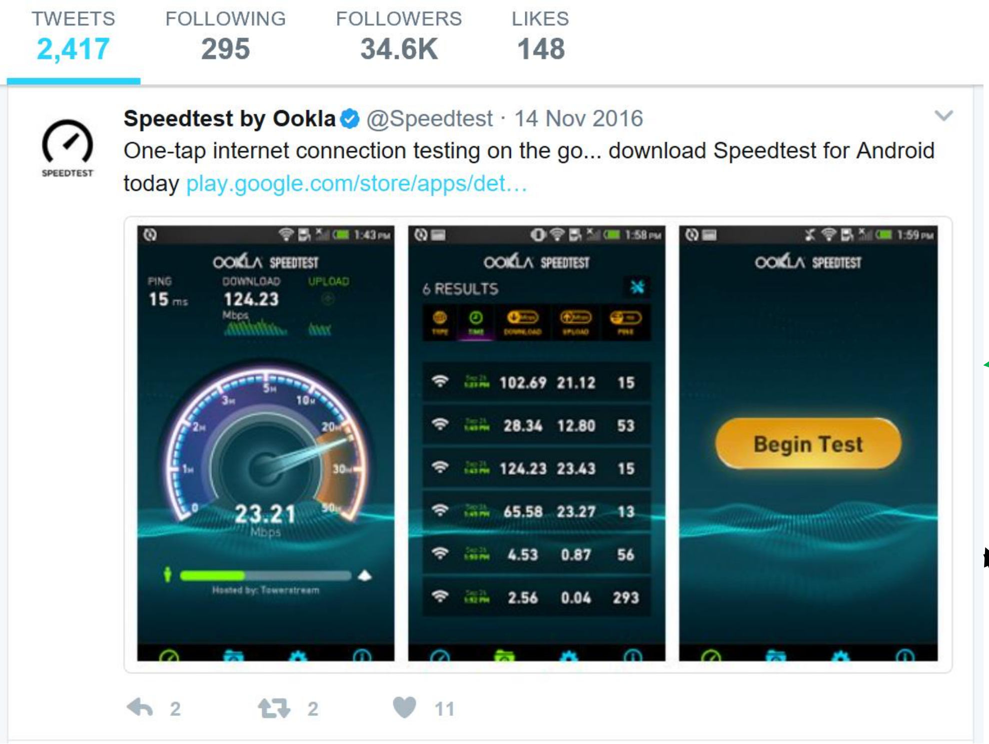
Everyone

Contains ads · Offers in-app purchases

You don't have any devices

Use Speedtest by Ookla for easy, one-tap connection testing in under 30 seconds—accurate anywhere thanks to our global network.

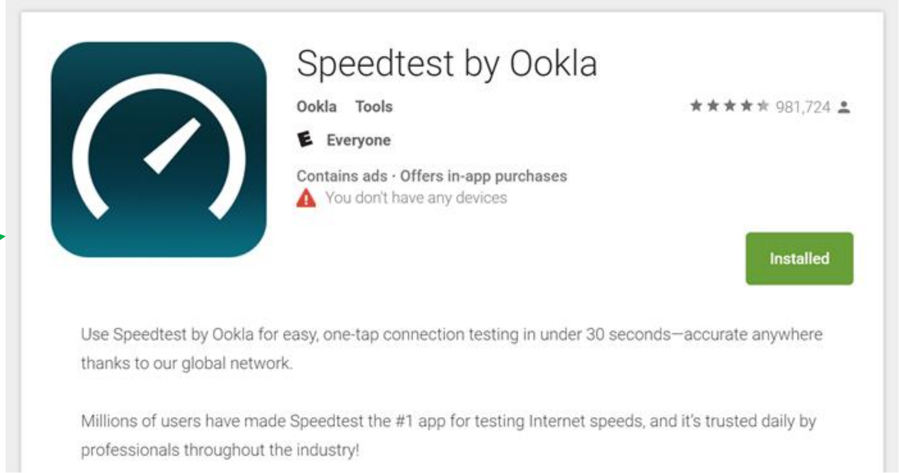
Millions of users have made Speedtest the #1 app for testing Internet speeds, and it's trusted daily by professionals throughout the industry!



