

# Mobile App Markets



**Apple App Store**



**Google Play**



**Microsoft Windows Phone**

# App Store beyond Mobile Apps!



Windows Phone

[Home](#) [The Opportunity](#) [Success Stories](#) [Start Building](#)

Make more money  
on your terms.

[Learn More](#)

Revenue sharing up to:

Windows

80%

Apple

70%

Google

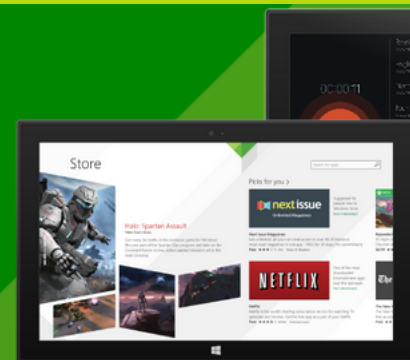
70%

Meet Windows 8.1

[Download](#)



[Learn More](#)

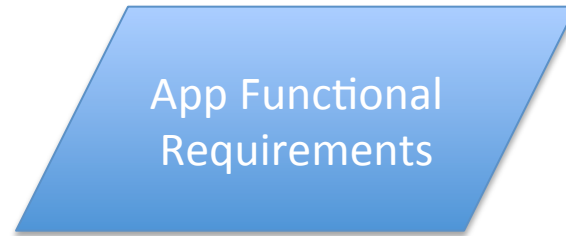


# What If Formal Specs Are Written?!

**APP DEVELOPERS**



informal: **app description**, etc.



**permission list**, etc.



**APP USERS**



# Informal App Functional Requirements: App Description



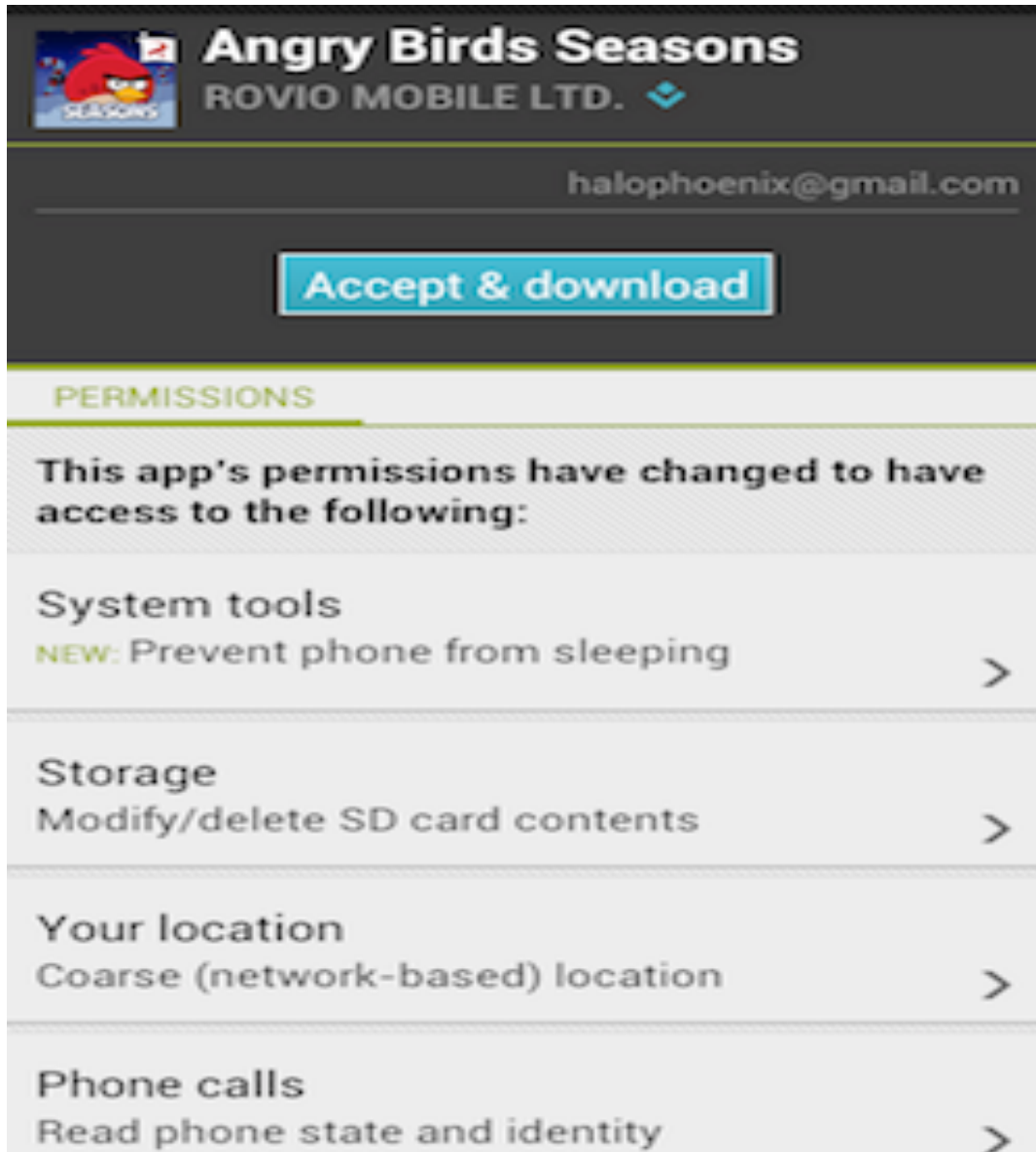
## Description


The survival of the Angry Birds is at stake. Dish out revenge on the greedy pigs who stole their eggs. Use the unique powers of each bird to destroy the pigs' defenses. Angry Birds features challenging physics-based gameplay and hours of replay value. Each level requires logic, skill, and force to solve.

