A Methodology for Empirical Analysis of Permission-Based Security Models and its Application to Android

David Barrera, Gunes Kayacik,
Paul van Oorschot and Anil Somayaji

Carleton
UNIVERSITY
Canada's Capital University

Outline

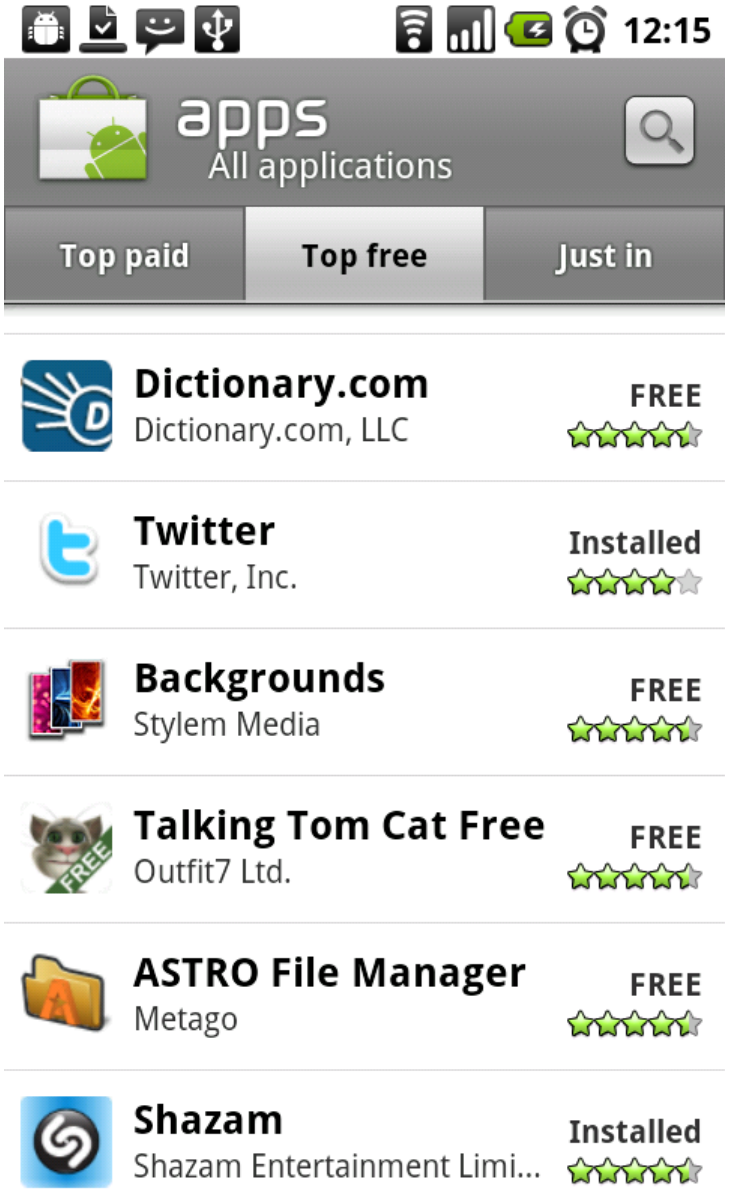
- Problem
- Motivation
- Methodology – Self Organizing Maps
- Results
- Other Applications
- Conclusions