TWEETS 2,417 FOLLOWING 295 FOLLOWERS 34.6K LIKES 148

Speedtest by Ookla @Speedtest · 14 Nov 2016

One-tap internet connection testing on the go... download Speedtest for Android today play.google.com/store/apps/det…



Speedtest by Ookla

Ookla Tools ★★★★★ 981,724

Everyone

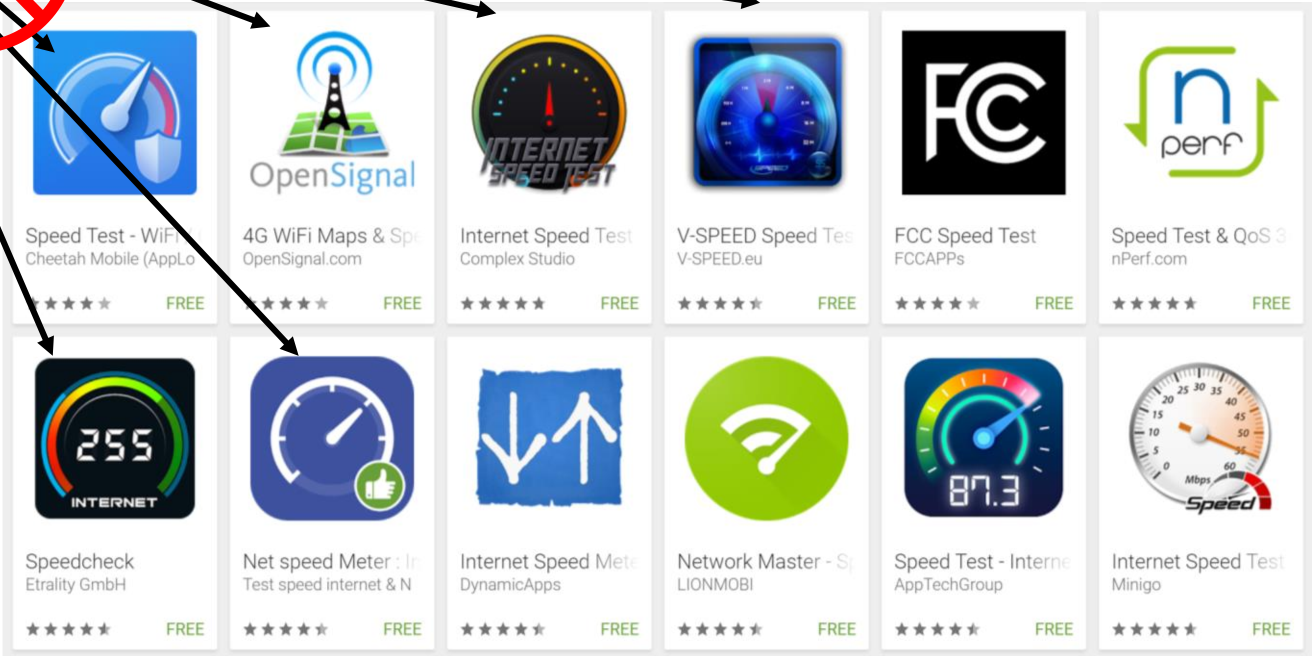
Contains ads · Offers in-app purchases

You don't have any devices

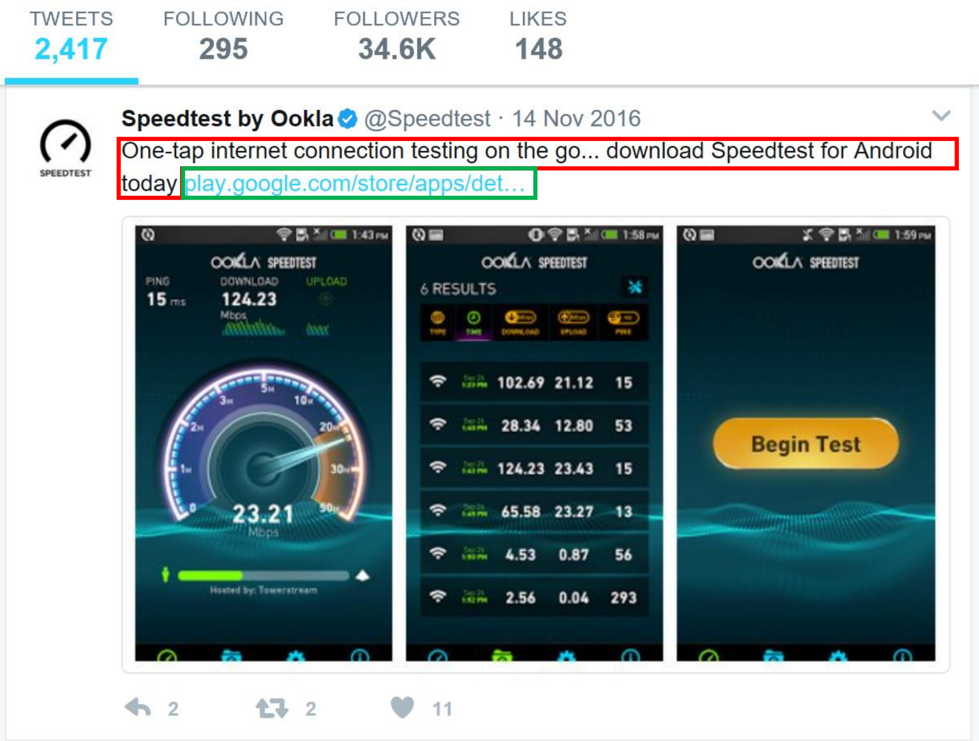
Installed

Use Speedtest by Ookla for easy, one-tap connection testing in under 30 seconds—accurate anywhere thanks to our global network.

