

Is this App Safe?

A large scale study on app permissions & risk signals

Pern Hui Chia

Norwegian University of Science and Technology

Yusuke Yamamoto

Kyoto University

N. Asokan

Nokia Research Center

WWW2012, Lyon France

Outline

- Background
 - User Consent Permission System
- Research Questions
- Data Collection
- Analysis
 - Popularity, rating and permission
 - Availability of reliable risk signals
 - Detecting potential trends of exploitations
- Summary

Background

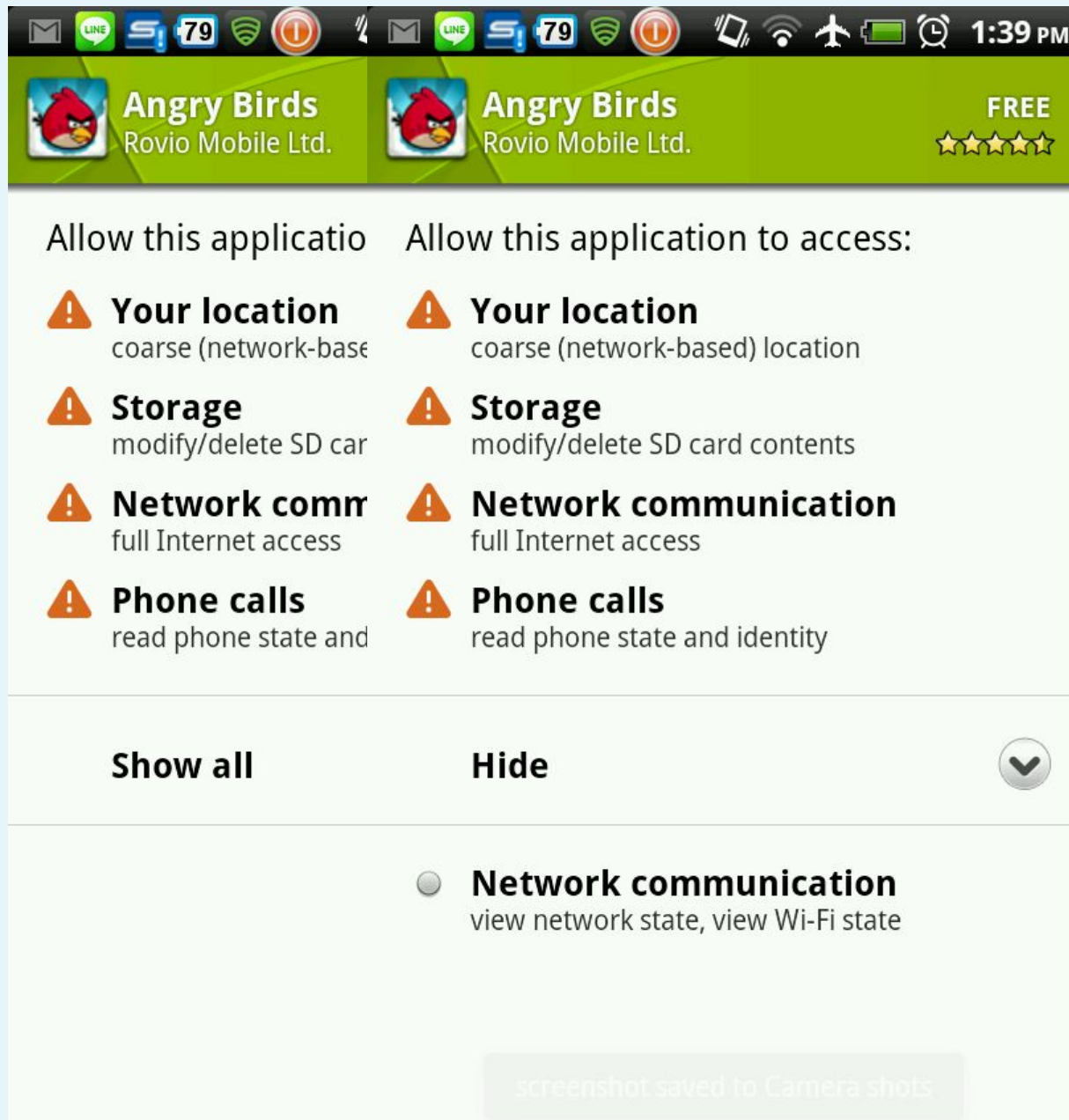
Background

- Apps = platform attractiveness
 - Web: Facebook, Chrome, ..
 - Mobile: iOS, Android, Windows, ..
- Platforms compete for third party developers
 - Increased risks and incentives for questionable activities
- Apps started with full privileges => malicious / inappropriate apps (Cohen 1989)
- OS and runtime platform security => principle of least authority
 - Adoption since Java Security Architecture & mobile platforms (Kostiainen et al. 2011)
 - Today, permission based model widely used on mobile and web platforms

