Smart Phone Security:

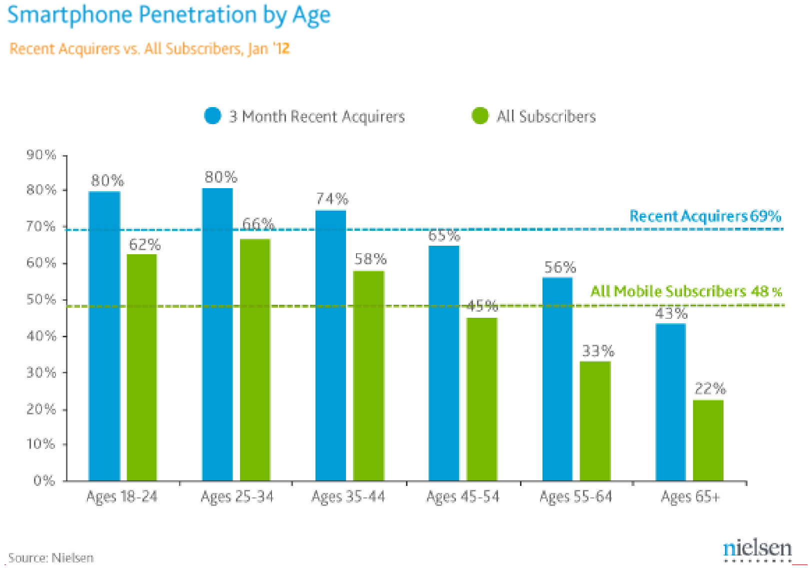
Technical and Human Considerations

Norman M. Sadeh, Ph.D.

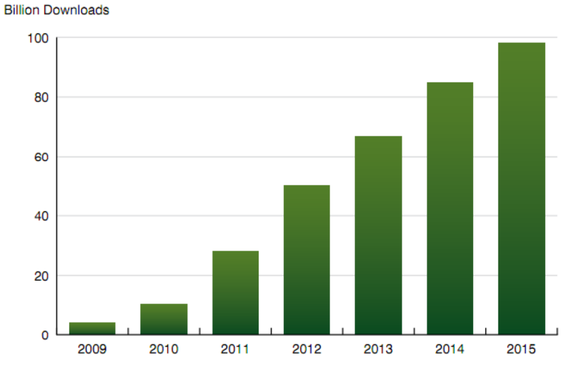
Professor, School of Computer Science
Director, Mobile Commerce Lab.
Carnegie Mellon University

mobile commerce lab

The Smart Phone Invasion



The App Economy



Mobile application downloads, billion downloads (World 2009–2015)

By 2015:

- **98 billion app downloads/year**
- **US$12B in direct annual revenue** (from $2B in 2010)
  - Apps & in-app purchases only *(source: Berg Insight, Oct 2011)*

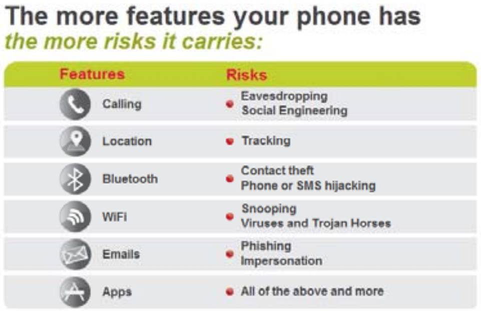
BYOD: The New Frontier

- □ 48% of employees will buy their own devices – *whether their organization approves that particular device **or NOT!*** (Forrester Research)
- □ **Blurring between work life & private life**
- □ **Unrealistic policies don't work** – even if they look good
- □ "If you can't fight them, join them"
  - □ **…hopefully under your own terms…**

Understanding the Risks: The Big Gap

Smartphones carry a lot of
sensitive information on them!
names>>addresses>>emails
email addresses>>phone numbers
confidential business information
calendar events>>documents
personal information >>texts
downloaded documents>>
apps>>financial information

© Wombat Security Technologies, 2011-2012



The more features your phone has
the more risks it carries:

Features	Risks
Calling	● Eavesdropping Social Engineering
Location	● Tracking
Bluetooth	● Contact theft Phone or SMS hijacking
WiFi	● Snooping Viruses and Trojan Horses
Emails	● Phishing Impersonation
Apps	● All of the above and more

