Eavesdropping on Fine-Grained User Activities Within Smartphone Apps Over Encrypted Network Traffic

Brendan Saltaformaggio, Hongjun Choi, Kristen Johnson, Yonghwi Kwon, Qi Zhang, Xiangyu Zhang, Dongyan Xu, John Qian*

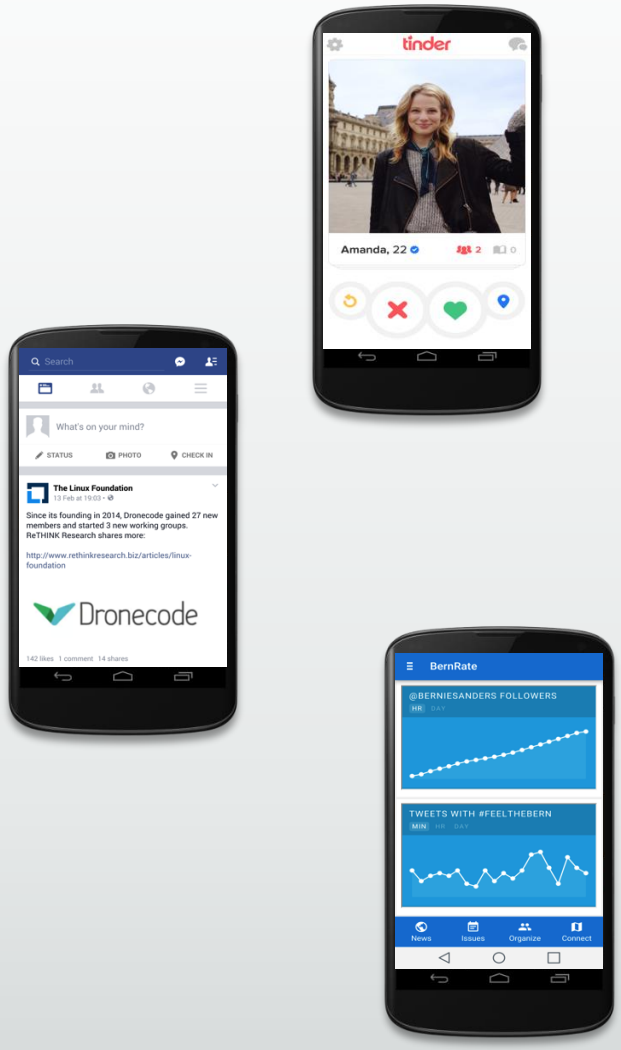
Purdue University *Cisco Systems

PURDUE UNIVERSITY CERIAS

Motivation

Smartphone apps are becoming **highly specialized**

Dating,
Social Media,
Political Campaigns,
Much More…



Modern apps rely on **fully encrypted communication** to protect users' network data

Thus packet content is not helpful to eavesdroppers

Motivation

But each specialized activity generates very **distinct patterns** in the encrypted network traffic

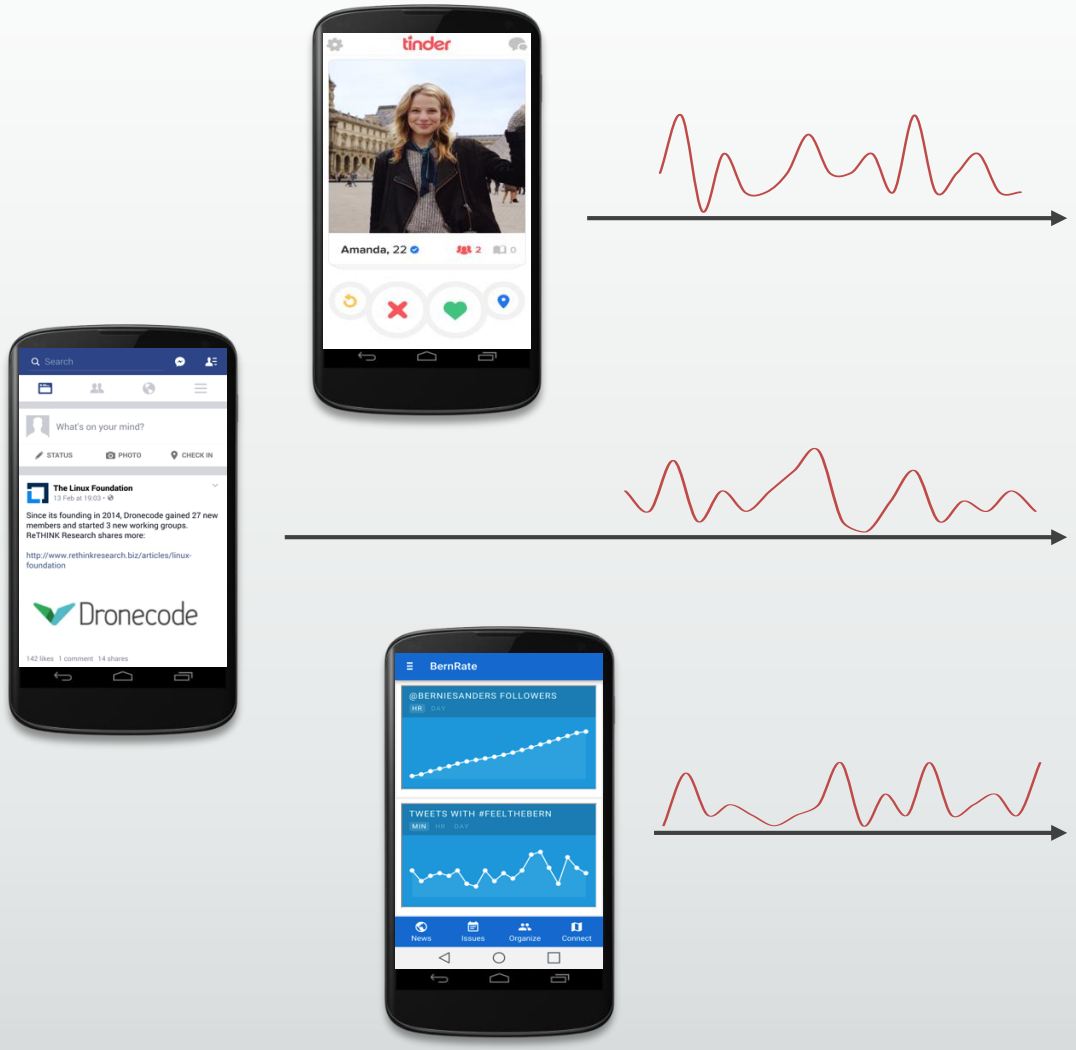
E.g.: Transfer Rates, Packet Exchanges, and Data Movement