Android App Installation

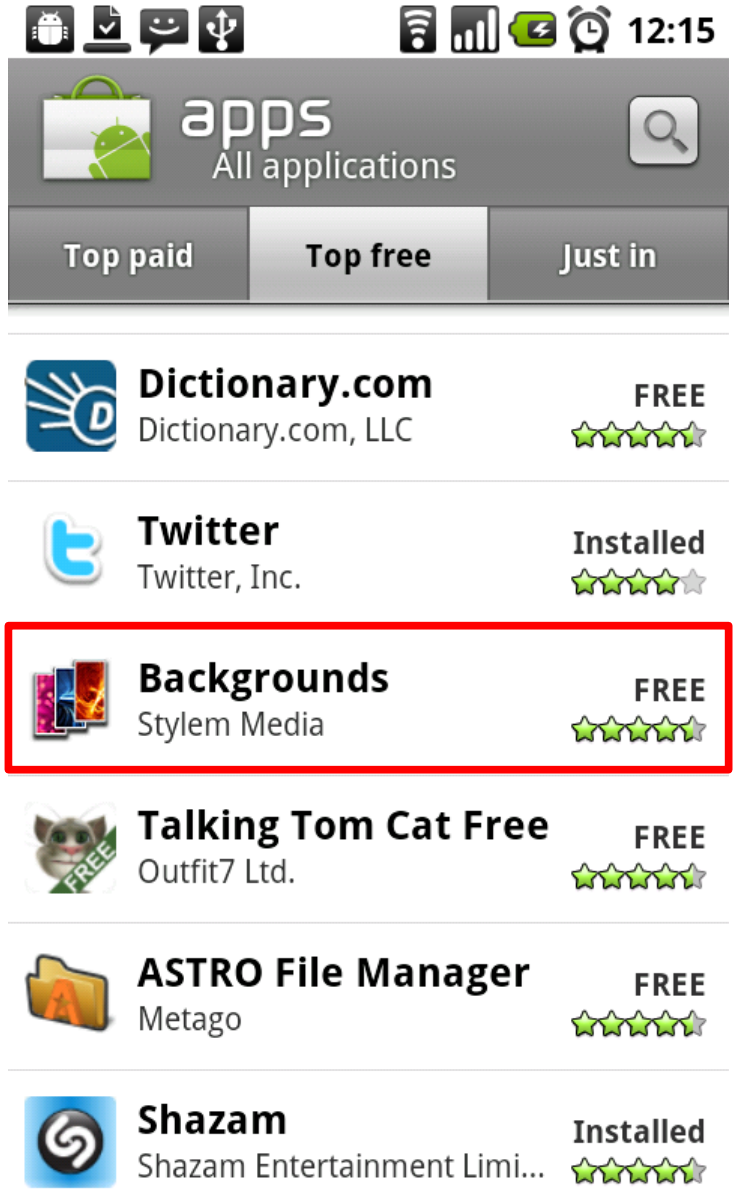
Android App Installation

Android App Installation

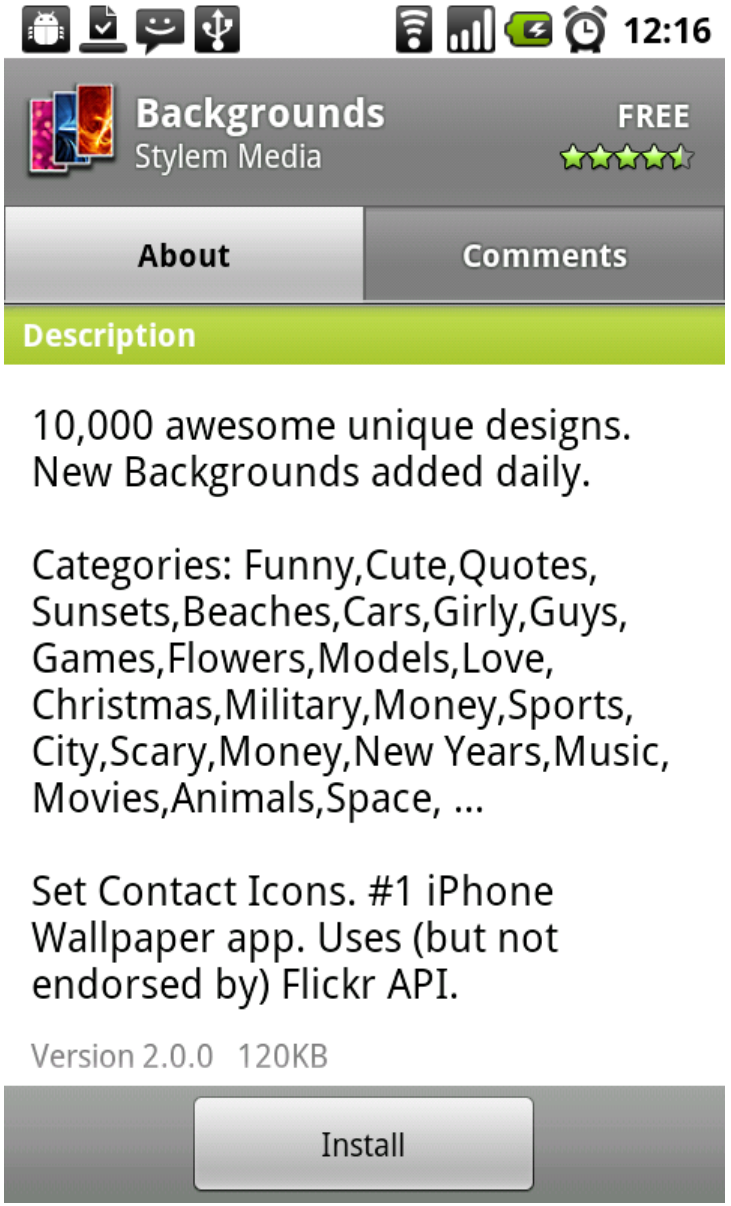
Android App Installation



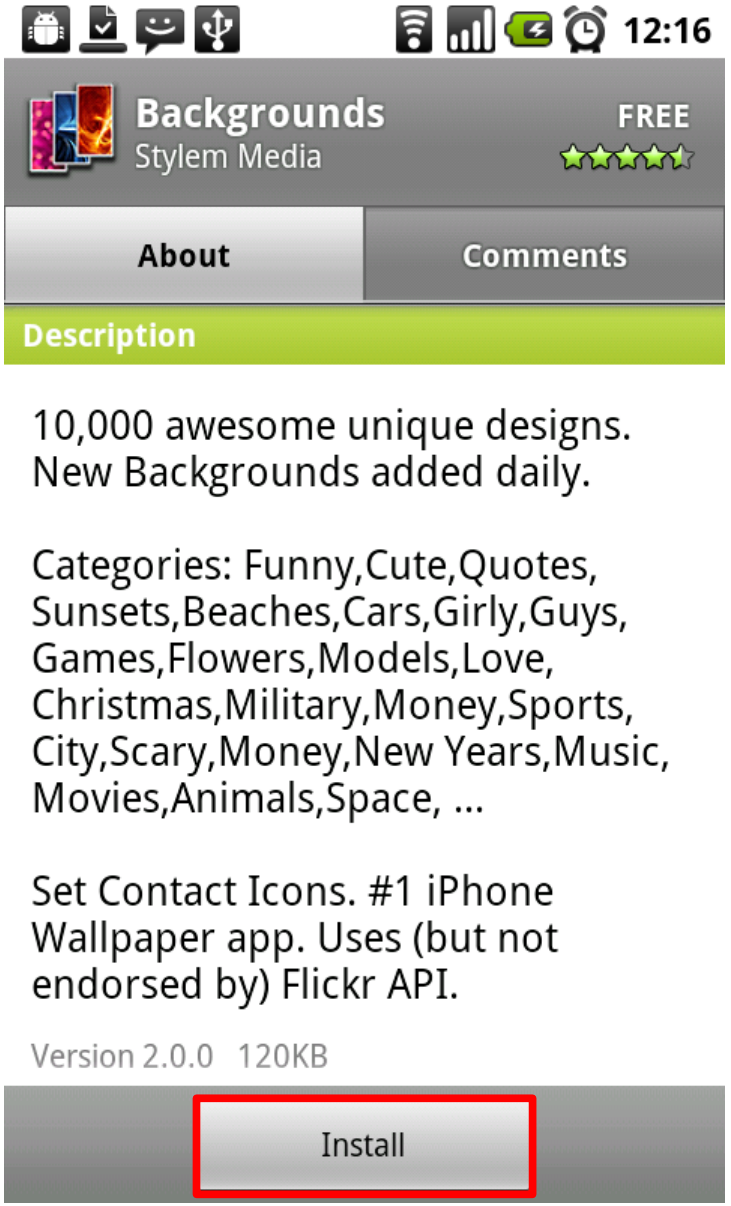
Android App Installation



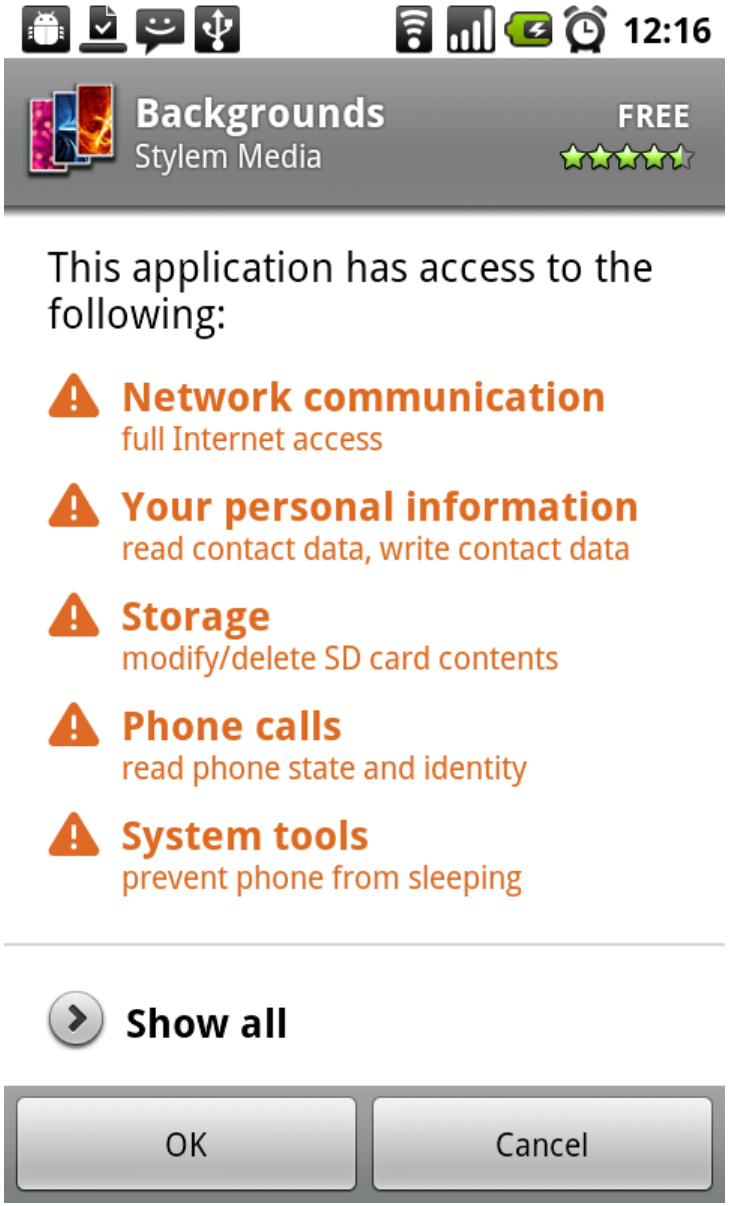
Android App Installation



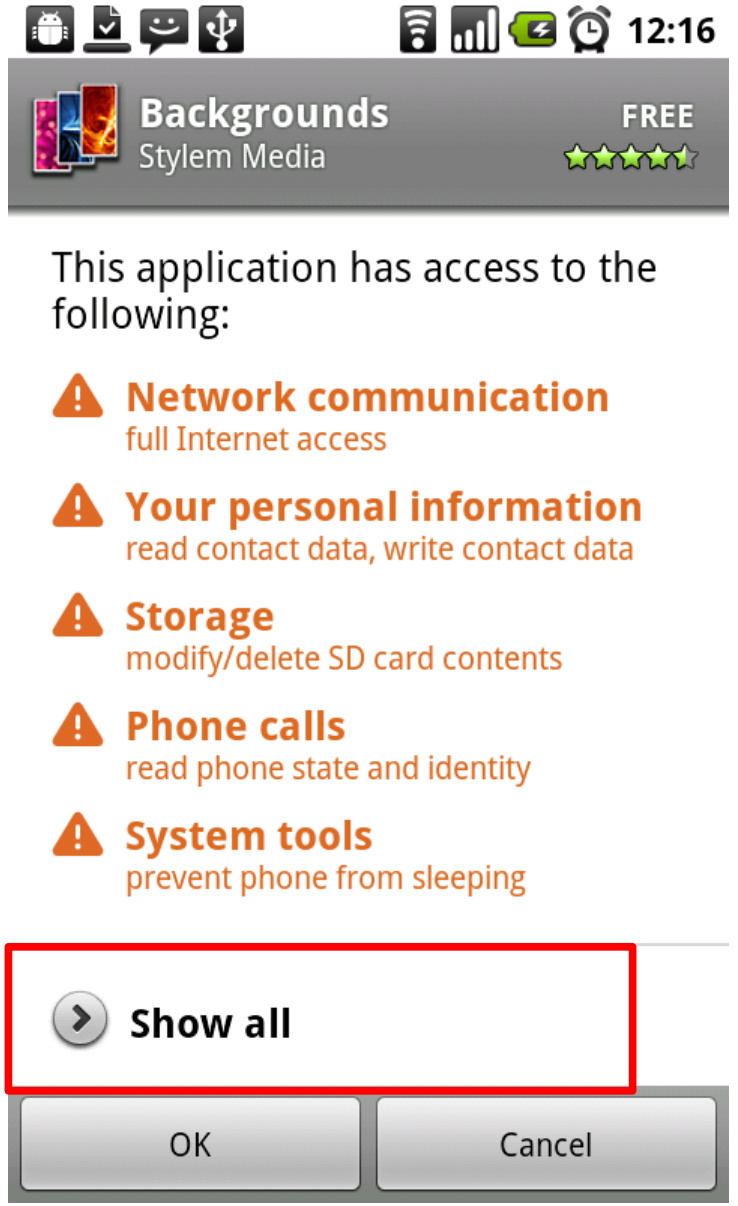
Android App Installation



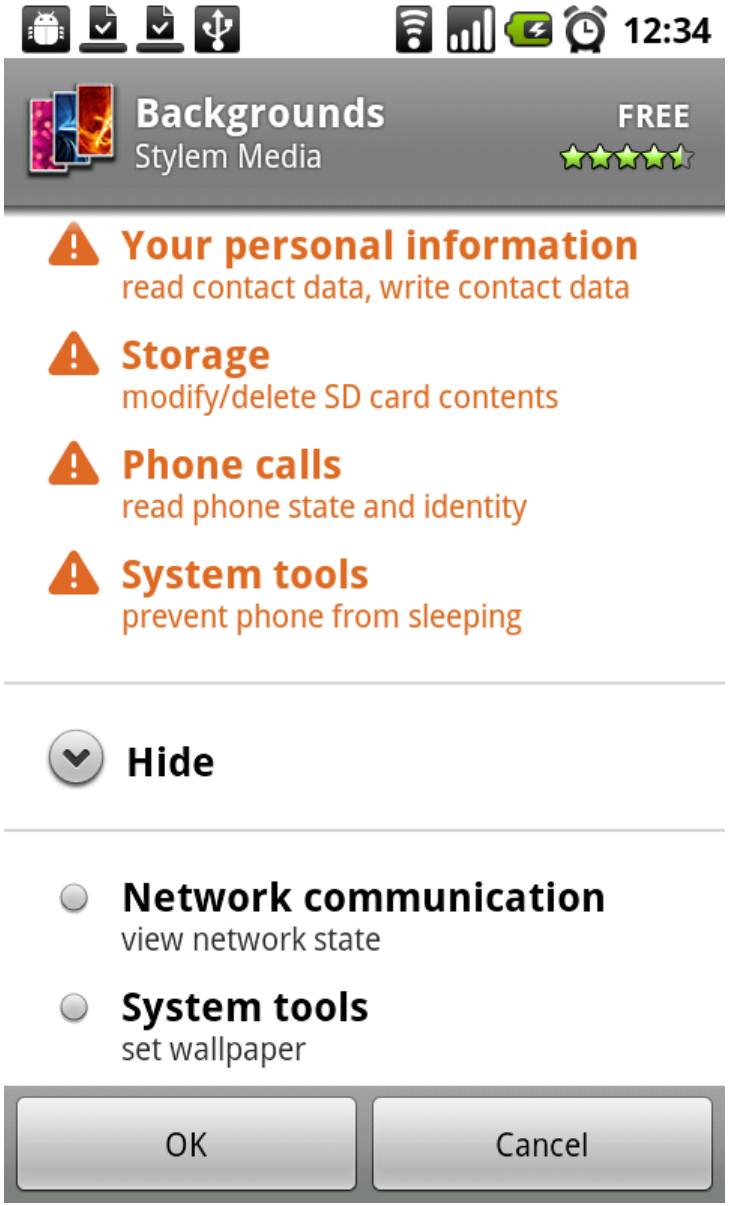
Android App Installation



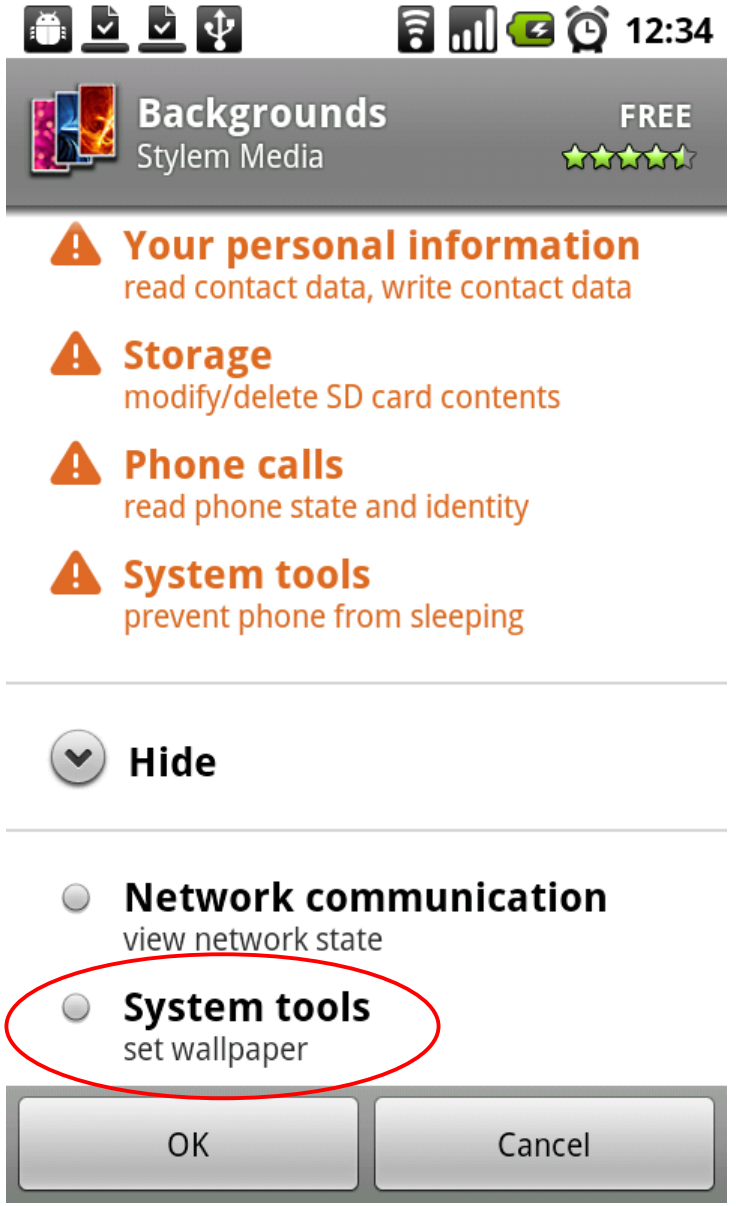
Android App Installation



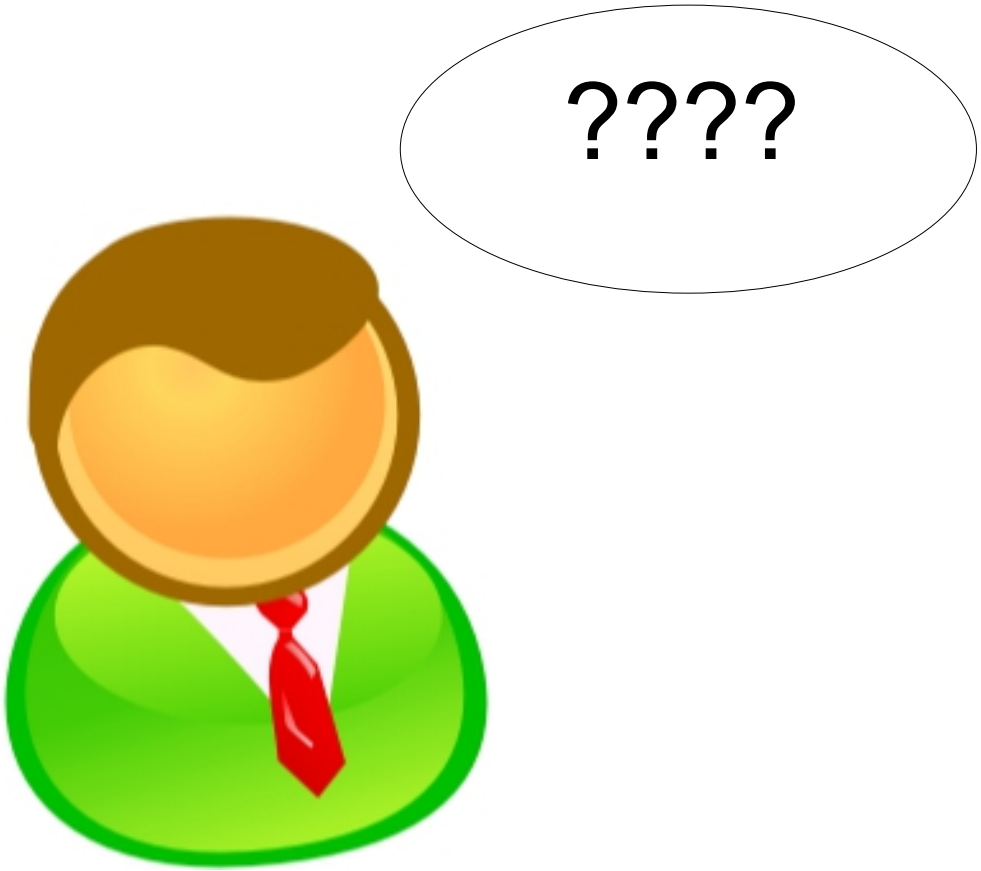
Android App Installation



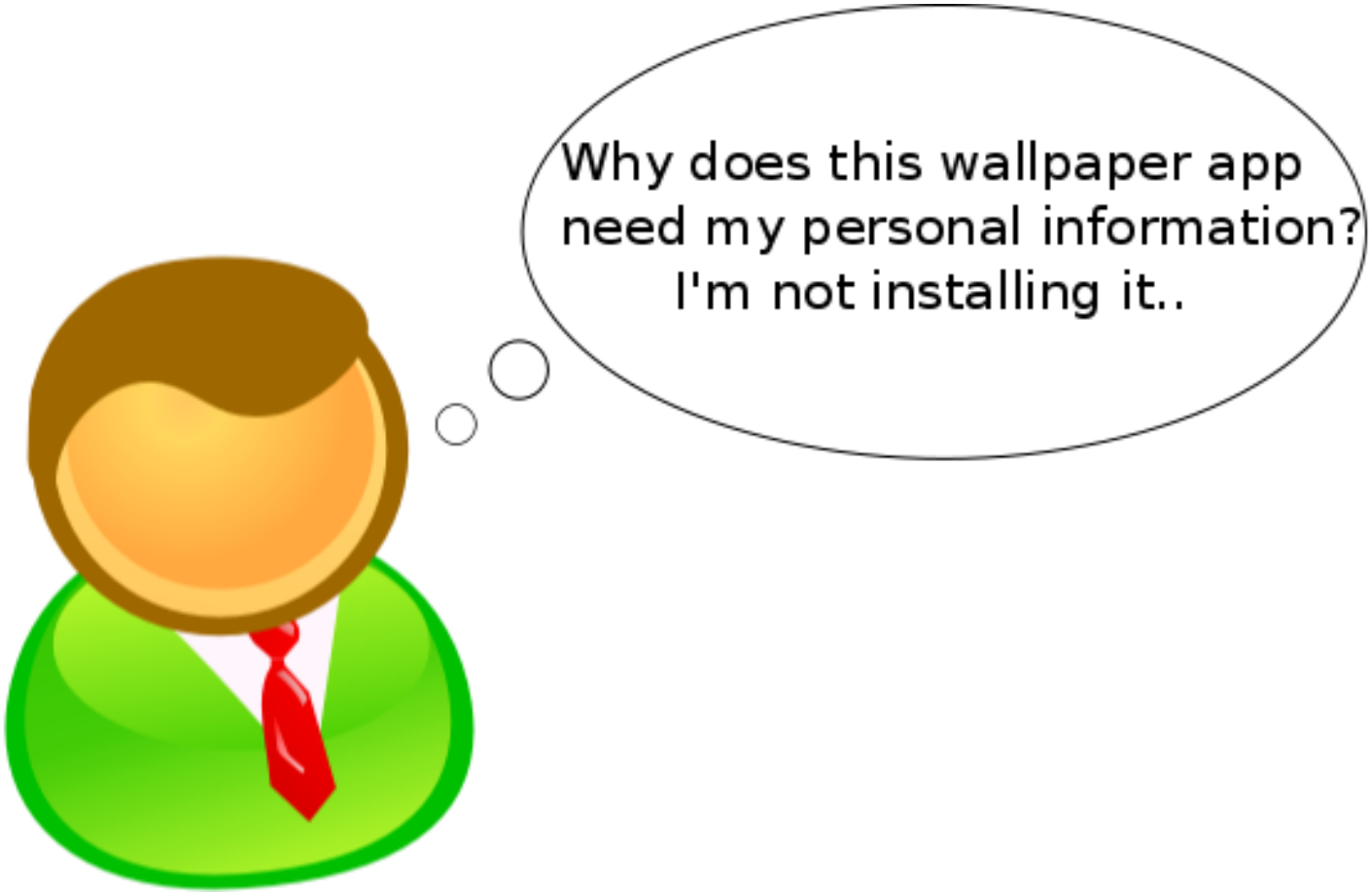
Android App Installation



Problem



Goal

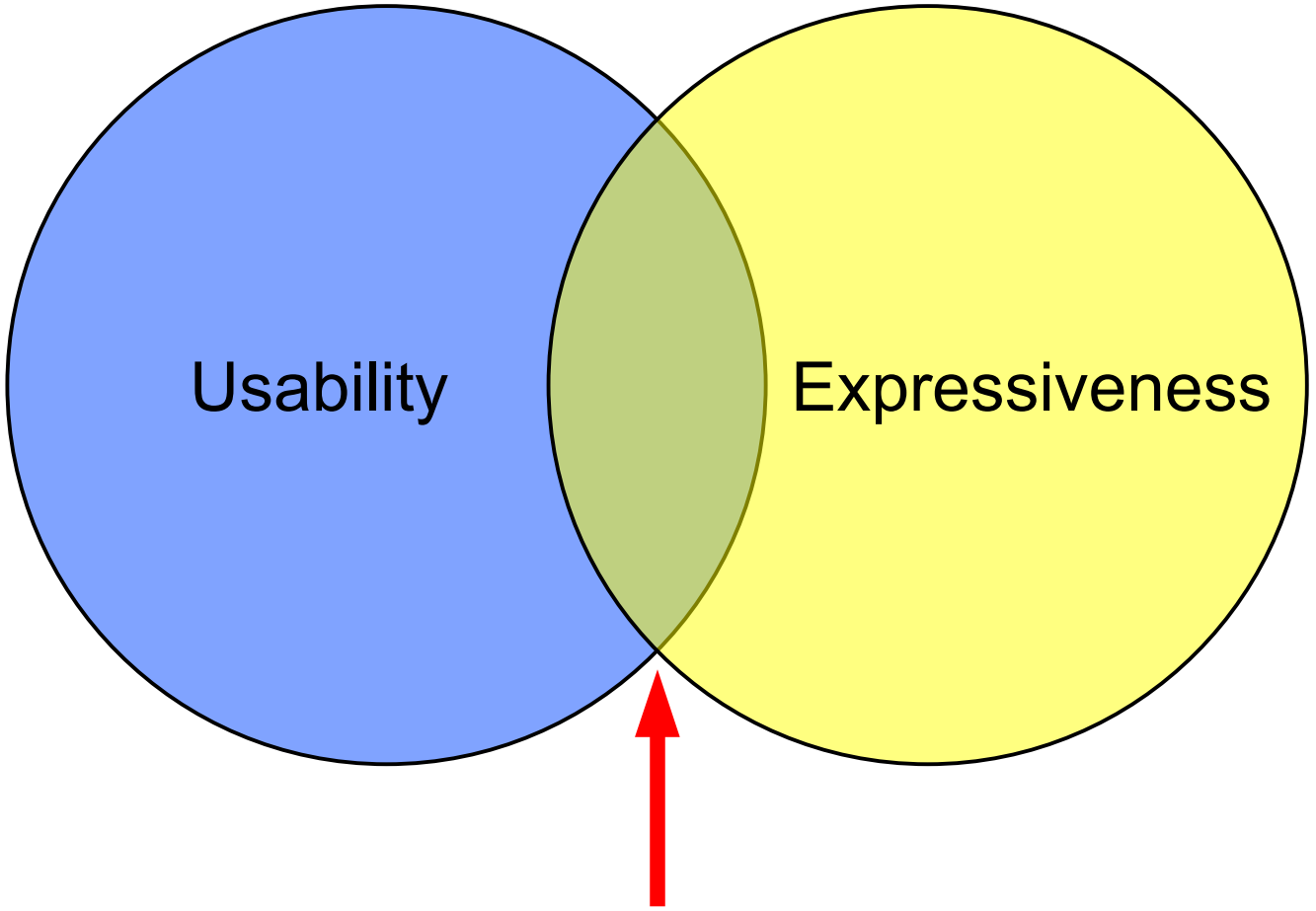

Why does this wallpaper app need my personal information? I'm not installing it..

Reality

Problem

- Usability challenges with the Android permission model.
- Not unique to Android
- If we want to improve these systems, where do we start?

Motivation



Motivation

- How is the permission model used in practice?
- Which permissions are used/not used?
- Which permissions are used together?
- Are permissions correlated to categories?
- More...

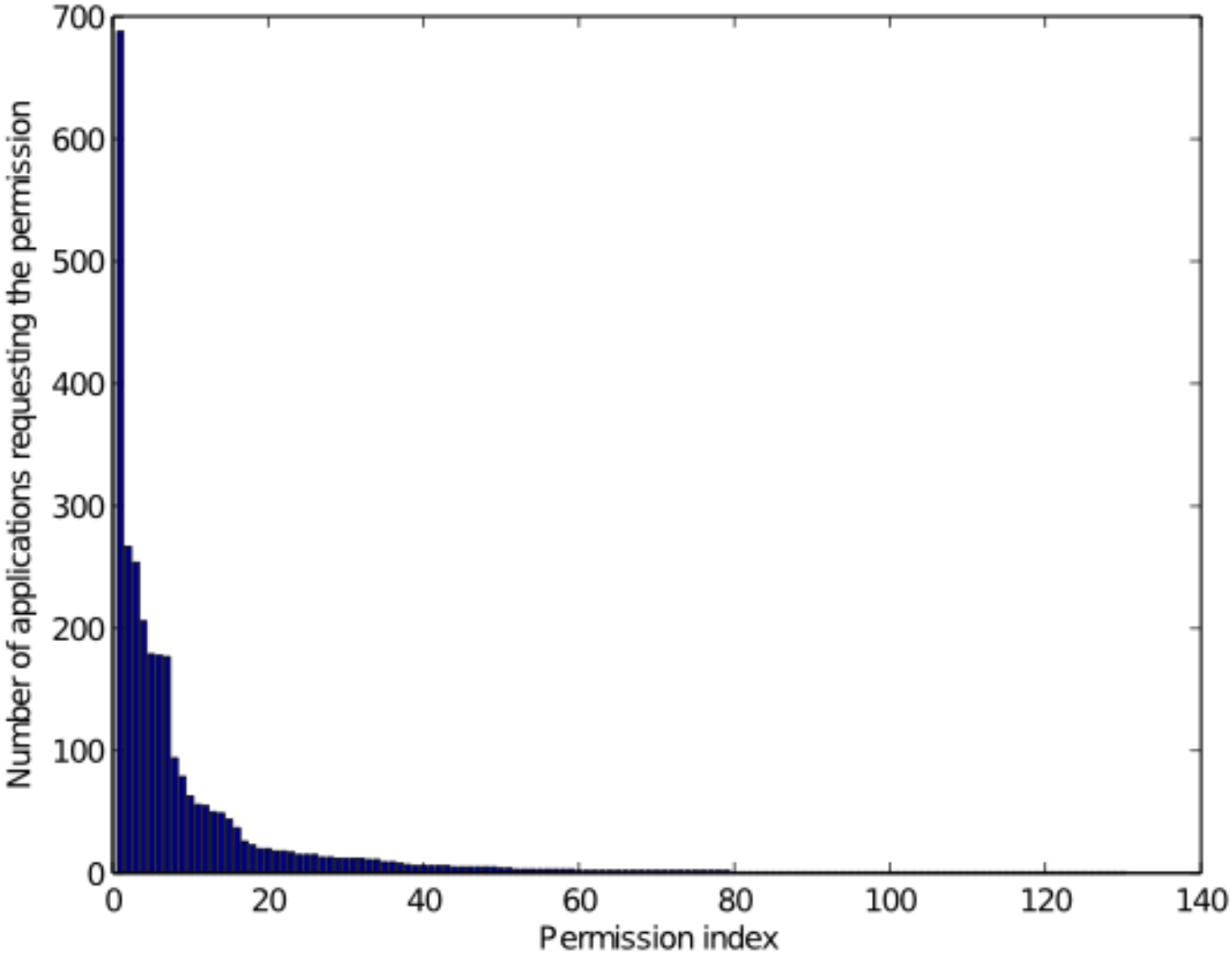
Motivation