Millions of users have made Speedtest the #1 app for testing Internet speeds, and it's trusted daily by professionals throughout the industry!



Speed Test - WiFi Cheetah Mobile (AppLo FREE	4G WiFi Maps & Sp OpenSignal.com FREE	Internet Speed Test Complex Studio FREE	V-SPEED Speed Tes V-SPEED.eu FREE	FCC Speed Test FCCAPPs FREE	Speed Test & QoS nPerf.com FREE
Speedcheck Etrality GmbH FREE	Net speed Meter : I Test speed internet & N FREE	Internet Speed Mete DynamicApps FREE	Network Master - S LIONMOBI FREE	Speed Test - Interne AppTechGroup FREE	Internet Speed Test Minigo FREE

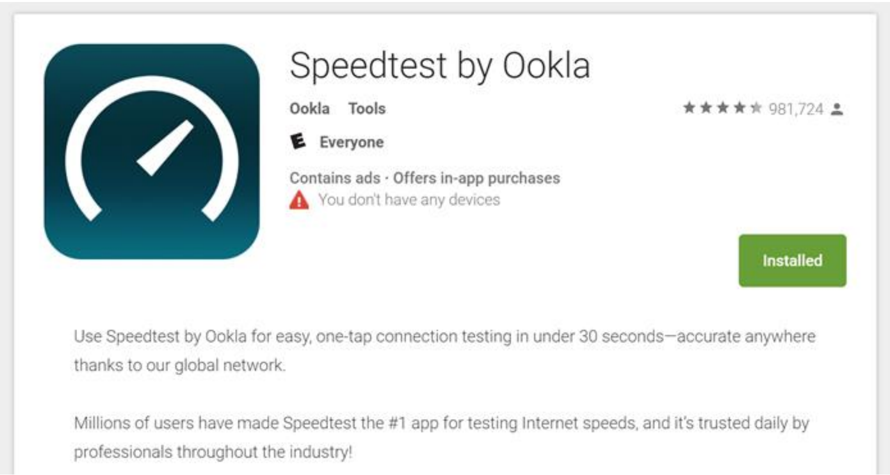


TWEETS 2,417 FOLLOWING 295 FOLLOWERS 34.6K LIKES 148

Speedtest by Ookla @Speedtest · 14 Nov 2016

One-tap internet connection testing on the go... download Speedtest for Android today play.google.com/store/apps/det…