Traffic Behavioral Clues

But each specialized activity generates very **distinct patterns** in the encrypted network traffic

E.g.: Transfer Rates, Packet Exchanges, and Data Movement



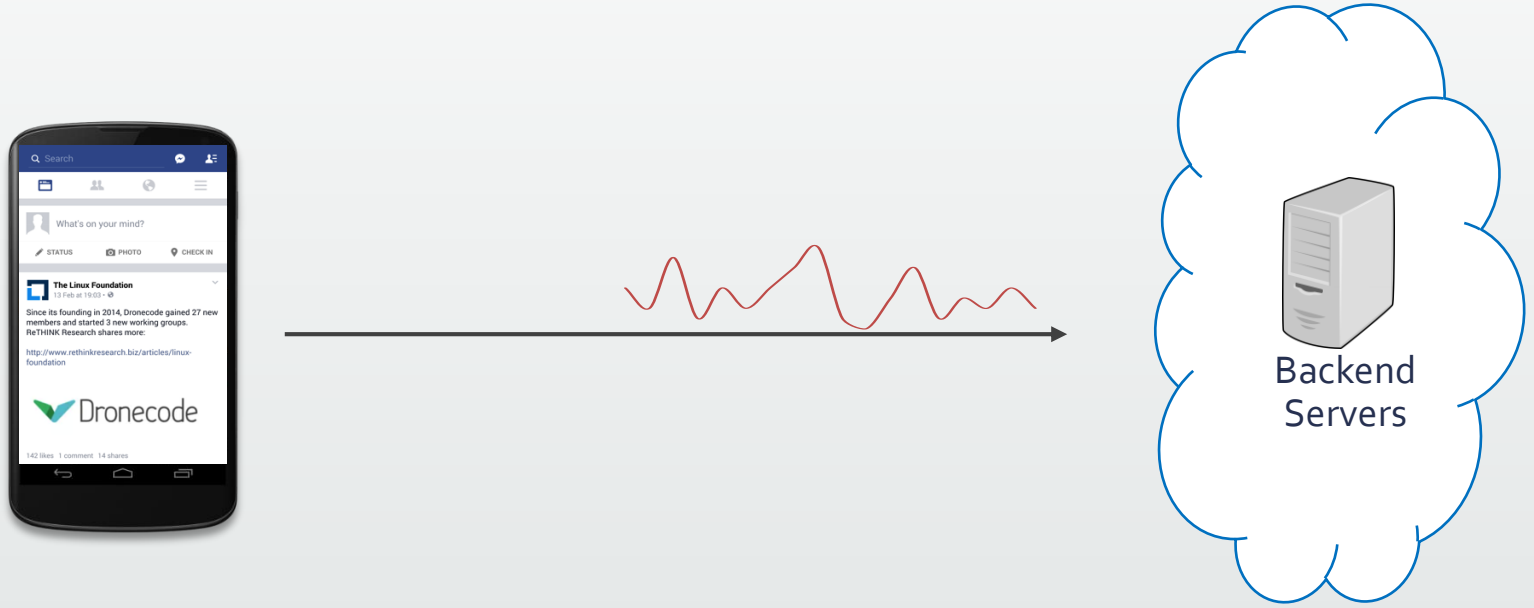
We call this the traffic's **behavior**

These can reveal sensitive info. about the apps

Traffic Behavioral Clues

Observation #1

An app's traffic behavior is mostly **shaped by the servers** the app communicates with