- Empirically analyze a permission-based access control system that's currently in use (Android)
- Generalize the Android case for use in other systems

Dataset

- Dataset
  - 1,100 Android apps
  - Top 50 apps in 22 categories (18+4)
  - December 2009
- Some stats
  - 119 distinct permissions (38/81)
  - Max permissions in one app: 22 (Handcent SMS)

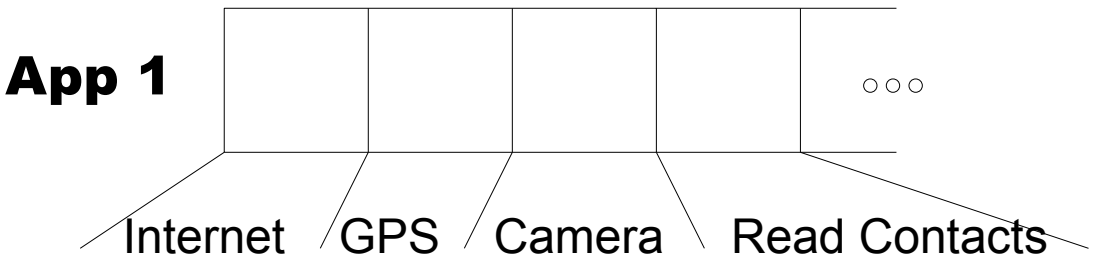
Dataset


Number of applications requesting the permission
700
600
500
400
300
200
100
0
0
20
40
60
80
100
120
140
Permission index

Methodology

- For each app, read the manifest and build a bit string

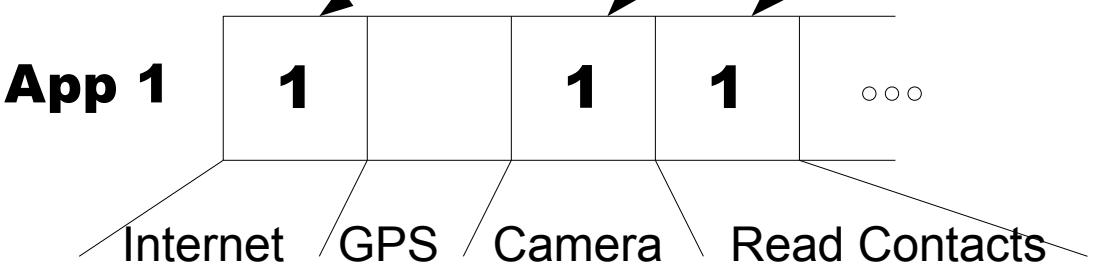
```
<manifest>
    ...
    <uses-permission android:name="android.permission.CAMERA" />
    <uses-permission android:name="android.permission.INTERNET" />
    <uses-permission android:name="android.permission.READ_CONTACTS" />
    ...
</manifest>
```



Methodology

- For each app, read the manifest and build a bit string

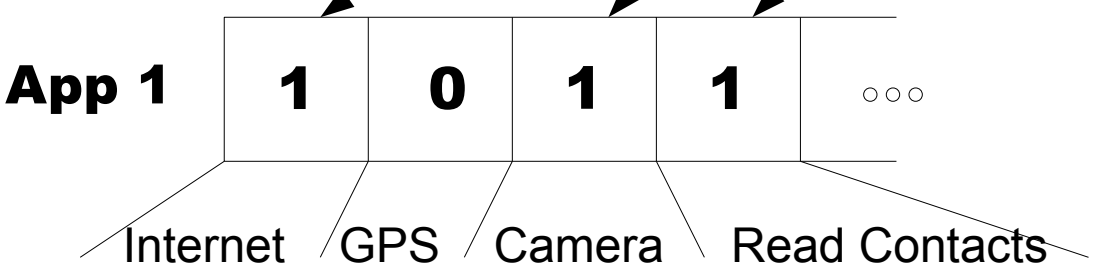
```
<manifest>
    ...
    <uses-permission android:name="android.permission.CAMERA" />
    <uses-permission android:name="android.permission.INTERNET" />
    <uses-permissionandroid:name="android.permission.READ_CONTACTS" />
    ...
</manifest>
```