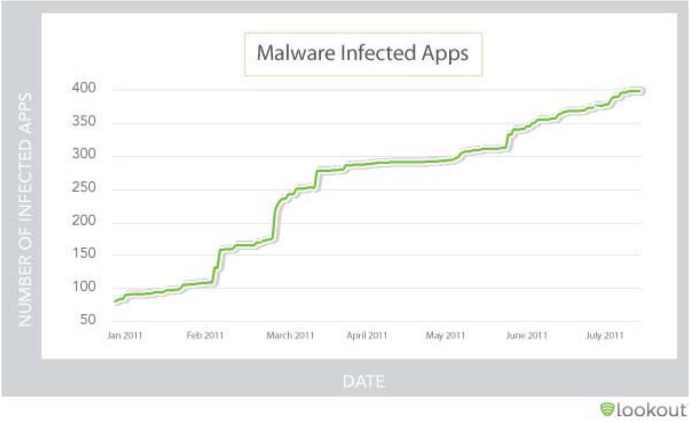
© Wombat Security Technologies, 2011-2012

Most people do not realize how sensitive their phones are

Malicious Apps – As an Example

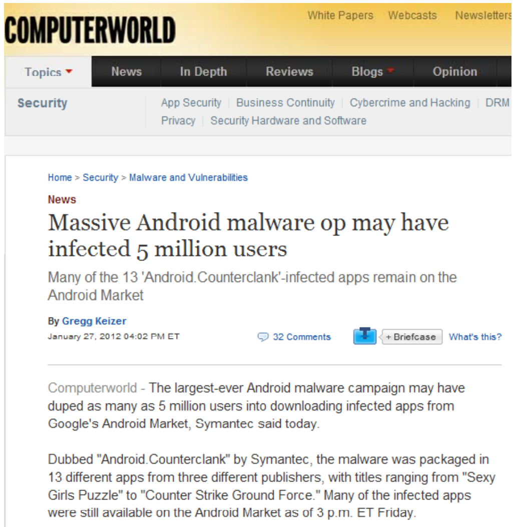
- App ecosystems compete based on the number of APIs they expose to developers
  - Contacts list
  - Camera
  - User location
  - etc.
- **Technically impossible to fully vet apps**
  - Apple has tried…Google recently started too
- **Tension between openness, usability, security / privacy, and business considerations**

Malware Infected Apps on the Rise



Source:https://www.mylookout.com/mobile-threat-report (June 2011)

Recent Headlines



News

Massive Android malware op may have infected 5 million users

Many of the 13 'Android.Counterclank'-infected apps remain on the Android Market

By Gregg Keizer
January 27, 2012 04:02 PM ET

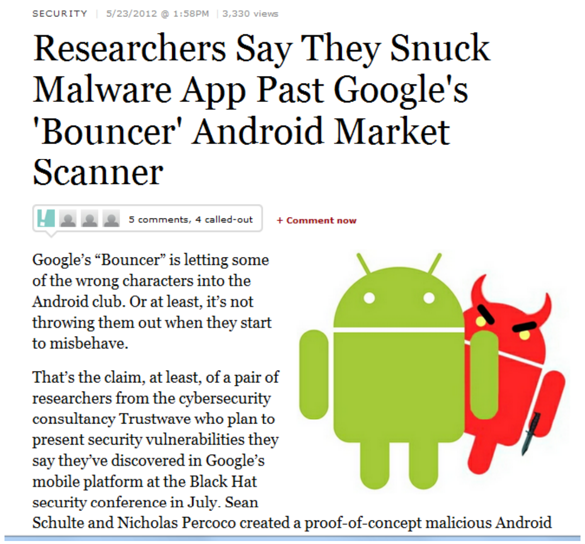
Computerworld - The largest-ever Android malware campaign may have duped as many as 5 million users into downloading infected apps from Google's Android Market, Symantec said today.

Dubbed "Android.Counterclank" by Symantec, the malware was packaged in 13 different apps from three different publishers, with titles ranging from "Sexy Girls Puzzle" to "Counter Strike Ground Force." Many of the infected apps were still available on the Android Market as of 3 p.m. ET Friday.

Review Process

- □ **Apple's App Store**
  - Apps are reviewed - not perfect
  - More restrictive sandbox
- □ **Android:**
  - **Android market/Google Play** relies on:
    - □ User's ability to do the evaluation…
    - □ …and report security problems
    - □ Recently announced "Bouncer Program"
  - **3rd party Android stores** (e.g. Amazon): manual review process – but this is not the case on all 3rd party Android stores

How Good is Google's Bouncer?