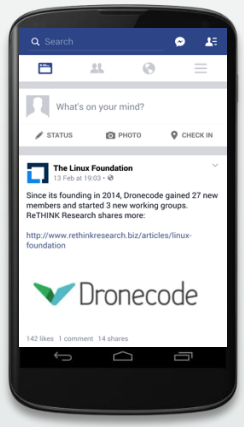


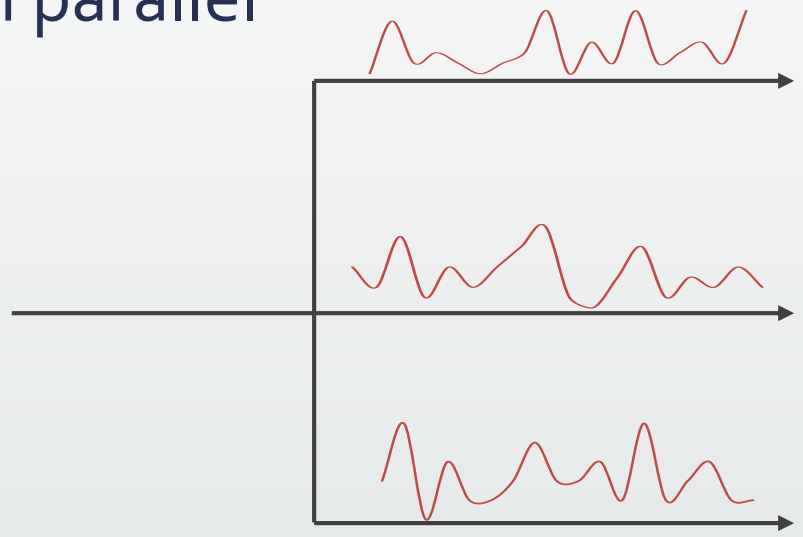
Traffic Behavioral Clues

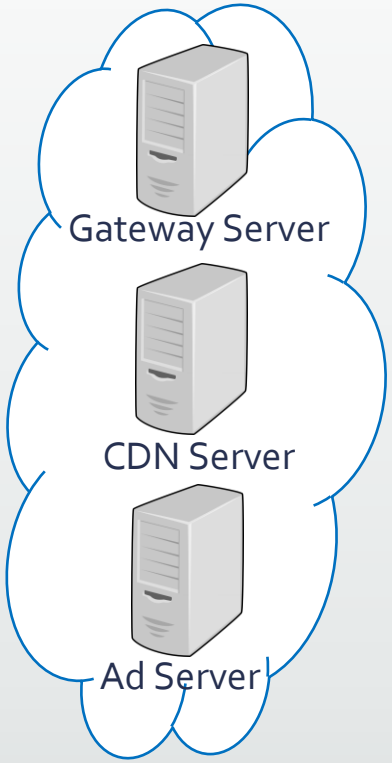
Observation #1

An app's traffic behavior is mostly **shaped by the servers** the app communicates with

Apps connect to many servers in parallel





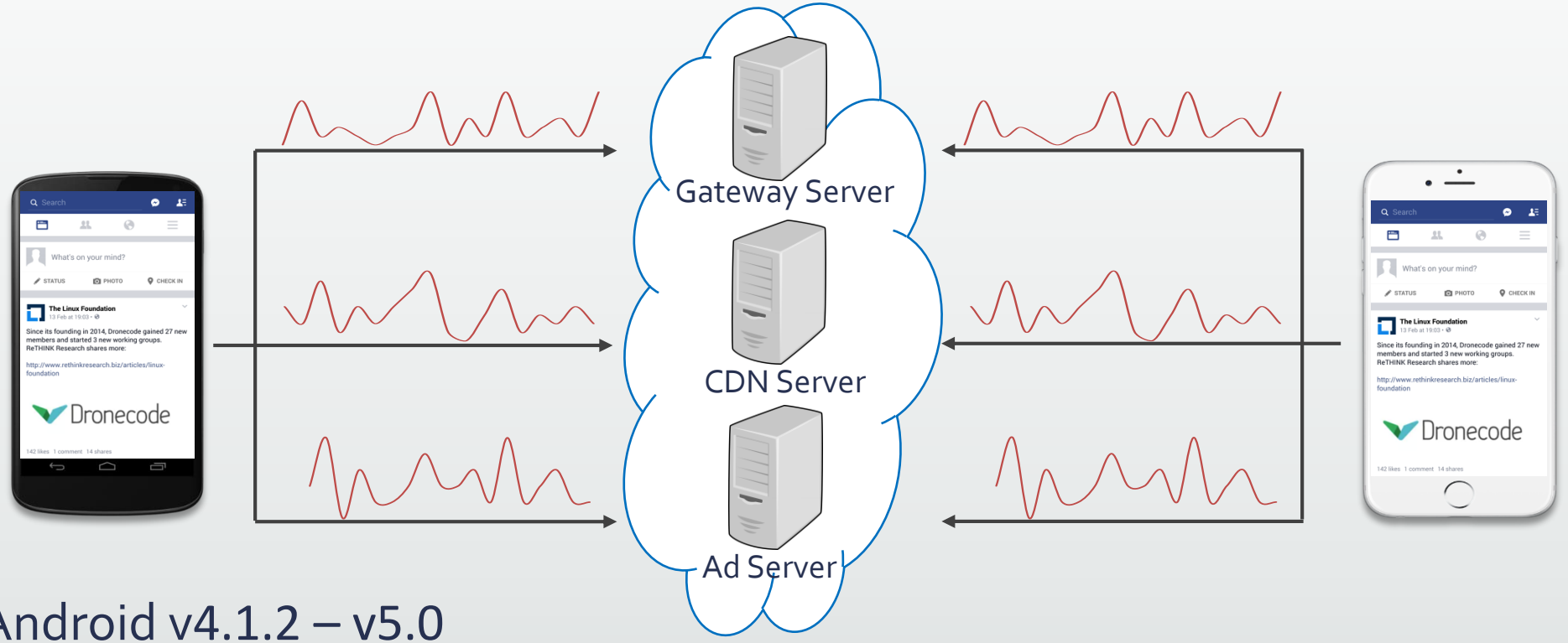


Each server's traffic behavior is shaped by its purpose

Cross-Platform Traffic Behaviors

Because servers shape the traffic behaviors…

Those behaviors are **common across smartphone platforms**



- 5 Vendor Customized Android v4.1.2 – v5.0

- iPhone 6, iPhone 6 Plus

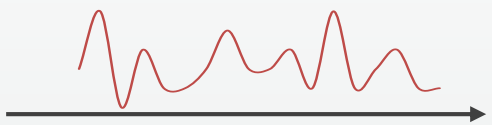
Activity Specific Traffic Behavior

Observation #2

Different activities within a single app will generate **discernibly different** traffic behaviors