2 2 11



Speedtest by Ookla

Ookla Tools

★★★★★ 981,724

Everyone

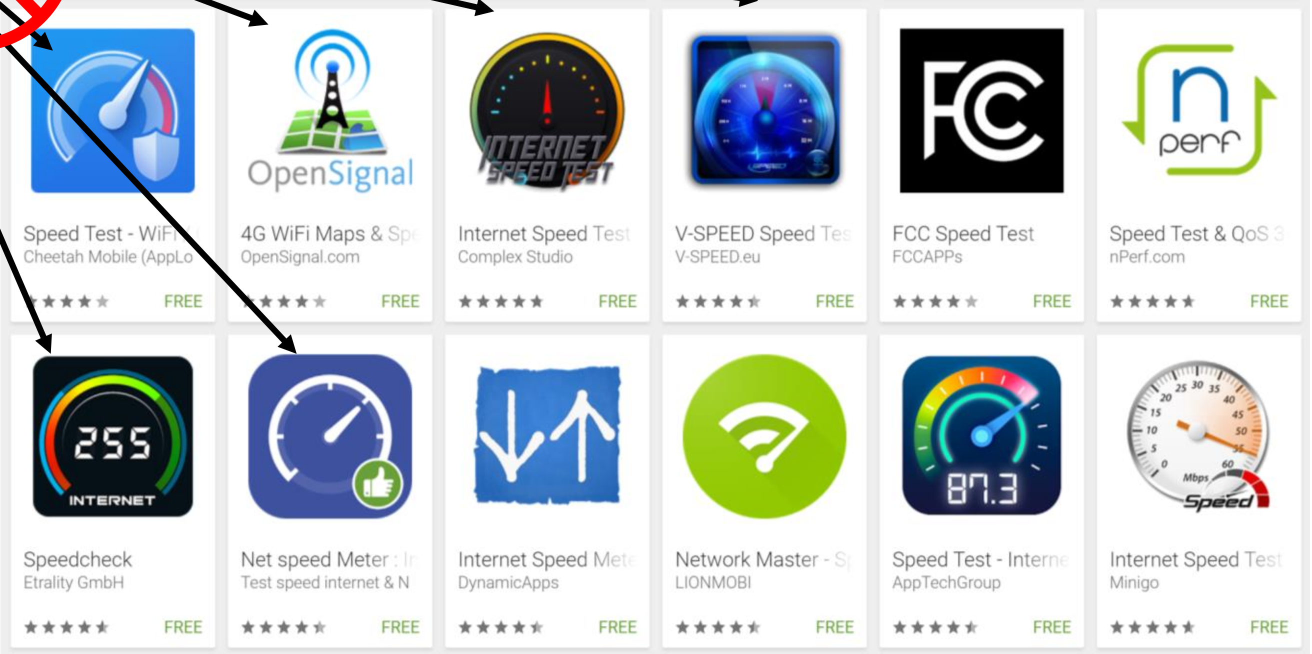
Contains ads · Offers in-app purchases

You don't have any devices

Installed

Use Speedtest by Ookla for easy, one-tap connection testing in under 30 seconds—accurate anywhere thanks to our global network.

Millions of users have made Speedtest the #1 app for testing Internet speeds, and it's trusted daily by professionals throughout the industry!



Speed Test - WiFi
Cheetah Mobile (AppLo
FREE

4G WiFi Maps & Sp
OpenSignal.com
FREE

Internet Speed Test
Complex Studio
FREE

V-SPEED Speed Tes
V-SPEED.eu
FREE

FCC Speed Test
FCCAPPs
FREE

Speed Test & QoS 3
nPerf.com
FREE

Speedcheck
Etrality GmbH
FREE

Net speed Meter : In
Test speed internet & N
FREE

Internet Speed Mete
DynamicApps
FREE

Network Master - S
LIONMOBI
FREE

Speed Test - Interne
AppTechGroup
FREE

Internet Speed Test
Minigo
FREE

Two Linkable Pieces:

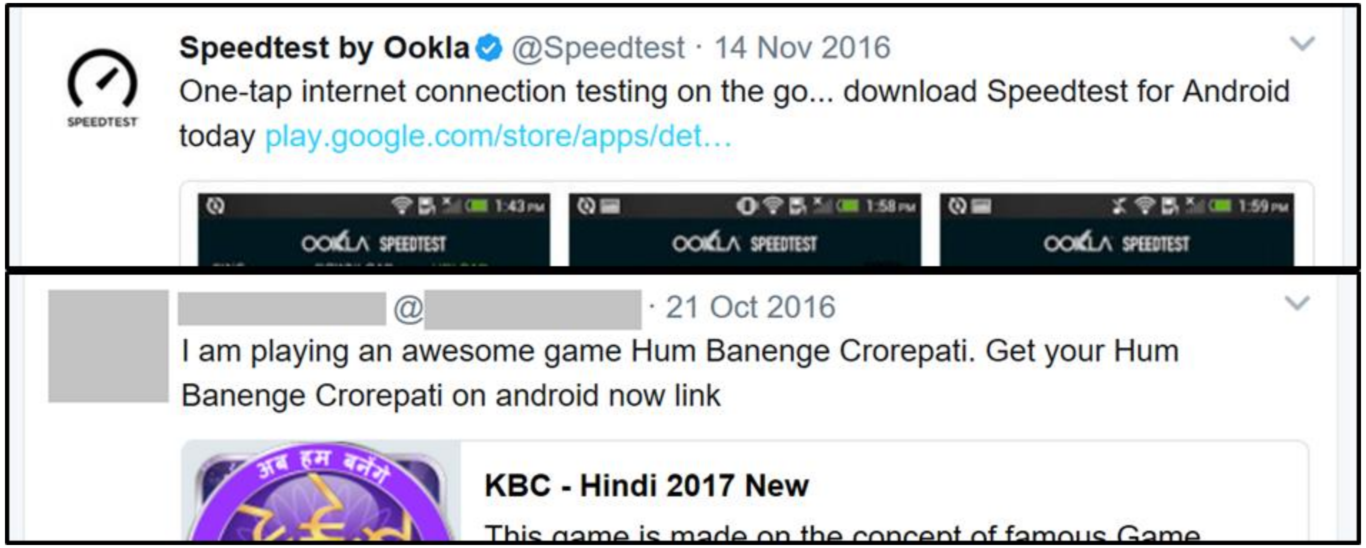
- Tweet Text
- Tweet Links

Two Key Challenges

1. How to relate a tweet with an app?
    1. An exact method based on direct links to the app store
    2. Approximate methods based on text matching
2. How to effectively use tweets to aid malware detection?