SECURITY | 5/23/2012 @ 1:58PM | 3,330 views

Researchers Say They Snuck Malware App Past Google's 'Bouncer' Android Market Scanner

5 comments, 4 called-out + Comment now

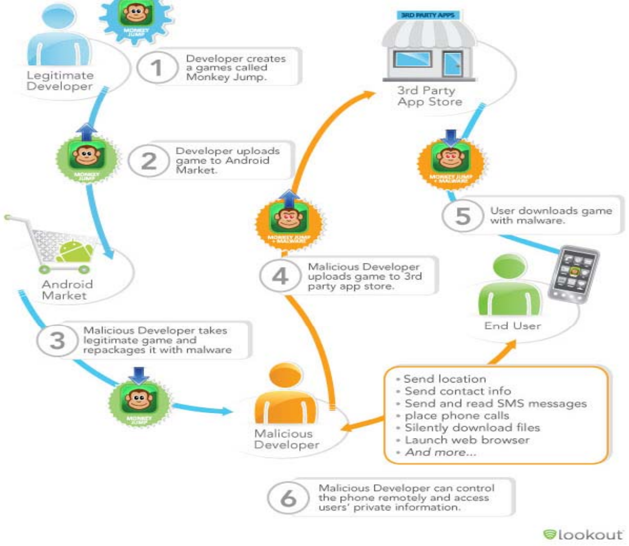
Google's "Bouncer" is letting some of the wrong characters into the Android club. Or at least, it's not throwing them out when they start to misbehave.

That's the claim, at least, of a pair of researchers from the cybersecurity consultancy Trustwave who plan to present security vulnerabilities they say they've discovered in Google's mobile platform at the Black Hat security conference in July. Sean Schulte and Nicholas Percoco created a proof-of-concept malicious Android

Source: Forbes, May 2012

Example of an Infection Scenario

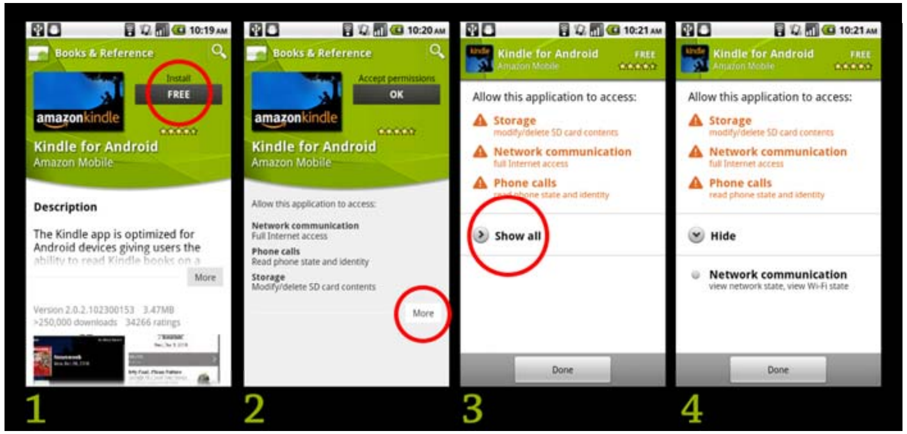
Source: https://www.mylookout.com/mobile-threat-report


Legitimate Developer
1 Developer creates a games called Monkey Jump.
2 Developer uploads game to Android Market.
Android Market
3 Malicious Developer takes legitimate game and repackages it with malware
Malicious Developer
4 Malicious Developer uploads game to 3rd party app store.
3RD PARTY APPS
3rd Party App Store
5 User downloads game with malware.
End User
• Send location
• Send contact info
• Send and read SMS messages
• place phone calls
• Silently download files
• Launch web browser
• And more…
6 Malicious Developer can control the phone remotely and access users' private information.
lookout

A Study of Android Users

P. Gage Kelley, S. Consolvo, L. Cranor, J. Jung, N. Sadeh, D. Wetherall, "**A Conundrum of Permissions: Installing Applications on an Android Smartphone**", USEC2012.