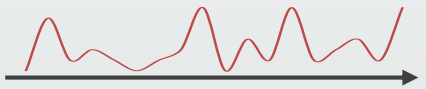
Browsing for Tinder Matches

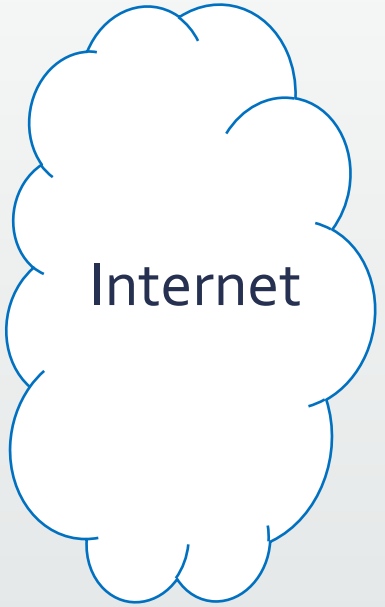




Chatting with Tinder Connections







Activity Specific Traffic Behavior (More In Paper)

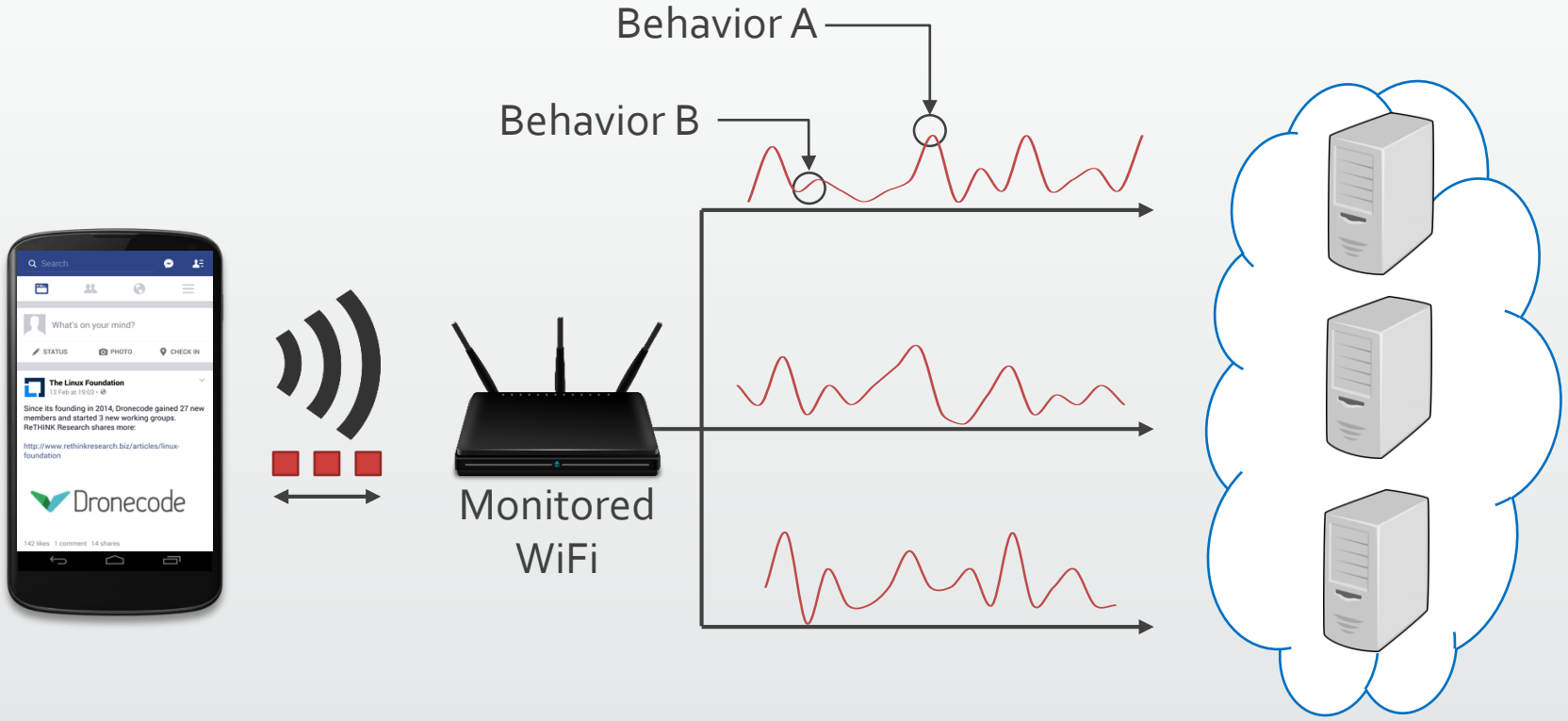
Category	App	Activity
News & Politics	CNN News	Browse news articles
	Bernie Sanders 2016	Read stances and updates
	Ben Carson 2016	Read stances and updates
Personal Health	HIV Atlas	Lookup treatment information
		Find HIV test clinics
Social	Facebook	Read Facebook Feed
		Post to Facebook
	Twitter	Post new tweet
		Read tweets
	Instagram	Browse Posts
		Post to Instagram
	Snapchat	Photo Chat

Category	App	Activity
Dating	Ashley Madison	Browse potential matches
	Tinder	Browse potential matches
		Chat with connections
	OkCupid	Browse potential matches
		Chat with connections
Communication	Gmail	Read email
		Send email
	Skype	Video call with friend
		Voice call with friend
		Message chat with friend
Media	YouTube	Watch videos
		Search and browse videos

NetScope: Eavesdropping on Fine-Grained Activities

Step 1: Model each app's semantic activities from **measured traffic behaviors**

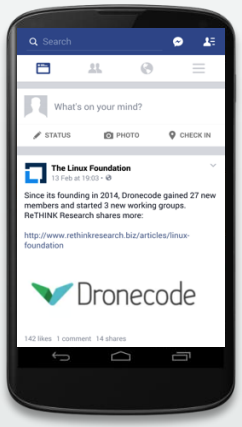
Step 2: Match a variety of behavior models for lightweight **online eavesdropping**