HTTP Links as Ground Truth

- Many tweets include a direct Google Play Store HTTP link from which we can confidently link an app and a Tweet
- Our combined Android app and Twitter dataset had
  - over 26,000 tweets with links to apps
  - 4,674 apps had at least one tweet



Speedtest by Ookla @Speedtest · 14 Nov 2016

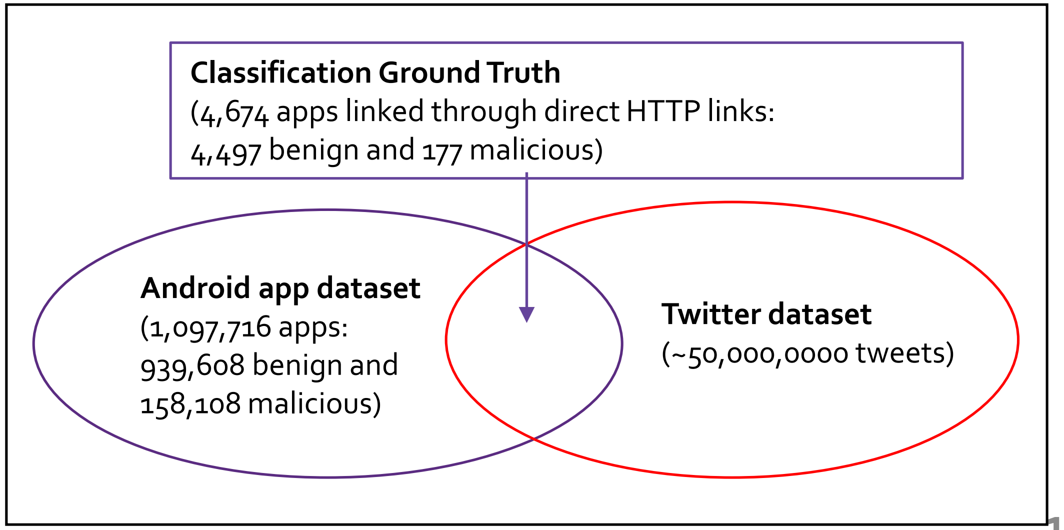
One-tap internet connection testing on the go... download Speedtest for Android today play.google.com/store/apps/det…

[redacted] [redacted] @[redacted] · 21 Oct 2016

I am playing an awesome game Hum Banenge Crorepati. Get your Hum Banenge Crorepati on android now link

KBC - Hindi 2017 New

This game is made on the concept of famous Game



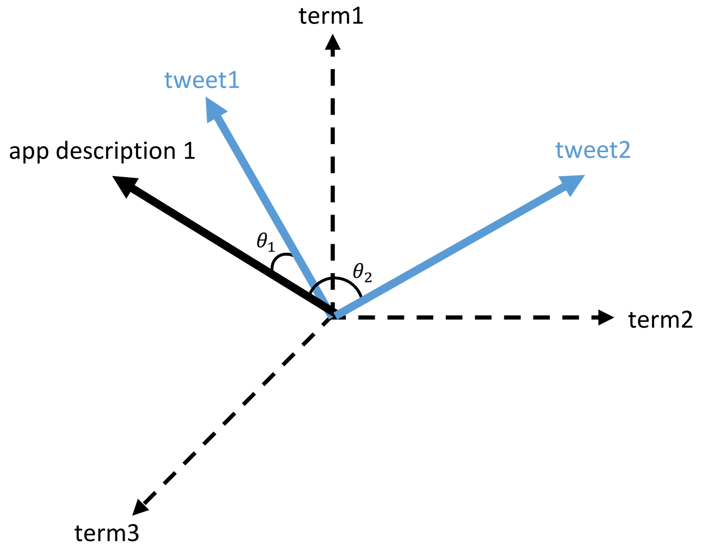
Classification Ground Truth
(4,674 apps linked through direct HTTP links:
4,497 benign and 177 malicious)

Android app dataset
(1,097,716 apps:
939,608 benign and
158,108 malicious)

Twitter dataset
(~50,000,0000 tweets)

Vector Space Models & TF-IDF

- We use a Vector Space Model (VSM) inspired approach for linking tweets and apps without an HTTP link
- We utilize Term Frequency-Inverse Document Frequency (TF-IDF) to vectorize these texts, and identify relationships between them by calculating text similarity
- For every tweet, we calculate and rank along the cosine similarity between the tweet and the apps with which they have at least one term in common