Android permissions screens



1. Kindle for Android
Amazon Mobile
Description
The Kindle app is optimized for Android devices giving users the ability to read Kindle books on a
Version 2.0.2.102300153 3.47MB
>250,000 downloads 34266 ratings

2. Kindle for Android
Amazon Mobile
Allow this application to access:
Network communication
Full Internet access
Phone calls
Read phone state and identity
Storage
Modify/delete SD card contents

3. Kindle for Android
Amazon Mobile
Allow this application to access:
Storage
modify/delete SD card contents
Network communication
full Internet access
Phone calls
read phone state and identity

4. Kindle for Android
Amazon Mobile
Allow this application to access:
Storage
modify/delete SD card contents
Network communication
full Internet access
Phone calls
read phone state and identity
Network communication
view network state, view Wi-Fi state

Android Permissions/Manifest

- □ Intended to help users decide whether they trust the application
  - □ Security
  - □ Privacy
- □ Over 120 Android permissions today
- □ Many developers abuse permissions
  - ■ Advertising and more

Interview Findings

- □ Users **do not understand Android permissions**.
- □ The terms are at best **vague**, and at worst **confusing**, misleading, jargon-filled, and poorly grouped
- □ This lack of understanding makes it **difficult for people to make informed decisions** when installing new software on their phones
- □ Largely, the permissions are ignored, with participants instead **trusting word of mouth, ratings, and Android market reviews**.
- □ While participants stated they try to find good applications in the market, they **believe they are protected by oversight processes which do not exist**.
- □ Overall, **users are not currently well prepared to make informed privacy and security decisions** around installing applications from the Android market.

So….What Are We Up Against?

- □ Devices that are even **more sensitive than computers/laptops**
- □ **Users** who:
  - ■ Do not **appreciate the risks**
  - ■ Are **ill prepared** to make the right decisions
  - ■ Suffer from bad habits & **cognitive biases**
- □ **Interfaces** that are **confusing** rather than helpful

Our Work at Carnegie Mellon

1. Effective User Training Software
2. Technologies to Help Users Make Better Security & Privacy Decisions

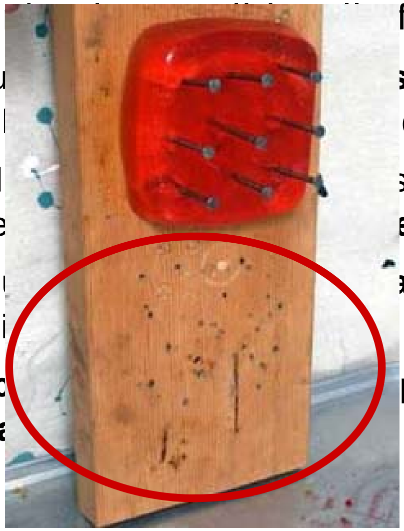
BYOD implies users who are:

- □ responsible

Do we really have a choice?

Training has a Big Role to Play

...But trai failed



- Secu **sk**: empl d to learn
- Trad s and content have **elling**
- **Req ast** & conti
- **Prac** ps are **not alwa**

Priming Users for Training

- □ Challenge them to take quizzes
- □ ...or better: Motivate them via mock attacks
- □ **Nothing beats showing a user how vulnerable (s)he is**

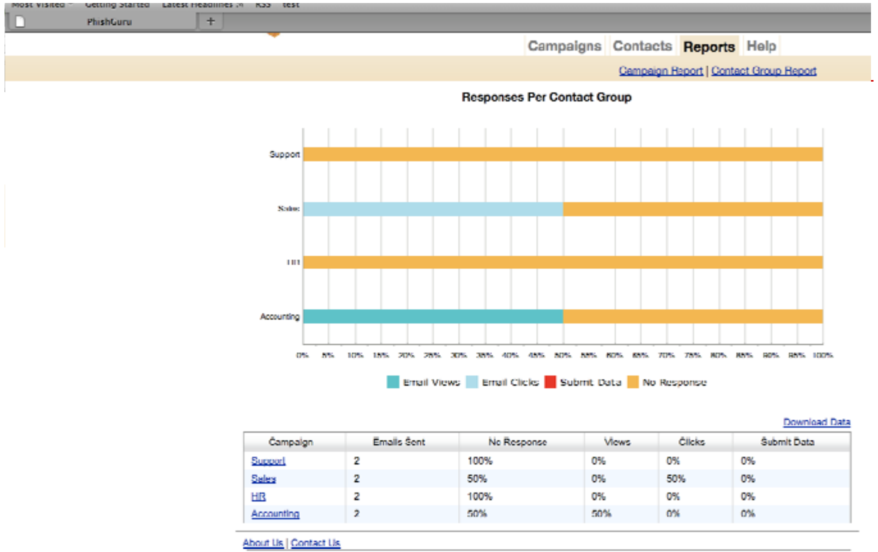
Phishing as An Example

- **Email phishing**: Much worse on mobile phones
  - Mobile users are first to arrive at phishing websites
  - Mobile users **3x more likely to submit credentials** than desktop users