If you get stuck in the game, you can purchase the Mighty Eagle! Mighty Eagle is a one-time in-app purchase for Angry Birds that gives unlimited use. This phenomenal creature will soar from the skies to wreak havoc and smash the pesky pigs into oblivion. There's just one catch: you can only use the aid of Mighty Eagle to pass a level once per hour. Mighty Eagle also includes all new gameplay goals and achievements!

In addition to the Mighty Eagle, Angry Birds now has power-ups! Boost your birds' abilities and three-star level

# App Security Requirements: Permission List



**Angry Birds Seasons**  
ROVIO MOBILE LTD. 

halophoenix@gmail.com

**Accept & download**

**PERMISSIONS**

**This app's permissions have changed to have access to the following:**

- System tools**  
NEW: Prevent phone from sleeping >
- Storage**  
Modify/delete SD card contents >
- Your location**  
Coarse (network-based) location >
- Phone calls**  
Read phone state and identity >



 **Angry Birds**  
Rovio Mobile Ltd. - October 17, 2013  
Arcade & Action

**Install** 

 You don't have any devices

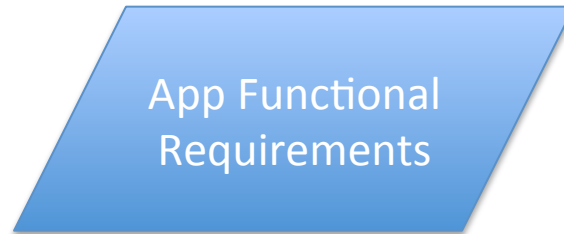
★★★★★ (1,750,676)  
 Top Developer

# What If Formal Specs Are Written?!

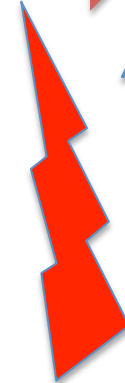
APP DEVELOPERS



informal: **app description**, etc.



**permission list**, etc.



APP USERS



# Example Android App: Angry Birds



[Strassia](#)

Guest

**Why does Angry Birds need to know who I call?**

11-19-2012, 06:15 PM

[DrDeth](#)

Charter Member

Marketing.

Rovio explains the new permission that Angry Birds Seasons requires

[Tweet](#) [ShareThis](#) [StumbleUpon](#) [Pinterest](#) [Reddit](#)

