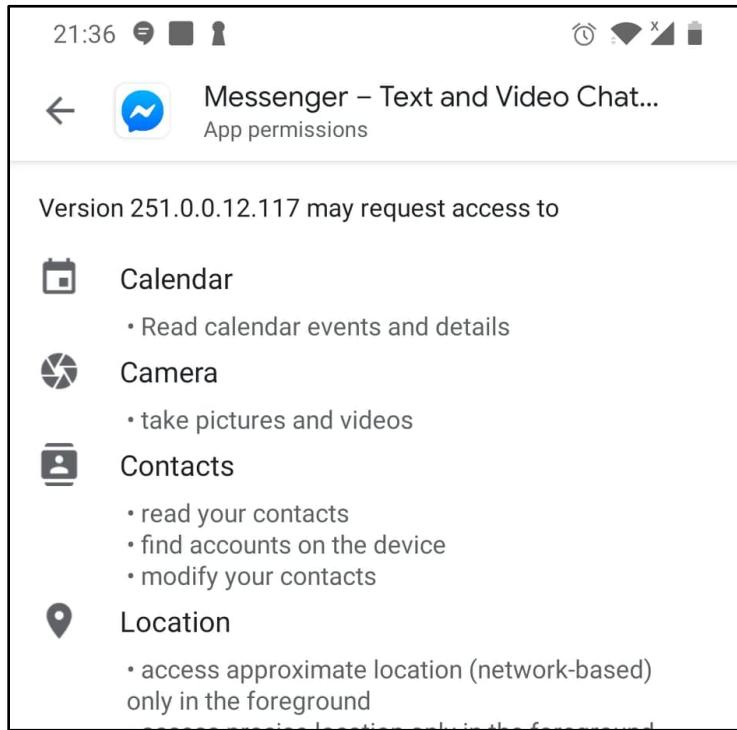


# TKPERM: Cross-platform Permission Knowledge Transfer to Detect Overprivileged Third-party Applications

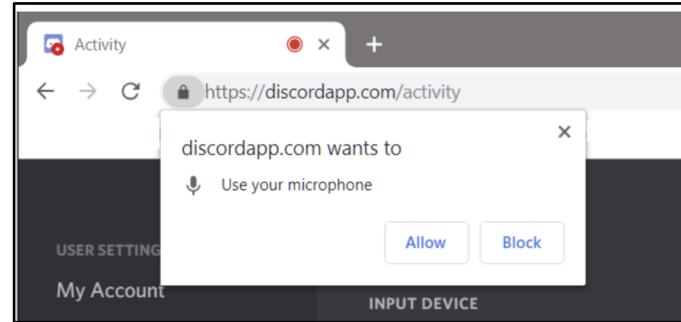
Faysal Hossain Shezan, Kaiming Cheng, Zhen Zhang,  
Yinzhi Cao, Yuan Tian



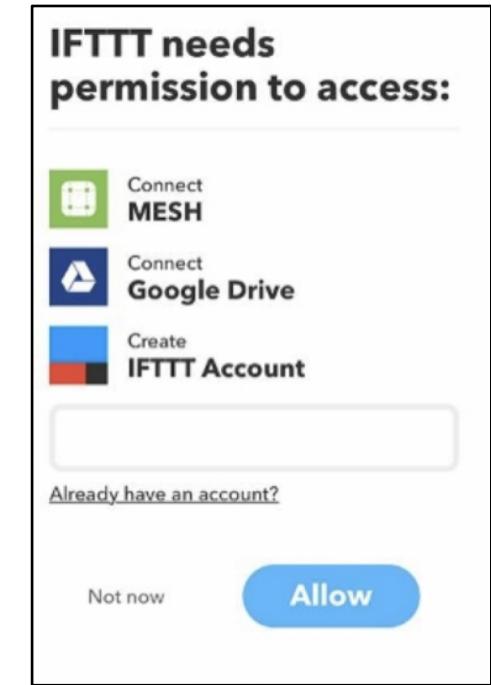
# Permission-based Access Control



Android



Chrome



IFTTT

# Permission Correlation with Description

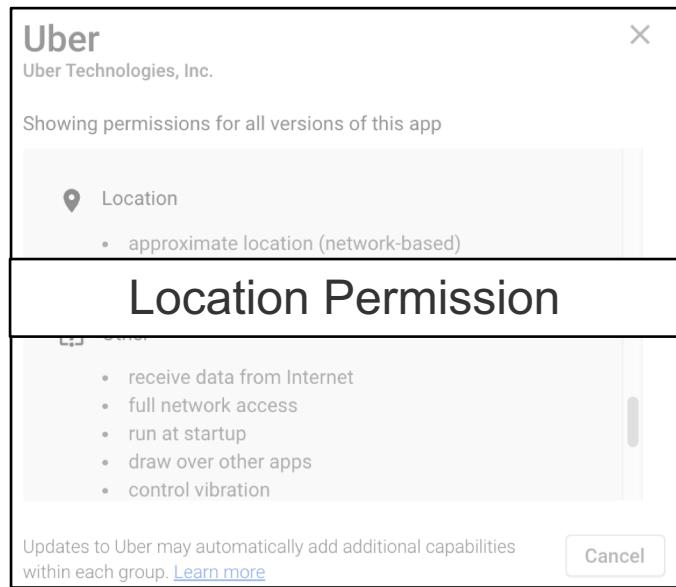


Android App

# Permission Correlation with Description



Android App

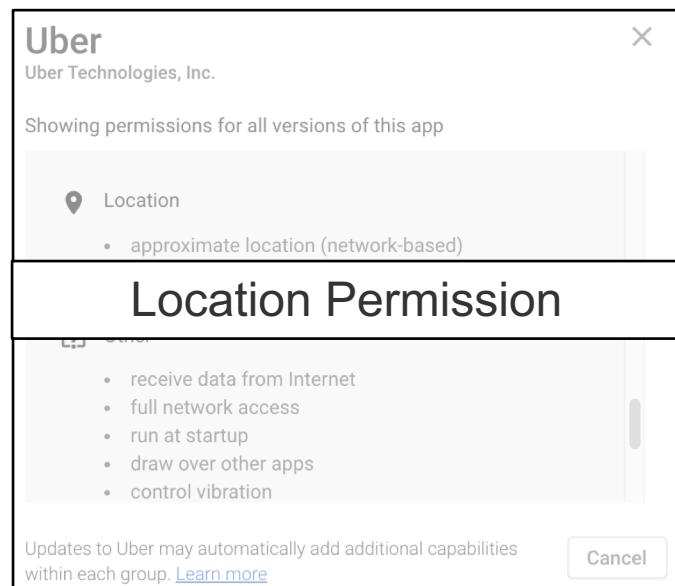


Requested Permission

# Permission Correlation with Description



Android App



Requested Permission

Uber is a ridesharing app for fast, reliable rides in minutes—day or night. There's no need to park or wait for a taxi or bus. With Uber, you just tap to request a ride, and it's easy to pay with credit or cash in select cities.

Whether you're going to the airport or across town, there's an Uber for every occasion. Uber is available in more than 630+ cities worldwide—download the app and take your first trip today.

Requesting your Uber is easy—here's how it works:

- Just open the app and tell us where you're going.
- The app uses your location so your driver knows where to pick you up.
- You'll see your driver's picture, vehicle details, and can track their arrival on the map.

Payment can be made by credit card, cash in select cities, Android Pay, PayPal, and more.

**The app uses your location so your driver knows where to pick you up.**

Want to save money on your ride? Take uberPOOL—you'll travel with other riders headed your way and enjoy a lower fare.

Want to elevate your experience? Take a high-end vehicle with UberBLACK. And there's still more options—whether you're traveling with a big group, or need a vehicle with accessibility features.

See if Uber is available in your city at <https://www.uber.com/cities>

Follow us on Twitter at <https://twitter.com/uber>

Like us on Facebook at <https://www.facebook.com/uber>

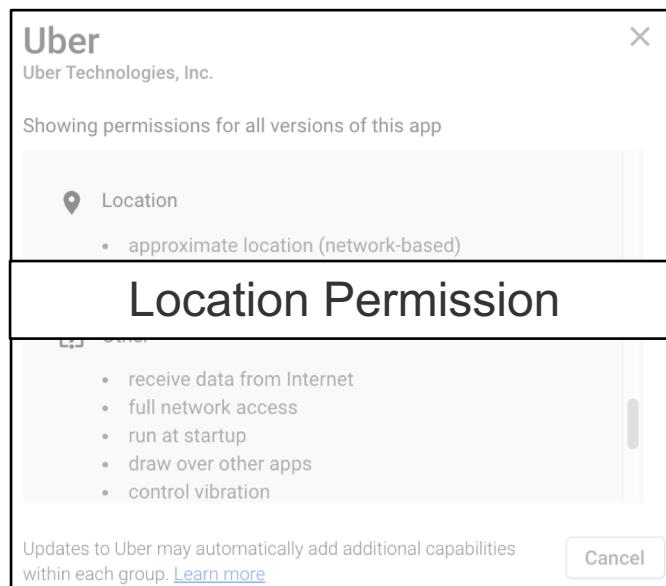
Have a question? Visit [uber.com/help](http://uber.com/help)

Uber Description

# Permission Correlation with Description



Android App



Requested Permission



Uber is a ridesharing app for fast, reliable rides in minutes—day or night. There's no need to park or wait for a taxi or bus. With Uber, you just tap to request a ride, and it's easy to pay with credit or cash in select cities.

Whether you're going to the airport or across town, there's an Uber for every occasion. Uber is available in more than 630+ cities worldwide—download the app and take your first trip today.

Requesting your Uber is easy—here's how it works:

- Just open the app and tell us where you're going.
- The app uses your location so your driver knows where to pick you up.
- You'll see your driver's picture, vehicle details, and can track their arrival on the map.

Payment can be made by credit card, cash in select cities, Android Pay, PayPal, and more.

**The app uses your location so your driver knows where to pick you up.**

Want to save money on your ride? Take uberPOOL—you'll travel with other riders headed your way and enjoy a lower fare.

Want to elevate your experience? Take a high-end vehicle with UberBLACK. And there's still more options—whether you're traveling with a big group, or need a vehicle with accessibility features.

See if Uber is available in your city at <https://www.uber.com/cities>

Follow us on Twitter at <https://twitter.com/uber>

Like us on Facebook at <https://www.facebook.com/uber>

Have a question? Visit [uber.com/help](http://uber.com/help)

Uber Description

# What is Overprivileged?

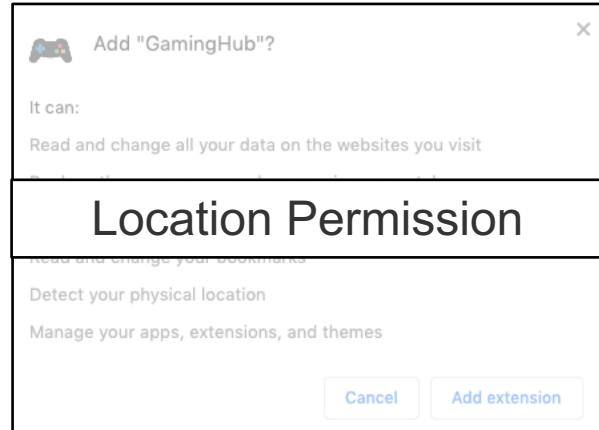


GamingHub  
(Chrome Extension)

# What is Overprivileged?



GamingHub  
(Chrome Extension)

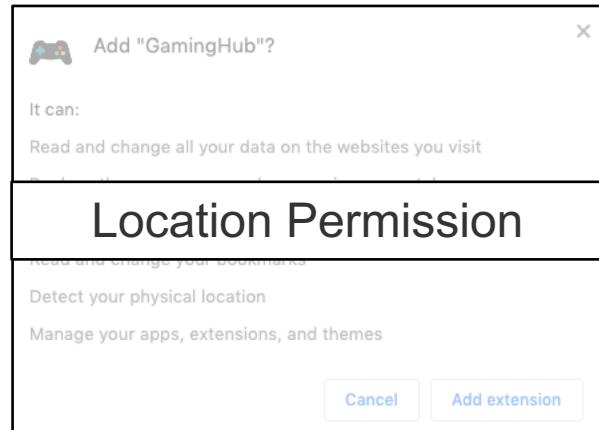


Requested Permission

# What is Overprivileged?



GamingHub  
(Chrome Extension)



Requested Permission

## Overview

Compatible with your device

GamingHub - Instant & Elegant Access to Online Web Games

## Primary Features:

1. Quick & Easy Access to popular web games
2. Minimalist & Elegant Design
3. Hand Picked High Quality Wallpapers that change according to mood
4. New & Exciting ways for accessing Online Content
5. Let us know what you'd like, more to come soon!

1. Minimalist & Elegant Design

3. Hand Picked High Quality Wallpapers that change according to mood

4. New & Exciting ways for accessing Online Content

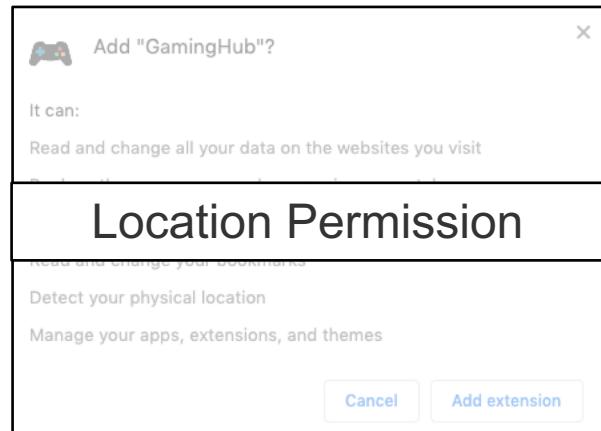
5. Let us know what you'd like, more to come soon!

GamingHub Description

# What is Overprivileged?



GamingHub  
(Chrome Extension)



Requested Permission



No Match

**Overview**

Compatible with your device

GamingHub - Instant & Elegant Access to Online Web Games

GamingHub enables you quick & elegant access to some of the most popular web games to date. It does so by displaying them as quick access links on your New Tab Page, which, if you like your games, makes for a quick access with a few simple clicks.

Coming soon: We are working hard on delivering the ability to pick & choose which games will be presented on quick access in order to deliver

**No Explanation for the Usage of Location Permission**

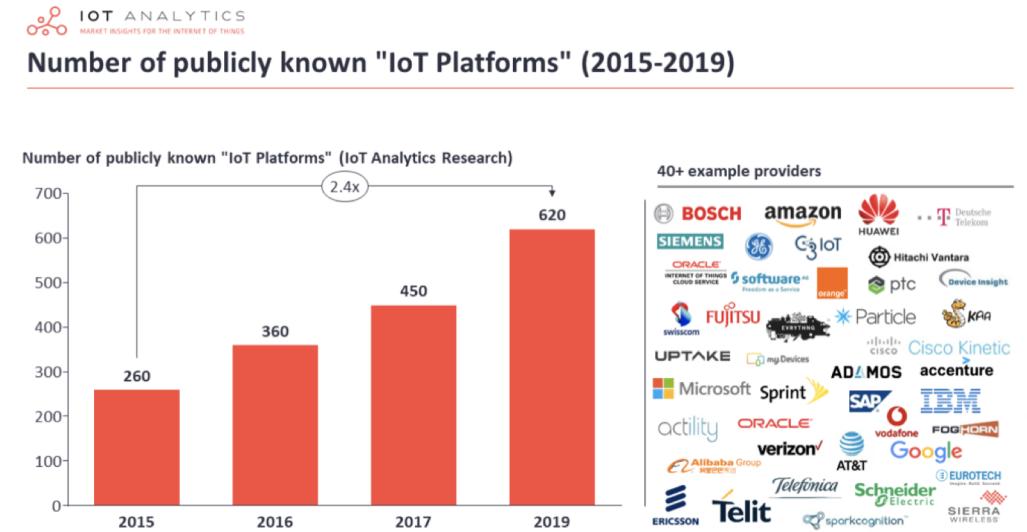
Enjoy our unique collection of high quality HD backgrounds, which will change according to mood, or, with a click of a button, refresh to find the perfect background for you at any given time. You can also lock onto a background you've especially loved, or just let GamingHub choose what background we think defines you today.

