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

HELLO
my name is

Bob
Android App Installation

HELLO
my name is

Bob
Android App Installation

Top paid

Top free

Dictionary.com
Dictionary.com, LLC
FREE

Twitter
Twitter, Inc.
Installed

Backgrounds
Stylem Media
FREE

Talking Tom Cat Free
Outfit7 Ltd.
FREE

ASTRO File Manager
Metago
FREE

Shazam
Shazam Entertainment Limi...
Installed
10,000 awesome unique designs. New Backgrounds added daily.

Categories: Funny, Cute, Quotes, Sunsets, Beaches, Cars, Girly, Guys, Games, Flowers, Models, Love, Christmas, Military, Money, Sports, City, Scary, Money, New Years, Music, Movies, Animals, Space, ...

Set Contact Icons. #1 iPhone Wallpaper app. Uses (but not endorsed by) Flickr API.

Version 2.0.0 120KB
Android App Installation

10,000 awesome unique designs. New Backgrounds added daily.

Categories: Funny, Cute, Quotes, Sunsets, Beaches, Cars, Girly, Guys, Games, Flowers, Models, Love, Christmas, Military, Money, Sports, City, Scary, Money, New Years, Music, Movies, Animals, Space, ...

Set Contact Icons. #1 iPhone Wallpaper app. Uses (but not endorsed by) Flickr API.

Version 2.0.0 120KB

Install
This application has access to the following:

⚠️ **Network communication**
full Internet access

⚠️ **Your personal information**
read contact data, write contact data

⚠️ **Storage**
modify/delete SD card contents

⚠️ **Phone calls**
read phone state and identity

⚠️ **System tools**
prevent phone from sleeping

[Show all]
This application has access to the following:

⚠️ **Network communication**
full Internet access

⚠️ **Your personal information**
read contact data, write contact data

⚠️ **Storage**
modify/delete SD card contents

⚠️ **Phone calls**
read phone state and identity

⚠️ **System tools**
prevent phone from sleeping

Show all
Android App Installation

⚠️ Your personal information
read contact data, write contact data

⚠️ Storage
modify/delete SD card contents

⚠️ Phone calls
read phone state and identity

⚠️ System tools
prevent phone from sleeping

Hide

Network communication
view network state

System tools
set wallpaper

OK  Cancel
Android App Installation

- **Your personal information**
  - read contact data, write contact data

- **Storage**
  - modify/delete SD card contents

- **Phone calls**
  - read phone state and identity

- **System tools**
  - prevent phone from sleeping

- **Network communication**
  - view network state

- **System tools**
  - set wallpaper
Problem

?????
Goal

Why does this wallpaper app need my personal information? I'm not installing it..
OMG WALLPAPERS!!!!!!
INSTALLL!!!11!!!1
MOOOAAR!!!!!
Problem

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

Usability

Expressiveness

18
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
Methodology

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

```xml
<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-permission android:name="android.permission.READ_CONTACTS" />

...</manifest>
Methodology

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

```xml
<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

• 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

App 1 Communications

App 2
Shopping
Methodology - Labeling

- App 1: Communications
- App 2: Shopping
- App 3: Shopping
Methodology - Labeling

- App 1: Communications
- App 2: Shopping
- App 3: Shopping
- App 4: Finance
Methodology - Labeling

App 1: Communications
App 3: Shopping
App 5: Shopping
App 2: Shopping
App 4: Finance
Methodology - Labeling

App 1
Communications

App 2
Shopping

App 3
Shopping

App 4
Finance

App 5
Shopping
Methodology - Labeling

- App 1: Communications
- App 2: Shopping
- App 4: Finance
- App 5: Shopping
- App 3: Shopping
Methodology - Labeling

Communications

Shopping

Shopping

Shopping
Results

- Principal component analysis
  - One graph per permission
  - How each permission is used
Results – Popular Perms.
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?
Contact

David Barrera
Carleton University

- email: dbarrera@ccsl.carleton.ca
- twitter: @davidbb
Access Control Kitty says: access denied