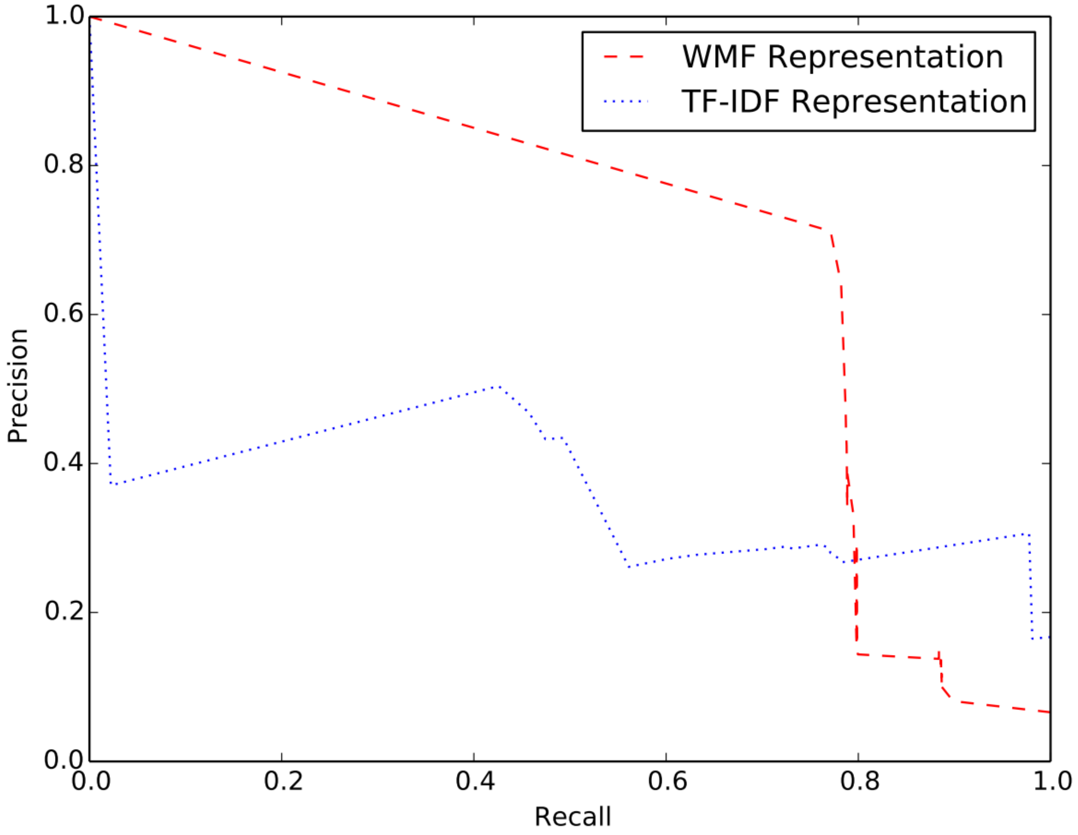


Weighted Matrix Factorization

- Twitter text is quite distinct from the text of other domains, in the sense that its corresponding vectors are exceptionally sparse.
- Dimensionality reduction techniques allow more equitable distribution of features in short-texts.
- WMF allows us to tune for missing words- beneficial for short-texts
- WMF Parameters
  - K, the number of latent components;
  - α, a multiplier used to vary the weight given to terms;
  - λ, a regularization parameter.

Evaluating Linking Approaches

- To evaluate, we want to consider relative certainness of a given link
- We leverage the Precision-Recall Curve (PRC) at various confidence levels
- PRC allows us to visualize the trade-off between a higher precision result, and that of a less precise, higher recall result set using a lower threshold.

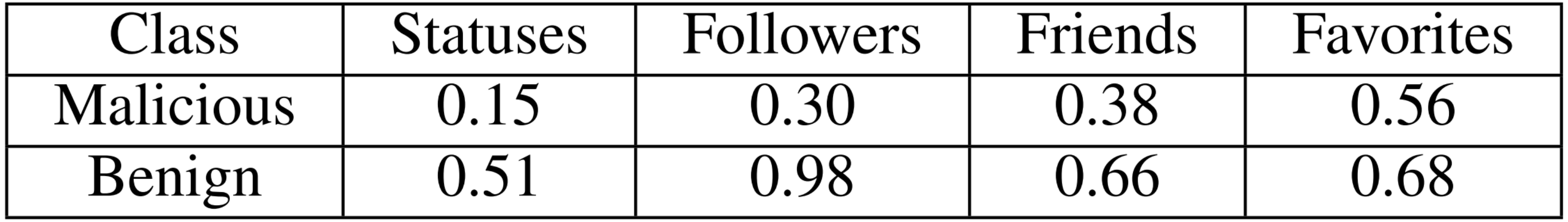


Two Key Challenges

1. How to relate a tweet with an app?
    1. An Exact Method
    2. Approximate Methods
2. How to effectively use tweets to aid malware detection?
    1. Tweet feature extraction
    2. Classification