Published on Friday, 02 December 2011 10:42

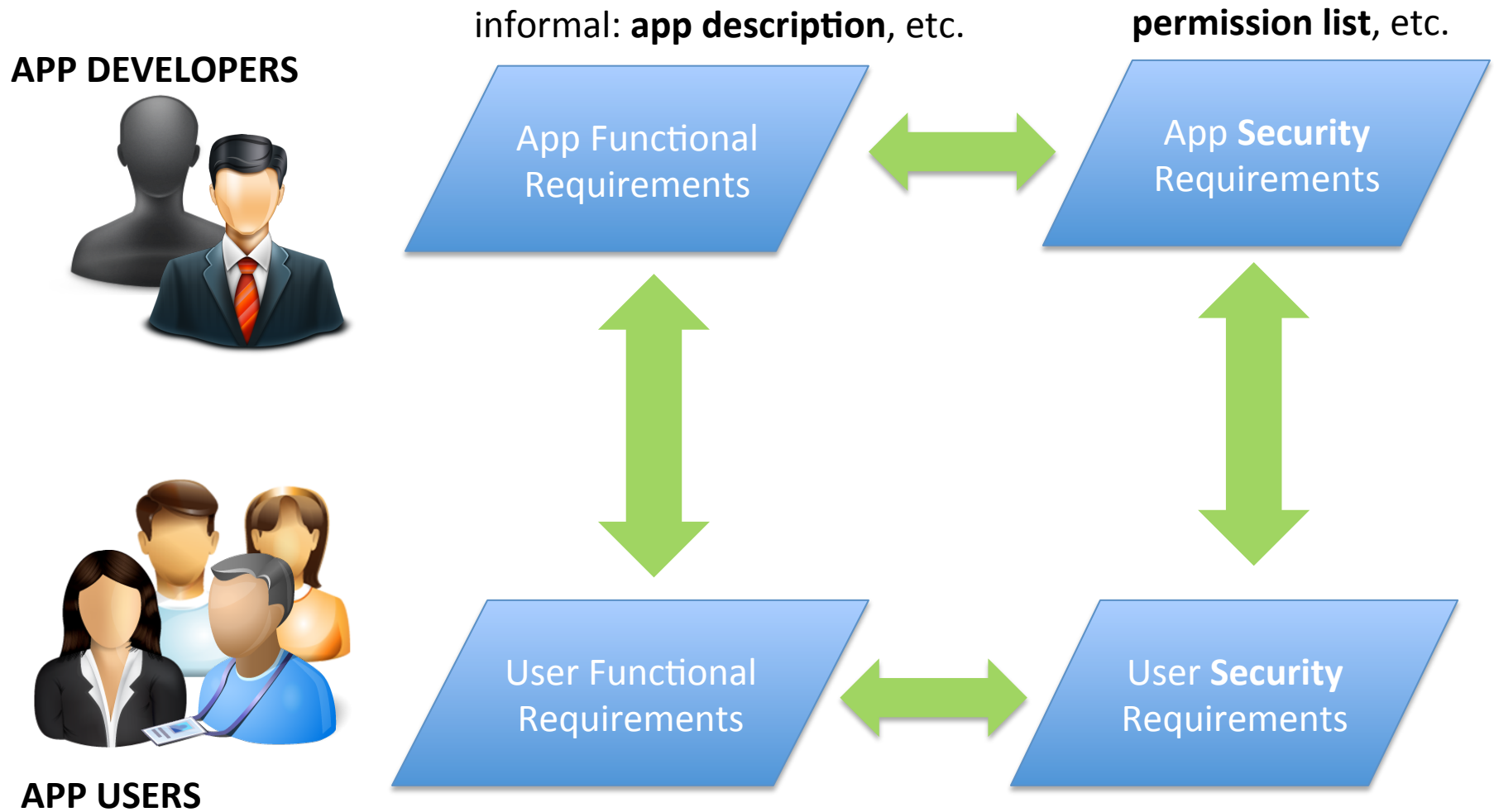
11-19-2012, 05:46 PM

[Baron Greenback](#)

Guest

Angry Birds just needs to know the phone state so that it can handle an incoming call when you are playing

# What If Formal Specs Are Written?!



In reality, few of these requirements are (formally) specified!!

➔ Hope?!: Bring human into the loop: user perception + judgment



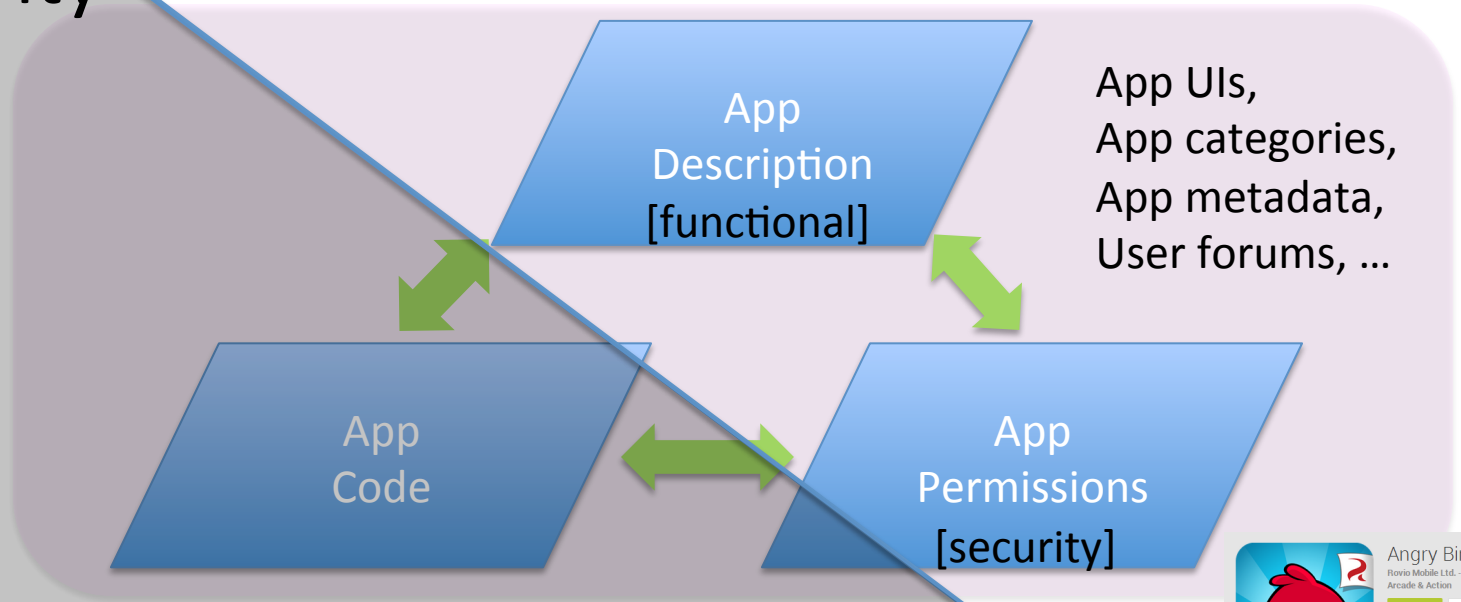
# Our Yin-Yang View on Mobile App Security