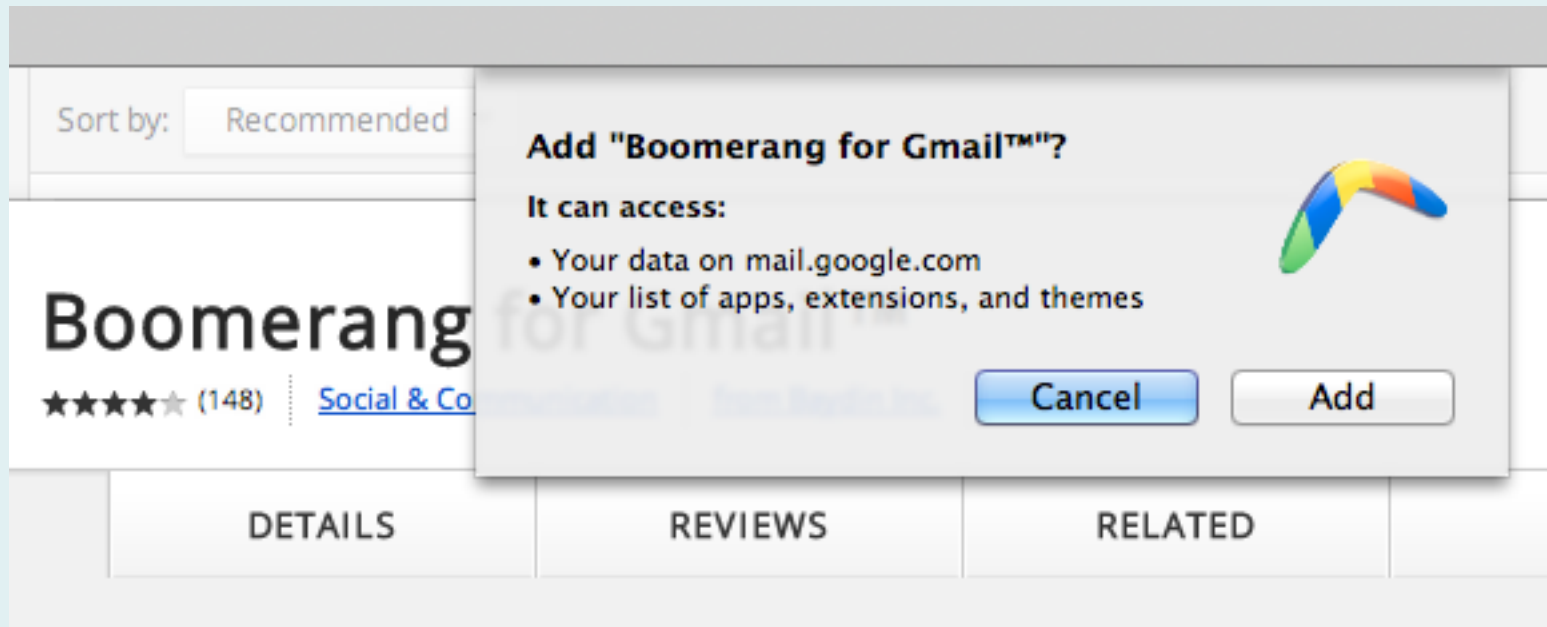
Background:

Centralized vs. User Consent Permission Model

- Centralized model
 - Apple decides which apps can use which permissions
 - But appropriateness is subjective: what is good or bad or gray?
- Laissez-faire: User consent model (e.g., Facebook, Android, Chrome)
 - Anyone can publish
 - User decides if requested permissions are ok
- HTML5 web apps => decentralized nature => user consent model
- But, are users equipped with reliable risk signals?



Chrome



Request for Permission

Daily Horoscope is requesting permission to do the following:



Access my basic information

Includes name, profile picture, gender, networks, user ID, list of friends, and any other information I've made public.