Source: Trusteer, Jan. 2011 – similar

Training via Mock Attacks: PhishGuru

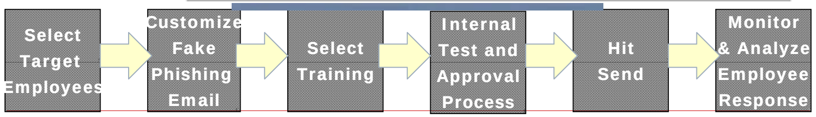
- Teach people **in the context** they would be attacked
- **If a person falls for simulated phish**, then pop up an intervention
- Unique "**teachable moment**"



Responses Per Contact Group

🟦 Email Views 🟦 Email Clicks 🟥 Submit Data 🟧 No Response

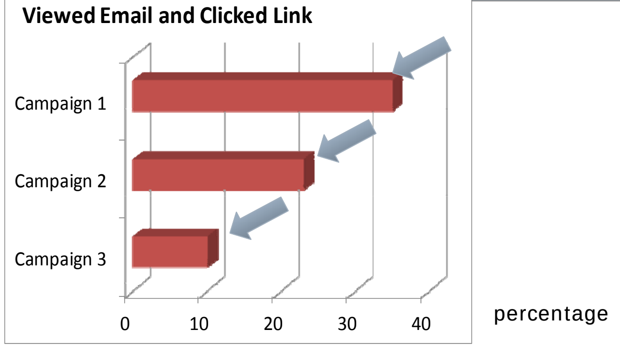
Campaign	Emails Sent	No Response	Views	Clicks	Submit Data
Support	2	100%	0%	0%	0%
Sales	2	50%	0%	50%	0%
HR	2	100%	0%	0%	0%
Accounting	2	50%	50%	0%	0%



Select Target Employees → Customize Fake Phishing Email → Select Training → Internal Test and Approval Process → Hit Send → Monitor & Analyze Employee Response

This really works!

Reduces the chance of falling for an attack by more than 70% !



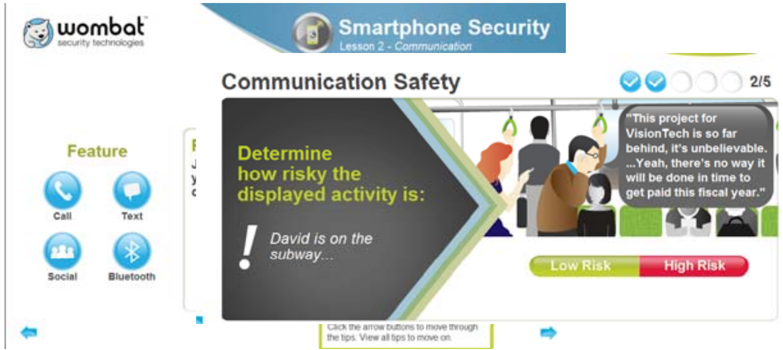
Actual Results

Starting with the Most Common Threats

- ➢ Millions of cell phones lost or stolen each year
- ➢ Majority of smart phone users still do not have PINs

Source for image: http://www.malaysianwireless.com/2011/09/advice-how-to-protect-your-smartphone/

Learning by Doing is Critical



wombat security technologies

Smartphone Security
Lesson 2 - Communication

Communication Safety

2/5

Feature

Call
Text
Social
Bluetooth

Determine how risky the displayed activity is:

! David is on the subway…

"This project for VisionTech is so far behind, it's unbelievable. …Yeah, there's no way it will be done in time to get paid this fiscal year."

Low Risk
High Risk

Click the arrow buttons to move through the tips. View all tips to move on.