**User-Perceived Information**

**App Security Behavior**

- Reason about user-perceived info, e.g., WHYPER (↑)
- Push app security behavior across the boundary (→)
- Check **consistency** across the boundary (↔)
- Reduce user judgment effort (↓)



# Assuring Market Security/Privacy

- **Apple** (*Market's* Responsibility)
  - Apple performs **manual inspection**
- **Google** (*User's* Responsibility)
  - **Users approve** permissions for security/privacy
  - Bouncer (static/dynamic malware analysis)
- **Windows Phone** (Hybrid)
  - Permissions / **manual inspection**

# Need More Than Program Analysis

- Previous approaches look at permissions  $\leftrightarrow$  code (runtime behaviors)
- *What does the users expect?*
  - **GPS Tracker**: record and send location
  - **Phone-Call Recorder**: record audio during phone call



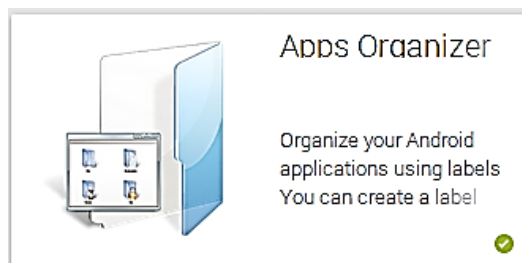
# Vision

*“Bridging the gap between user expectation ↔ app behaviors”*



- User expectations
  - user perception + user judgment
- Focus on permission ↔ app descriptions
  - permissions (protecting user understandable resources) should be discussed

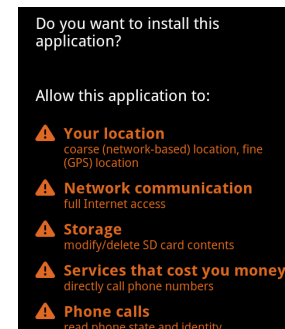
## App Description Sentence



## Linkage



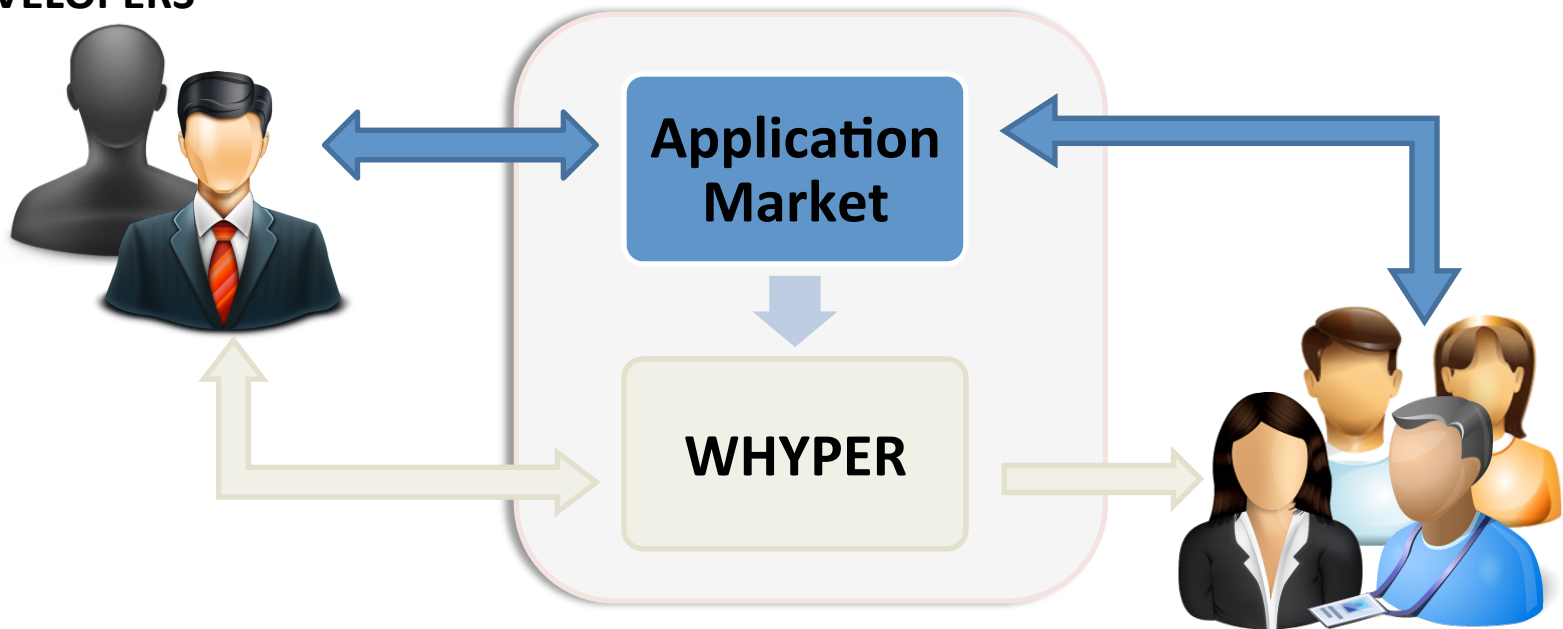
## Permission



# WHYPER Overview

- Enhance **user experience** while installing apps
- Enforce **functionality disclosure** on **developers**
- Complement **program analysis** to ensure justifications