Send me email

Daily Horoscope may email me directly at iceasky@hotmail.com · [Change](#)



Post to Facebook as me

Daily Horoscope may post status messages, notes, photos, and videos on my behalf



Access my data any time

Daily Horoscope may access my data when I'm not using the application



Access my profile information

Birthdays



Access information people share with me

Birthdays



Daily Horoscope




Facebook

By proceeding, you agree to Daily Horoscope's [Terms of Service](#) and [Privacy Policy](#) · [Report App](#)

New permission UI and groupings
(after our data collection process)

Facebook



Daily Horoscope


Daily Horoscope

[Go to App](#) [Cancel](#)

ABOUT THIS APP


You can see your daily horoscope in your profile.

Who can see posts this app makes for you on your Facebook timeline: [?]

 Friends

THIS APP WILL RECEIVE:

- Your basic info [?]
- Your e-mail address (iceasky@hotmail.com)
- Your birthday
- Friends' birthdays

 This app may post on your behalf, including horoscopes you read and more.

By proceeding, you agree to Daily Horoscope's [Terms of Service](#) and [Privacy Policy](#) - [Report App](#)

Research Questions

Research Questions

- How do popularity and permission relate with one another?
- How reliable are the 'risk signals' currently available to users?
- Can we detect any trends of exploitations?
 - Free and mature apps
 - Look-alike app names

Data Collection

Data Collection

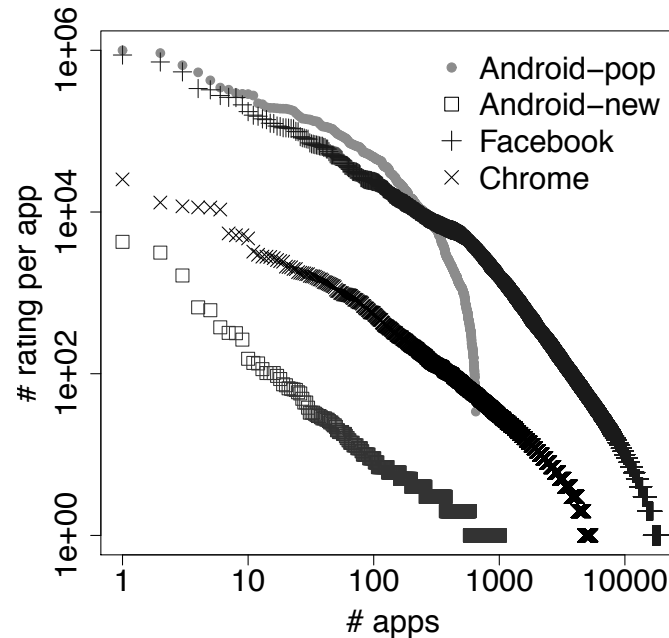
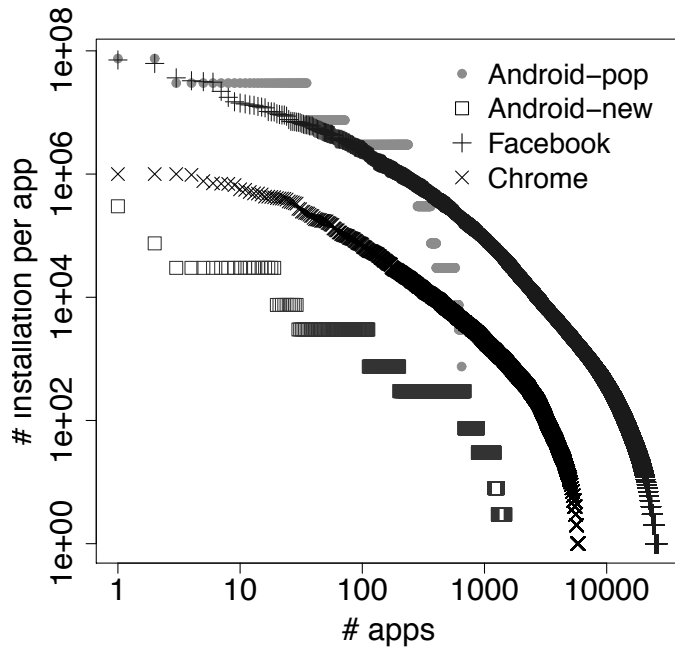
- Goal: to include new apps
 - Referred to lists of new apps from AppBrain.com, SocialBakers.com
 - Mid June to early October 2011
- Android
 - 650 popular apps
 - 1210 new apps (4 month old => to mitigate transient behaviors)
 - 20500 most recent apps (used for look-alike name analysis)
- Chrome
 - 5943 extensions (mixed of popular and new)