Primary Features:

1. Quick & Easy Access to popular web games
2. Minimalist & Elegant Design
3. Hand Picked High Quality Wallpapers that change according to mood
4. New & Exciting ways for accessing Online Content
5. Let us know what you'd like, more to come soon!

GamingHub Description

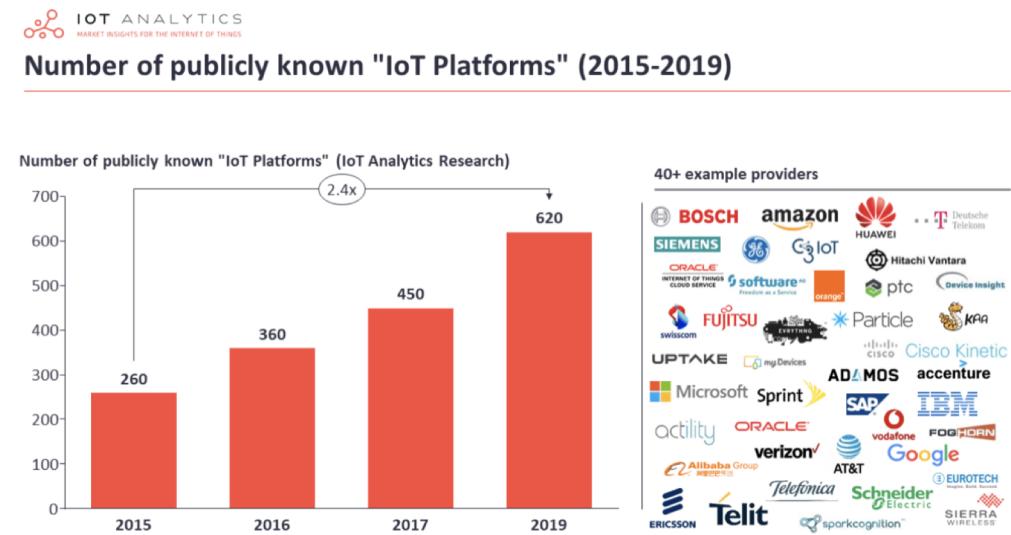
# Challenges



# Challenges

Extensive data labeling and parameter tuning on new platforms

Some platforms have limited data



# Key Insights



FlySmart

FlySmart mobile application Travel & Local

Everyone

⚠ You don't have any devices.

You can share this with your family. [Learn more about Family Library](#)

Android App

Permission Knowledge  
Location

Chrome Web Store

Oplao weather offered by oplao.com

Add to Desktop

The screenshot shows the Oplao weather extension running in a browser window. It displays a 3-day forecast for Moscow, Russia, with temperatures ranging from -1°C to 11°C and various weather conditions like cloudy, rainy, and snow. Below the forecast, there's a status bar with current weather information. The extension has a 5-star rating of 477 and 5,017 users.

News & Weather

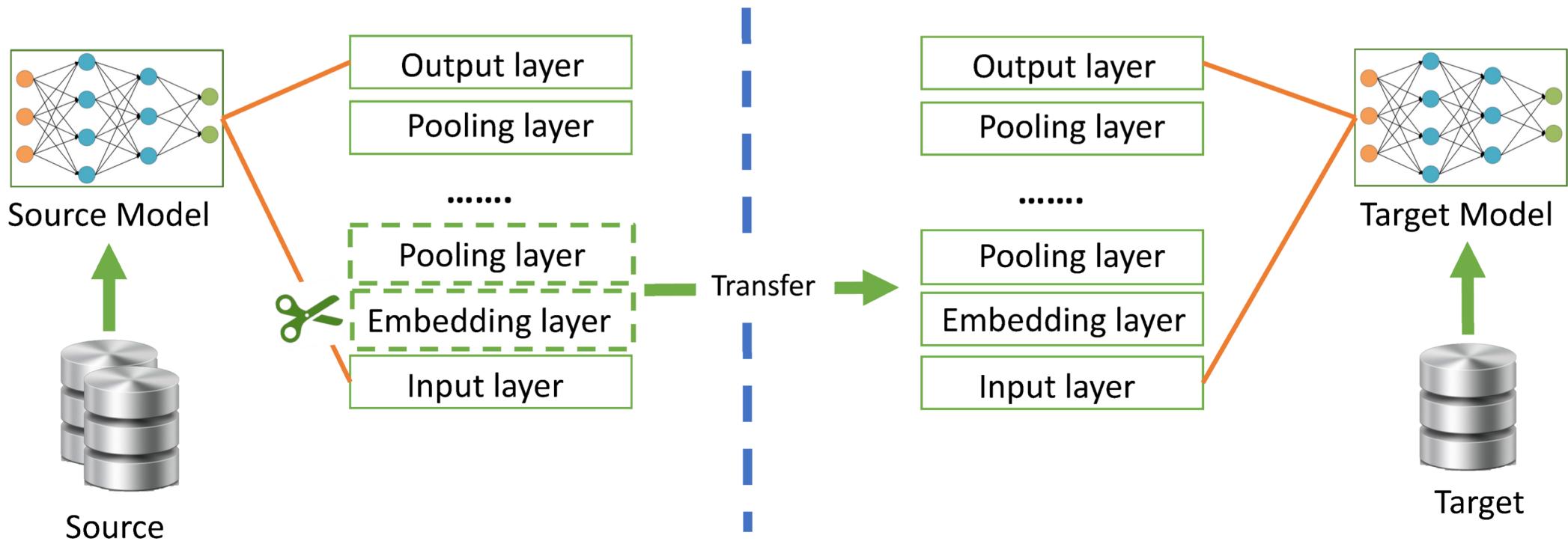
Overview

**Accurate weather forecast. Local to Global.**

The best Chrome weather extension. 5 star rated. Easy to use. Oplao weather plugin for Google Chrome contains status bar icon, current weather, detailed forecast, 3 day forecast, fast locations change button (up to 7 locations).

Chrome App

# Solution- Transfer Learning



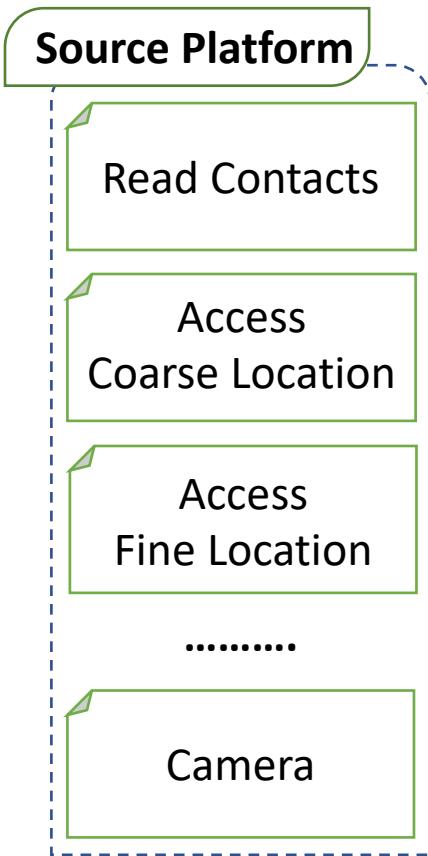
# Goal

General framework to detect  
unexpected permissions

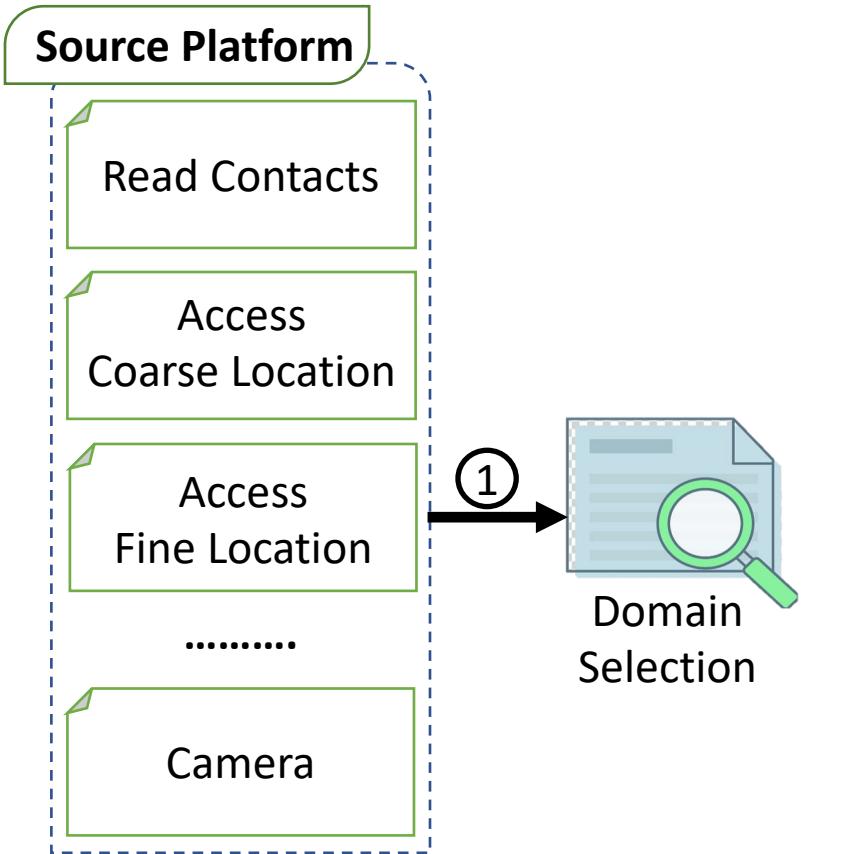
# Research Questions

1. What knowledge to transfer? (e.g., what original domain should we select, what permissions in Android should we use)?
2. How to minimize the amount of labeled data needed?