Feature Extraction from Tweets

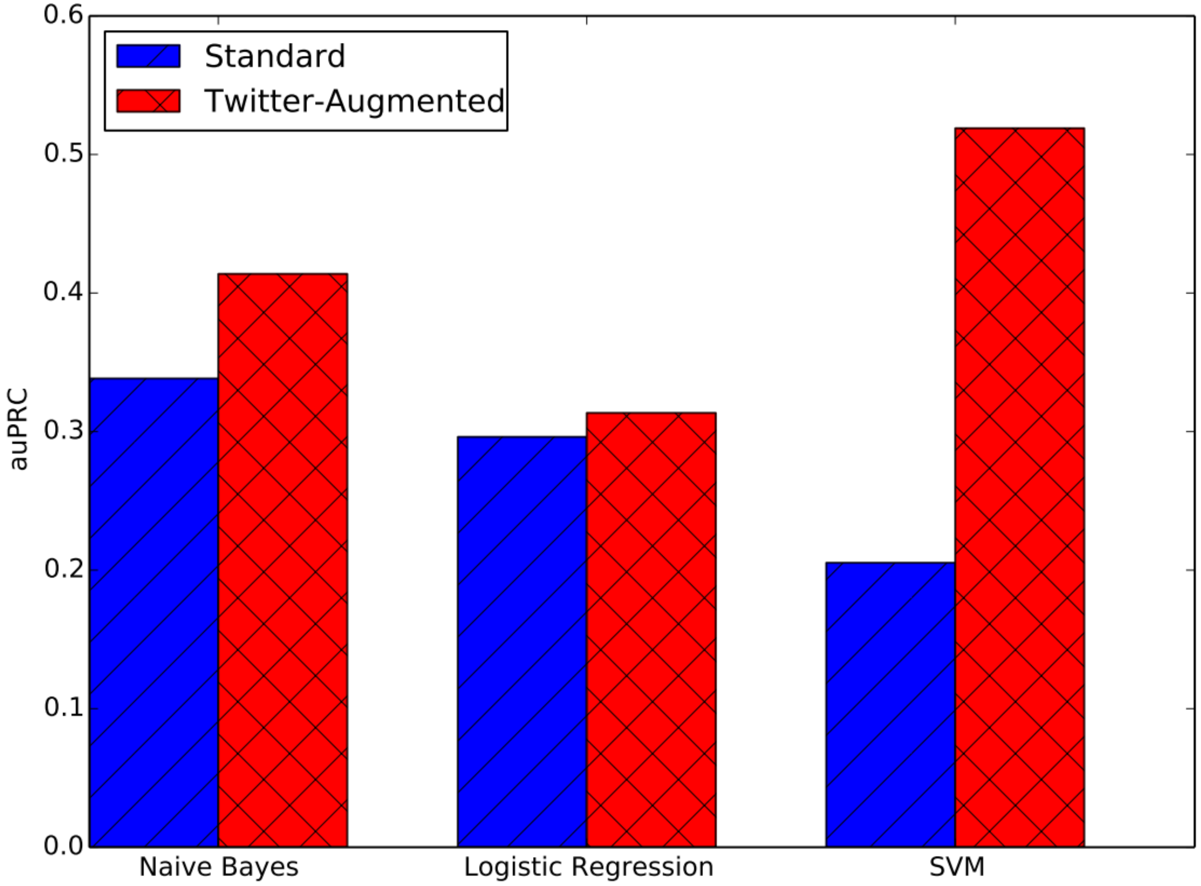
- Given a set of tweets linked to an app, they need to be included in the feature vector
- We use metrics provided by Twitter to represent both the tweet and the tweet author as features
  - We find them to be statistically distinct
  - Based on prior related research, the peer feedback metrics (#favorites, #followers, etc.) are key in determining spam users and tweets
- For each metric, we average the values corresponding to the tweets linked to an app, and append the average values to the binary feature vector



Class	Statuses	Followers	Friends	Favorites
Malicious	0.15	0.30	0.38	0.56
Benign	0.51	0.98	0.66	0.68