- Facebook
 - 27,029 apps (from 34,370 appIDs on SocialBakers.com)
 - 7k unavailable: removed by developers, blocked by FB, and so on
 - List of permissions recorded on first access
 - Possible for app to request for more permissions as user navigates around
- We share our datasets: <http://aurora.q2s.ntnu.no/app>

Analysis:

Popularity, Rating and Permission

Popularity and Rating

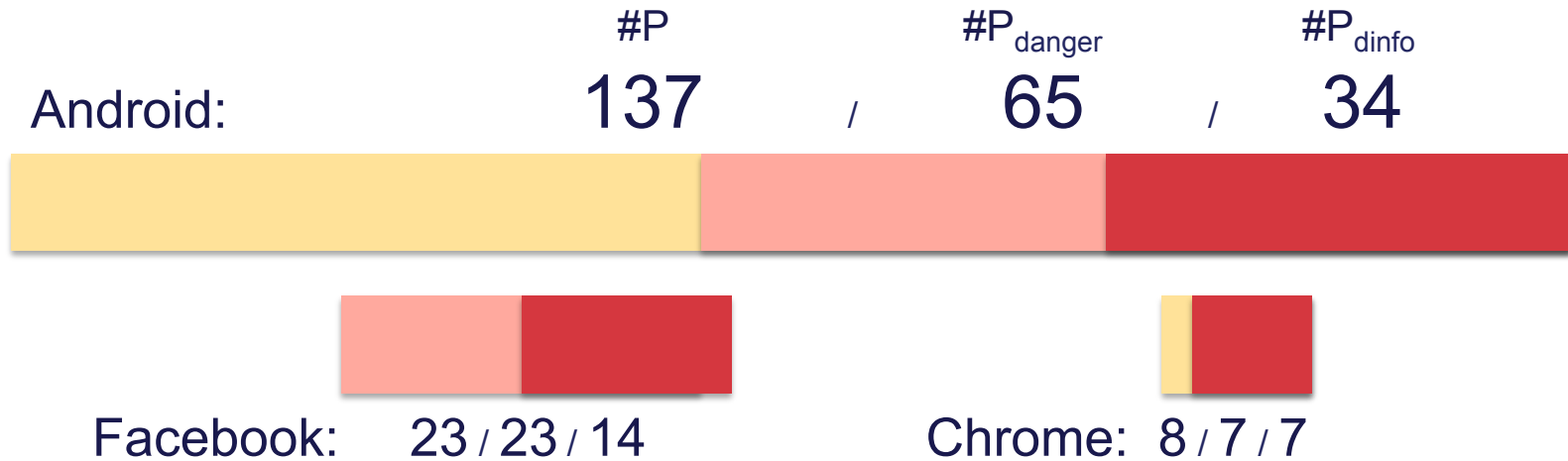


- Skewed distributions, define

$$\text{popularity} = \log(\#\text{installation})$$

$$\text{adjusted rating} = (\text{rating} - 3) * \log(\#\text{rating})$$
- Popularity correlates positively with adjusted rating

Permission



- #permission as intrusiveness measure
 - $P \geq P_{\text{danger}} \geq P_{\text{dinfo}}$ (dangerous and information relevant)
 - Our results are applicable to all 3 subsets
- Across 3 platforms:
 - Low average #P_{danger} : Facebook (1), Android (3, 2), Chrome (1)
 - High maximum #P_{danger}: Facebook (13), Android (10, 11), Chrome (5)
 - Certain permissions are more frequently requested

Analysis:

Availability of Reliable Risk Signals?

Two major signals: Popularity and Rating

- Prior study:
 - Popular Chrome extensions request more permissions (Felt et al. 2011)
 - Hypothesis: popular = more functionalities and thus more permissions needed
- Our results across all 3 platforms:
 - Positive correlation between popularity and #permission
 - No negative correlation between adjusted rating and #permission
 - In fact, there is a weak positive correlation
 - Perhaps not too surprising: current ratings not risk oriented
 - But thus we are ‘training’ the users to be careless!