(Ahead Of Time) Offline Training

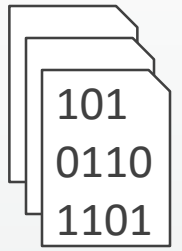
Eavesdropper first performs **offline training** with the apps/activities to detect







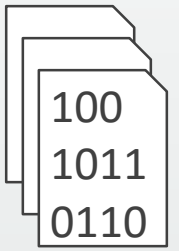
NetScope collects packet traces of the encrypted traffic



"Tinder Browse"



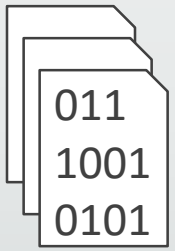
Packet Collection



"Facebook Read"

The granularity of an "activity" is based on detection results

The eavesdropper gives each a label

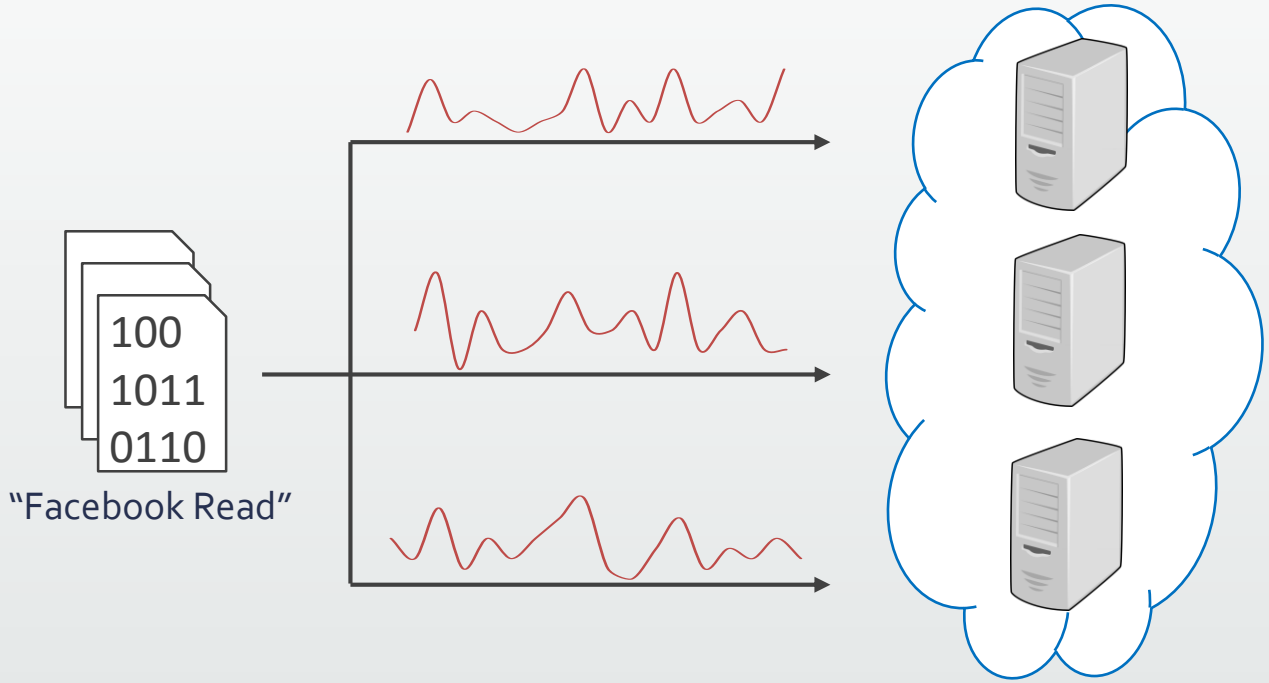


"Feelin' the Bern"

Building Behavioral Models

Following our observation of servers shaping traffic behaviors:

NetScope partitions the packets by remote server transactions



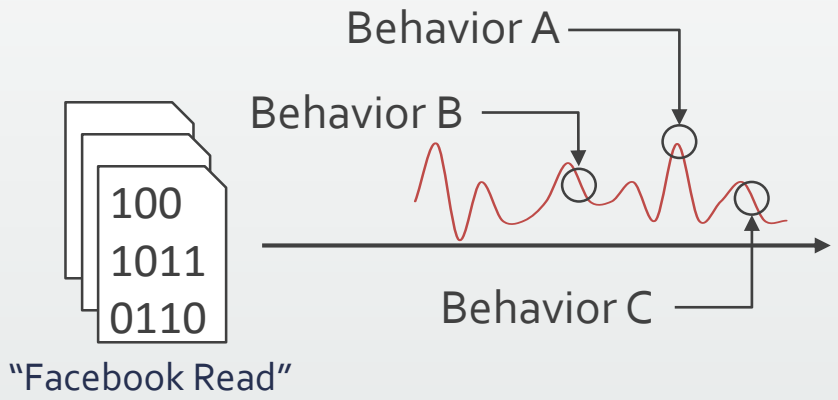
NetScope requires no packet content and no access to/knowledge of any target (victim) devices

Building Behavioral Models

For each server transaction:

NetScope divides the packets into 5ms windows of time

and computes behavior measurements within each window



Behavior Measurements:
(26 data points total)