Methodology

- For each app, read the manifest and build a bit string

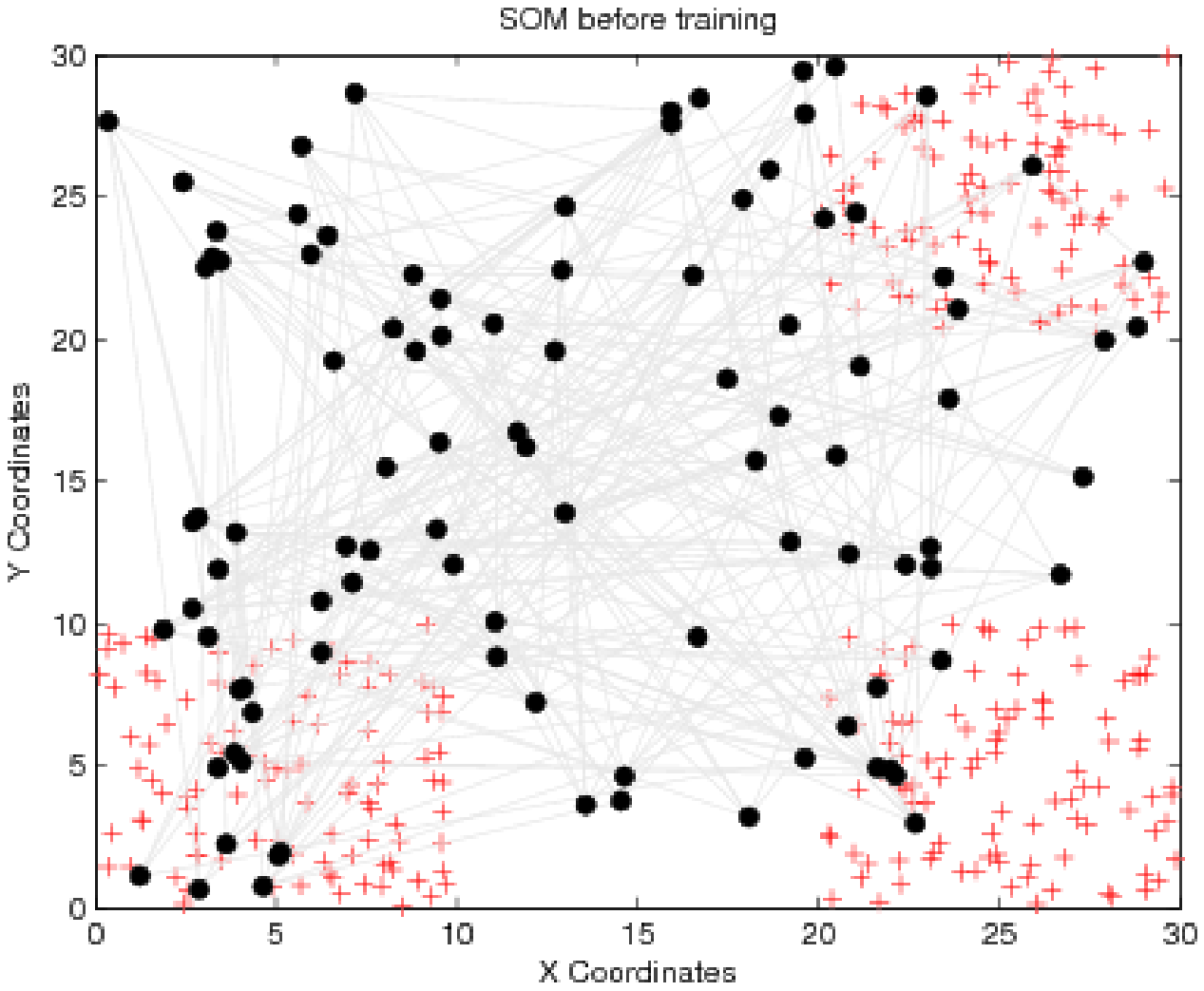
```
<manifest>
    ...
    <uses-permission android:name="android.permission.CAMERA" />
    <uses-permission android:name="android.permission.INTERNET" />
    <uses-permissionandroid:name="android.permission.READ_CONTACTS" />
    ...
</manifest>
```



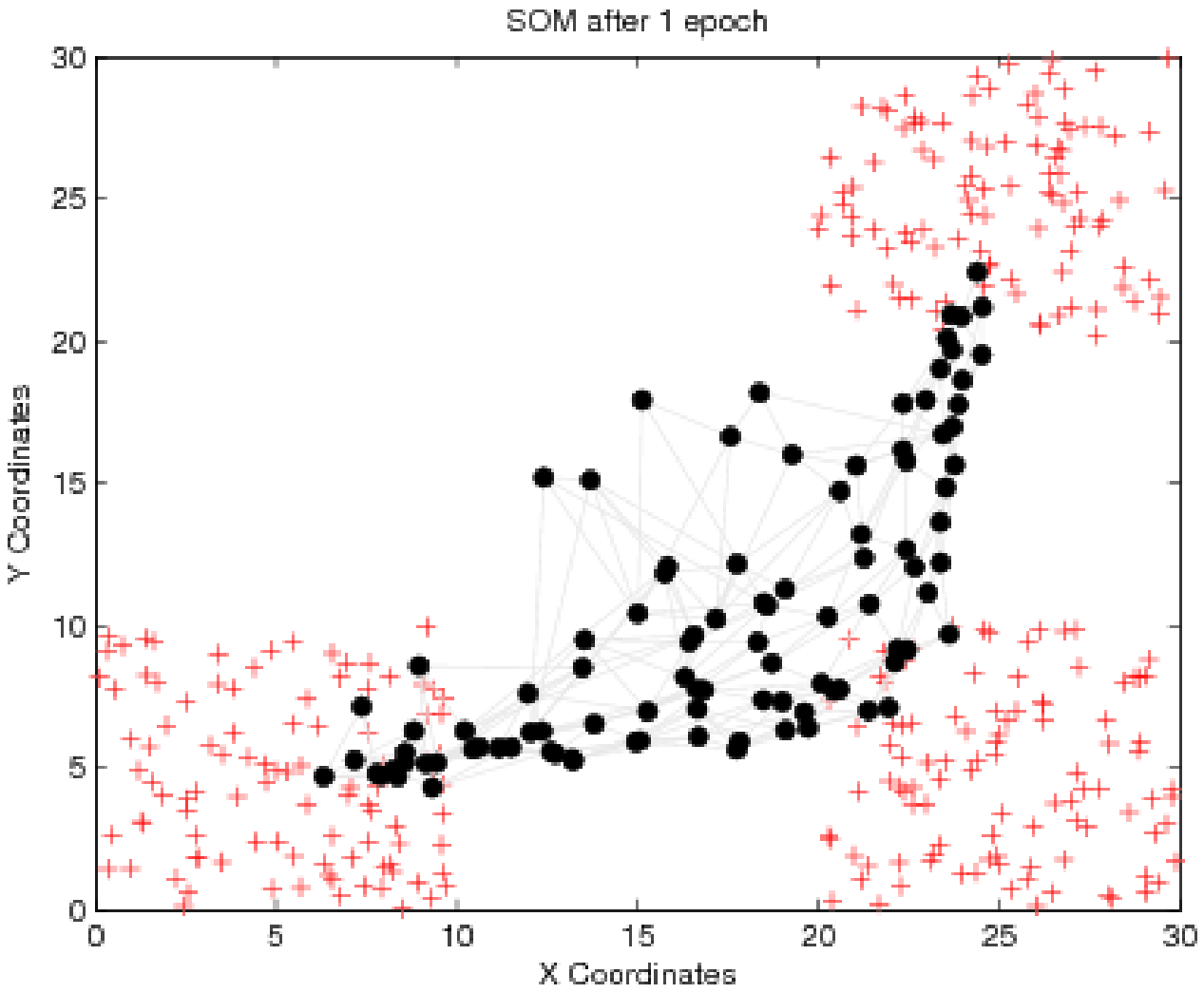
Methodology

- Self Organizing Maps (SOM)
  - Unsupervised neural-network learning algorithm
  - Provides clustering and dimensionality reduction
  - Helps with data exploration for large datasets