© Wombat Security Technologies, 2011-2012

- □ Teach people to better **appreciate the risks**
- □ Create **mock situations**
- □ Force them to **make decisions**
- □ Provide them with **feedback**

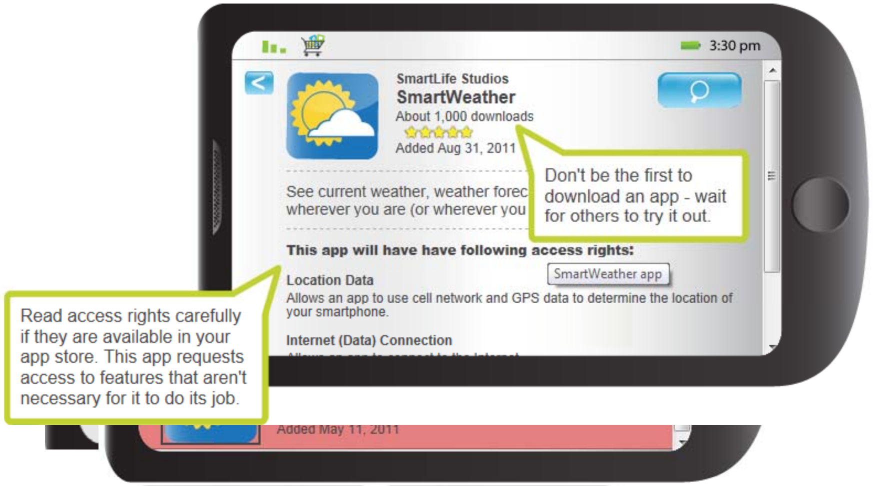
Gradually Move Towards More Complex Tasks

- □ Mobile Apps
- □ Location
- □ Social Networking

Mobile Apps

- □ **Challenge**: difficult to come up with full-proof rules
- □ Train people to be suspicious & look for possible red flags
- □ Emphasis on:
  - ■ **Learning by doing**
  - ■ **Feedback**
  - ■ **Opportunities for reflection**

From Simple to Increasingly Realistic



3:30 pm

SmartLife Studios

SmartWeather

About 1,000 downloads

Added Aug 31, 2011

See current weather, weather forec
wherever you are (or wherever you

This app will have have following access rights:

SmartWeather app

Location Data

Allows an app to use cell network and GPS data to determine the location of your smartphone.

Internet (Data) Connection

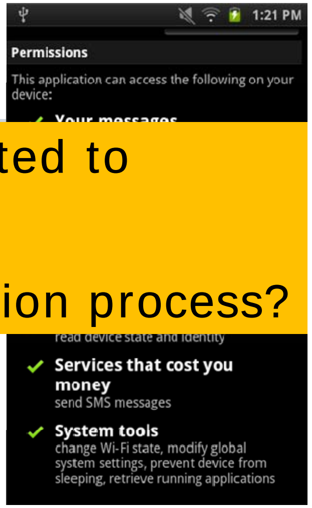
Don't be the first to download an app - wait for others to try it out.

Read access rights carefully if they are available in your app store. This app requests access to features that aren't necessary for it to do its job.

Added May 11, 2011

Click on the safer app.

Simplifying User Decisions



1:21 PM

Permissions

This application can access the following on your device:

✓ Your messages

read device state and identity

✓ **Services that cost you money**
send SMS messages

✓ **System tools**
change Wi-Fi state, modify global system settings, prevent device from sleeping, retrieve running applications

-How can a user be expected to make sense out of this?

-Can we simplify the decision process?

J. Lin, S. Amini, J. Hong, N. Sadeh, J. Lindqvist, J. Zhang, "Expectation and Purpose: Understanding Users' Mental Models of Mobile App Privacy through Crowdsourcing", Proc. of the 14th ACM International Conference on Ubiquitous Computing, Pittsburgh, USA, Sept. 2012

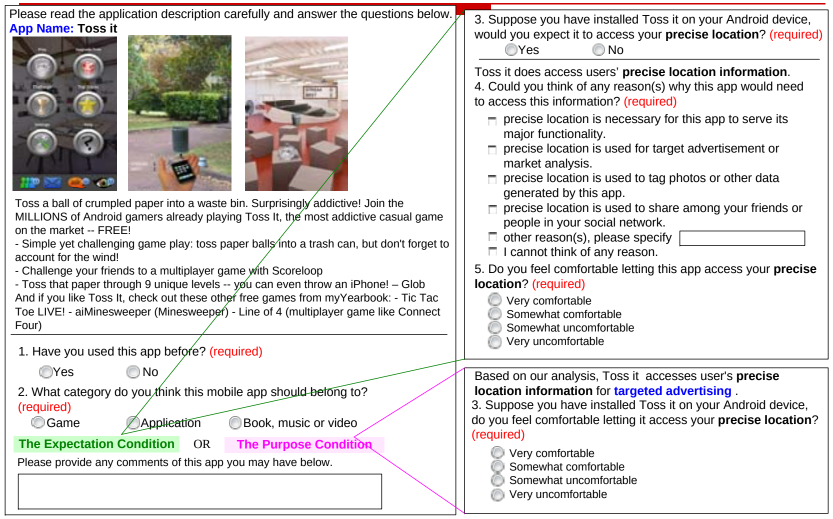
Basic Idea

- □ Not all apps require the same permissions
- □ Can we leverage the **wisdom of crowds** to determine what permissions are reasonable for an app to request?
- □ Can we use this information to develop simpler interfaces?
  - ■ **Highlight those permissions that are unusual for a given category of apps**