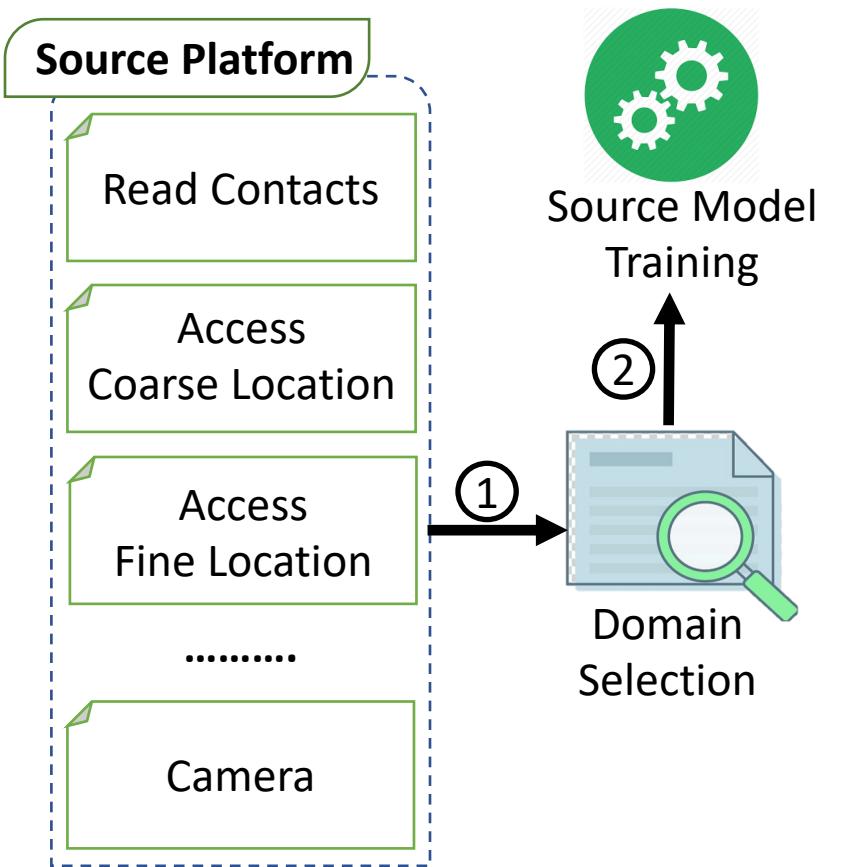
# System Overview of TKPERM



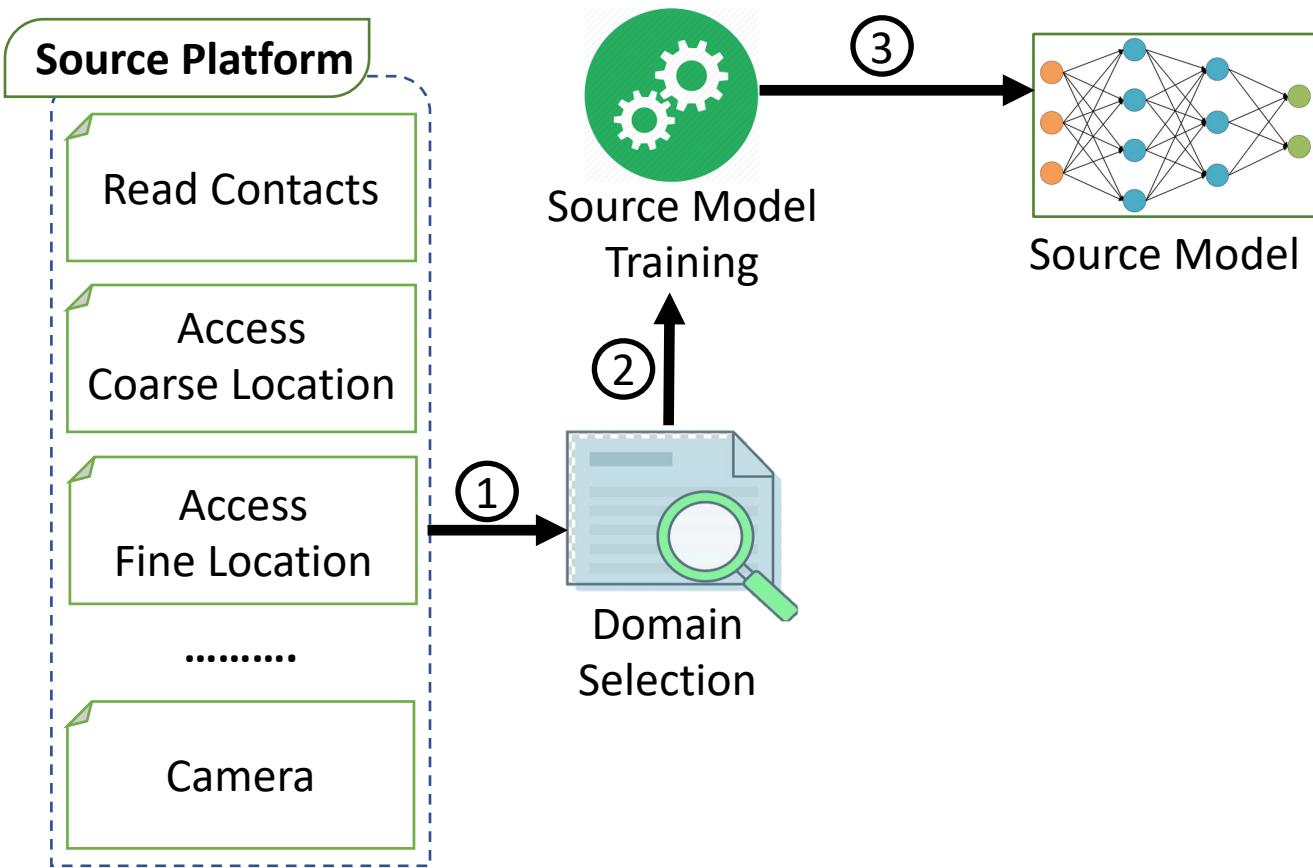
# System Overview of TKPERM



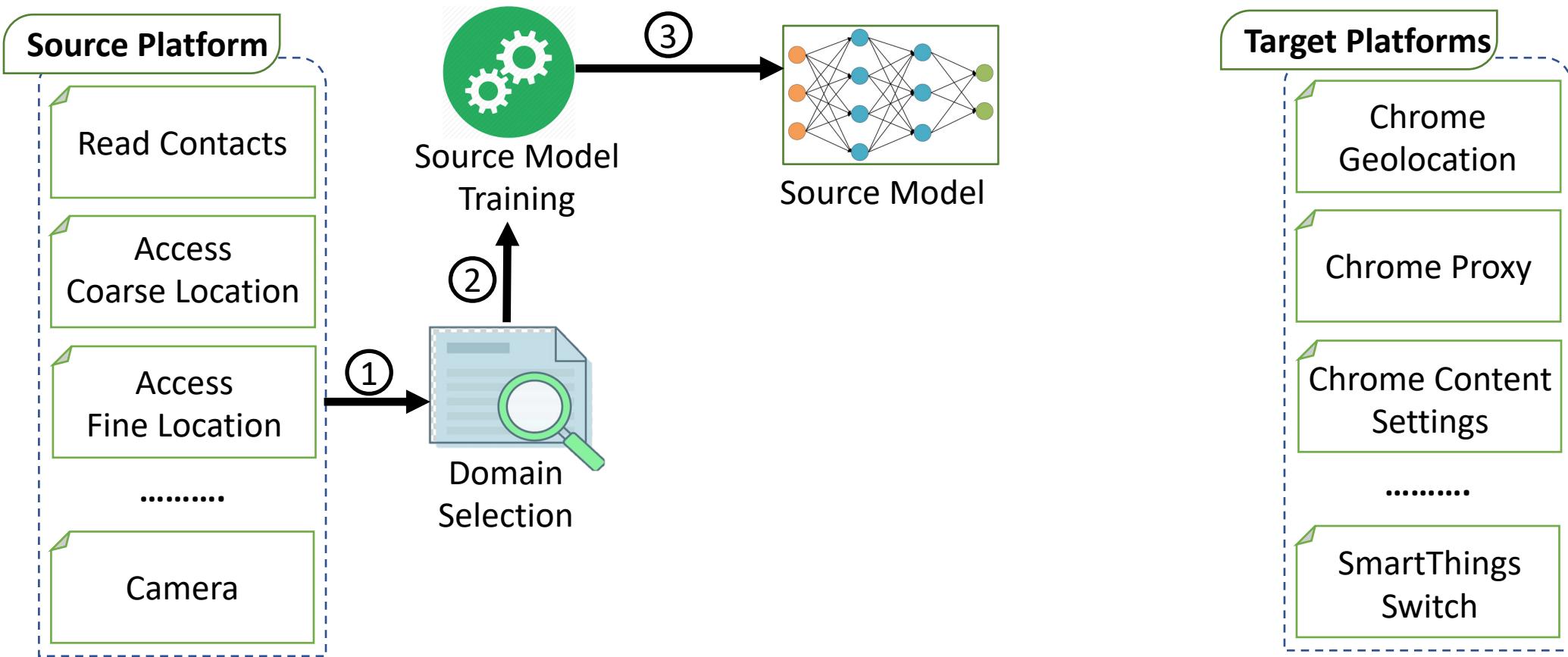
# System Overview of TKPERM



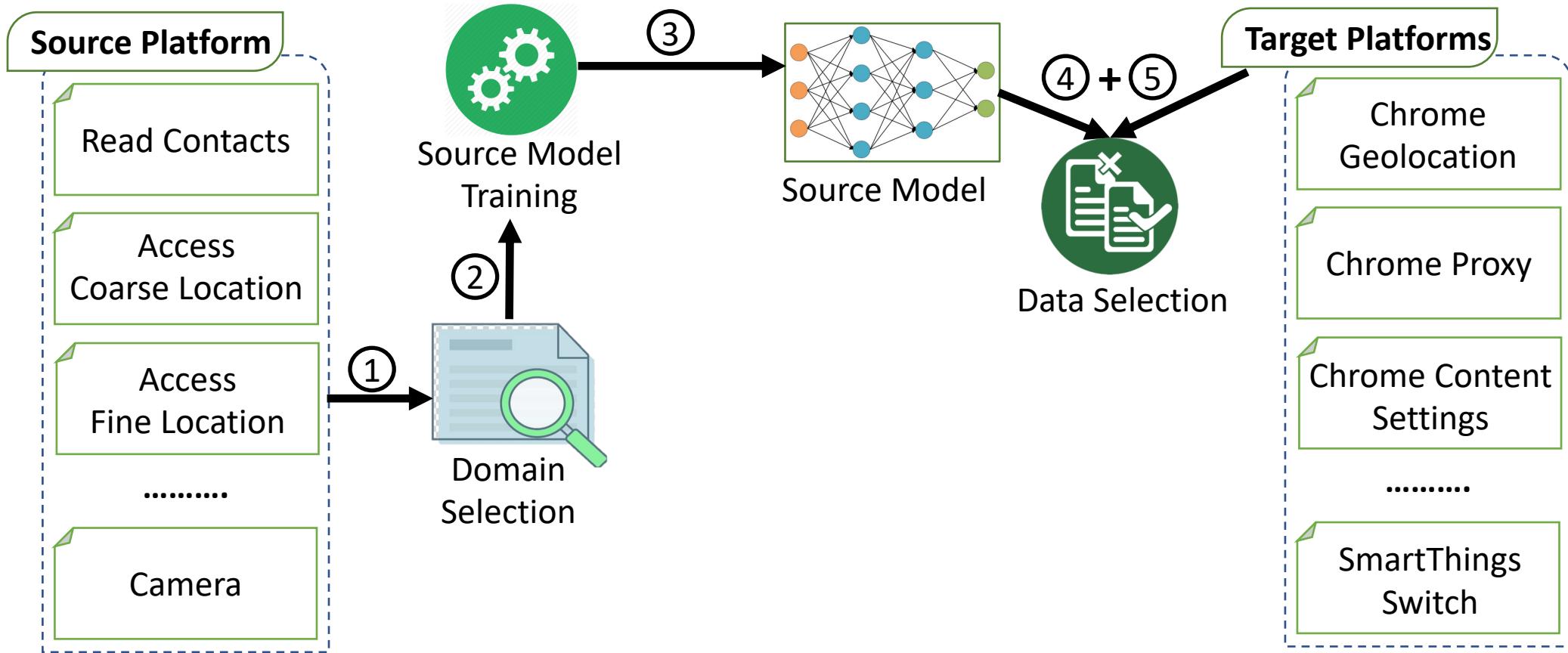
# System Overview of TKPERM



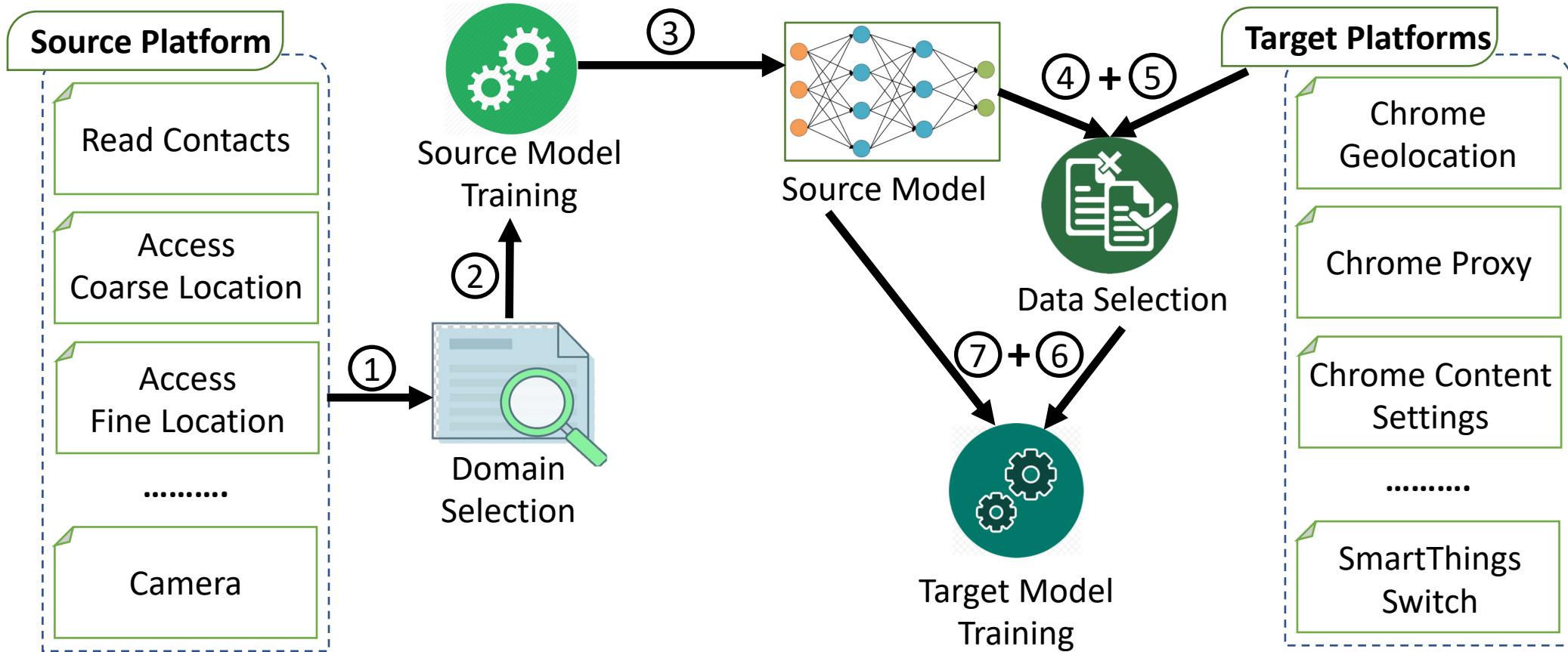
# System Overview of TKPERM



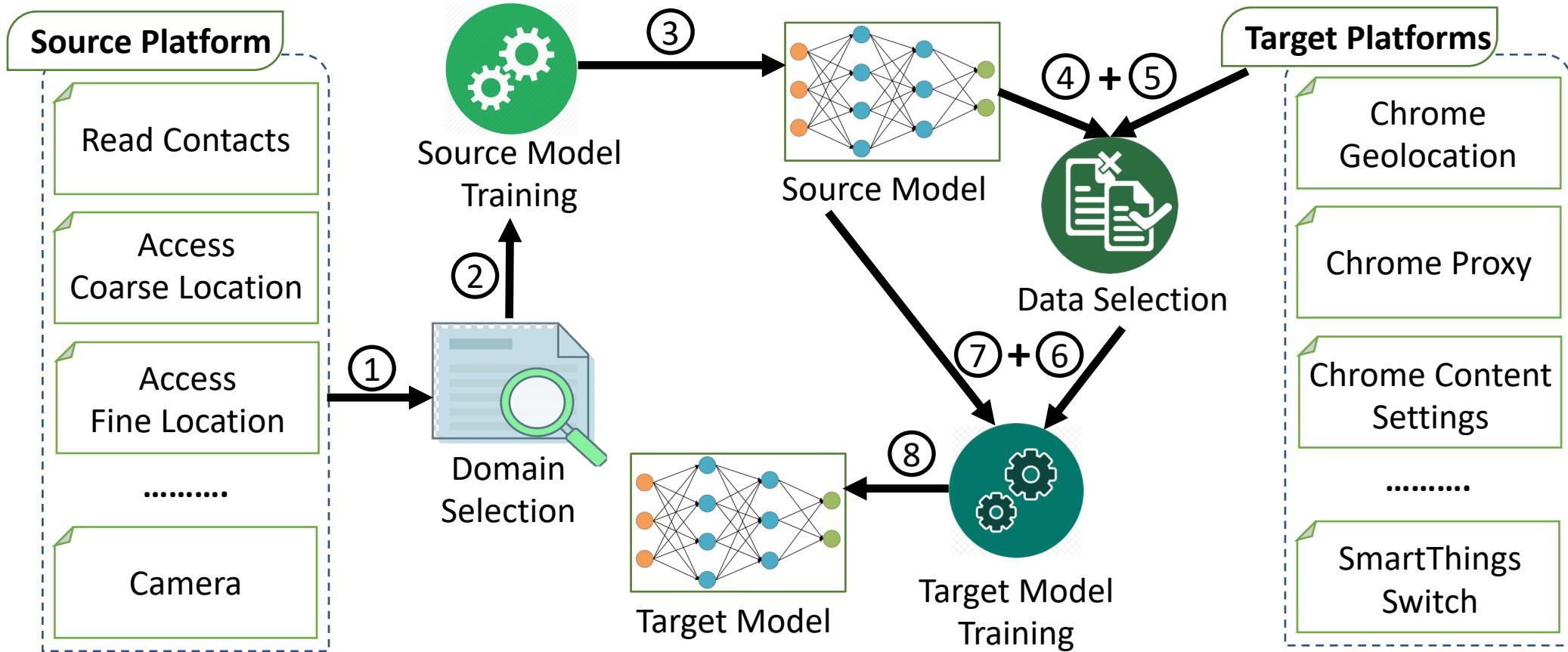
# System Overview of TKPERM



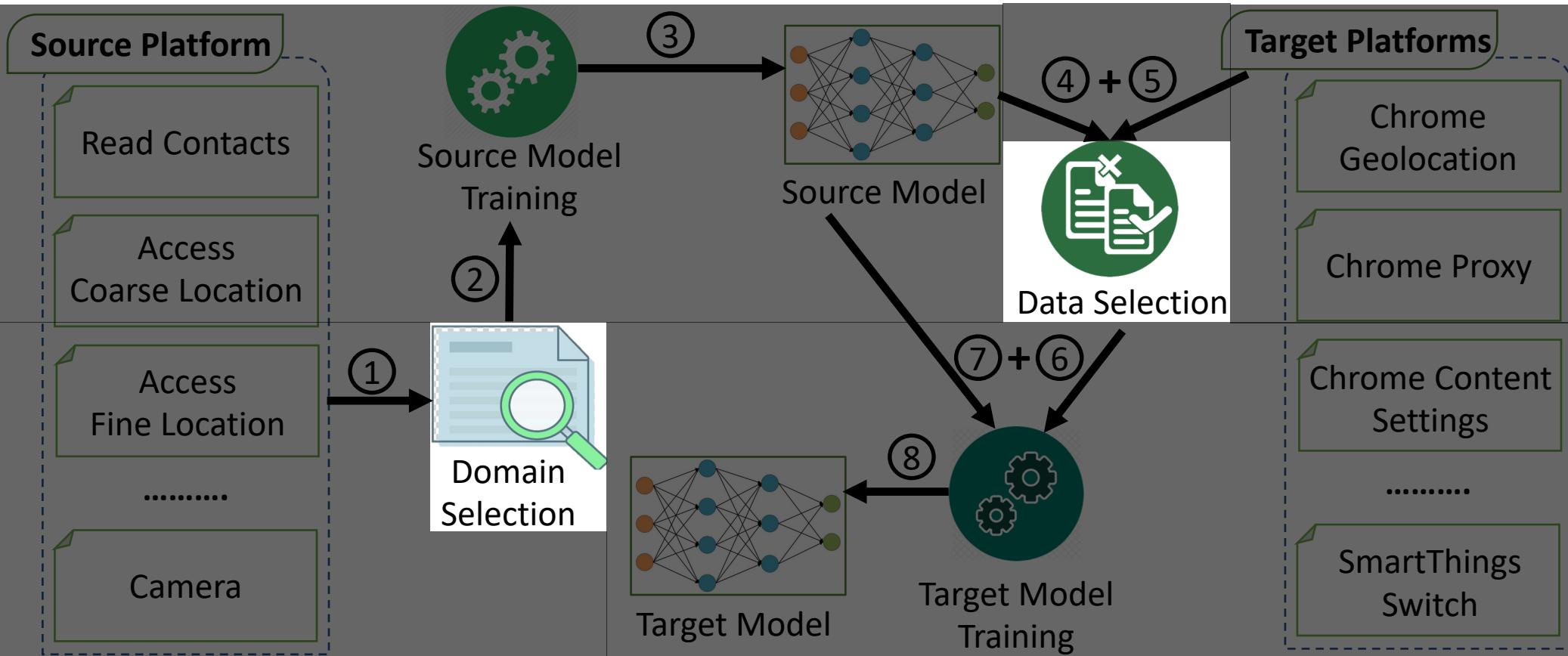
# System Overview of TKPERM



# System Overview of TKPERM



# System Overview of TKPERM



# Domain Selection

**Research Question: What knowledge to transfer?**

## Greedy Selection Approach

Compute and  
aggregate source  
domain(s)  
performs

# Domain Selection

**Research Question: What knowledge to transfer?**

## Greedy Selection Approach

Compute and aggregate source domain(s) performs

Remove source domain(s) which work worst

# Domain Selection

**Research Question: What knowledge to transfer?**

## Greedy Selection Approach

Compute and aggregate source domain(s) performs

Remove source domain(s) which work worst

Find the best combination of the source domain(s)