Other signals

- #app by developer
 - Does not correlate with #permission
- Existence of developer website (Android, Chrome)
 - Correlates positively with #permission
 - Identity comes with more permissions
- Existence of developer privacy policy (Facebook)
 - Correlates (weakly) negatively with #permission
 - But, false assurance possible; we did not analyze the policy content

Analysis: Detecting Potential Trends of Exploitations

Free Apps and Mature Content

'Free' comes with permissions

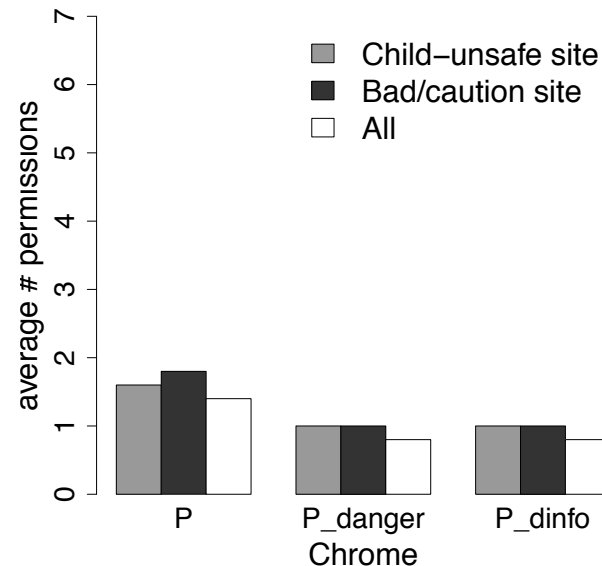
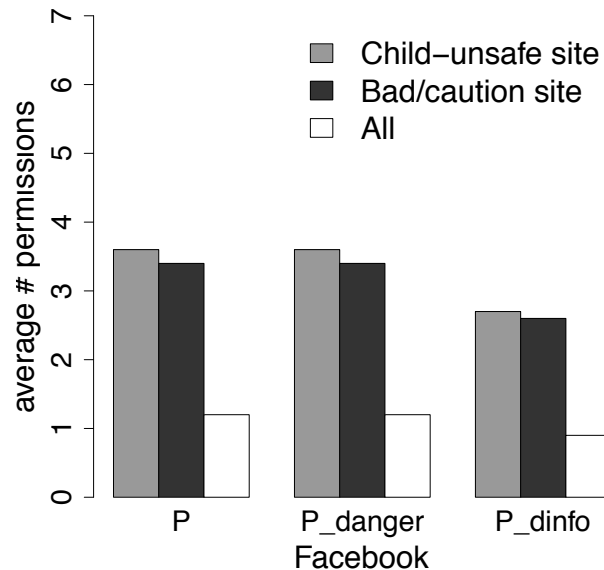
- Free Android apps request higher #permission than paid ones

	#P	#P _{danger}	#P _{dinfo}
Popular:	+1.3	+0.9	+0.5
New:	+2.5	+1.7	+0.7

- Pronounced difference among new apps
- Free apps often supported by ads (Felt et al. 2011, Barrera et al. 2010)
 - Excluding typical permissions of third party ad libraries (INTERNET plus 5 others), free apps still request for more #permission

Mature apps

- Android app maturity level correlates with #permission
 - Note: mature apps = mature content, location publication, user finding each other
- No maturity rating for Chrome and Facebook apps
 - Checked external ratings (from Web of Trust [8])
 - Apps with child-unsafe or bad/cautious developer site request more permissions



Analysis: Detecting Potential Trends of Exploitations

Look-alike app names

Look-alike Names

- Typo-squatting a problem on the Web
 - Supported by pay-per-click ads (Moore & Edelman 2010)
- Apps have unique IDs, but not user friendly
 - Angry Birds = com.rovio.angrybirds
 - FarmVille = 102452128776
 - Last.fm = bbncpldmanoknoahidbgmkgobgmhnafh
- Also, app names not unique
- Analysis
 - Compared apps to the 200 most popular
 - Measured normalized Damerau-Levenshtein edit distance
 - Excluding apps from same developers