**DEVELOPERS**



**USERS**

# Example Sentence in App Desc.

- E.g., “Also you can *share* the yoga exercise *to your friends via Email and SMS.*”
  - Implication of using the **contact** permission
  - Permission sentences

I   
Ctrl+F

# Problems with Ctrl + F

- **Confounding effects:**
  - Certain keywords such as “**contact**” have a confounding meaning
  - E.g., “... displays user **contacts**, ...” vs “... **contact** me at [abc@xyz.com](mailto:abc@xyz.com)”.
- **Semantic inference:**
  - Sentences often describe a sensitive operation without actually referring to keywords
  - E.g., “share yoga exercises with your friends via Email and SMS”

# Natural Language Processing

- Natural Language Processing (NLP) techniques help computers understand NL artifacts

- In
- N
- fe

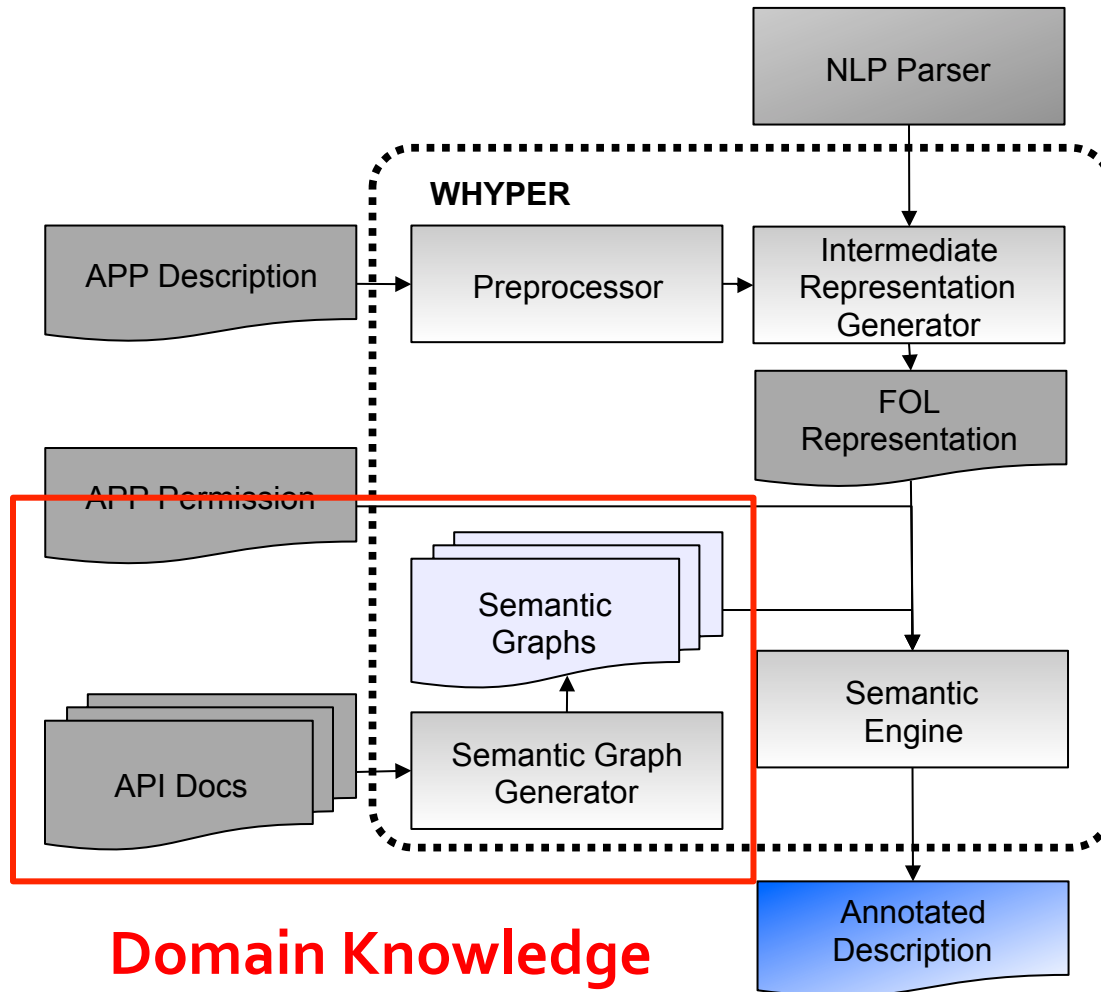


2]

]