# Domain Selection

## Greedy Selection Approach

Compute and aggregate source domain(s) performs

Remove source domain(s) which work worst

Find the best combination of the source domain(s)



**Research Question: What knowledge to transfer?**

# Data Selection

**Research Question: How to minimize the amount of labeled data needed?**

Use source  
model to rank  
the unlabeled  
document

# Data Selection

**Research Question: How to minimize the amount of labeled data needed?**

Use source  
model to rank  
the unlabeled  
document

Pick the top 20  
documents from  
the target  
domain

# Data Selection

**Research Question: How to minimize the amount of labeled data needed?**

Use source model to rank the unlabeled document

Pick the top 20 documents from the target domain

Ask human annotator to label data

# Data Selection

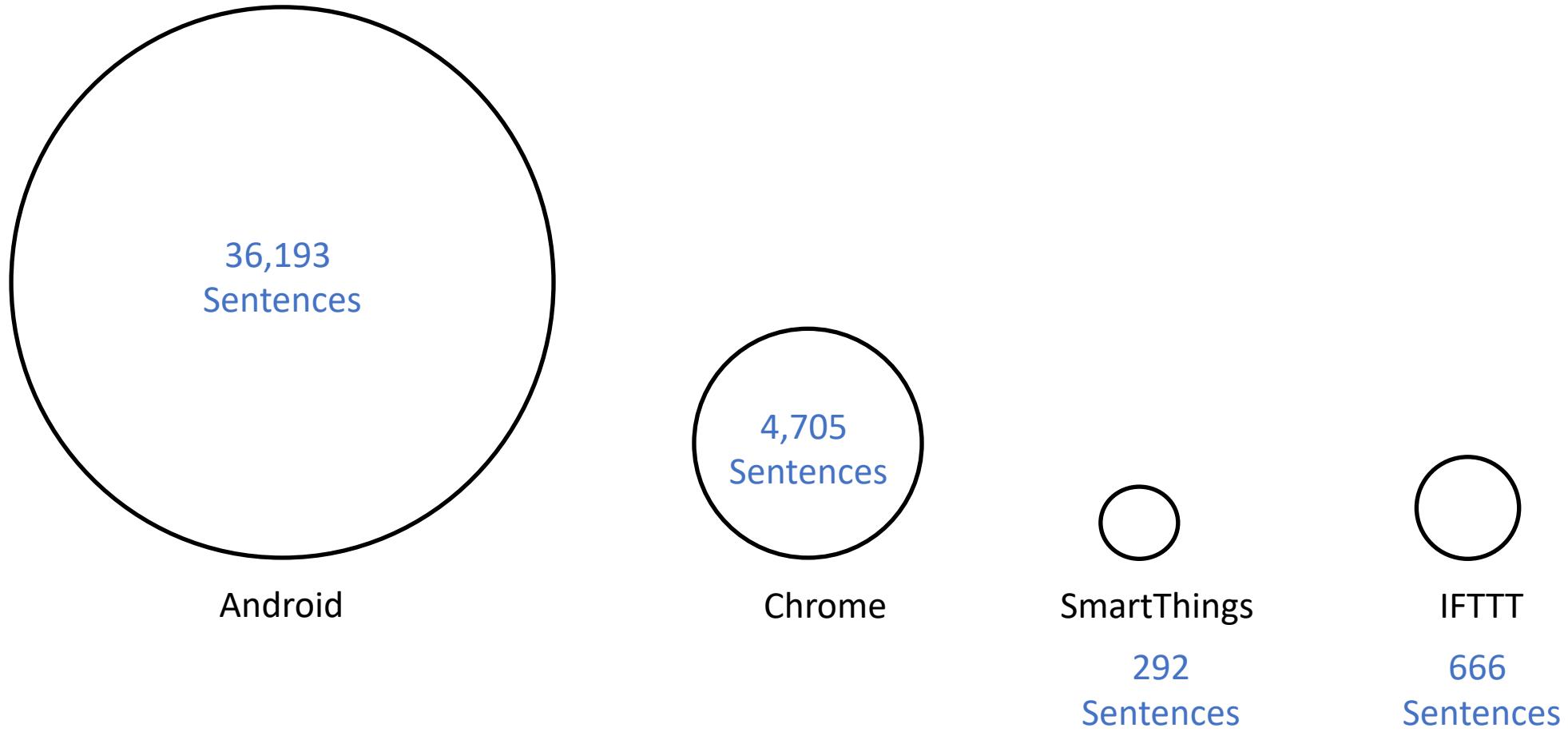
Use source model to rank the unlabeled document

Pick the top 20 documents from the target domain

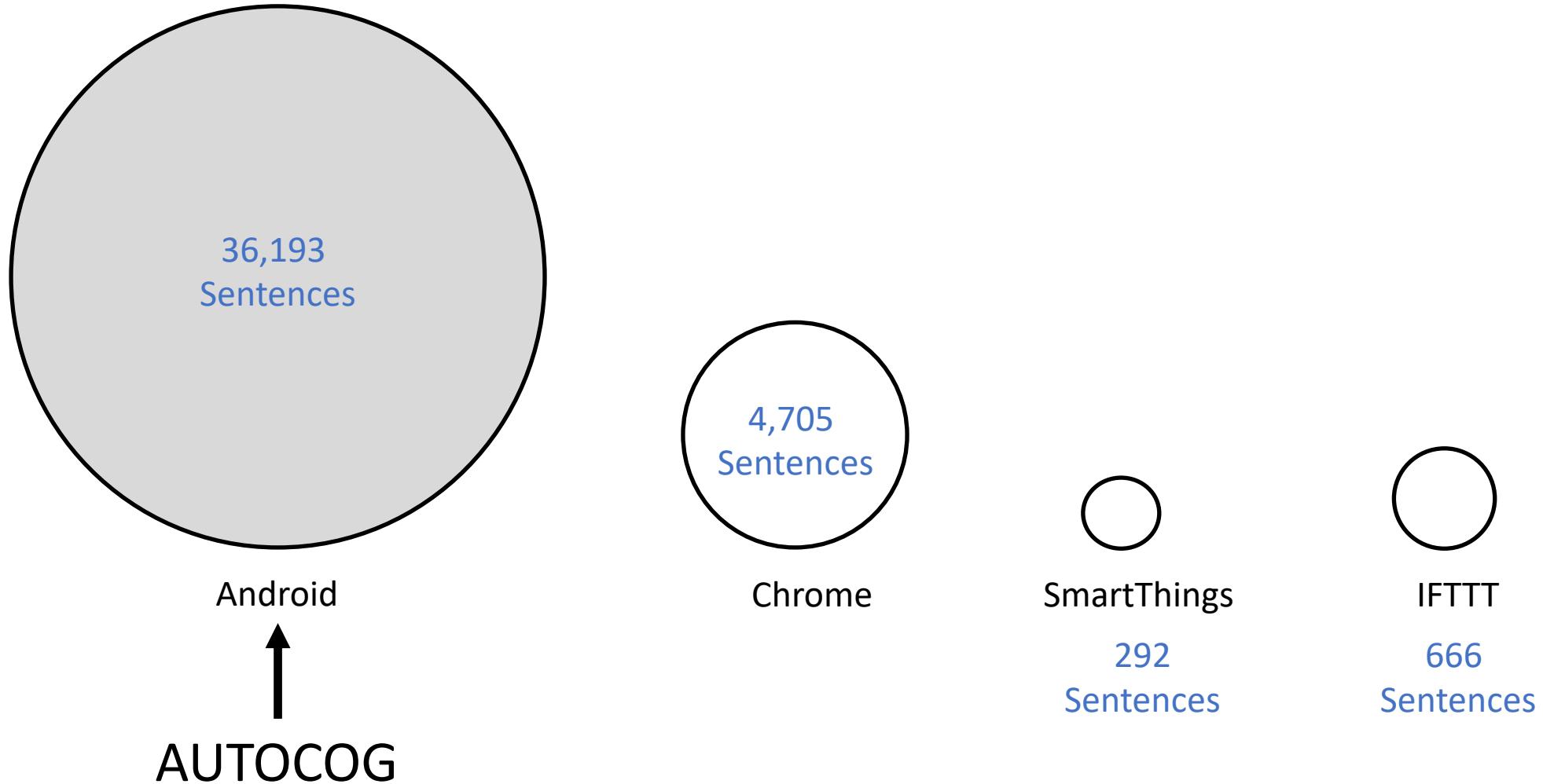
Ask human annotator to label data

✓ **Research Question: How to minimize the amount of labeled data needed?**

# Dataset



# Dataset



# Evaluation

Question 1. What is the end-to-end performance of TKPERM?

Question 2. What is the performance of each component  
in TKPERM?

Question 3. What is the computation overhead of TKPERM?

# Evaluation

Question 1. What is the end-to-end performance of TKPERM?

Question 2. What is the performance of each component  
in TKPERM?

Question 3. What is the computation overhead of TKPERM?

Effectiveness

# Evaluation (Effectiveness)

## Source Domain Selection: H-divergence v/s Greedy Selection in IFTTT Platform

Target Domain	Source Selection	Source Domain(s)	F1
Evernote	H-Divergence	Read Calendar	75.86%
	Greedy Selection	Coarse Location + Fine Location + Camera	83.13%
BMW Lab	H-Divergence	Read Contact	92.30%
	Greedy Selection	Send SMS + Record Audio	95.24%
Facebook	H-Divergence	Read Calendar	76.09%
	Greedy Selection	Camera	88.09%
Google Calendar	H-Divergence	Read Calendar	91.30%
	Greedy Selection	Read Calendar + Coarse Location	92.30%
Google Contact	H-Divergence	Read Contacts	99.20%
	Greedy Selection	Read Contacts	99.20%

# Evaluation (Effectiveness)

## Source Domain Selection: H-divergence v/s Greedy Selection in IFTTT Platform

Target Domain	Source Selection	Source Domain(s)	F1
Evernote	H-Divergence	Read Calendar	75.86%
	Greedy Selection	Coarse Location + Fine Location + Camera	83.13%
BMW Lab	H-Divergence	Read Contact	92.30%
	Greedy Selection	Send SMS + Record Audio	95.24%
Facebook	H-Divergence	Read Calendar	76.09%
	Greedy Selection	Camera	88.09%
Google Calendar	H-Divergence	Read Calendar	91.30%
	Greedy Selection	Read Calendar + Coarse Location	92.30%
Google Contact	H-Divergence	Read Contacts	99.20%
	Greedy Selection	Read Contacts	99.20%

# Evaluation (Effectiveness)

## Data Selection: Comparison of With & Without Data Selection

Platform	Performance	Configuration		
		No Transfer	Without Data Selection	With Data Selection
IFTTT	F1 Score	84.25%	91.08%	91.83%
	Improvement	-	6.83%	7.58%
Chrome	F1 Score	70.60%	84.36%	89.13%
	Improvement	-	13.76%	18.53%
SmartThings	F1 Score	72.80%	84.65%	89.1%
	Improvement	-	11.85%	16.3%

# Evaluation (Effectiveness)

## Data Selection: Comparison of With & Without Data Selection

Platform	Performance	Configuration		
		No Transfer	Without Data Selection	With Data Selection
IFTTT	F1 Score	84.25%	91.08%	91.83%
	Improvement	-	6.83%	7.58%
Chrome	F1 Score	70.60%	84.36%	89.13%
	Improvement	-	13.76%	18.53%
SmartThings	F1 Score	72.80%	84.65%	89.1%
	Improvement	-	11.85%	16.3%

# Evaluation (Effectiveness)

## TKPERM Performance Analysis (Metric: F1 Score)

Platform	Target Domain	Source Domain	Transfer	No Transfer	Improvement
IFTTT	Evernote	Coarse Location + Fine Location + Camera	83.13%	79.78%	3.35%
	BMW Lab	Send SMS + Record Audio	95.24%	85.71%	9.53%
	Facebook	Camera	88.09%	75.00%	13.09%
	Google Calendar	Read Calendar + Coarse Location	94.30%	83.54%	10.76%
	Google Contact	Read Contact	98.41%	97.22%	1.19%
Chrome	Geolocation	Fine Location + Coarse Location + Read Contact	88.29%	62.50%	25.79%
	Proxy	Send SMS + Fine Location	93.78%	89.69%	4.09%
	Content Settings	Fine Location + Read Contact	85.31%	59.61%	25.70%
SmartThings	Lock	Write Setting	85.71%	75.00%	10.71%
	Motion Sensor	Read Contact	87.10%	53.33%	33.77%
	Switch	Send SMS + Read Calendar	94.39%	90.09%	4.30%

# Evaluation (Effectiveness)

## TKPERM Performance Analysis (Metric: F1 Score)

Platform	Target Domain	Source Domain	Transfer	No Transfer	Improvement
IFTTT	Evernote	Coarse Location + Fine Location + Camera	83.13%	79.78%	3.35%
	BMW Lab	Send SMS + Record Audio	95.24%	85.71%	9.53%
	Facebook	Camera	88.09%	75.00%	13.09%
	Google Calendar	Read Calendar + Coarse Location	94.30%	83.54%	10.76%
	Google Contact	Read Contact	98.41%	97.22%	1.19%
Chrome	Geolocation	Fine Location + Coarse Location + Read Contact	88.29%	62.50%	25.79%
Android	Proxy	Send SMS + Fine Location	93.78%	89.69%	4.09%
	Content Settings	Fine Location + Read Contact	85.31%	59.61%	25.70%
SmartThings	Lock	Write Setting	85.71%	75.00%	10.71%
	Motion Sensor	Read Contact	87.10%	53.33%	33.77%
	Switch	Send SMS + Read Calendar	94.39%	90.09%	4.30%

# Evaluation (Effectiveness)

## TKPERM Performance Analysis (Metric: F1 Score)

Platform	Target Domain	Source Domain	Transfer	No Transfer	Improvement
IFTTT	Evernote	Coarse Location + Fine Location + Camera	83.13%	79.78%	3.35%
	BMW Lab	Send SMS + Record Audio	95.24%	85.71%	9.53%
	Facebook	Camera	88.09%	75.00%	13.09%
	Google Calendar	Read Calendar + Coarse Location	94.30%	83.54%	10.76%
	Google Contact	Read Contact	98.41%	97.22%	1.19%
Chrome	Geolocation	Fine Location + Coarse Location + Read Contact	88.29%	62.50%	25.79%
	Proxy	Send SMS + Fine Location	93.78%	89.69%	4.09%
	Content Settings	Fine Location + Read Contact	85.31%	59.61%	25.70%
SmartThings	Lock	Write Setting	85.71%	75.00%	10.71%
	Motion Sensor	Read Contact	87.10%	53.33%	33.77%
	Switch	Send SMS + Read Calendar	94.39%	90.09%	4.30%

# Evaluation (Effectiveness)

## TKPERM Performance Analysis (Metric: F1 Score)

Platform	Target Domain	Source Domain	Transfer	No Transfer	Improvement
IFTTT	Evernote	Coarse Location + Fine Location + Camera	83.13%	79.78%	3.35%
	BMW Lab	Send SMS + Record Audio	95.24%	85.71%	9.53%
	IFTTT	Send SMS + Read Contact	99.99%	77.99%	12.93%
SmartThings	Content Settings	Fine Location + Read Contact	85.51%	85.51%	0.00%
	Lock	Write Setting	85.71%	75.00%	10.71%
	Motion Sensor	Read Contact	87.10%	53.33%	33.77%
SmartThings	Switch	Send SMS + Read Calendar	94.39%	90.09%	4.30%

12.93% improvement compared  
to No Transfer

# Evaluation

Question 1. What is the end-to-end performance of TKPERM?