- ~1% look-alike names with edit distance threshold=0.3
- Manually break down into 5 classes:
Same, Letter Change, Serialization, Term change, Term addition/deletion
 - First 3 likely to be intentional/suspicious
- Ratio of likely suspect names: Android (0.2%), Facebook (0.6%), Chrome (0.4%)
 - Figures could be higher
 - Excluded non-Latin names
 - No developer name for 40% of Facebook apps



Daily Horoscope

Daily Horoscope

Based on our counting in Oct 2011:

#p = 6
#user = 13,754,471

Go to App

Cancel



Daily Horoscope

Daily Horoscopes

#p = 6
#user = 135,050

Go to App

Cancel



Daily Horoscope

#p = 9
#user = 818,784

Go to App

Cancel

ABOUT THIS APP

Daily Horoscope gives you a detailed look into your future. The best astrology and horoscope application on Facebook.

Who can see posts this app makes for you on your Facebook timeline: [?]

Friends ▾

THIS APP WILL RECEIVE:


- Your basic info [?]
- Your e-mail address (iceasky@hotmail.com)
- Your profile info: activities, birthday, interests, likes, location, relationship status and religious and political views
- Your stories: checkins, events, photos and status updates
- Friends' profile info: birthdays, locations and work histories
- Stories shared with you: checkins, photos and status updates



This app may post on your behalf, including status updates, photos and


- Letter change

Apps




PhotoMania
App
2,400,000 monthly users

Apps




Pho.to Mania
App
70,000 monthly users

- Serialization (e.g., with additional words like “Pro” and “v2”)



Reader Plus
★★★★★ (631) | [Social & Communication](#) | ✓ from www.pitaso.com | 59,042 users



ReaderPlus+
★★★★★ (3) | [Social & Communication](#) | ✓ from www.the-umbrella.eu | 111 users

- Risks with look-alike apps
 - #permission higher than general average
 - Android: +0.9, Facebook: +0.9, Chrome: +0.4
- Reactions
 - Rating not statistically different than popular targets and general average
 - Factoring in #rating, adjusted rating is lower than popular targets
 - But install screen may not display #rating

Summary

Summary

- Popular apps request more permissions
 - Same on 3 platforms despite different UI and permission granularities
 - Intentional or not, developer have ‘no disincentives’ for over-privileging
- No reliable app risk signals currently
 - App ratings do not say about risks
 - Cannot depend on permission lists or popularity
 - Popularity-Permission Effect: If popular apps have high #permission, maybe I should not worry about #permission?

- Free apps & mature apps request higher #permission
 - Excluding typical ad permissions, free apps still request more #permission
 - Facebook apps with child-unsafe developer site request more #permission
- Look-alike name trick
 - App IDs unique, not user friendly
 - App names are cheap identity currently
 - Look-alike apps do not request more #permission than popular targets, but request more than the general average

Limitations & Future Work

- No code analysis
 - Higher #permission does not necessarily imply malicious intent
- Not sure if users willingly accepting higher risks of free/mature apps
 - Study on privacy tradeoff could be interesting
- Next steps:
 - Deeper look into ‘gray apps’
 - New metric for app safety?
 - Suggesting gray apps automatically?

Reference

1. F. Cohen. Computational aspects of computer viruses. *Computers & Security*, 8(4):297–298, 1989.
2. K. Kostianen, E. Reshetova, J.-E. Ekberg, and N. Asokan. Old, new, borrowed, blue –: a perspective on the evolution of mobile platform security architectures. In *Proc. CODASPY 2011*.
3. A. P. Felt, K. Greenwood, and D. Wagner. The effectiveness of application permissions. In *Proc. USENIX WebApps 2011*.
4. D. Barrera, P. C. van Oorschot, and A. Somayaji. A Methodology for Empirical Analysis of Permission-Based Security Models and its Application to Android Categories and Subject Descriptors. In *Proc. CCS 2010*.
5. T. Moore and B. Edelman. Measuring the perpetrators and funders of typosquatting. In *Proc. FC 2010*.
6. AppBrain. <http://www.appbrain.com>
7. Socialbakers – Applications on Facebook. <http://www.socialbakers.com/facebook-applications>
8. Web of Trust. <http://www.mywot.com>

Thank you. Questions?

Pern Hui Chia chia@q2s.ntnu.no

Yusuke Yamamoto yamamoto@dl.kuis.kyoto-u.ac.jp

N. Asokan n.asokan@nokia.com

Data sets shared at: <http://aurora.q2s.ntnu.no/app>