Send and Receive Average Inter-Packet Times

Send and Receive Packet Count Ratios

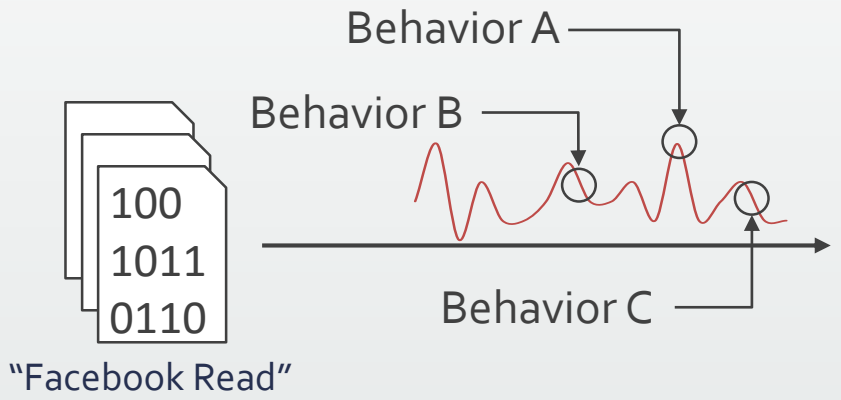
Send and Receive Data Size Ratios

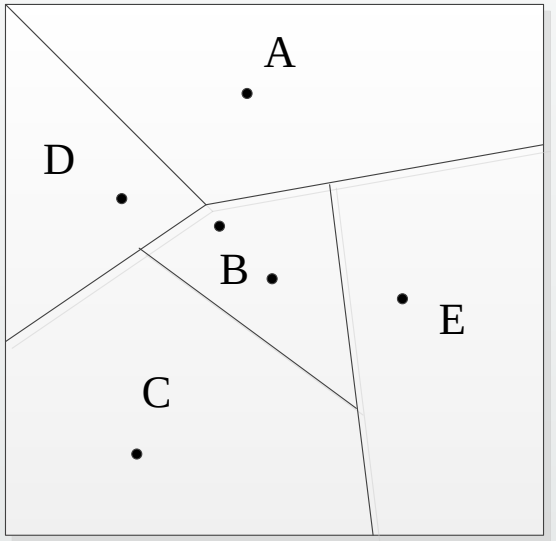
Packet Size Classification

Building Behavioral Models

Many behavior measurements will be similar across multiple activities

To group isolate behaviors, NetScope uses a behavioral feature clustering algorithm across all training activities

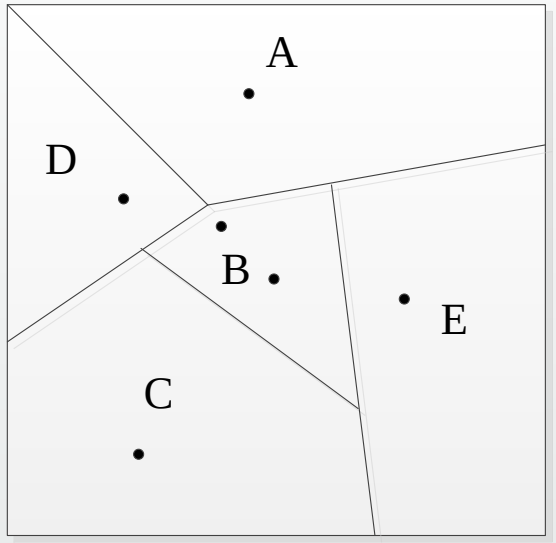




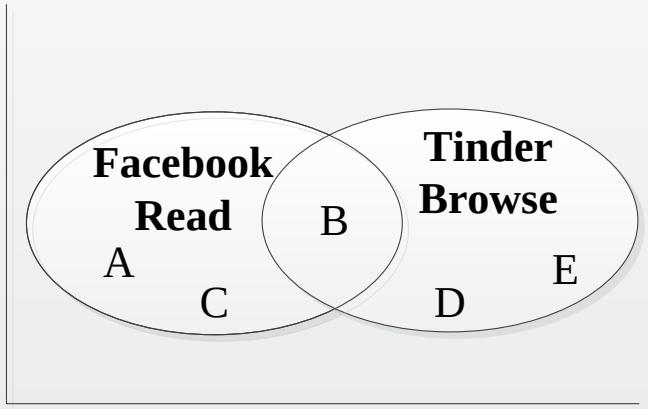
The behavior measurements are used as features to build a K-Means based clustering model

Building Behavioral Models

NetScope then learns the connection between behavior groups and training activities



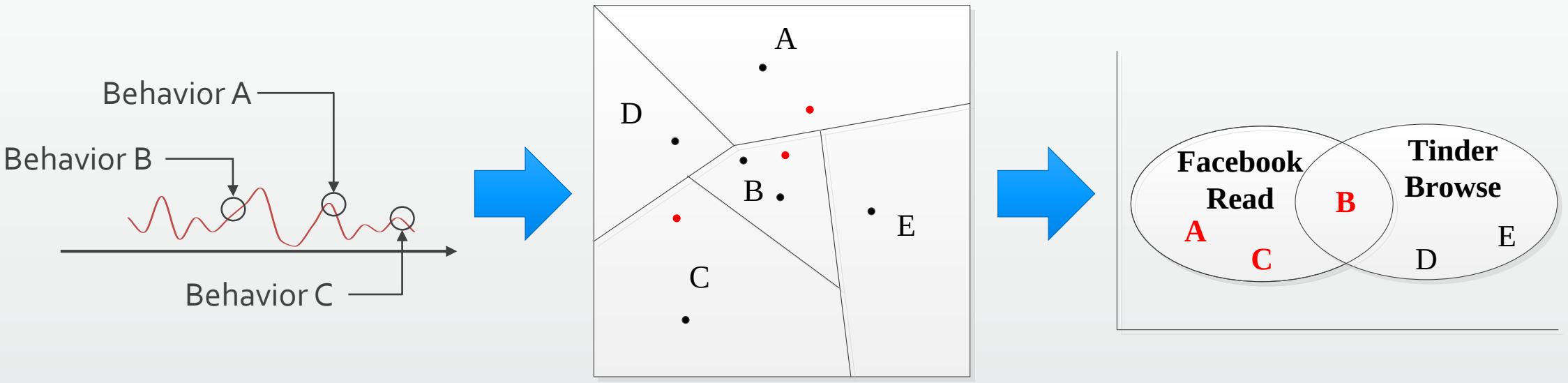




A multi-class SVM model is trained with a binary matrix of the behavior groups

The final trained behavioral models are packaged into an Online Detection Module

Online Activity Inference



NetScope takes behavior measurements from the live traffic for each server transaction