# Overview of *WHYPER*



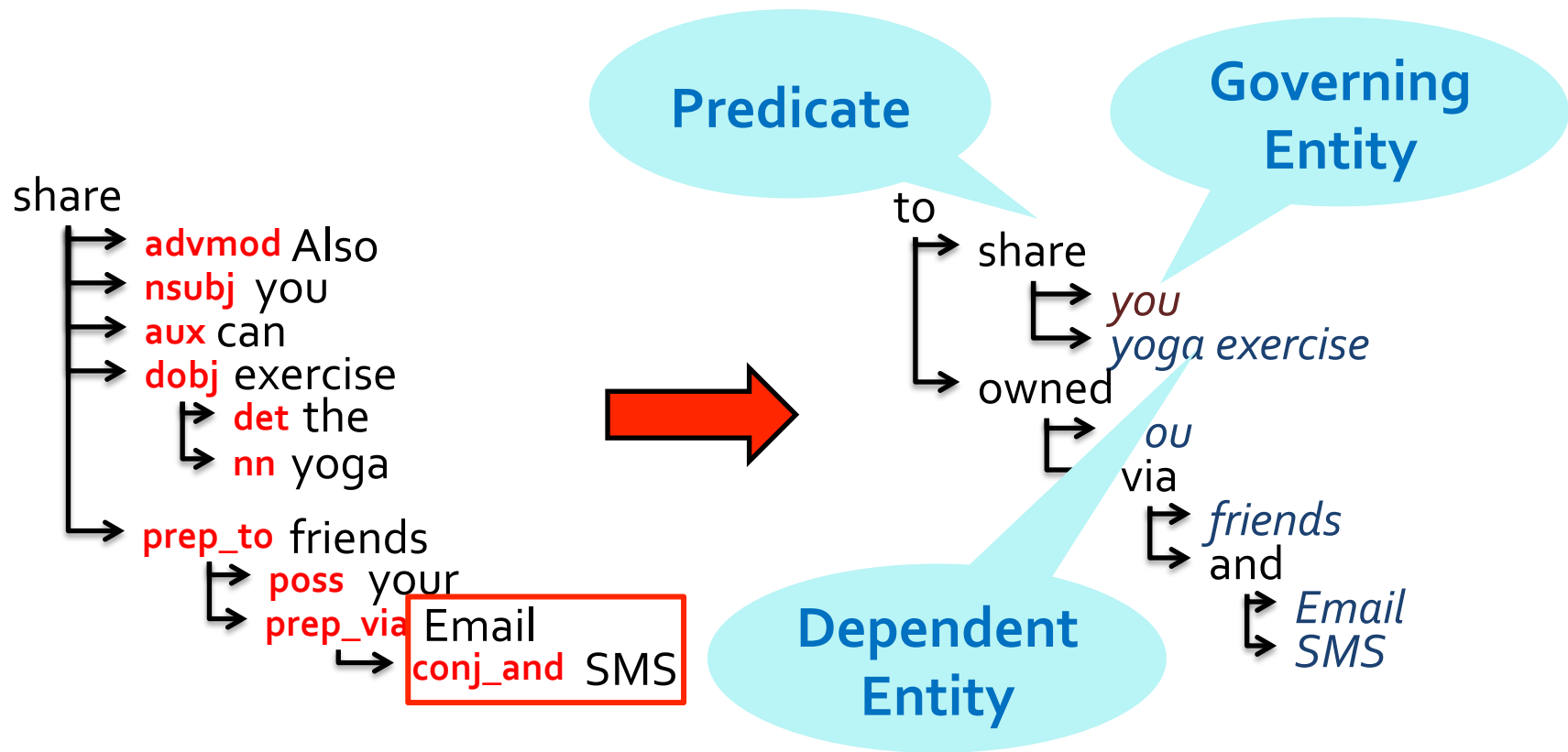
# Preprocessor

- Period Handling
  - Decimals, ellipsis, shorthand notations (**Mr., Dr.**)
- Sentence Boundaries
  - Tabs, bullet points, delimiters (:)
  - Symbols (\*,-) and enumeration sentence
- Named Entity Handling
  - E.g., **"Pandora internet radio"**
- Abbreviation Handling
  - E.g., **"Instant Message (IM)"**