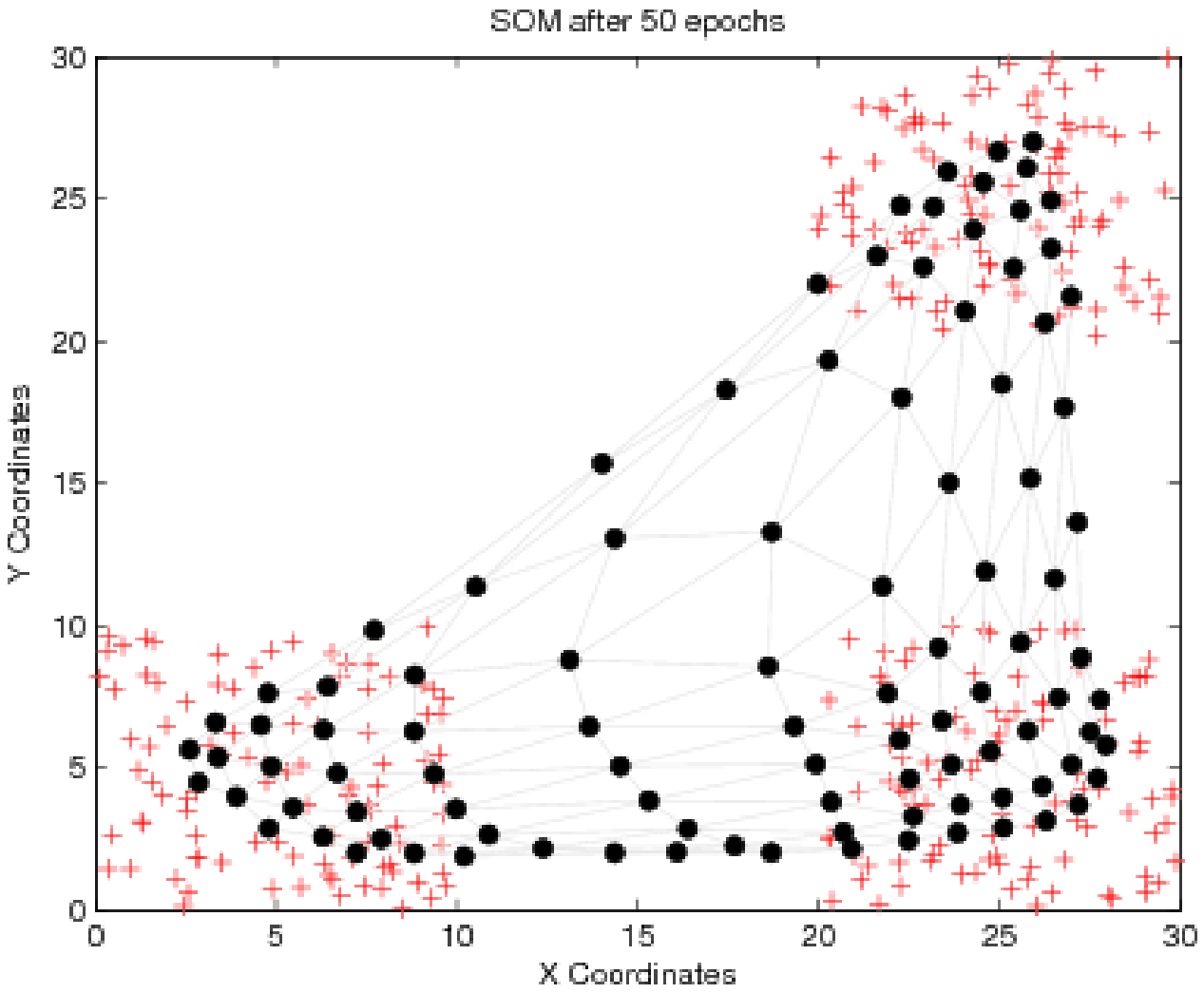
Methodology - Example



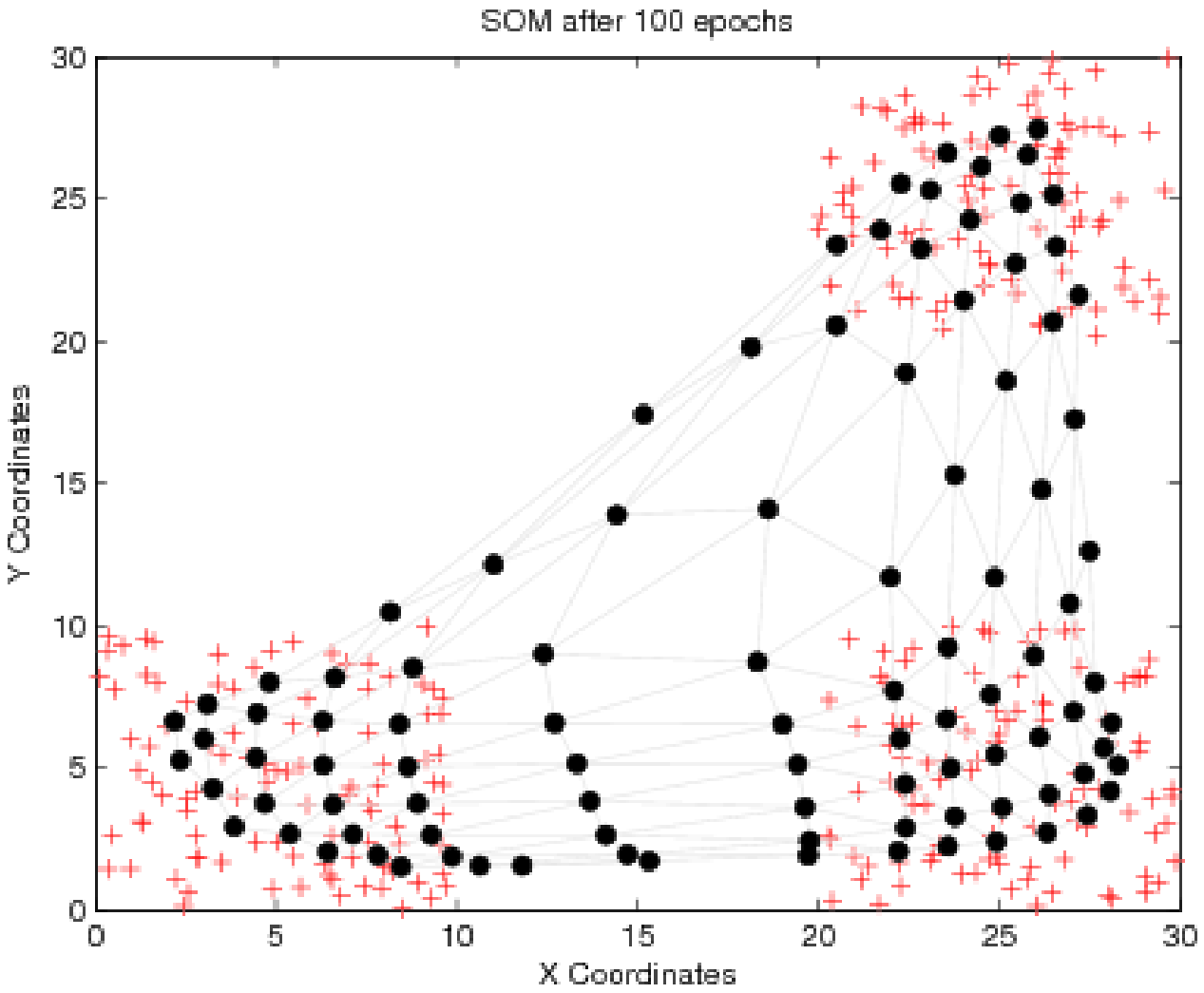
Methodology - Example



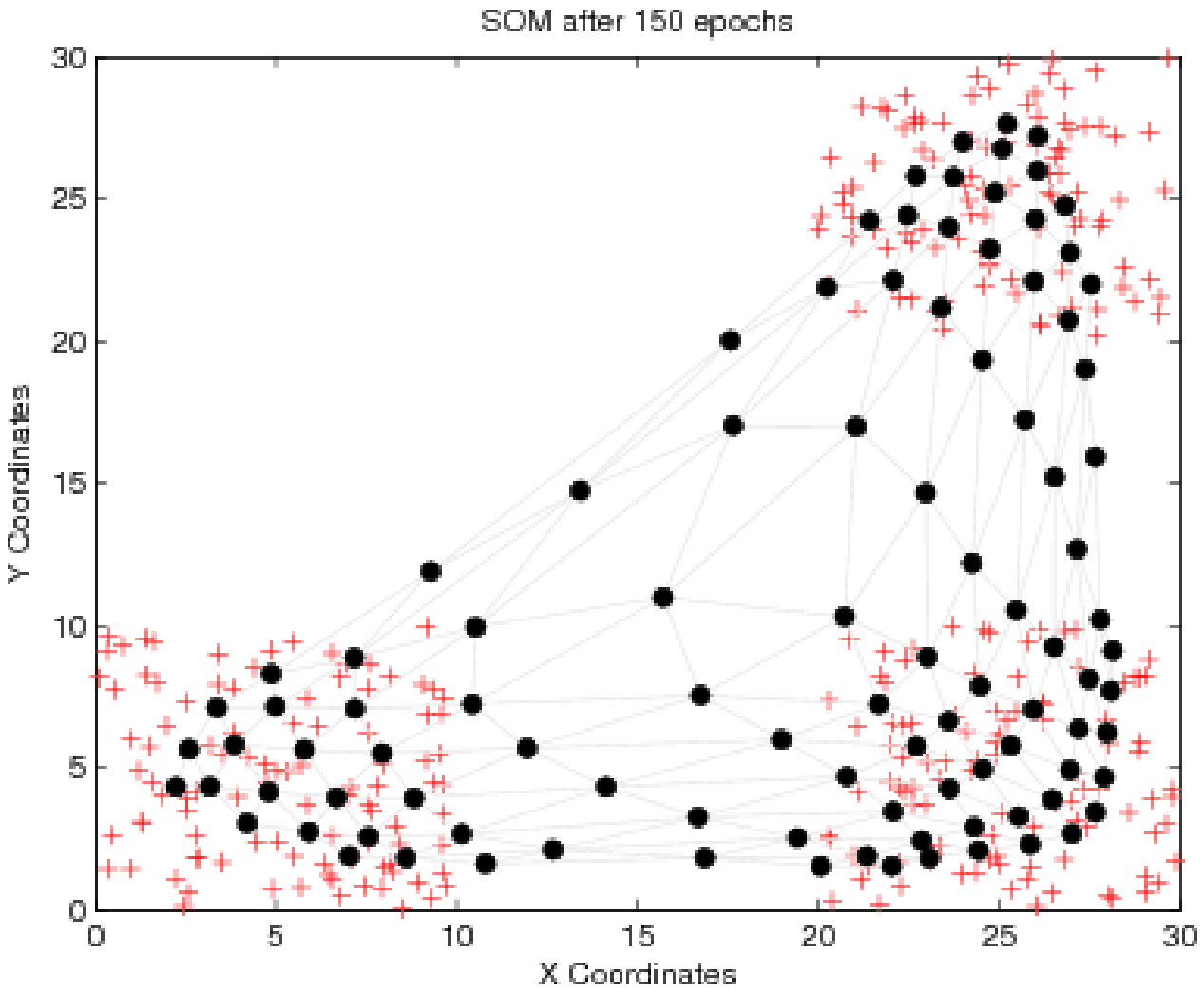
Methodology - Example



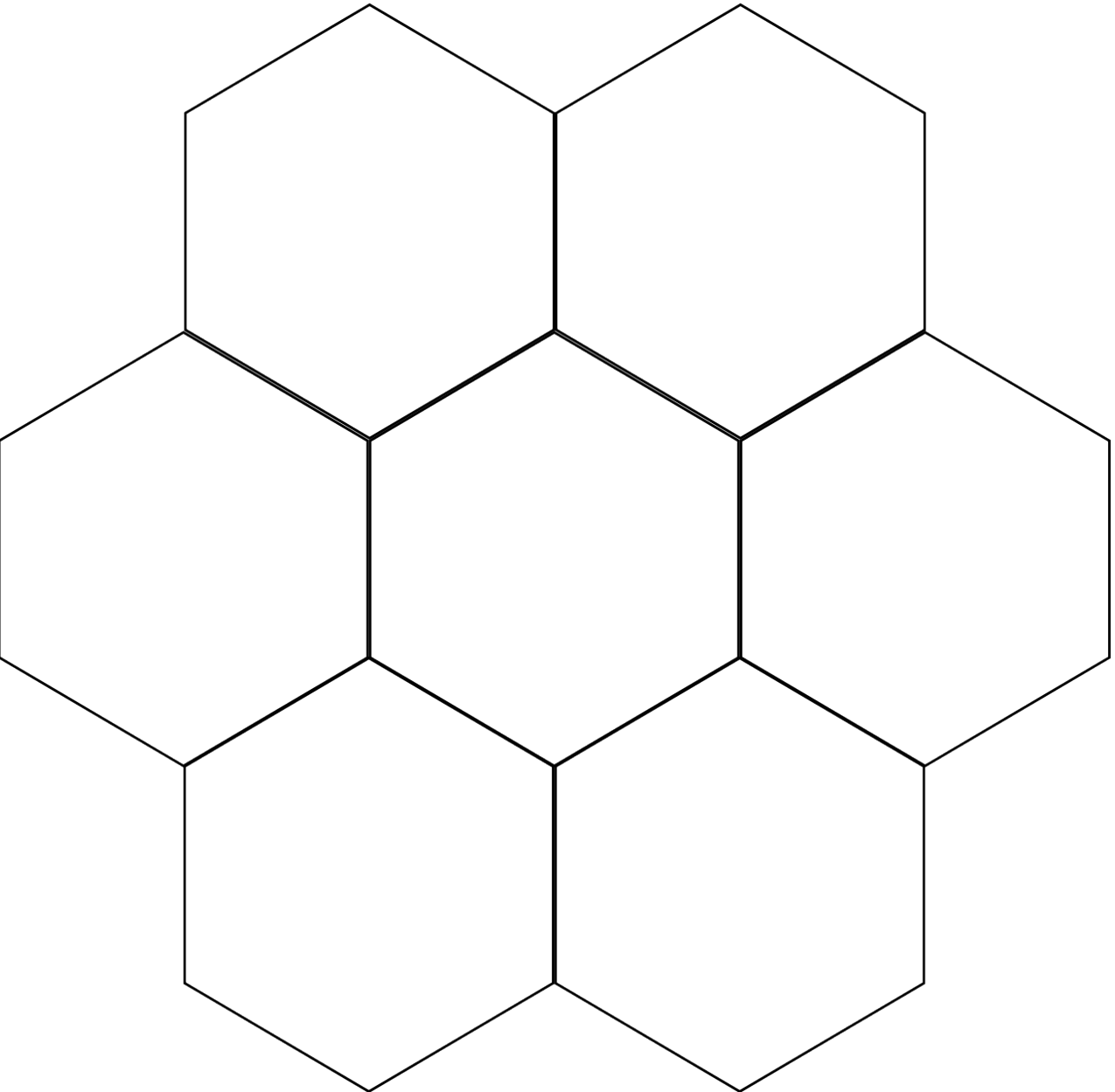
Methodology - Example



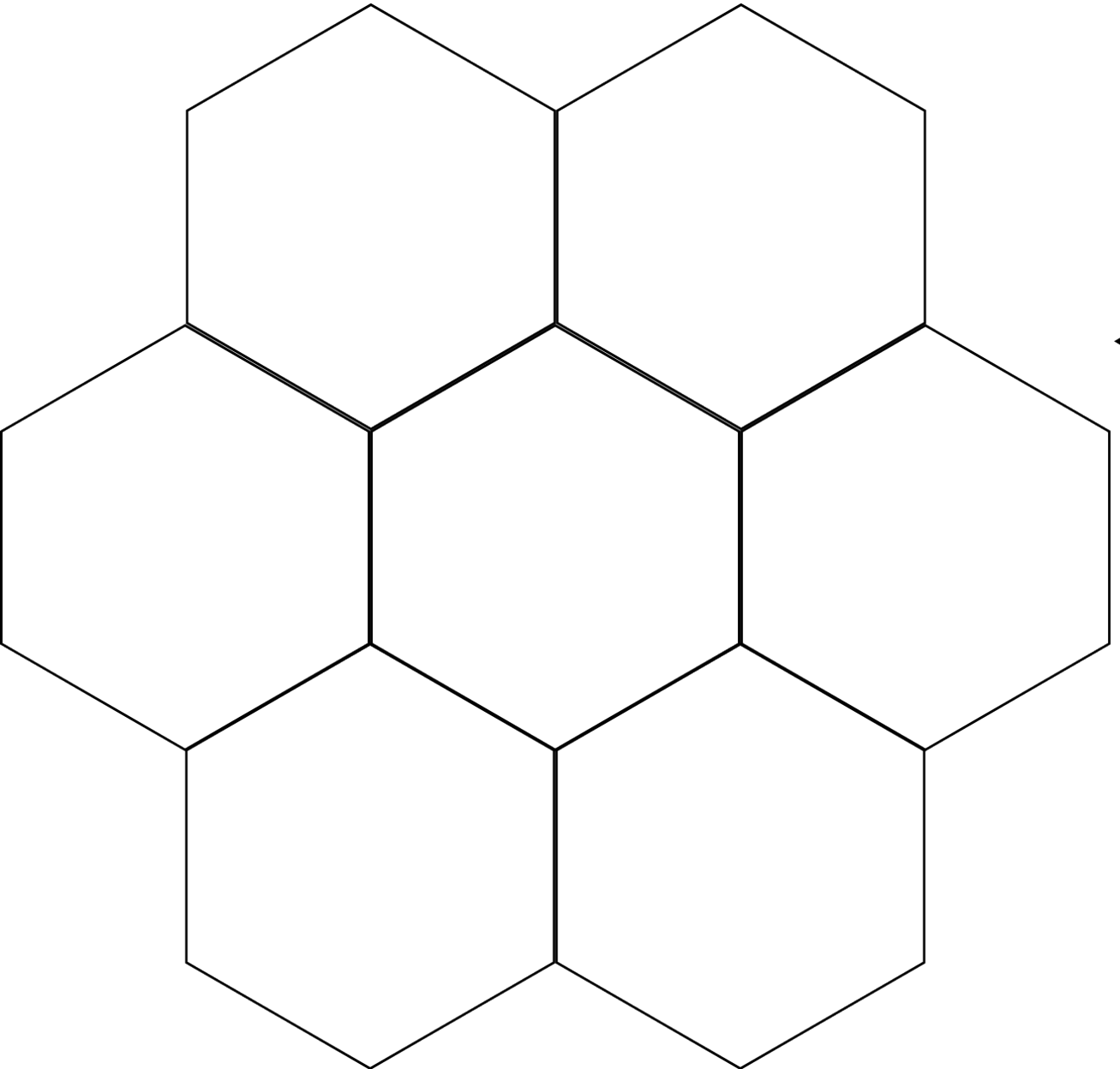
Methodology - Example



Methodology - Labeling

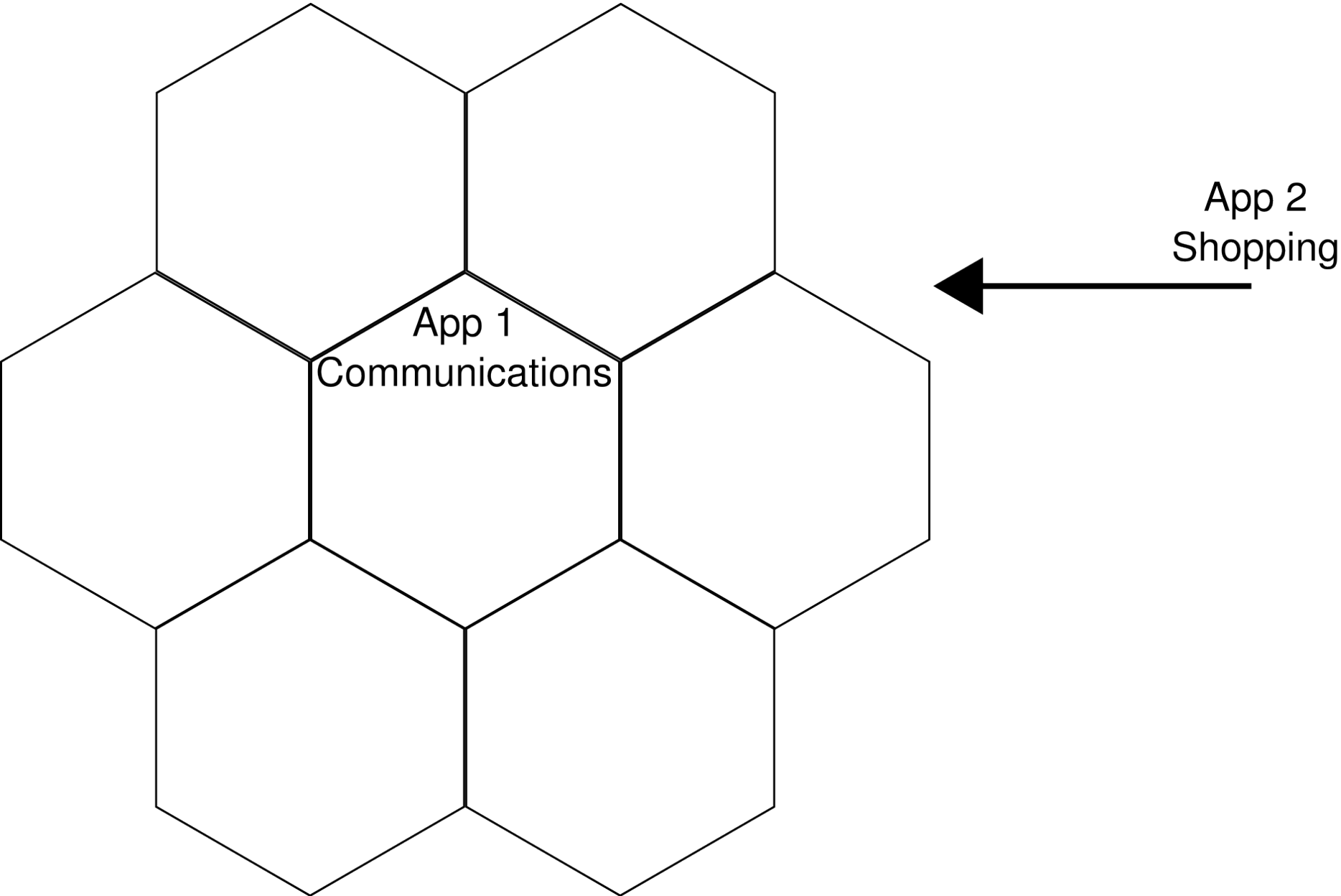


Methodology - Labeling

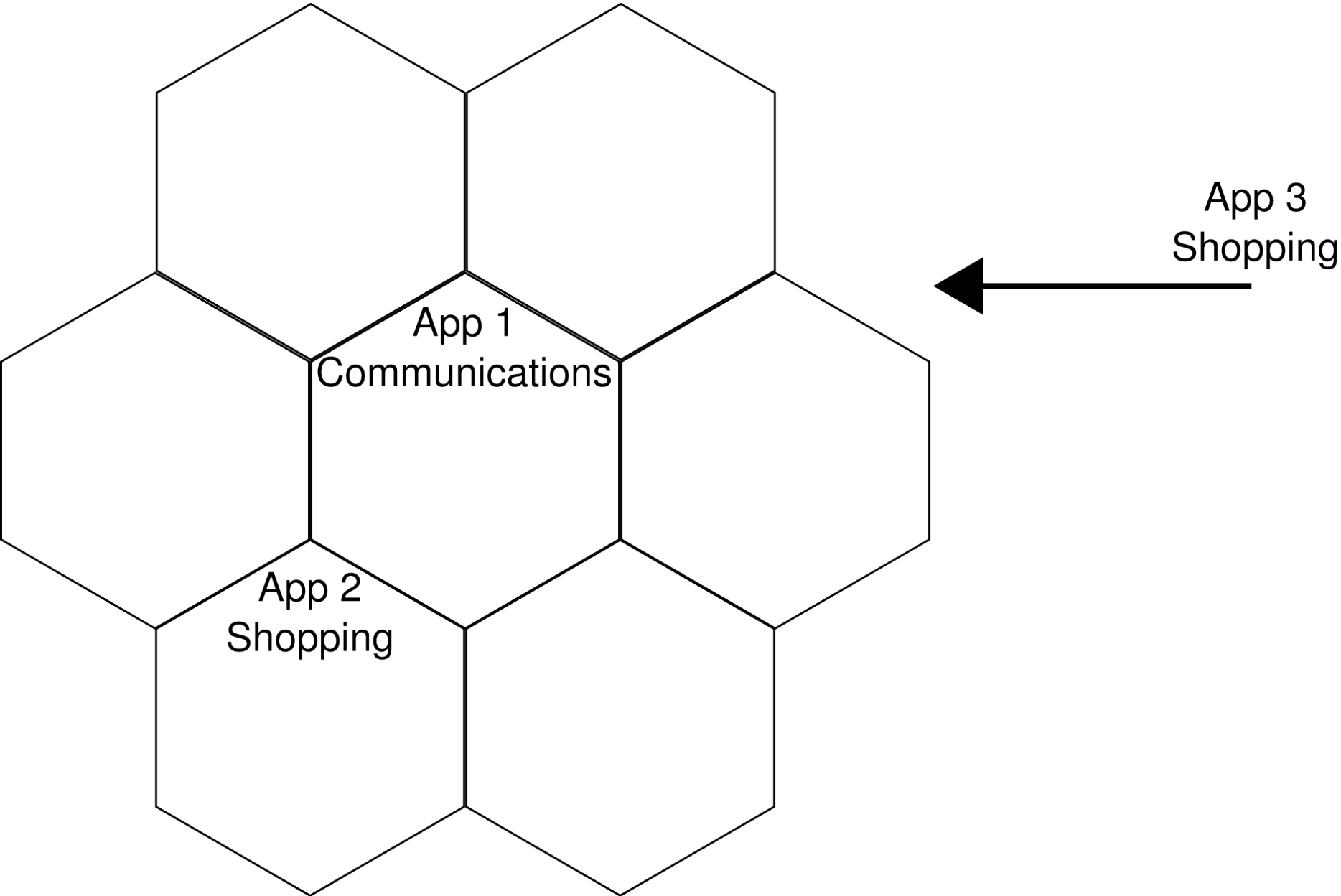


App 1
Communications

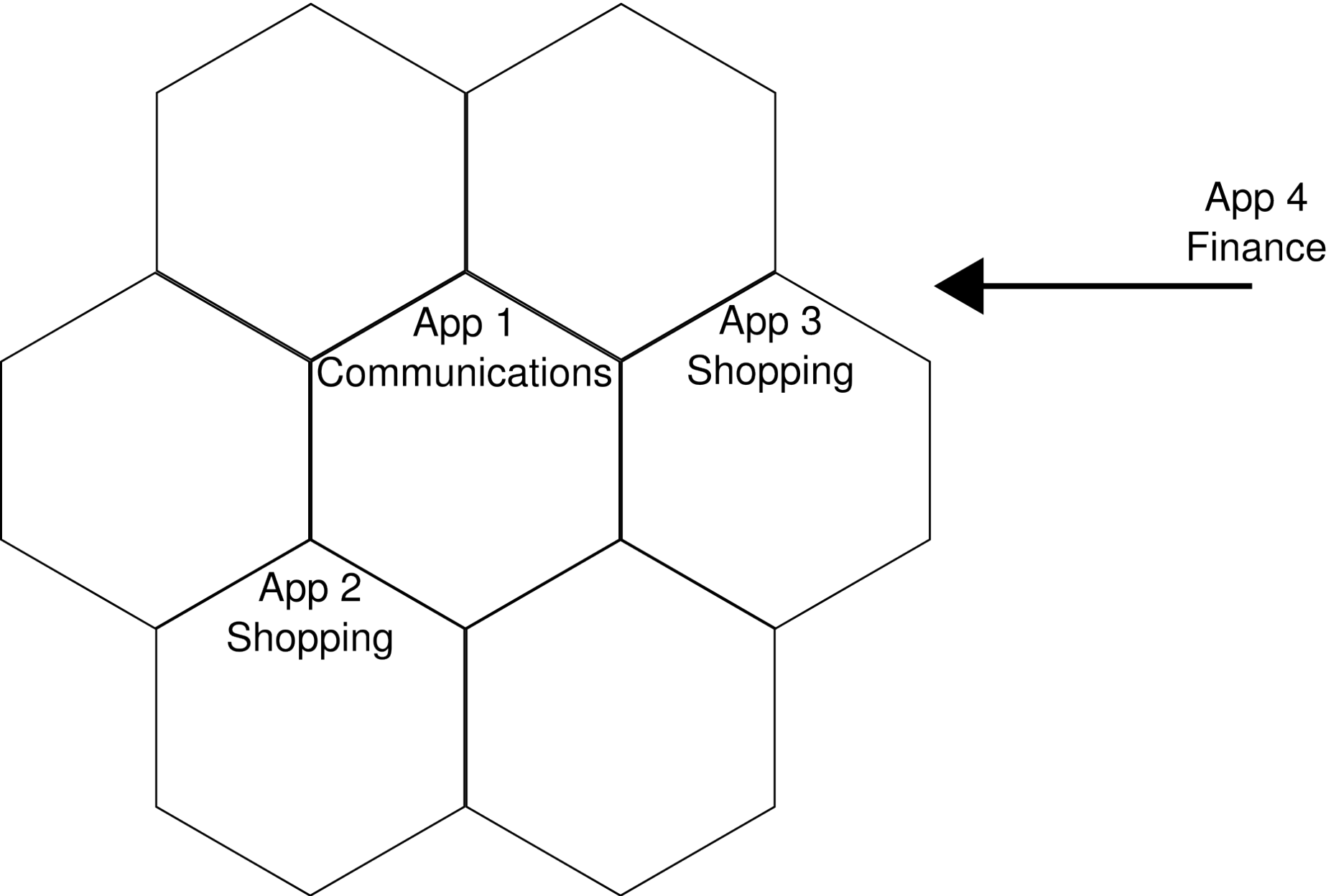
Methodology - Labeling



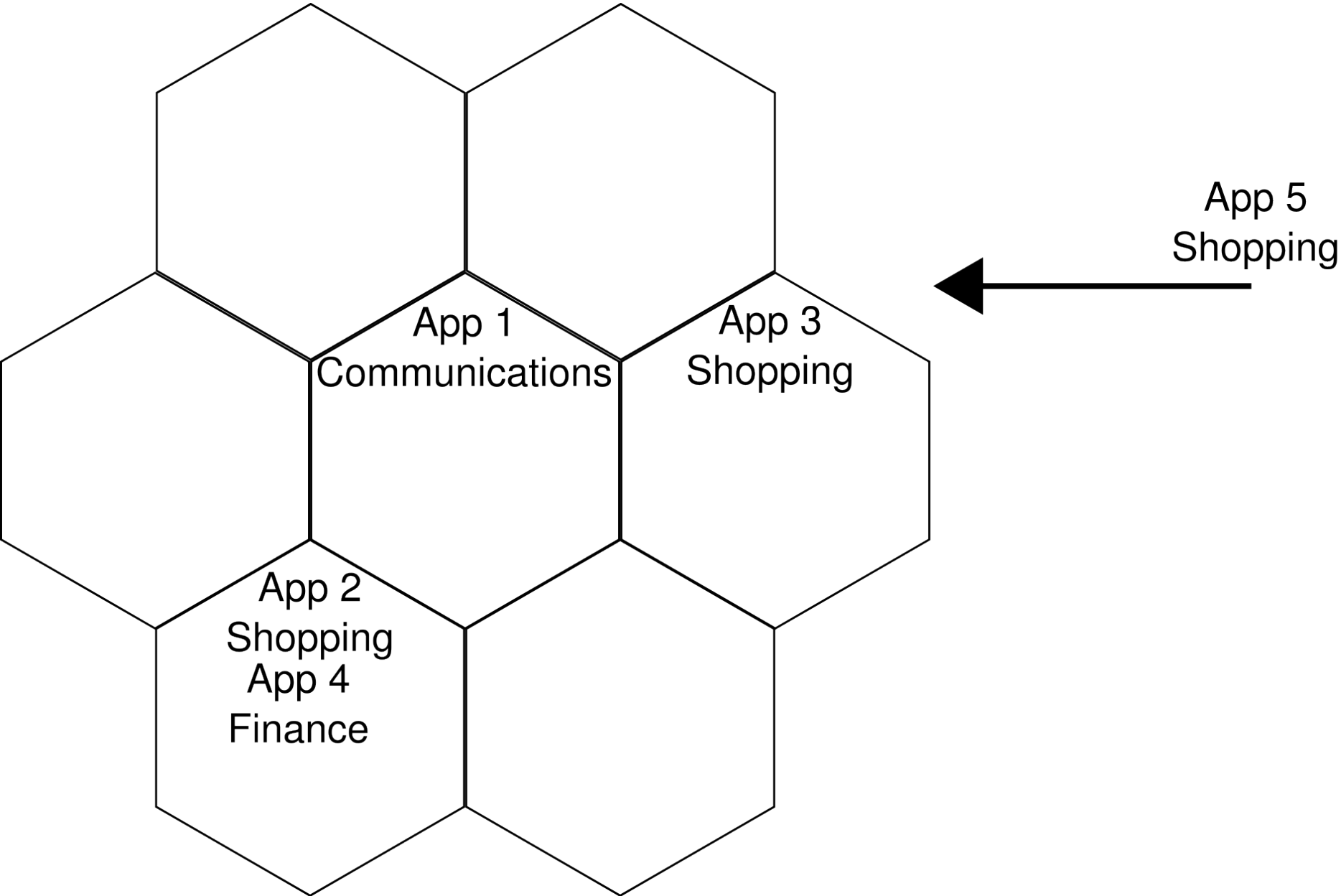
