

# EECS 448 Smartphone Security

Xusheng Xiao

Electrical Engineering and Computer Science  
Case Western Reserve University

# Instructor and Lectures

**Instructor:** Xusheng Xiao, [xusheng.xiao@case.edu](mailto:xusheng.xiao@case.edu), Olin 506

**Classroom:** Olin 313, T-TH 4:00 - 5:15 pm

Web page: on Canvas (<https://canvas.case.edu/>)

**TA:** TBD

**Office hours:** T-TH 2:30 - 3:30 pm (or by appointment)

# Course Style

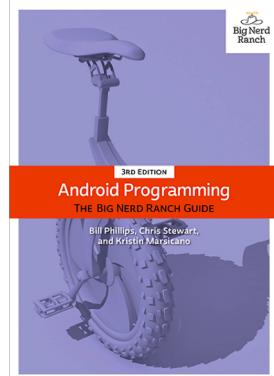
- **Mixed with lectures, labs, and paper presentations/discussions**
- **Project-oriented course**
  - You can learn a set of state-of-the-art Android analysis tools
  - You will build your own tools with innovative analysis on Android apps
- Start installing Java and Android Studio right away
  - <https://developer.android.com/studio/index.html>

# Syllabus

[https://docs.google.com/document/d/17gOYOIDY\\_noxxfL69mhYqUGx4eRVLGvdIXj3vpe1ueQ](https://docs.google.com/document/d/17gOYOIDY_noxxfL69mhYqUGx4eRVLGvdIXj3vpe1ueQ)

# Textbook and Materials

**Text:** “Android Programming – The Big Nerd Ranch Guide”, Bill Phillips, Chris Stewart, and Kristin Marsicano



## Materials:

- [Google's Android Developer pages](#) - make this your starting point for all your explorations
- [Android Source Documentation](#) (for understanding the architecture of Android)
- Google Scholar (for finding related papers)

# Paper Presentations and Discussions

- Team-based presentation
  - # teams: 10
  - Preferred # members: 3 or 4
  - A team cannot have two Ph.D. students
- Paper presentation and discussions
  - Each team is assigned a direction (totally 5 directions, introduced later)
  - Besides recommended papers, you may find related papers to present
  - You may download slides, or make your own!
  - You will write summary of other students' presentations in class

# Survey and Course Project

- Survey
  - Each team submits a survey paper
  - Survey paper should include at least 9 papers
  - Survey topics should be different among teams
- Course Project
  - Each team builds an app analysis tool based on their survey topic
  - Deliverables includes an initial report, presentation slides, experiment results, and final project report

# ACM/IEEE Digital Library

**IEEE Xplore®  
Digital Library**

Institutional Sign In | IEEE

Browse | My Settings | Get Help | Subscribe

All android security

Advanced Search | Other Search Options

Search within results

Show: All Results | Per Page: 25 | Export | Set Search Alerts | Search History

Displaying results 1-25 of 1,770 for android security

Conferences (1,597)  Journals & Magazines (142)  Early Access Articles (28)  
 Books (2)  Standards (1)

Year: Single Year | Range | From 2002 To 2018

Author

Select All on Page | Sort By: Relevance | Need Full-Text | REQUEST A FREE TRIAL | MyXplore Mobile App

Research on Android Intent Security Detection Based on Machine Learning  
Lv Zhuo; Guo Zhimin; Chen Cen  
2017 4th International Conference on Information Science and Control Engineering (ICISCE)  
Year: 2017  
Pages: 569 - 574  
IEEE Conferences  
Abstract | html | PDF (1361 Kb) |

SIGN IN | SIGN UP | android security | SEARCH | [advanced search]

ACM DL DIGITAL LIBRARY

Searched for android security [new search] [edit/save query]

Searched The ACM Full-Text Collection: 487,457 records [Expand your search to The ACM Guide to Computing Literature: 2,741,639 records] ?

33,653 results found | Export Results: bibtex | endnote | acmref | csv

434 videos found | Result 1 – 20 of 33,653 | Result page: 1 2 3 4 5 6 7 8 9 10 >>

Sort by: relevance

Refine by People  
Names ▾ Institutions ▾ Authors ▾ Editors ▾ Reviewers ▾

Refine by Publications  
Publication Names ▾ ACM Publications ▾ All Publications ▾ Content Formats ▾ Publishers ▾

Refine by Conferences  
Sponsors ▾ Events ▾ Proceeding Series ▾

1 Security implications of Android: a closed system, open software mobile platform  
Hassen Saidi | October 2011 | SPSM '11: Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices | Publisher: ACM | Bibliometrics: Citation Count: 0 | Downloads (6 Weeks): 5, Downloads (12 Months): 59, Downloads (Overall): 967 | Full text available: PDF | Smartphones blur the boundaries between the traditional feature phone and a general purpose computer such as a laptop. The Android OS, from Google, was created to be an open alternative to fully closed platforms such as Apple's iOS or Microsoft's Windows Phone OS. However, upon closer inspection, there are closed ... | Keywords: open software, android, security | [result highlights]