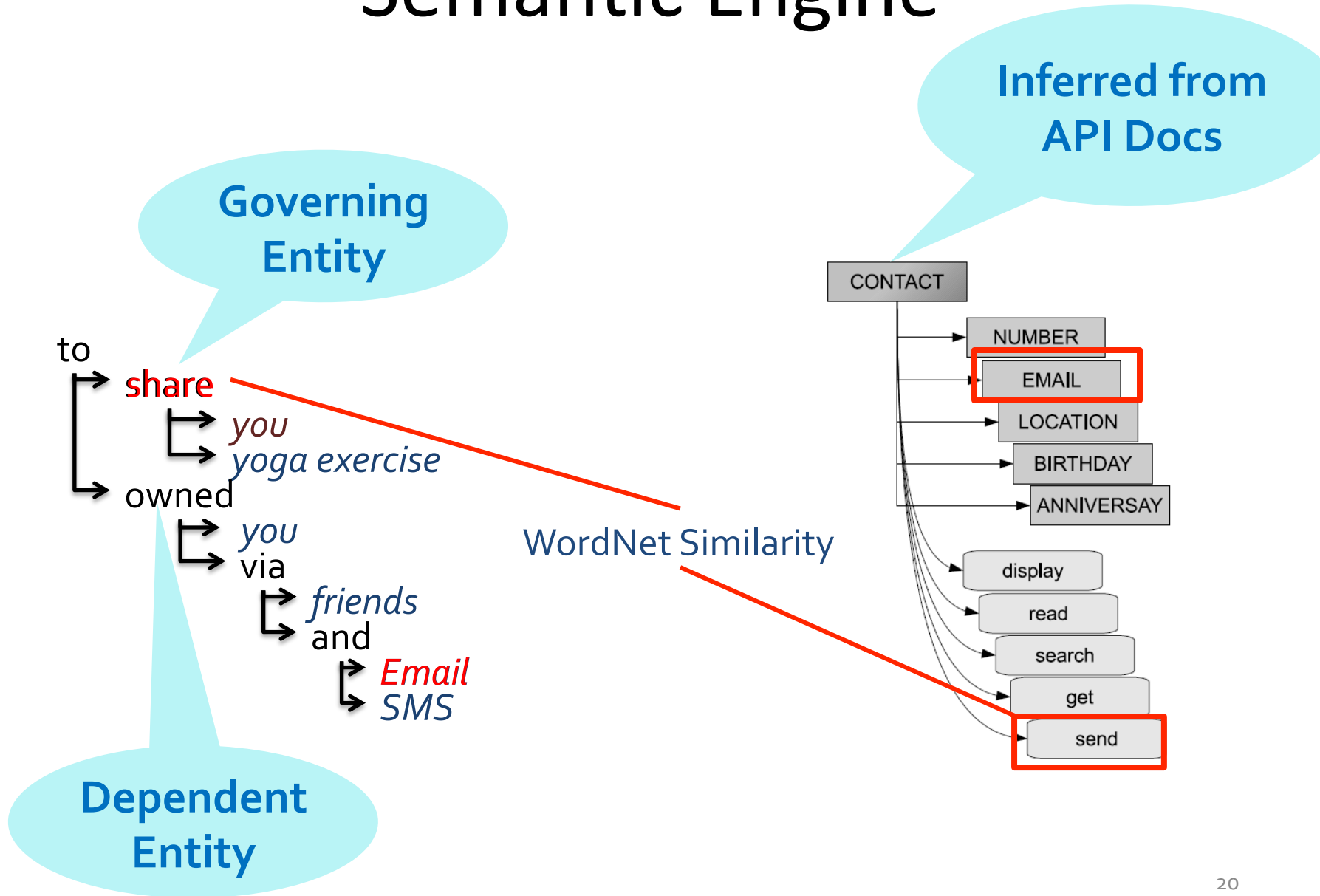
# Intermediate-Representation Generator

Also you can share the yoga exercise to your friends via Email and SMS

RB PRP MD VB DT NN NN PRP NNS NNP NNP



# Semantic Engine





# Evaluation

- Subjects
  - Permissions:
    - READ\_CONTACTS
    - READ\_CALENDAR
    - RECORD\_AUDIO
  - 581 application descriptions
  - **9,953** sentences
- Evaluation setup
  - Manual annotation of the sentences
  - WHYPER for identifying permission sentences
  - Comparison to keyword-based searching

# Evaluation Results

- Precision and recall of **WHYPER**
  - Average precision (**82.8%**) and recall (**81.5%**)

Permission	Keywords
READ_CONTACTS	contact, data, number, name, email
READ_CALENDAR	calendar, event, date, month, day, year
RECORD_AUDIO	record, audio, voice, capture, microphone

- Comparison to keyword-based searching
  - Improving precision (**41.6%**) and recall (**-1.2%**)
  - E.g., *microphone-blow into* and *call-record*

# Access Control Policies (ACP) in Requirements Document

- Access control is often governed by security policies called Access Control Policies (ACP)
  - Includes rules to control which principals have access to which resources

ex.

“The Health Care Personnel (HCP) does not have the ability to edit the patient's account.”

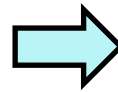
- A policy rule includes four elements
  - Subject – HCP
  - Action – edit
  - Resource - patient's account
  - Effect - deny



# Overview of Text2Policy

## Linguistic Analysis

A HCP should not change patient's account.

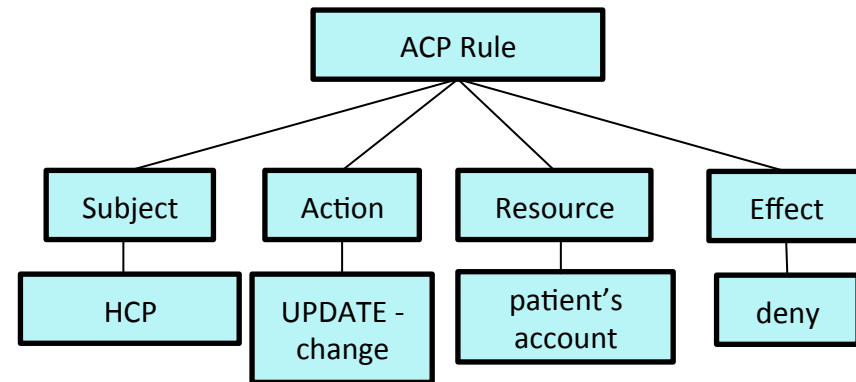
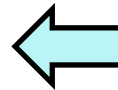


An [*subject*: HCP] should not [*action*: change] [*resource*: patient's account].