Question 2. What is the performance of each component  
in TKPERM?

Question 3. What is the computation overhead of TKPERM?

Effectiveness

# Evaluation

Question 1. What is the end-to-end performance of TKPERM?

Question 2. What is the performance of each component  
in TKPERM?

Question 3. What is the computation overhead of TKPERM?

Effectiveness

Scalability

# Evaluation (Scalability)

**Computation Overhead** (Run in Amazon Elastic Compute Cloud (EC2), NVIDIA Tesla V100)

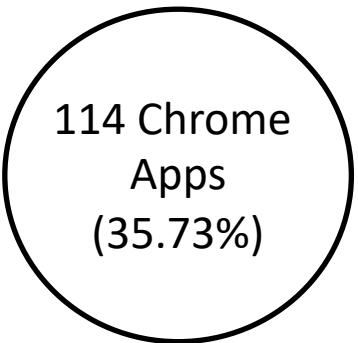
Platform	Target Domain	Time (hh:mm:ss)
IFTTT	Evernote	33:27:03
	BMW Lab	14:08:40
	Facebook	22:57:20
	Google Calendar	15:15:18
	Google Contact	18:40:17
Chrome	Geolocation	07:37:28
	Proxy	06:54:01
	Content Settings	09:42:45
SmartThings	Lock	03:47:59
	Motion Sensor	04:09:44
	Switch	14:11:08

# Evaluation (Scalability)

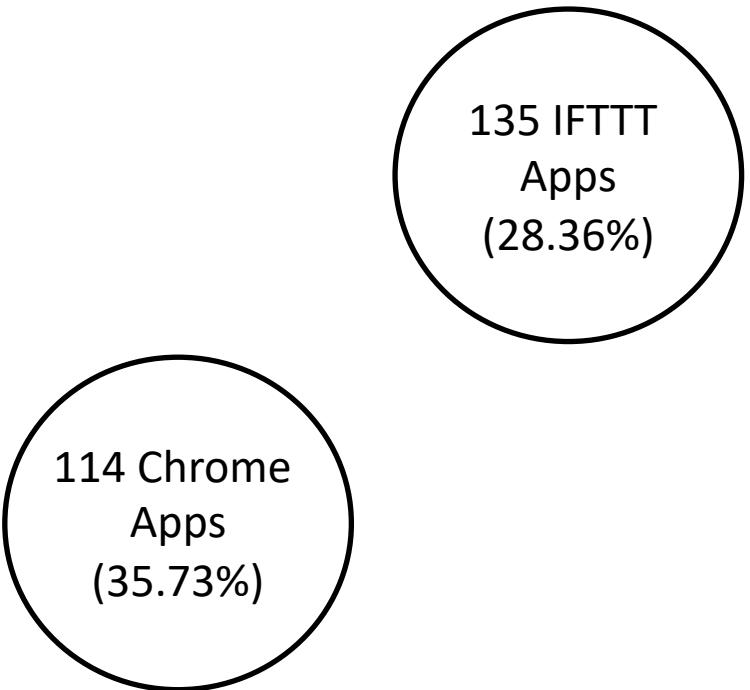
**Computation Overhead** (Run in Amazon Elastic Compute Cloud (EC2), NVIDIA Tesla V100)

Platform	Target Domain	Time (hh:mm:ss)
IFTTT	Evernote	33:27:03
	BMW Lab	14:08:40
	Facebook	22:57:20
	Google Calendar	15:15:18
	Google Contact	18:40:17
Chrome	Geolocation	07:37:28
SmartThings	Proxy	06:54:01
	Content Settings	09:42:45
	Lock	03:47:59
	Motion Sensor	04:09:44
	Switch	14:11:08

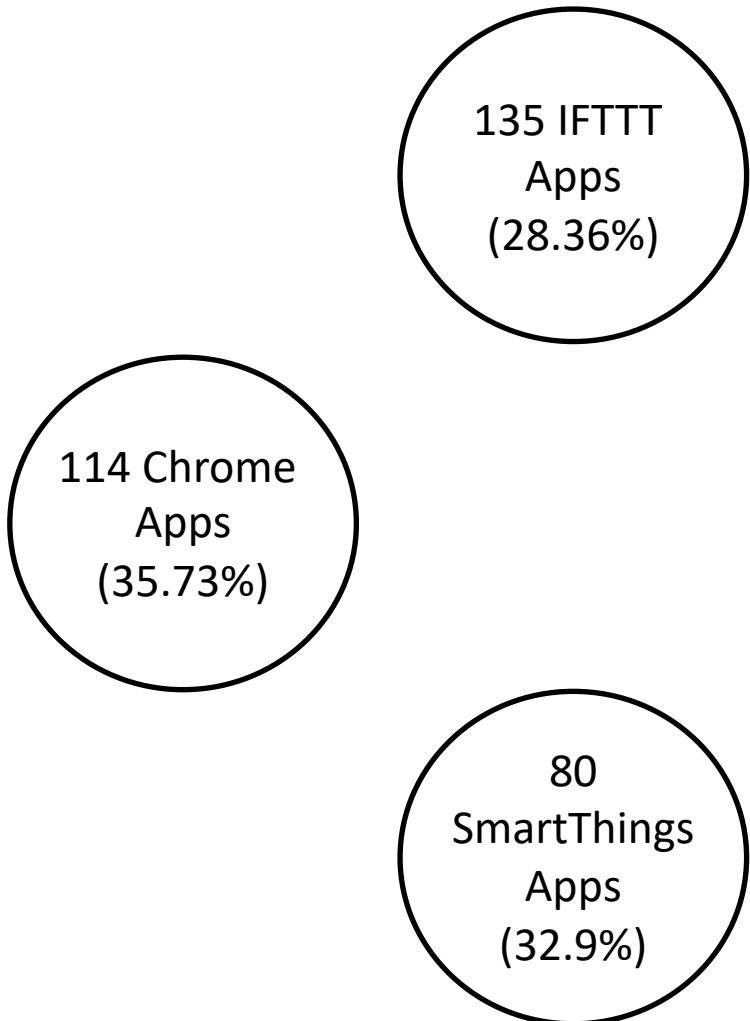
# Measurement Result



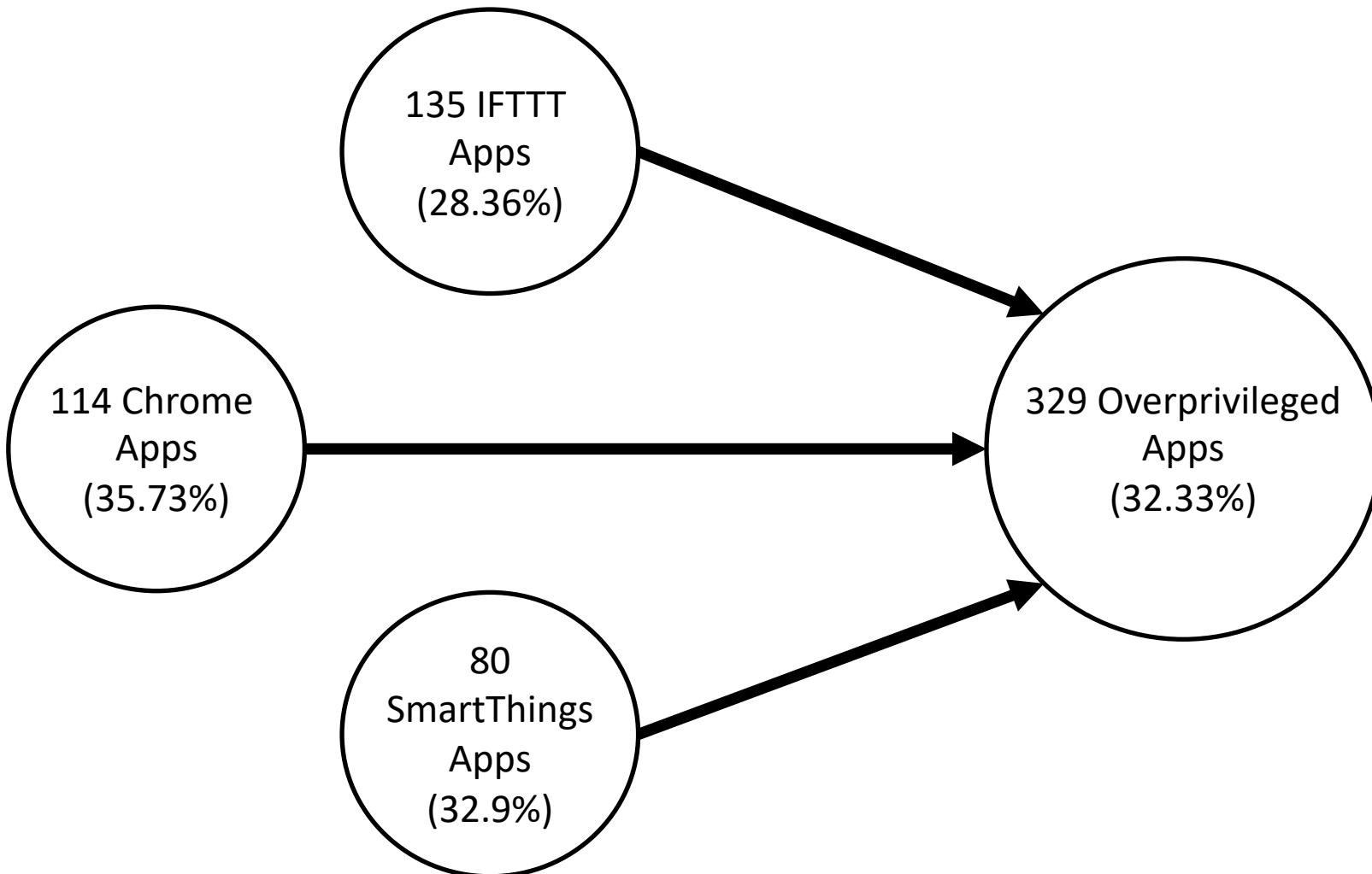
# Measurement Result



# Measurement Result



# Measurement Result



# Conclusion

## 1. General Framework

General framework to detect  
Overprivileged applications in new platforms

# Conclusion

## 1. General Framework

↑ Posted by u/CraftedCrows 3 years ago ━

26 Just got the VR why do some apps ask for so many permissions?  
↓

For example some games want permission for Camera "Take pictures and video" Phone "Read phone status and identity" Microphone "Record audio" the game in question is singleplayer.. Storage "Modify or delete SD card contents", most games only ask for read content on SD card.

It seems fishy at least that some games ask for so many permissions and to be honest I stayed away from games like this.

7 Comments Share Save Hide Report 82% Upvoted

# Conclusion

## 1. General Framework

Posted by u/CraftedCrows 3 years ago

26 Just got the VR why do some apps ask for so many permissions? For example some games ask for so many permissions and to be honest I stayed away from them like this.

How to identify overprivileged application in VR (new platform)?



7 Comments Share Save Hide Report 82% Upvoted

# Conclusion

## 1. General Framework

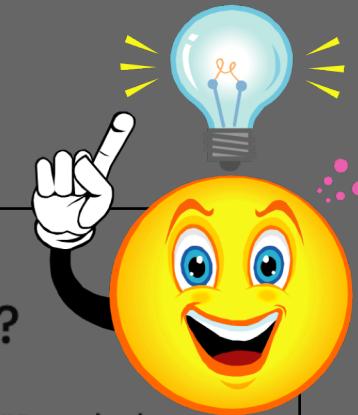
Posted by u/CraftedCrows 3 years ago ▾ 26

Just got the VR why do some apps ask for so many permissions?

For example some games want permission for Camera "Take pictures and video" Phone "Read phone status and identity" Microsoft "Change system settings" Google Play "Modify or delete SD card contents"...

It seems fishy at least that some games ask for so many permissions and to be honest I stayed away from games like this.