When enough measurements are collected, they are matched to a behavior model

The detected behavior models are then classified based on the known activity behaviors

Evaluation Setup

Training:

Samsung Galaxy S4 training device

22 apps with 35 total activities, 4 collections per activity

Purposely **restrictive** training set to test the generality of behavior models (more would be even better)

Deployment:

We set up a "rogue" WiFi Hotspot in our lab and recorded all packets

7 authors' unmodified smartphones plus 2 laptops

(NetScope filters out non-smartphone traffic)

Evaluation Highlights

NetScope achieves high detection accuracy:

78.04% average precision (among all identifications 78.04% of them are correct)

76.04% average recall (76.04% of the activity were correctly detected)

NetScope can distinguish between similar activities in different apps:

E.g., Pandora and Spotify "listening to music" both have above 76% precision and 72% recall

Roughly 50 and 300 behavior measurements to match the activity models reliably

Thus between ~0.25 to ~1.5 seconds of traffic observation to yield a result

Cross-Platform Results

Device	OS Version	Ground Truth Activities	Detected Activities	Missed Activities	False Positives	Precision	Recall
LG G3	Android 4.4.2	125	112	0	13	89.6%	89.6%
LG G2	Android 5.0	35	26	0	9	74.29%	74.29%
HTC Desire 500	Android 4.1.2	95	67	2	26	72.04%	70.53%
Samsung Galaxy S4	Android 5.0	88	60	7	21	74.07%	68.18%
Samsung Galaxy S4 (training)	Android 4.4.2	147	137	0	10	93.2%	93.2%
iPhone 6	iOS 8	78	46	0	32	58.97%	58.97%
iPhone 6 Plus	iOS 8	99	43	0	56	43.43%	43.43%

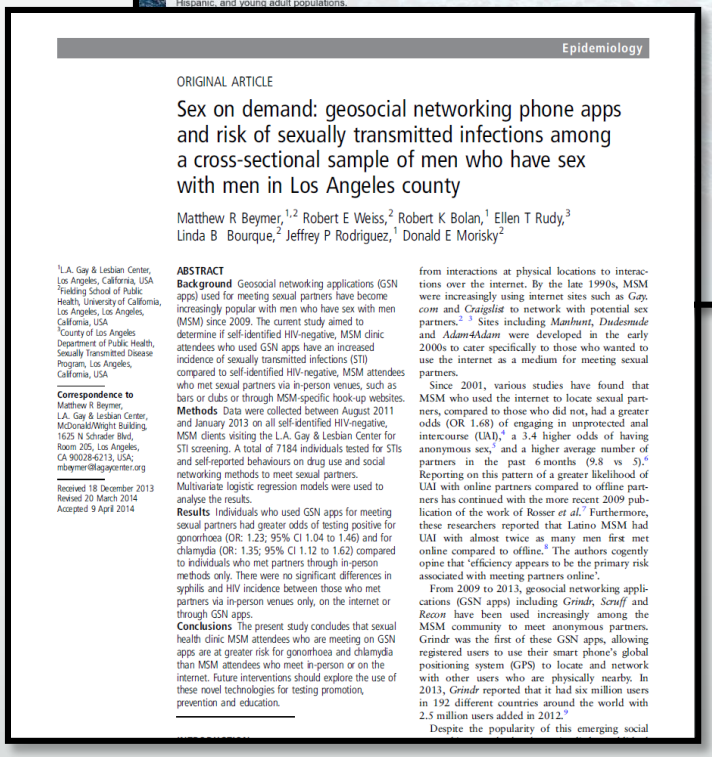
User Privacy Implications

Authorities might want to secretly tracking how actively community members use dating apps

E.g., passively browsing for matches versus frequently chatting with connections

Tinder, OkCupid, and Ashley Madison have an average of 92.3% precision and 88.33% recall among all of these apps' activities