Methodology - Labeling



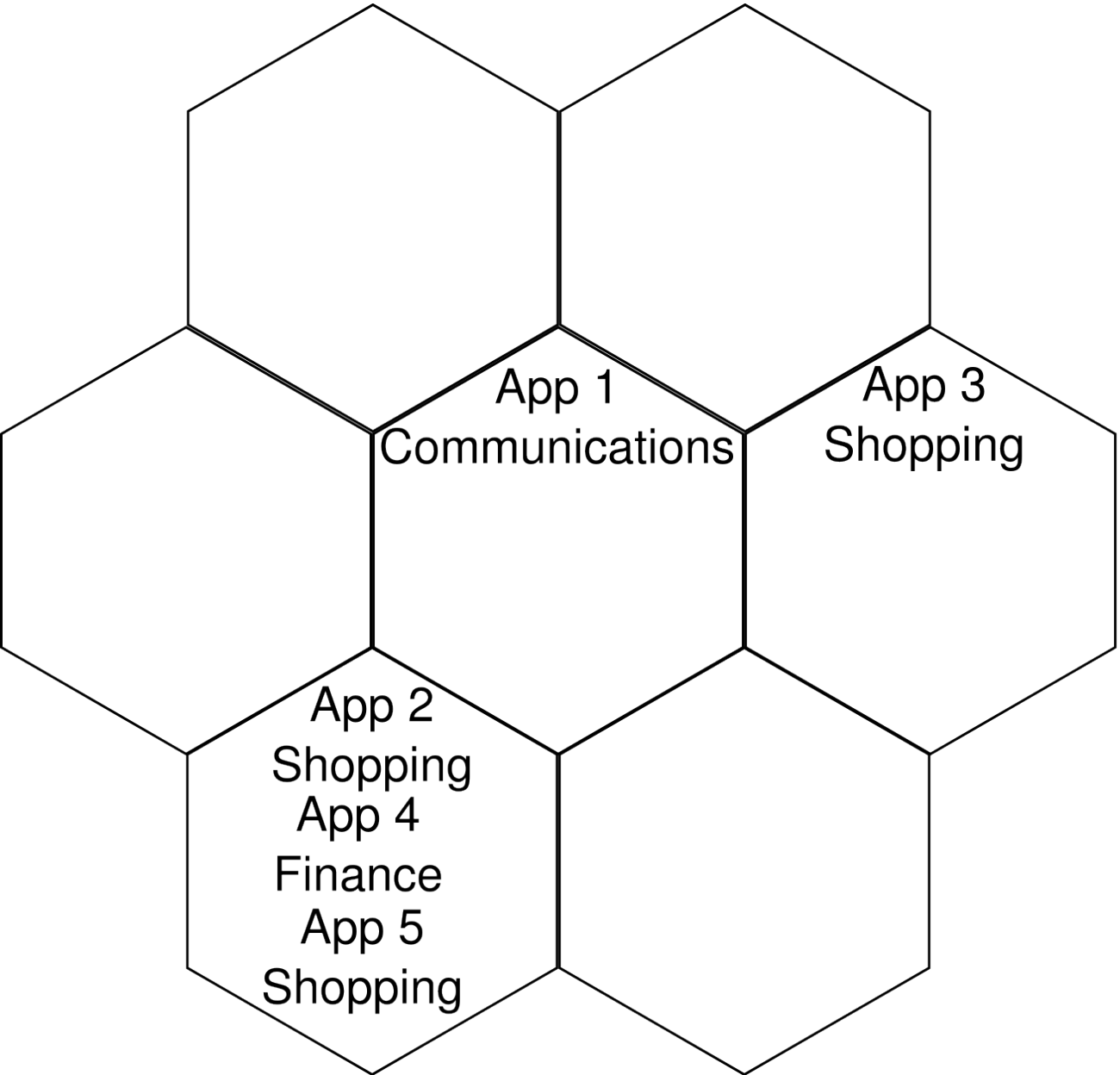
Methodology - Labeling



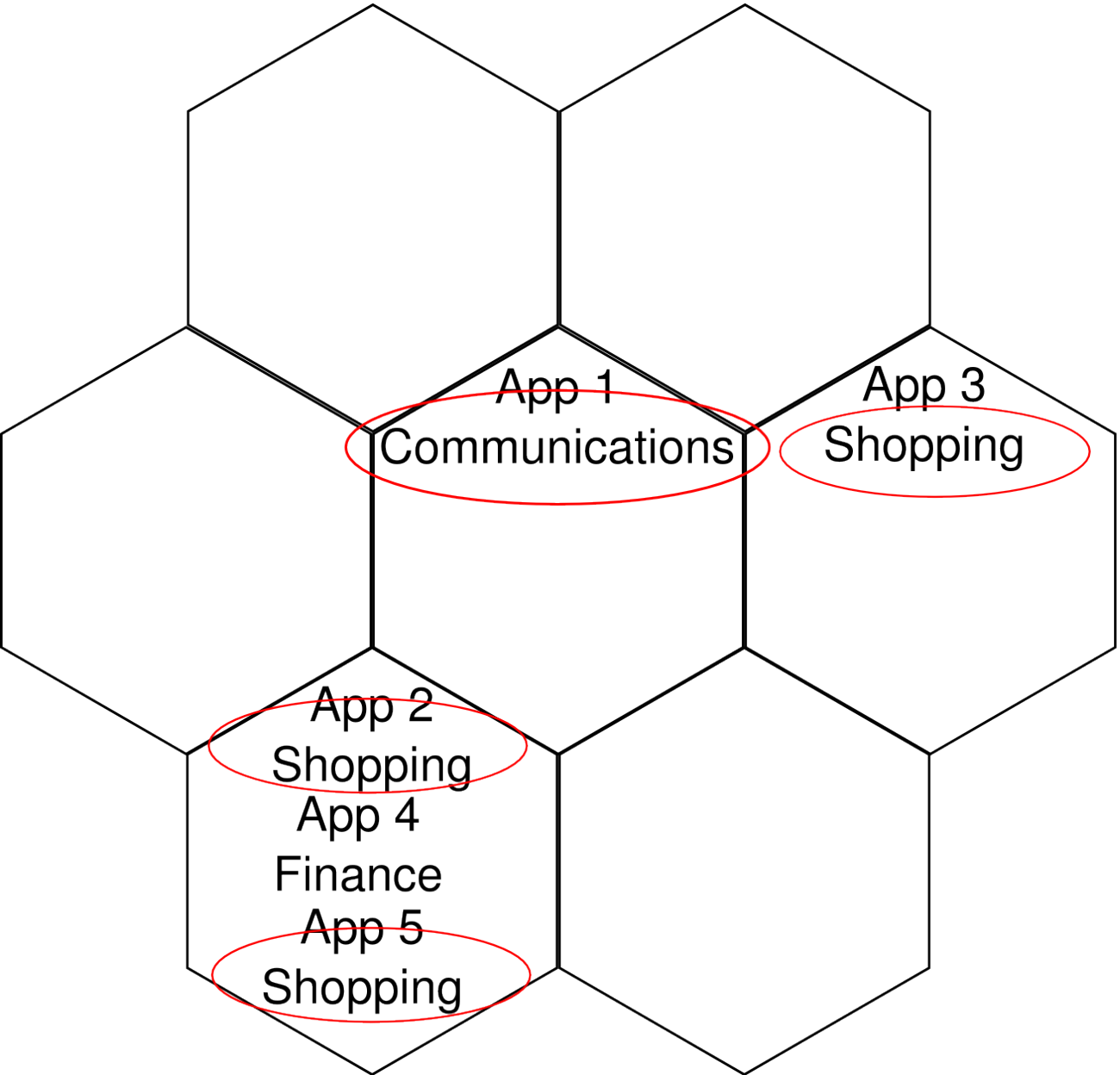
Methodology - Labeling



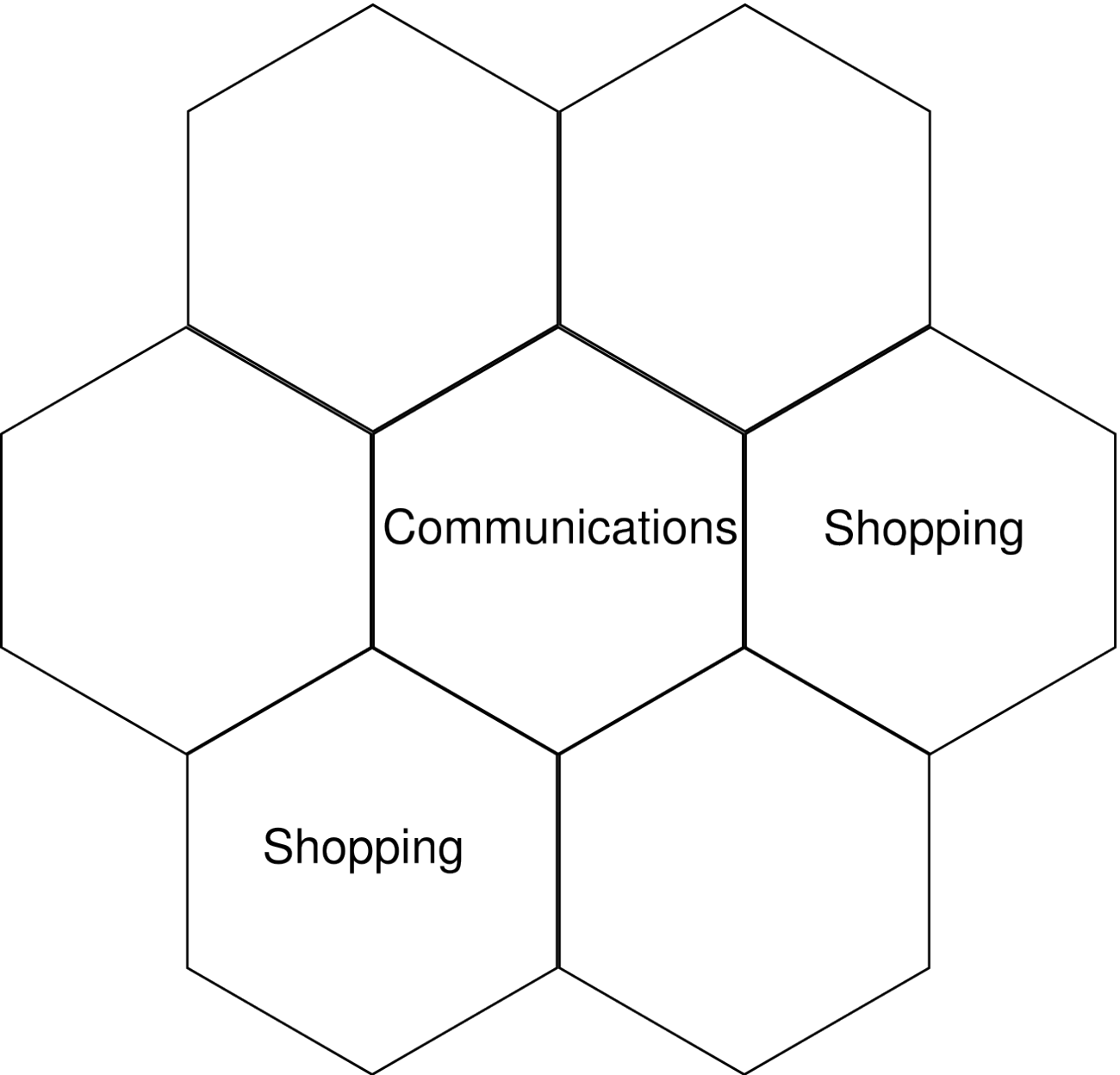
Methodology - Labeling

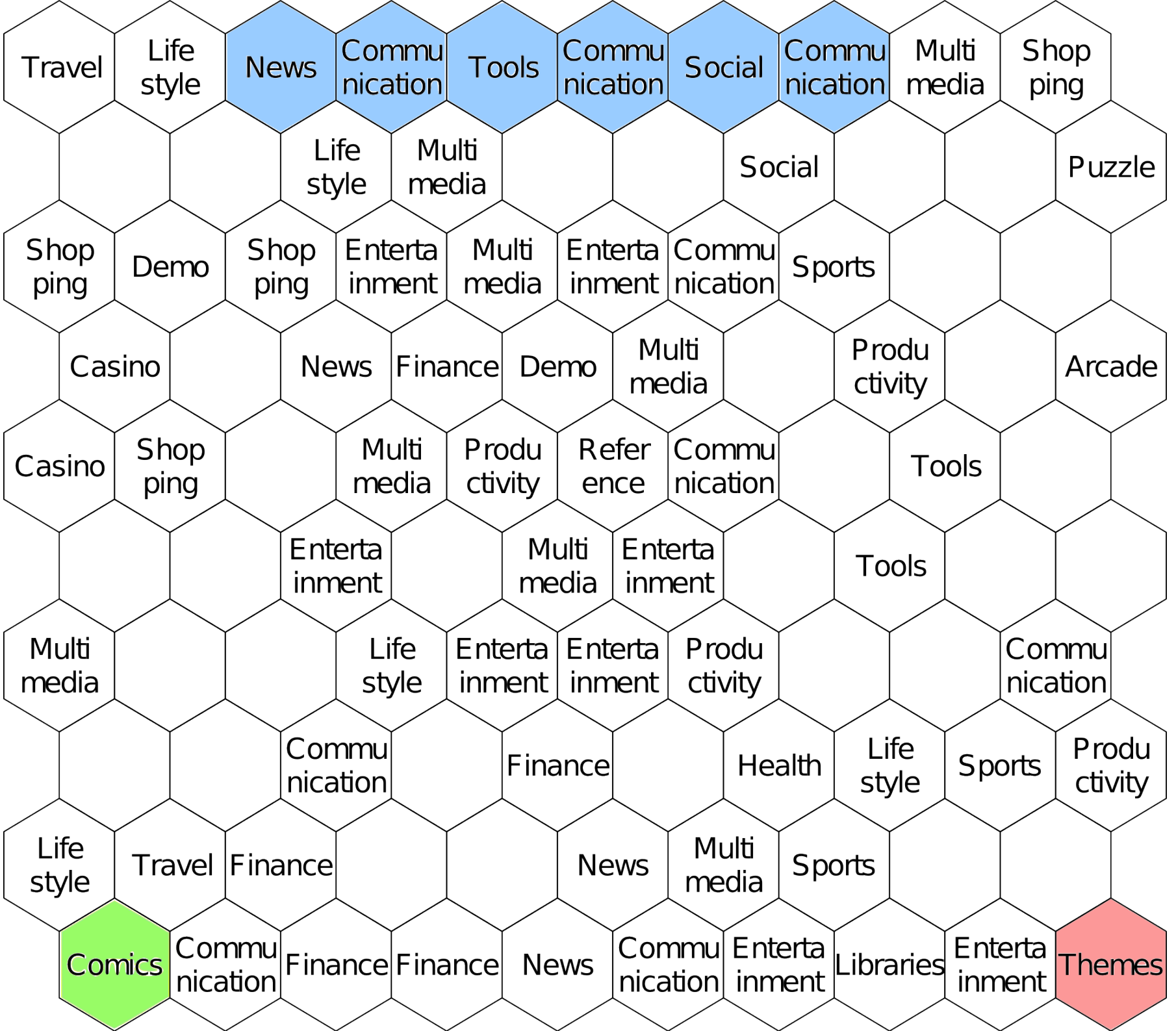


Methodology - Labeling



Methodology - Labeling



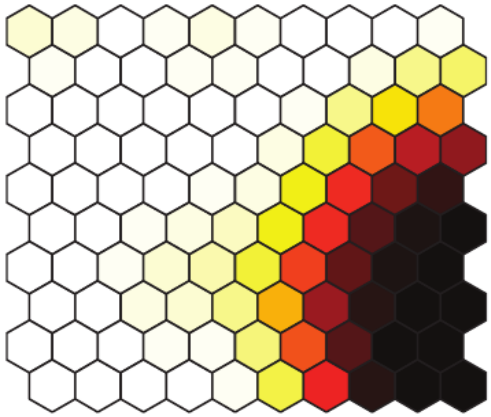

Travel
Life style
News
Communication
Tools
Communication
Social
Communication
Multi media
Shopping
Life style
Multi media
Social
Puzzle
Shopping
Demo
Shopping
Entertainment
Multi media
Entertainment
Communication
Sports
Casino
News
Finance
Demo
Multi media
Productivity
Arcade
Casino
Shopping
Multi media
Productivity
Reference
Communication
Tools
Entertainment
Multi media
Entertainment
Tools
Multi media
Life style
Entertainment
Entertainment
Productivity
Communication
Communication
Finance
Health
Life style
Sports
Productivity
Life style
Travel
Finance
News
Multi media
Sports
Comics
Communication
Finance
Finance
News
Communication
Entertainment
Libraries
Entertainment
Themes

Results

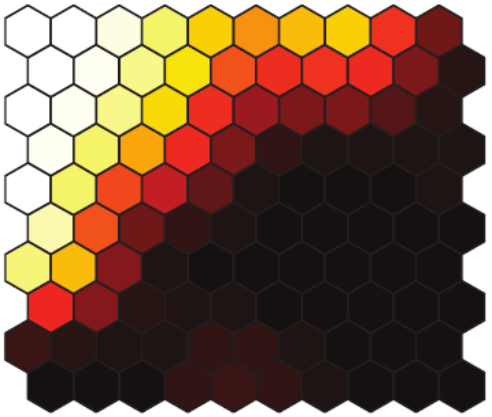
- Principal component analysis
  - One graph per permission
  - How each permission is used

Results – Popular Perms.