7 Comments Share Save Hide Report 82% Upvoted



# Conclusion

1. General Framework
2. Result

**TKPERM works well  
(90.02% F1 score on avg.)**

# Conclusion

1. General Framework
2. Result
3. Public Dataset



# Thank You!

Contact: Faysal Hossain Shezan (Email-[fs5ve@virginia.edu](mailto:fs5ve@virginia.edu))

# Conclusion

- 1. General Framework
- 2. Result
- 3. Public Dataset



Dataset

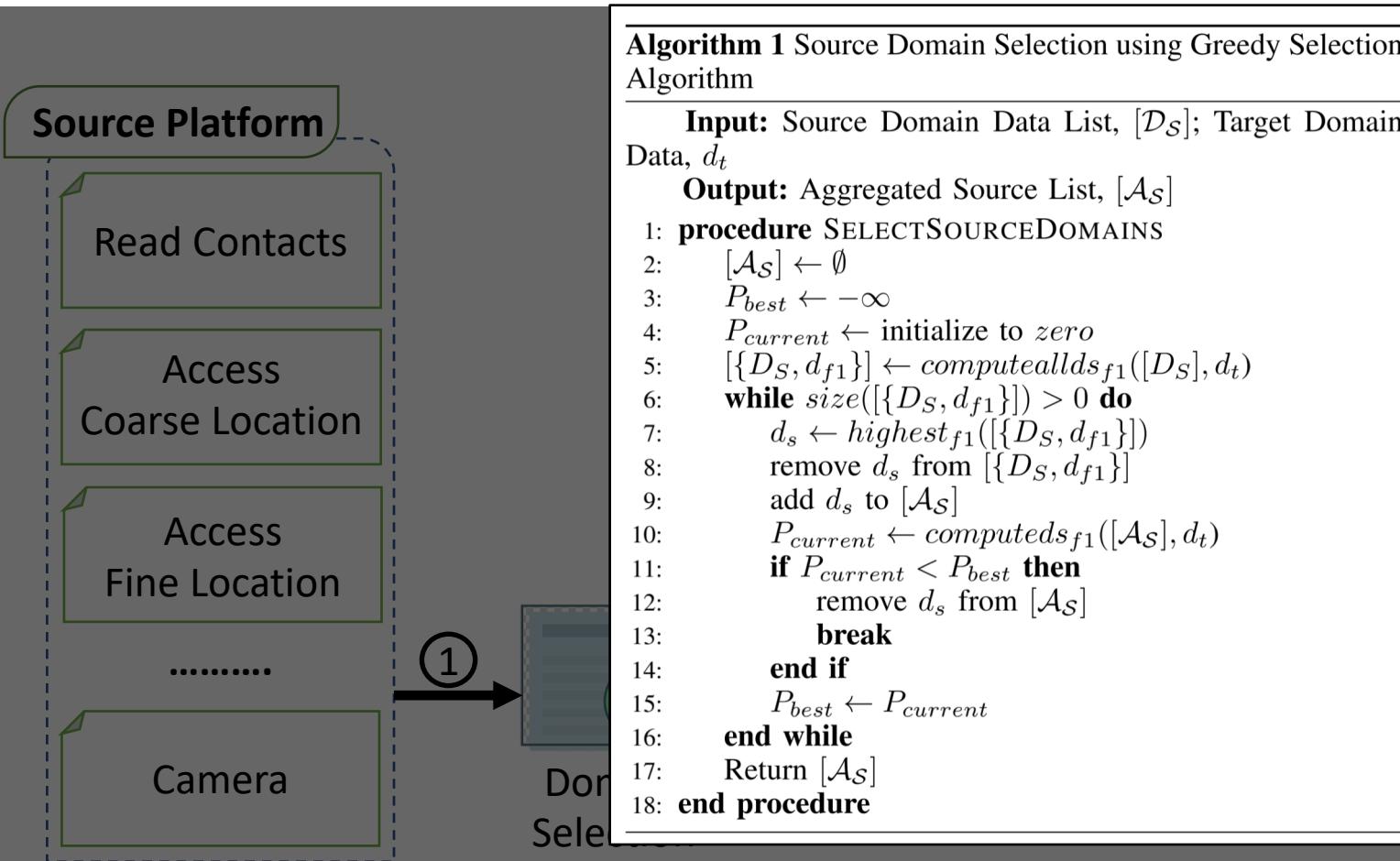
Email: fs5ve@virginia.edu

# Backup Slides

<b>Plat.</b>	<b>Perform.</b>	<b>Word Embedding</b>	
		<b>Target</b>	<b>Source</b>
<b>IFTTT</b>	F1 score	86%	91.83%
	Improv.	-	5.83%
<b>Chrome</b>	F1 score	88%	89.13%
	Improv.	-	1.13%
<b>Smart Things</b>	F1 score	85%	89.1%
	Improv.	-	4.1%

<b>Permission</b>	<b>Performance</b>			
	<b>Acc.</b>	<b>Prec.</b>	<b>Rec.</b>	<b>F1</b>
<b>Fine Location</b>	85%	73%	84%	78%
<b>Coarse Location</b>	84%	53%	84%	65%
<b>Camera</b>	88%	80%	89%	85%
<b>Read Calendar</b>	89%	87%	89%	88%
<b>Read Contact</b>	92%	92%	90%	91%
<b>Record Audio</b>	84%	83%	83%	83%
<b>Write Settings</b>	87%	69%	86%	77%
<b>Send SMS</b>	93%	93%	100%	97%
<b>Write APN</b>	92%	88%	97%	94%
<b>Total</b>	88.22%	79.78%	89.11%	84.20%

# System Overview (Domain Selection)



# System Overview (Data Selection)

**Algorithm 2** Selecting fine-tune dataset for target model using Data Selection Module.

**Input:** Source Model,  $\mathcal{M}_S$ ; Unlabeled Target Domain Dataset,  $[\mathcal{A}_{\sqcup}]$   
**Output:** Fine-tune Dataset,  $[\mathcal{D}_F]$

```
1: procedure SELECTFINETUNEDATASET
2:   for each document,  $\mathcal{A} \in [\mathcal{A}_{\sqcup}]$  do
3:     for each sentence,  $d_t \in \mathcal{A}$  do
4:        $pred \leftarrow \text{prediction}(d_t, \mathcal{M}_S)$ 
5:       if  $pred = 1$  then
6:          $\mathcal{R}_{\mathcal{A}} \leftarrow \mathcal{R}_{\mathcal{A}} + 1$ 
7:       end if
8:     end for
9:     add  $\{\mathcal{A}, \mathcal{R}_{\mathcal{A}}\}$  to  $[\mathcal{D}_{\mathcal{R}}]$ 
10:    end for
11:     $[\mathcal{D}_{\mathcal{R}}]^* \leftarrow \text{sorted}_{desc}([\mathcal{D}_{\mathcal{R}}])$ 
12:     $[\mathcal{D}_F] \leftarrow \text{top}_{20}([\mathcal{D}_{\mathcal{R}}]^*)$ 
13:    Return  $[\mathcal{D}_F]$ 
14: end procedure
```

**Ranking:**

$$\mathcal{R}_{\mathcal{A}} = \sum_{j=1}^{len(\mathcal{A})} 1 \mid [\mathcal{P}(y_j | x_j)] = 1$$

$\forall$  sentence,  $x_j \in$  document,  $\mathcal{A}$

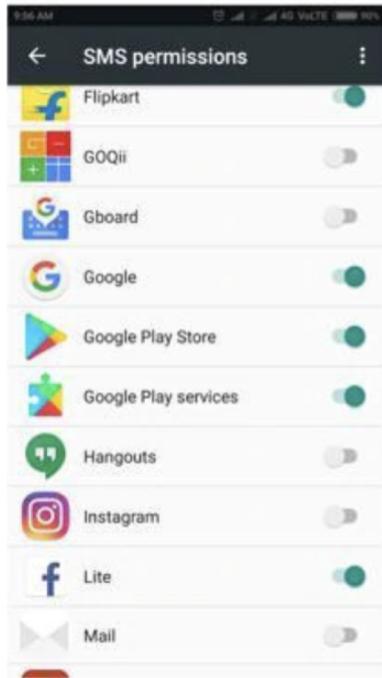
Model



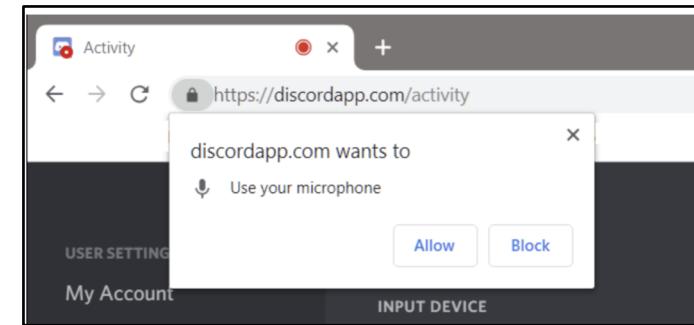
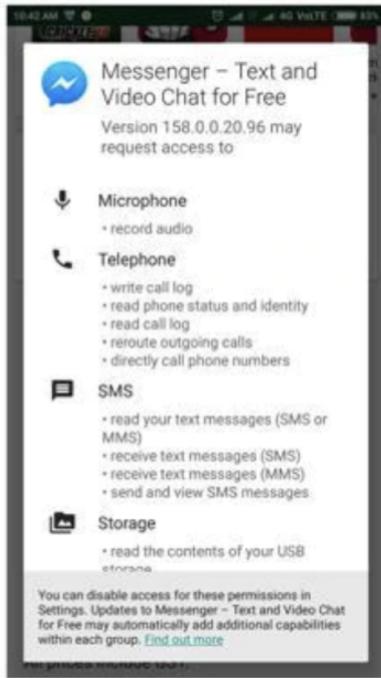
**Selection:**

$$[\mathcal{D}_F] = [sort_{desc}[\{\mathcal{A}_i, \mathcal{R}_{\mathcal{A}_i}\}_{i=1}^m]]_{j=1}^n$$