Mobile App Privacy through Crowdsourcing

- □ **Experiment:** 179 Amazon Turk participants
- □ **Top 100 most popular apps in Android Market**
- □ **Targeted resources**
  - ■ Location: GPS (24) and network location (29)
  - ■ Unique ID(56)
  - ■ Contact List (25)
- □ 20 unique responses / Human Intelligence Tasks ("HIT") in the form of app-resource pair
  - □ US$0.12/HIT

Sample Questions



Please read the application description carefully and answer the questions below.

App Name: Toss it

Toss a ball of crumpled paper into a waste bin. Surprisingly addictive! Join the MILLIONS of Android gamers already playing Toss It, the most addictive casual game on the market -- FREE!
- Simple yet challenging game play: toss paper balls into a trash can, but don't forget to account for the wind!
- Challenge your friends to a multiplayer game with Scoreloop
- Toss that paper through 9 unique levels -- you can even throw an iPhone! – Glob
And if you like Toss It, check out these other free games from myYearbook: - Tic Tac Toe LIVE! - aiMinesweeper (Minesweeper) - Line of 4 (multiplayer game like Connect Four)

1. Have you used this app before? (required)

○Yes ○No

2. What category do you think this mobile app should belong to? (required)

○Game ○Application ○Book, music or video

The Expectation Condition OR **The Purpose Condition**

Please provide any comments of this app you may have below.

3. Suppose you have installed Toss it on your Android device, would you expect it to access your **precise location**? (required)

○Yes ○No

Toss it does access users' **precise location information**.

4. Could you think of any reason(s) why this app would need to access this information? (required)

- □ precise location is necessary for this app to serve its major functionality.
- □ precise location is used for target advertisement or market analysis.
- □ precise location is used to tag photos or other data generated by this app.
- □ precise location is used to share among your friends or people in your social network.
- □ other reason(s), please specify
- □ I cannot think of any reason.

5. Do you feel comfortable letting this app access your **precise location**? (required)

- ○ Very comfortable
- ○ Somewhat comfortable
- ○ Somewhat uncomfortable
- ○ Very uncomfortable

Based on our analysis, Toss it accesses user's **precise location information** for **targeted advertising** .

3. Suppose you have installed Toss it on your Android device, do you feel comfortable letting it access your **precise location**? (required)

- ○ Very comfortable
- ○ Somewhat comfortable
- ○ Somewhat uncomfortable
- ○ Very uncomfortable

Least Expected Permissions

Resource	App name	% Expected	Avg Comfort
Network Location	Brightest Flashlight	5%	-1.25
	Toss It	10%	-1.15
	Angry Birds	10%	-0.43
	Air Control Lite	20%	-0.55
	Horoscope	20%	-1.05
GPS Location	Brightest Flashlight	10%	-0.95
	Toss It	5%	-0.95
	Shazam	20%	-0.05
Device ID	Brightest Flashlight	5%	-1.35
	TalkingTom Free	10%	-0.78
	Mouse Trap	15%	-0.85
	Dictionary	15%	-0.69
	Tiny Flashlight	20%	-0.80
	Ant Smasher	20%	-1.13
	FxCamera	20%	-0.73
	Horoscope	20%	-1.03
Contact List	Backgrounds HD Wallpapers	10%	-1.35
	Pandora	20%	-0.70
	GO Launcher EX	20%	-0.75

- □ Strong correlation observed (r=0.91) between people's expectation and their comfort level
- □ Tied to perceived necessity
- □ W27 *"Why does a flashlight need to know my location? I love this app, but now I know it accesses my location, I may delete it." (Brightest Flashlight)*
- □ W56 *"I do not feel that games should ever need access to your location. I will never download this game." (Toss it)*

Comfort ratings ranging between -2.0 (very uncomfortable) to +2.0 (very comfortable).