<https://dl.acm.org>

<http://ieeexplore.ieee.org/>

# Google Scholar

The screenshot shows the Google Scholar interface. In the top left, there's a sidebar with filters like 'Any time', 'Sort by relevance', 'Include patents', 'Create alert', and a large blue box labeled 'Filters'. The main search bar contains 'android permissions'. Below it, a blue callout labeled 'Keywords' points to the search term. The results list four papers:

- Android permissions demystified** by AP Felt, E Chin, S Hanna, D Song... - Proceedings of the 18th..., 2011 - dl.acm.org. A blue callout labeled 'Paper (may come with pdf)' points to this result. It includes a snippet about the Abstract Android permission system.
- Android permissions: User attention, comprehension, and behavior** by AP Felt, E Ha, S Egelman, A Haney, E Chin... - Proceedings of the..., 2012. It includes a snippet about the permission system's intention to inform users.
- A conundrum of permissions: installing applications on an android smartphone** by P Kelley, S Consalvo, L Cranor, J Jung... - ... cryptography and data..., 2012 - Springer. It includes a snippet about the user's choices regarding permissions.
- Android permissions: a perspective combining risks and benefits** by BP Sarma, N Li, C Gates, R Potharaju... - Proceedings of the 17th..., 2012 - dl.acm.org. It includes a snippet about the growth of the Android platform and its risks.

Each result entry includes a star rating, citation count, related articles, and all versions links. PDF links are provided for each paper: [PDF] berkeley.edu, [PDF] semanticscholar.org, [PDF] purdue.edu.