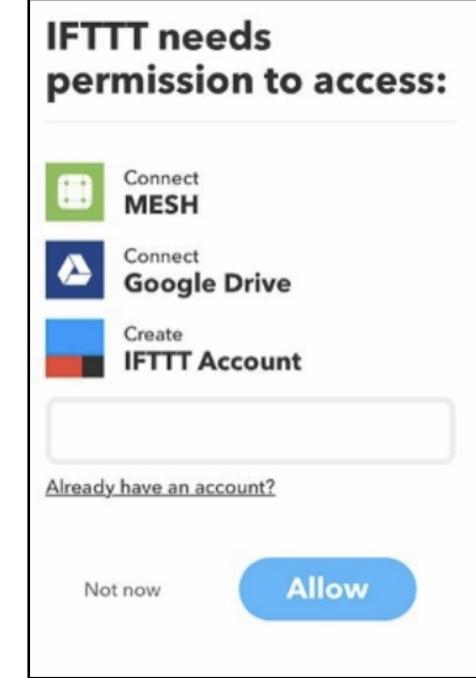
# Permission-based Access Control



Android



Chrome

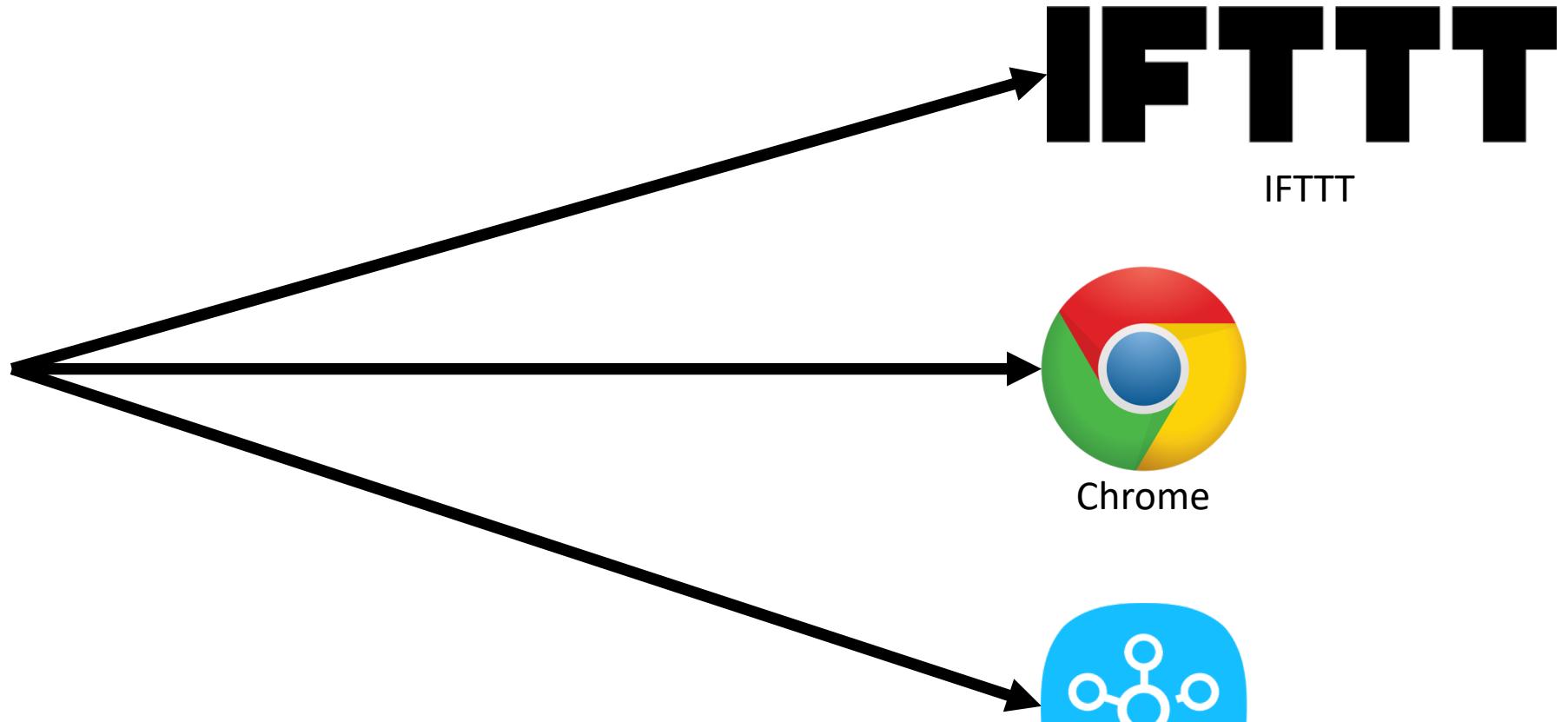


IFTTT

Goal



Android

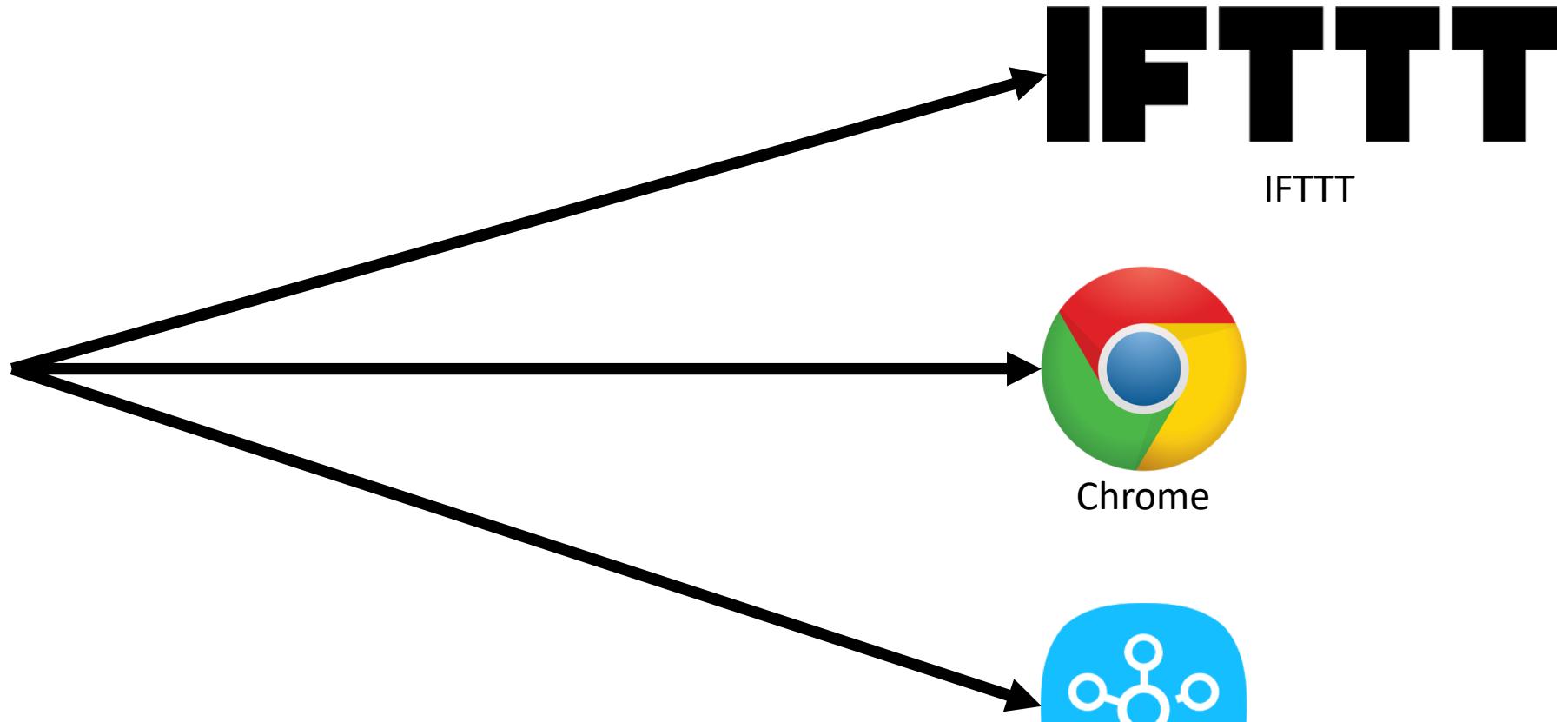


## G1. Semantic Knowledge

Goal



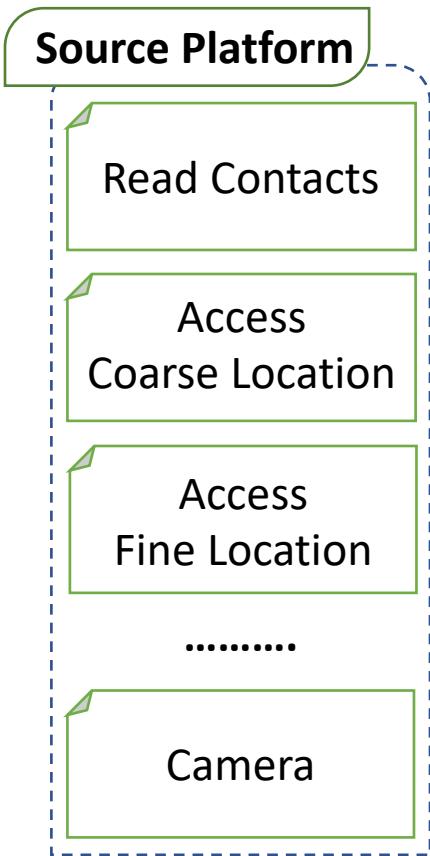
Android



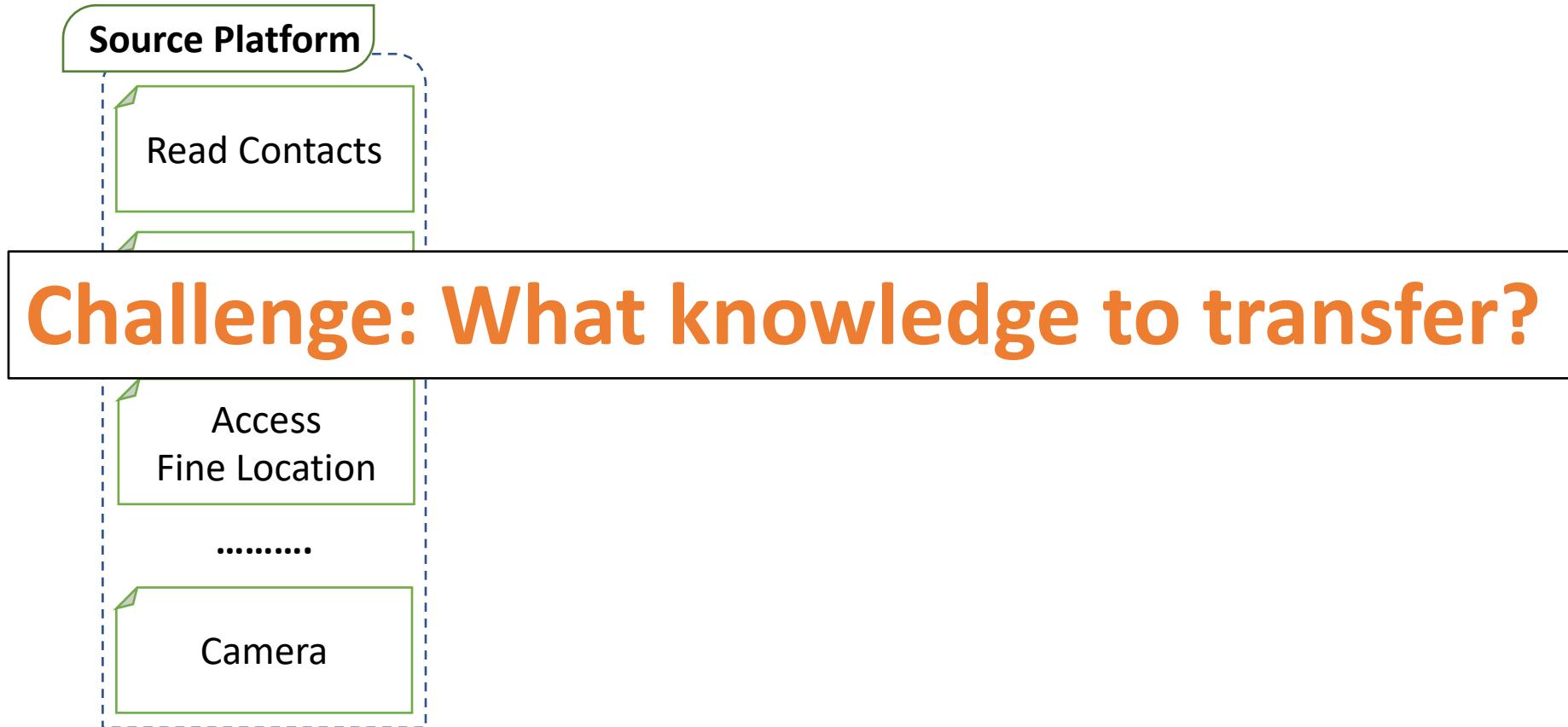
G1. Semantic Knowledge

G2. Permission Knowledge

# System Overview



# System Overview



# Domain Selection

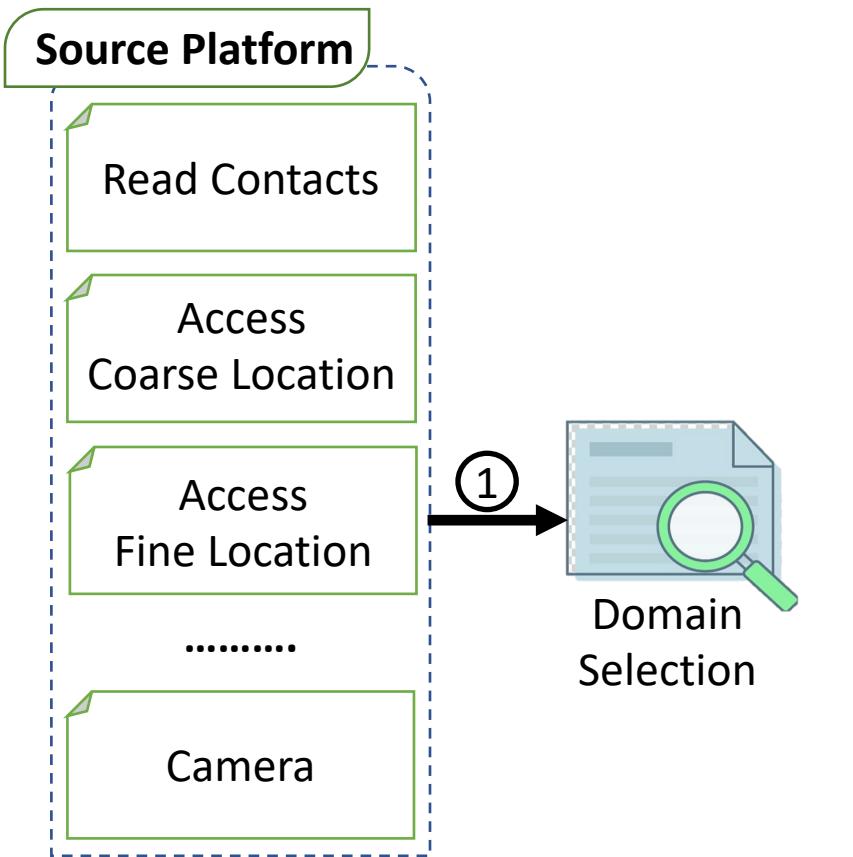
## Greedy Selection Approach

Aggregate source domain(s) which performs best

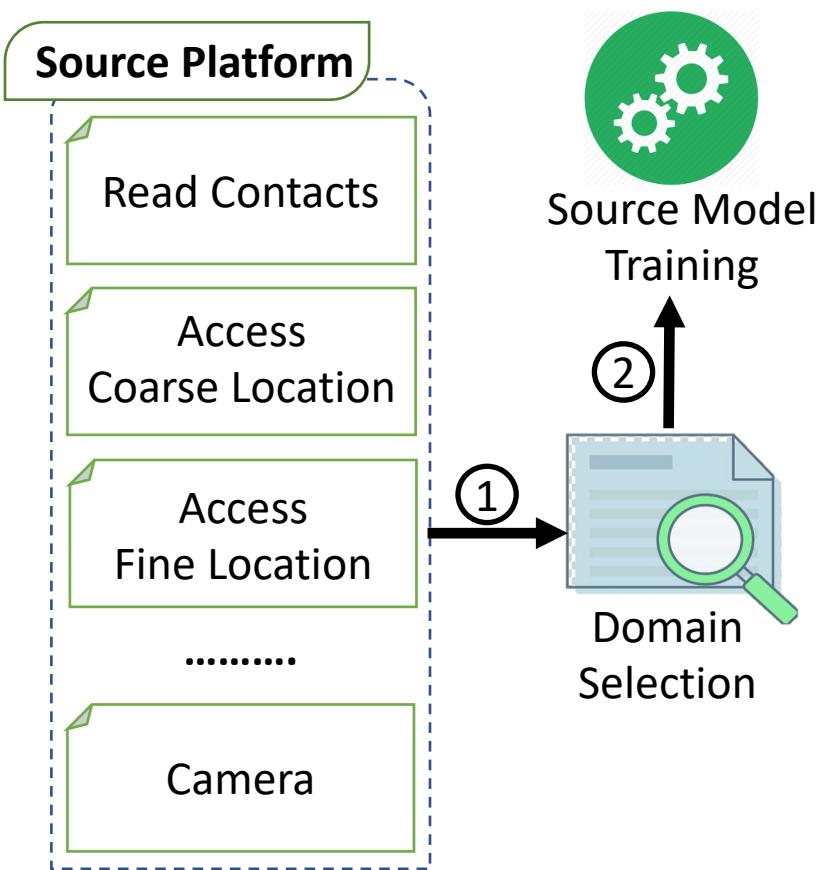
Remove source domain(s) which work worst

Find the best combination of the source domain(s)