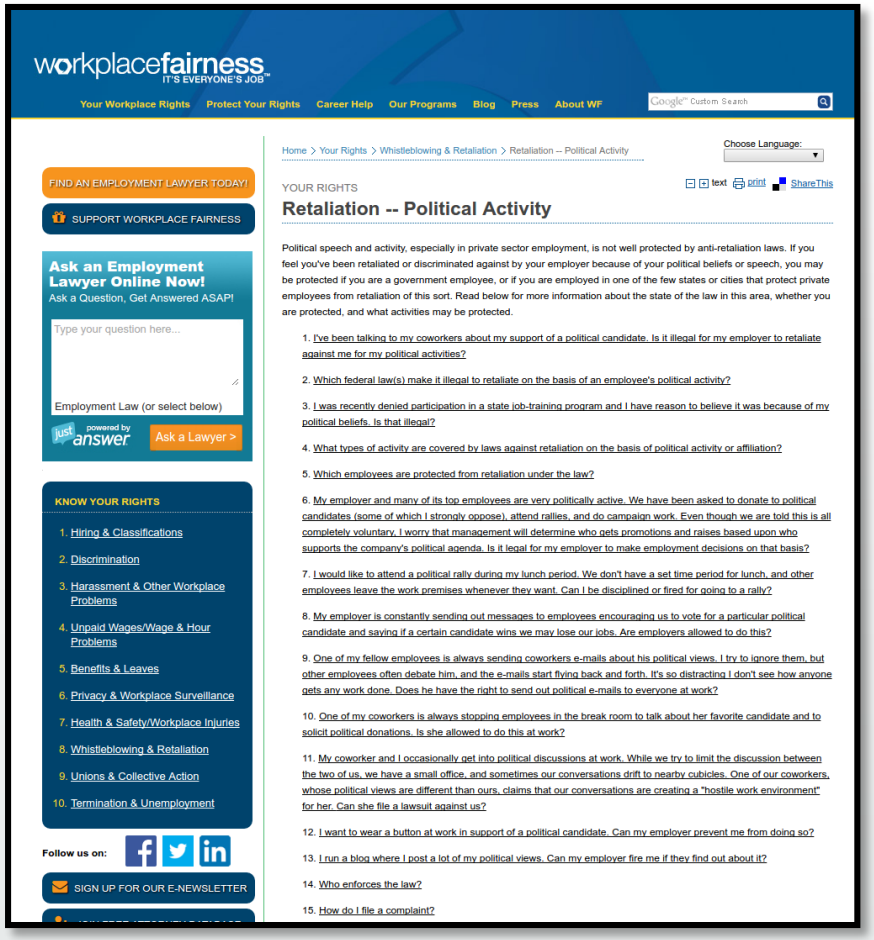




PURDUE UNIVERSITY
CERIAS

User Privacy Implications

Employee discrimination on the basis of political affiliation ***is*** legal in most states



Highly specialized apps, such as Bernie Sanders and Ben Carson presidential campaign apps, reveal such political affiliations

Bernie app has 96.15% precision and 100% recall

Carson app has 86.67% precision and 61.9% recall

PURDUE UNIVERSITY CERIAS

Related Works - Encrypted Network Traffic

Zhang , F., He , W., Liu , X., And Bridges , P. G. Inferring users' online activities through traffic analysis. In Proc. ACM Conference on Wireless Network Security 2011.

Cai , X., Zhang , X. C., Joshi , B., Johnson , R. Touching from a distance: Website fingerprinting attacks and defenses. In Proc. CCS 2012.

Sun , Q., Simon , D. R., Wang , Y.-M., Russell , W., Padmanabhan , V. N., Qiu , L. Statistical identification of encrypted web browsing traffic. In Proc. IEEE S&P 2002.

Wright , C., Monrose , F., Masson , G. M. Hmm profiles for network traffic classification. In Proc. ACM Workshop on Visualization and Data Mining for Computer Security 2004.

Wright , C. V., Ballard , L., Coull , S. E., Monrose , F., Masson , G. M. Spot me if you can: Uncovering spoken phrases in encrypted voip conversations. In Proc. IEEE S&P 2008.

Wright , C. V., Ballard , L., Monrose , F., Masson ,G. M. Language identification of encrypted voip traffic: Alejandra y roberto or alice and bob? In Proc. USENIX Security 2007.

Verde , N. V., Ateniese , G., Gabrielli , E., Mancini , L. V., Spognardi , A. No nat'd user left behind: Fingerprinting users behind nat from netflow records alone. In Proc. IEEE International Conference on Distributed Computing Systems 2014.

Liberatore , M., Levine , B. N. Inferring the source of encrypted http connections. In Proc. CCS 2006.

Moore , A. W., And Zuev , D. Internet traffic classification using bayesian analysis techniques. In Proc. ACM SIGMETRICS International Conference on Measurement and Modeling of Computer Systems 2005.

Related Works - Smartphone Traffic Analysis

Stöber, T., F Rank , M., S Chmitt , J., M Artinovic , I. Who do you sync you are?: smartphone fingerprinting via application behaviour. In Proc. ACM Conference on Security and Privacy in Wireless and Mobile Networks 2013.

Conti , M., Mancini , L. V., Spolaor , R., Verde , N. V. Can't you hear me knocking: Identification of user actions on android apps via traffic analysis. In Proc. ACM Conference on Data and Application Security and Privacy 2015.

Tongaonkar , A., Dai , S., Nucci , A., Song , D. Understanding mobile app usage patterns using in-app advertisements. In Passive and Active Measurement 2013.

Sapio , A., Liao , Y., Baldi , M., Ranjan , G., Risso , F., Tongaonkar , A., Torres , R., Nucci , A. Per-user policy enforcement on mobile apps through network functions virtualization. In Proc. ACM Workshop on Mobility in the Evolving Internet Architecture 2014.

Xu , Q., Liao , Y., Miskovic , S., Mao , Z. M., Baldi , M., Nucci , A., Andrews , T. Automatic generation of mobile app signatures from traffic observations. In Proc. IEEE INFOCOM 2015.

Coull , S. E., Dyer , K. P. Traffic analysis of encrypted messaging services: Apple imessage and beyond. ACM SIGCOMM Computer Communication Review 44, 5 2014.

Xu , Q., Erman , J., Gerber , A., Mao , Z., Pang , J., Venkataraman , S. Identifying diverse usage behaviors of smartphone apps. In Proc. ACM Internet Measurement Conference 2011.

Wei , X., Gomez , L., Neamtiu , I., Faloutsos , M. ProfileDroid: multi-layer profiling of android applications. In Proc. Annual International Conference on Mobile Computing and Networking 2012.

Conclusion

Modern, highly specialized mobile apps leave behind fingerprints of their activities in (encrypted) wireless network traffic

NetScope automatically builds models of user activities based on their measured traffic behaviors

NetScope can perform inference of user activities with high accuracy by observing only IP packet headers, for both Android and iOS devices

Thank you!

Questions?

Brendan Saltaformaggio
bsaltafo@cs.purdue.edu