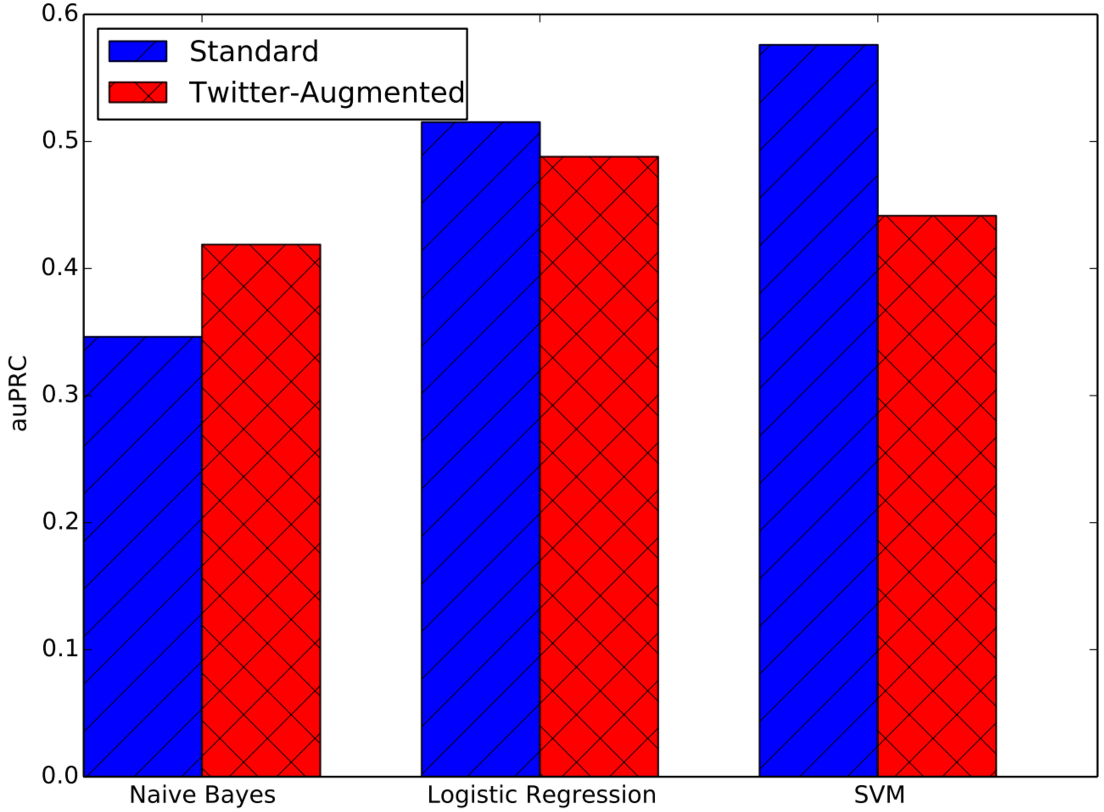
Malware Detection Results on the HTTP-Linked Ground Truth Dataset

- Using HTTP links, Twitter-augmented detection outperforms the standard detection approaches that use only features extracted from app binaries
- While overall auPRC is low - we attribute this to dataset size - Twitter-augmented detection shows a net gain



Approximate-Linked Classification Results

- We used a subset of our dataset of roughly 45,000 app descriptions and 1.6 million tweets for automated linking.
- Using WMF we return any links thresholded at 0.6 similarity or above
- We speculate one reason for decreased performance is that the inaccuracy of some app tweet links impairs classification
- While our previous experiments clearly show that Twitter data helps in the classification process, this experiment shows further research into linking is necessary



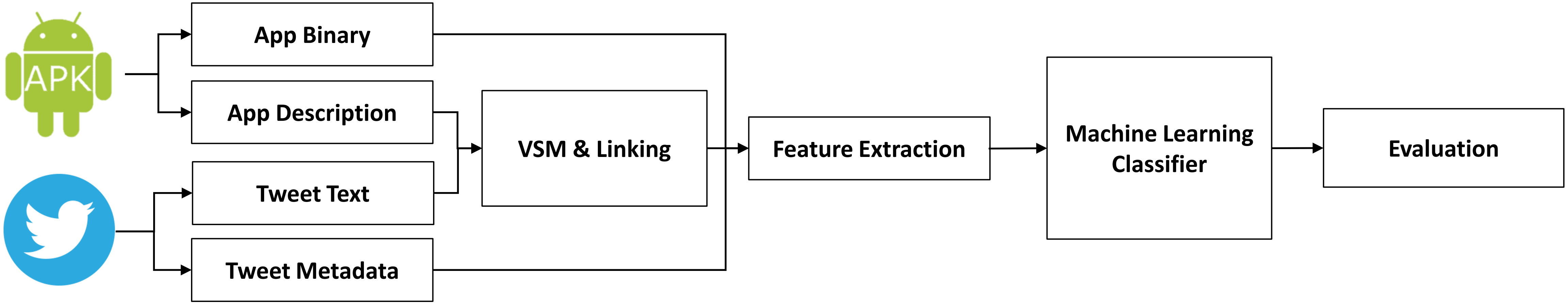
Conclusions

- We presented a novel approach for augmenting machine learning approaches with Twitter data to improve Android malware detection
- We introduced three linking techniques, which allow us to make connections between tweets and the apps that they reference
- Our preliminary findings show that Twitter data is a beneficial addition
- We believe larger datasets and more robust linking methods will improve classifier performance
- Our work, the first of its kind integrating social media data with Android malware detection, proves to be a promising avenue for future research
- Malware increasingly spreads through social media, so it only makes sense to holistically consider tweets as an avenue when attempting to detect malware

Questions?

jordan.deloach@microsoft.com

Social ML-Approach Architecture



APK
App Binary
App Description
Tweet Text
Tweet Metadata
VSM & Linking
Feature Extraction
Machine Learning Classifier
Evaluation