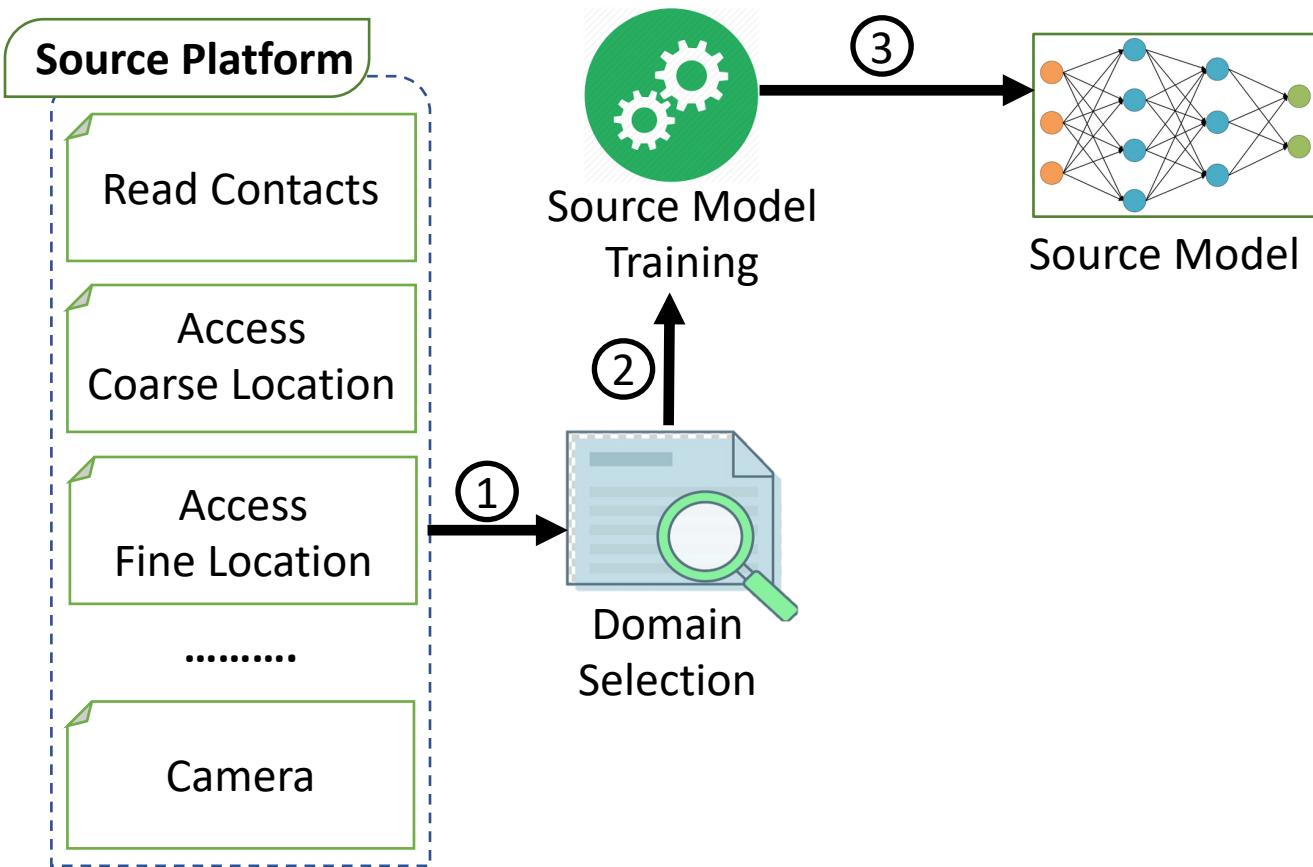
# System Overview



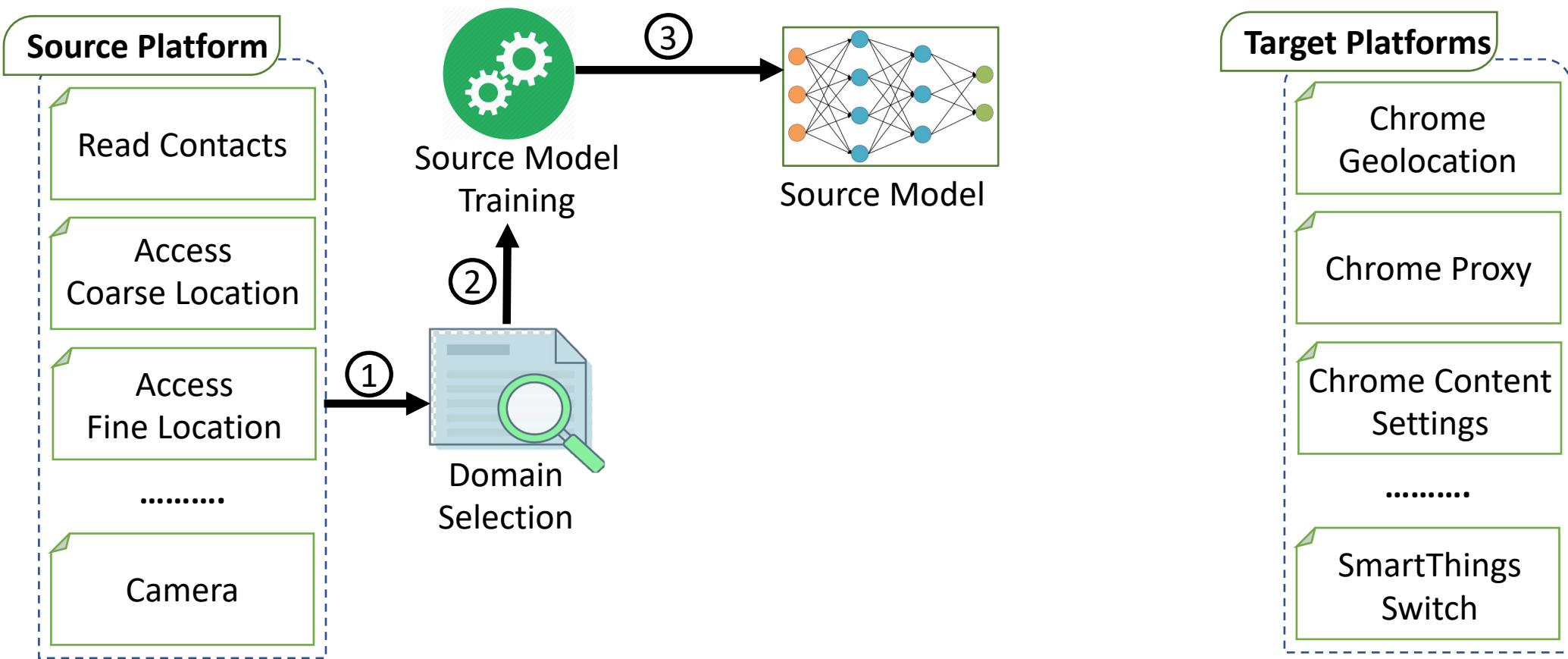
# System Overview



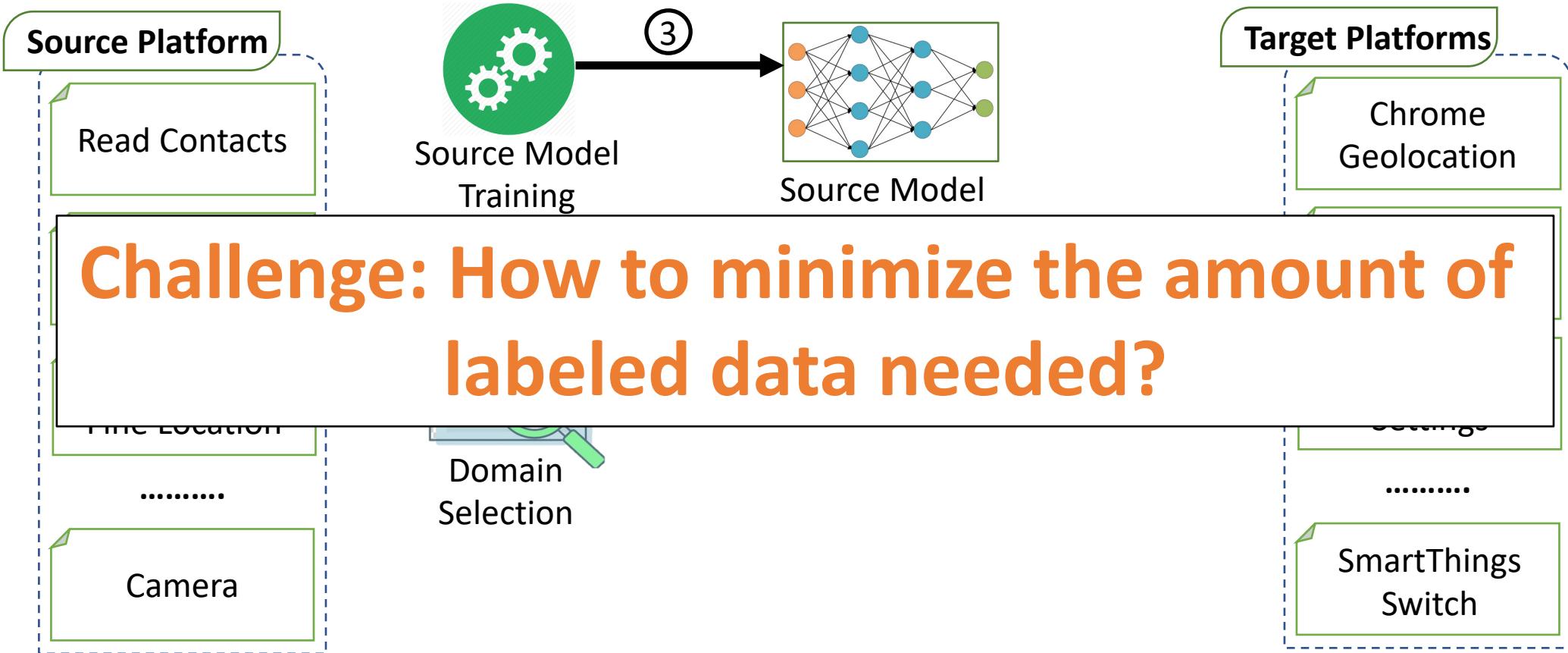
# System Overview



# System Overview



# System Overview



# Data Selection

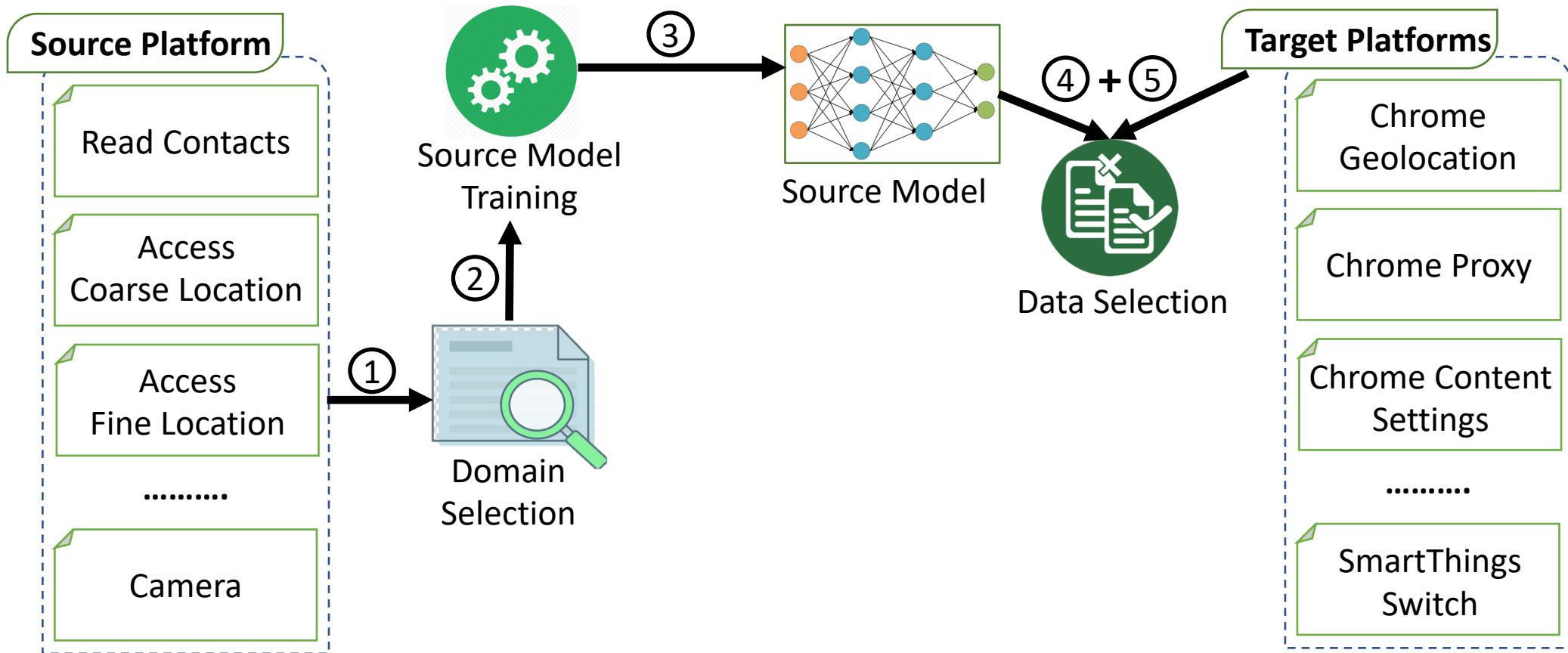
Use source model to rank the document

Rank unlabeled documents from the target domain

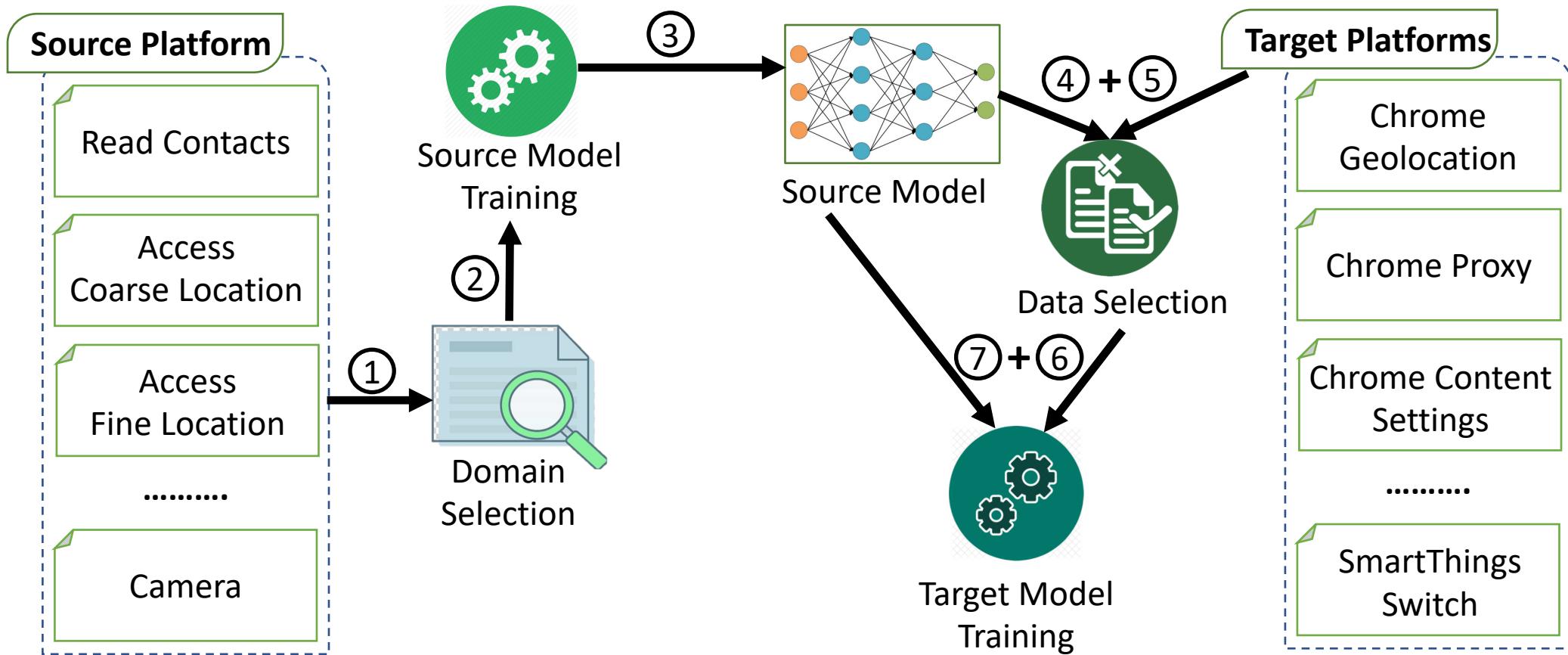
Pick the top 20 documents from a target domain

Ask human annotator to label data

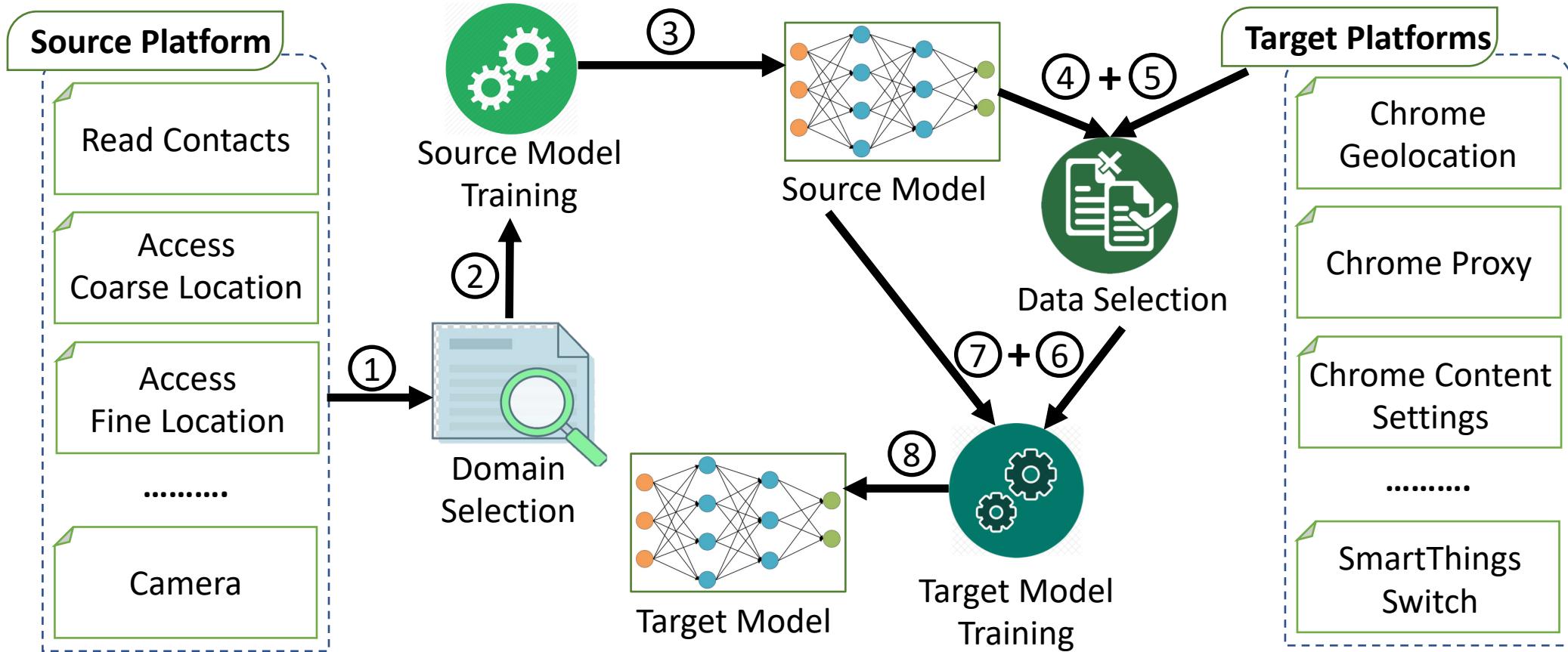
# System Overview



# System Overview



# System Overview



# Conclusion

- IFTTT – 135 apps
- Chrome Extension – 114 apps
- SmartThings – 80 apps