Lay Users Can't Figure the Reasons Behind some Permissions

Resource Type	Resource used for [1] Major functionality [2] Tagging or sharing [3]Advertising or market analysis	% of accurate guess	% of no idea
Contact List (25)	[1]---------------------20	56%	8%
	[2]----------------------2	28%	35%
	[1]+[2]-----------------2	19%	16%
	[1]+[2]+[3]------------1	27%	14%
GPS Location (24)	[1]---------------------14	74%	11%
	[2]----------------------4	80%	10%
	[3]----------------------2	35%	55%
	[1]+[3]-----------------3	15%	27%
	[2]+[3]-----------------1	15%	40%
Network Location (29)	[1]---------------------15	77%	8%
	[2]----------------------2	55%	10%
	[3]----------------------7	29%	63%
	[1]+[3]-----------------3	15%	22%
	[2]+[3]-----------------2	13%	25%
Device ID (56)	[1]---------------------14	51%	29%
	[3]---------------------30	22%	58%
	[1]+[3]----------------12	7%	55%

- ❑ TaintDroid used to identify ground truth.
- ❑Very low accuracy when sensitive resources used for multiple purposes

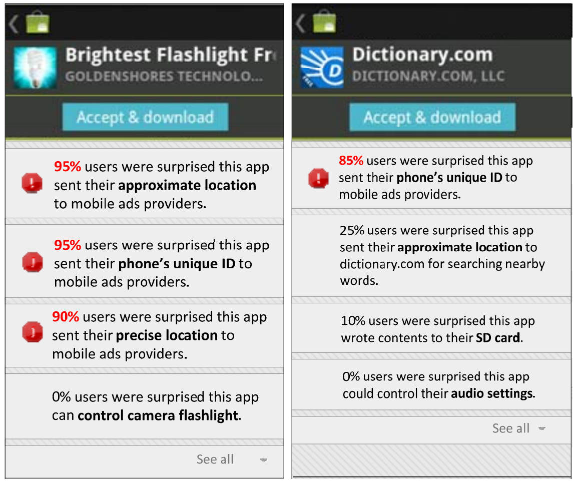
Purpose Critical to Informed Decisions

Resource Type	comfort rating w/ purpose	comfort rating w/o purpose	df	T	p
Device ID	0.47(0.30)	-0.10(0.41)	55	7.42	0.0001
Contact List	0.66(0.22)	0.16(0.54)	24	4.47	0.0002
Network Location	0.90(0.53)	0.65(0.55)	28	3.14	0.004
GPS Location	0.72(0.62)	0.35(0.73)	23	3.60	0.001

Comfort ratings ranging between -2.0 (very uncomfortable) and +2.0 (very comfortable).

- □ **Average comfort rating 0.3 higher when purpose is explained.**
- □ Argues for including purpose in permission request
  - ■ **…basic privacy principle…**

Towards New Interfaces



95% users were surprised this app sent their **approximate location** to mobile ads providers.

95% users were surprised this app sent their **phone's unique ID** to mobile ads providers.

90% users were surprised this app sent their **precise location** to mobile ads providers.

0% users were surprised this app can **control camera flashlight.**

85% users were surprised this app sent their **phone's unique ID** to mobile ads providers.

25% users were surprised this app sent their **approximate location** to dictionary.com for searching nearby words.

10% users were surprised this app wrote contents to their **SD card**.

0% users were surprised this app could control their **audio settings.**

Personas

- □ When it comes to privacy, not all users feel the same
- □ **Privacy personas & app categories could help simplify decisions**
  - Our earlier research has demonstrated the power of privacy personas in the context of location sharing apps

Ramprasad Ravichandran, Michael Benisch, Patrick Gage Kelley, and Norman M. Sadeh. Capturing Social Networking Privacy Preferences: Can Default Policies Help Alleviate Tradeoffs between Expressiveness and User Burden? *PETS '09.*

Concluding Remarks

- □ Mobile users do not appreciate the security risks associated with smart phone usage
- □ BYOD exacerbates the risks but it would be an illusion for industry to think that it can fight the trend
  - e.g. blurring between personal and work life
- □ **What is required**:
  - Better technologies to mitigate attacks
    - □ ...but malware detection cannot solve everything...
    - □ ...MDM and device virtualization go only so far too...
  - Realistic corporate policies
  - More effective user training solutions
  - More usable security and privacy interfaces

Q&A

mobile commerce lab

http://mcom.cs.cmu.edu

Acknowledgement: Some of the mobile security software examples are based on work now commercialized by Wombat Security Technologies (www.wombatsecurity.com)