## Model-Instance Construction



```
<Policy PolicyId="ACP2" RuleCombAlgId="deny-overrides">
  <Target/>
  <Rule Effect="Deny" RuleId="rule-1">
    <Target>
      <Subjects><Subject><SubjectMatch MatchId="string-equal">
        <AttrValue>HCP</AttrValue>
        <SubjectAttrDesignator.../></SubjectMatch></Subject>
      </Subjects>
      <Resources><Resource><ResourceMatch MatchId="string-equal">
        <AttrValue>patient.account</AttrValue>
        <ResourceAttrDesignator.../></ResourceMatch></Resource>
      </Resources>
      <Actions><Action><ActionMatch MatchId="string-equal">
        <AttrValue DataType="string">UPDATE</AttrValue>
        <ActionAttrDesignator.../></ActionMatch></Action>
      </Actions>
    </Target></Rule></Policy>
```



## Transformation

# Example Technical Challenges in ACP Extraction

ACP 1: An HCP cannot change patient's account.

ACP2: An HCP is disallowed to change patient's account.

- Semantic Structure Variance
  - different ways to specify the same rule
- Negative Meaning Implicitness
  - verb could have negative meaning

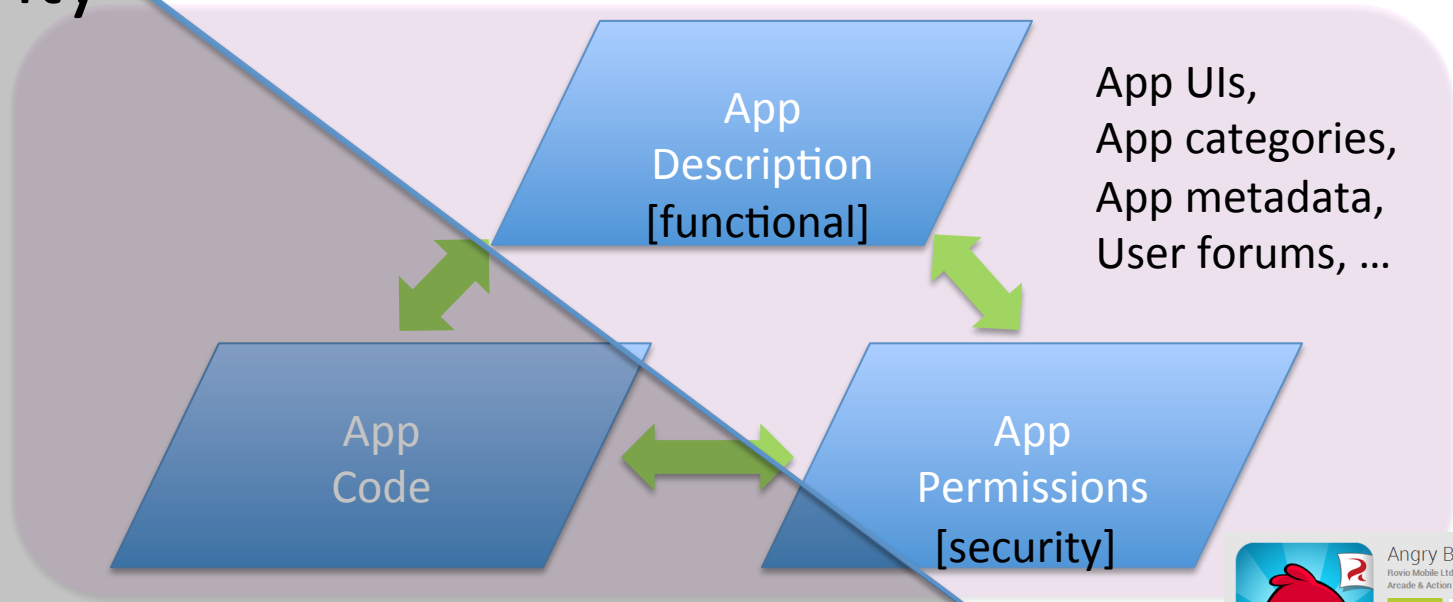
# Road Ahead: Yin-Yang View



**User-Perceived Information**

**App Security Behavior**

- Reason about user-perceived info, e.g., WHYPER (↑)
- Push app security behavior across the boundary (→)
- Check **consistency** across the boundary (↔)
- Reduce user judgment effort (↓)



# Text Analytics for Mobile App Security and Beyond



[taoxie@illinois.edu](mailto:taoxie@illinois.edu)