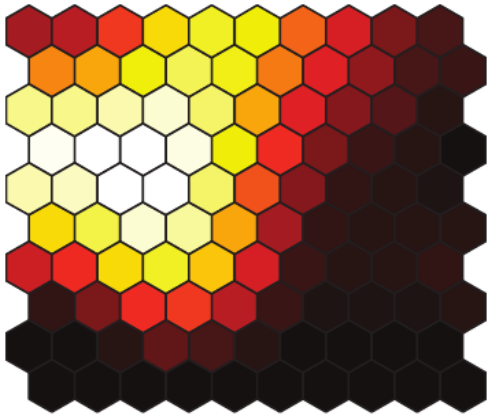
internet

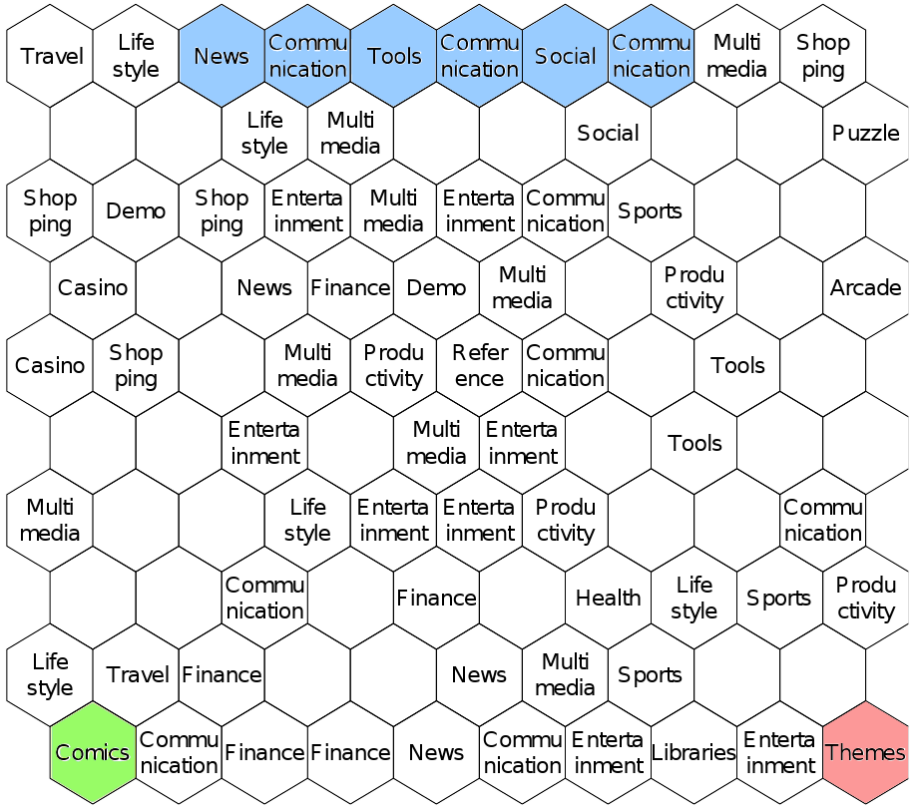


access_coarse_location



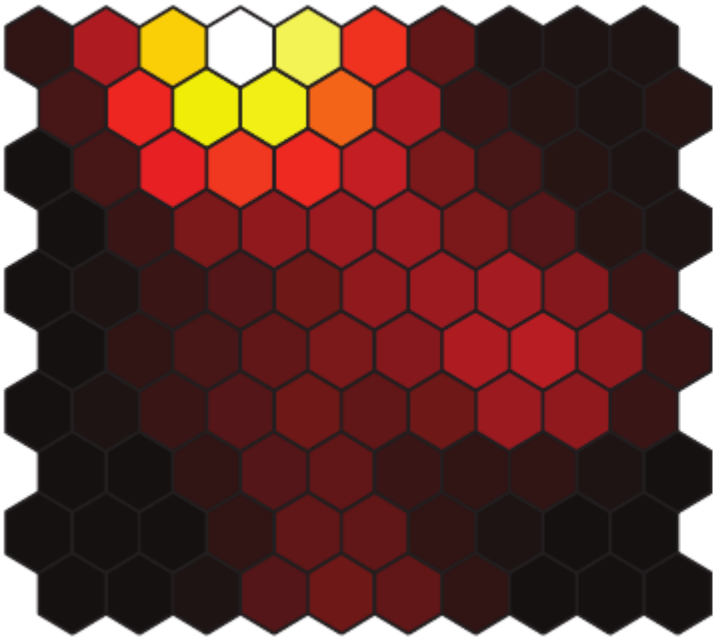
read_phone_state



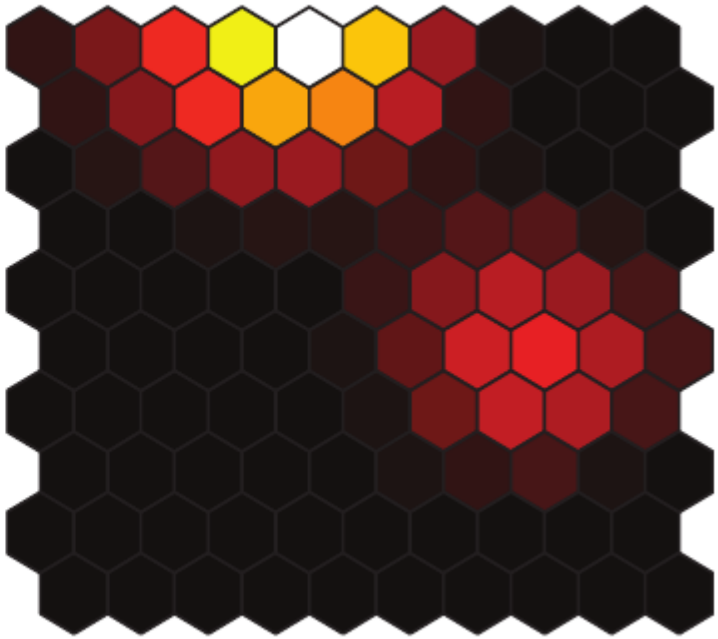


Results - Supersets

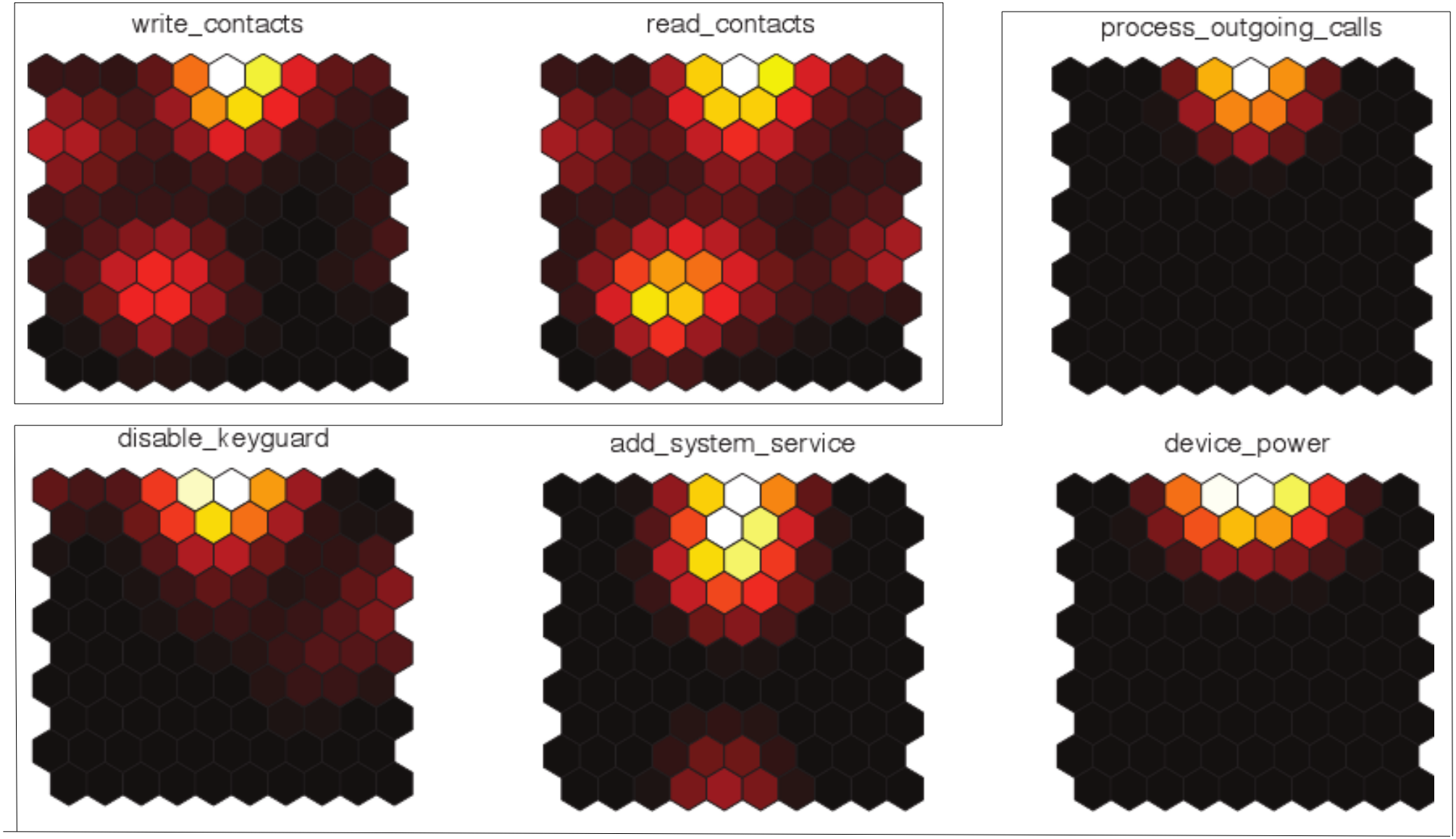
access_wifi_state



change_wifi_state



Results – Commonly Grouped



Other Applications

- Apply methodology to other permission-based systems
  - E.g., Google Chrome

Conclusions

- To improve a system, we need to analyze and understand it.
- To analyze you need techniques
- This technique allows us to gain insight and find areas for improvement
- Can be generalized for different systems

Questions?

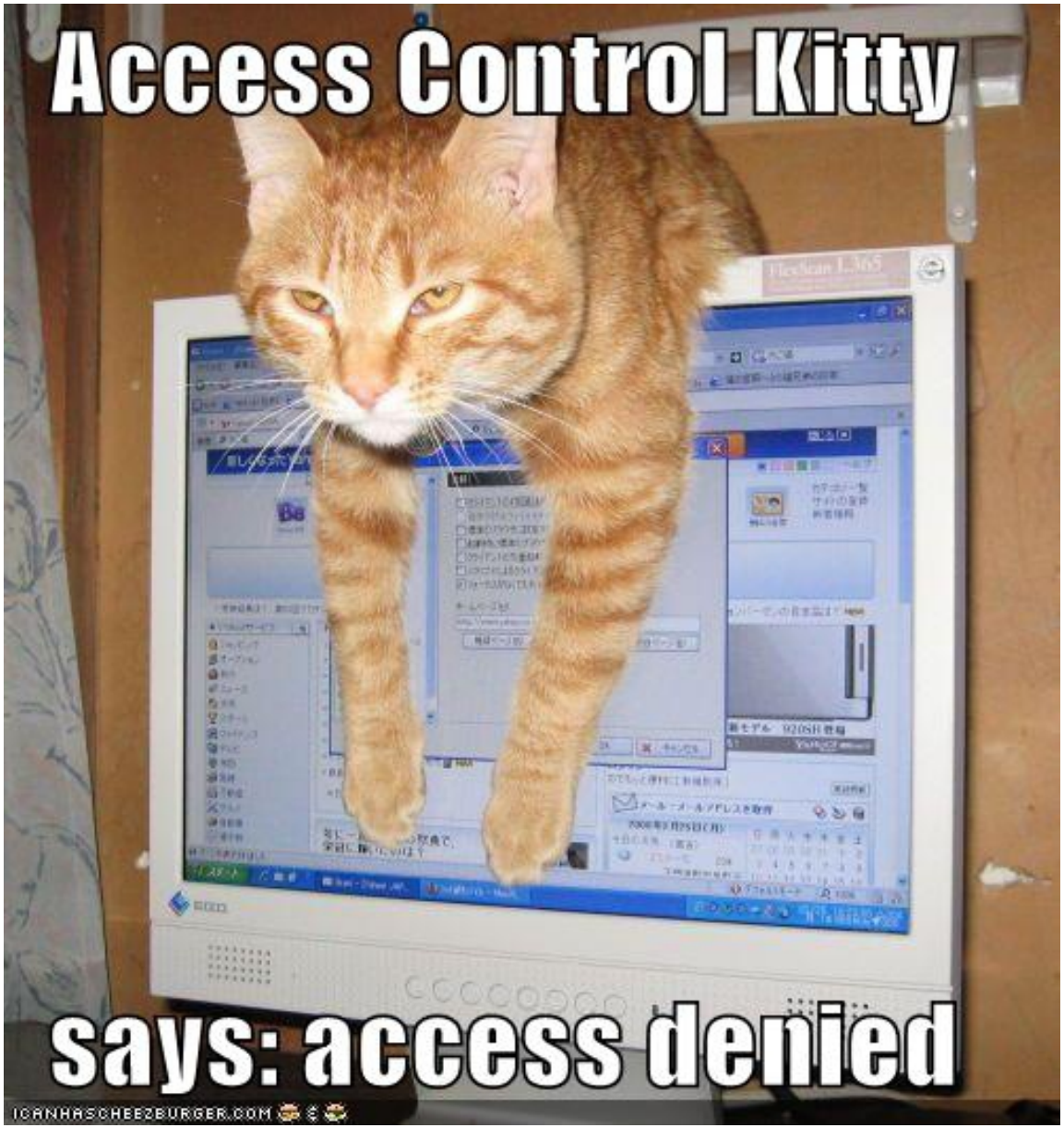

access
use
applications
users
without
permission-based
shows
application
example
category
market
function
categories
set
dataset
control
figure
permissions
os
many
extension
make
different
similar
best
defined
methodology
input
request
systems
neurons
work
developer
data
requested
component
also
user
section
paper
training
requesting
map
identify
known
manifest
allows
written
functionality
developers
neuron
permission
analysis
operating
number
one
system
plane
features
matching
android
communication
visualization
device
empirical
model
used
location
large
region
distance
time
labels
security
som

Contact

David Barrera

Carleton University

- email : dbarrera@ccsl.carleton.ca
- twitter: @davidbb


Access Control Kitty
says: access denied
ICANHASCHEEZBURGER.COM