<https://scholar.google.com>

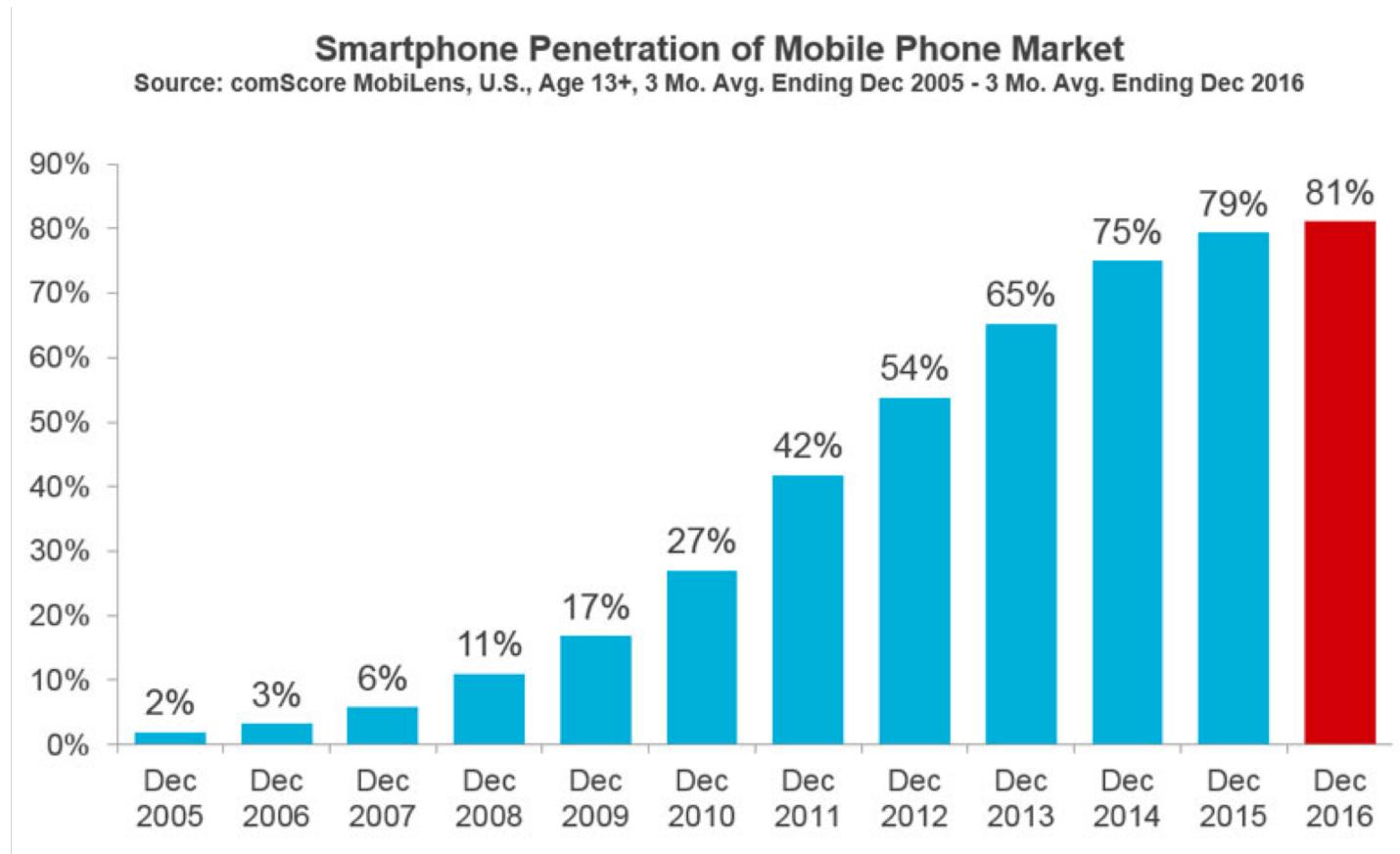
# Final Project Report

- Format: ACM SIG Proceedings Templates
  - <https://www.acm.org/publications/proceedings-template-16dec2016>
  - Templates available in Word and Latex
  - Submission must be PDF
- Content
  - Sections: Abstract, Introduction, Background, Study or Tool Design, Results, Related Work, Discussions, References
  - Example papers will be provided
  - Expected length is 8 – 12 pages

# Grading

- Paper presentation participation and interaction – 10%
- Homework assignments - 10%
- Quiz and Exams – 30%
- Survey Paper - 10%
- Paper presentation - 10%
- Projects – 30%
- **Late Assignment and Project Policy:** All homeworks are due at the end of the due day. Late submissions are accepted until the third day of the due day subject to penalty (20%, 40%, 60%).
- **Final Project Demo and Report:** Each team will do a demo at the last week of the course, and submit a final project report. Report templates follow ACM style.

# Smartphone Is Everywhere!!



# Mobile Apps and App Markets

Modern mobile-device platforms provide a central place for distributing software

- App Store (iOS) and Google Play
- Third-party applications (apps)

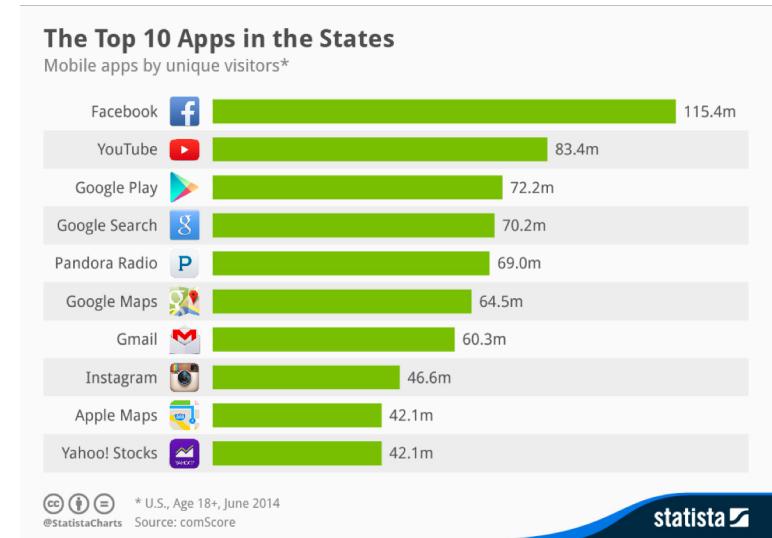
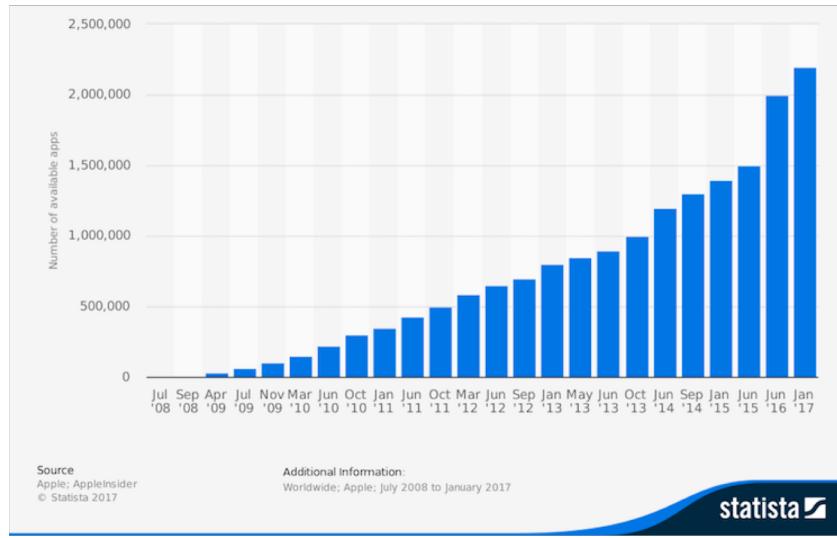


Apple App Store



Google Play

# Popularity of Mobile Apps



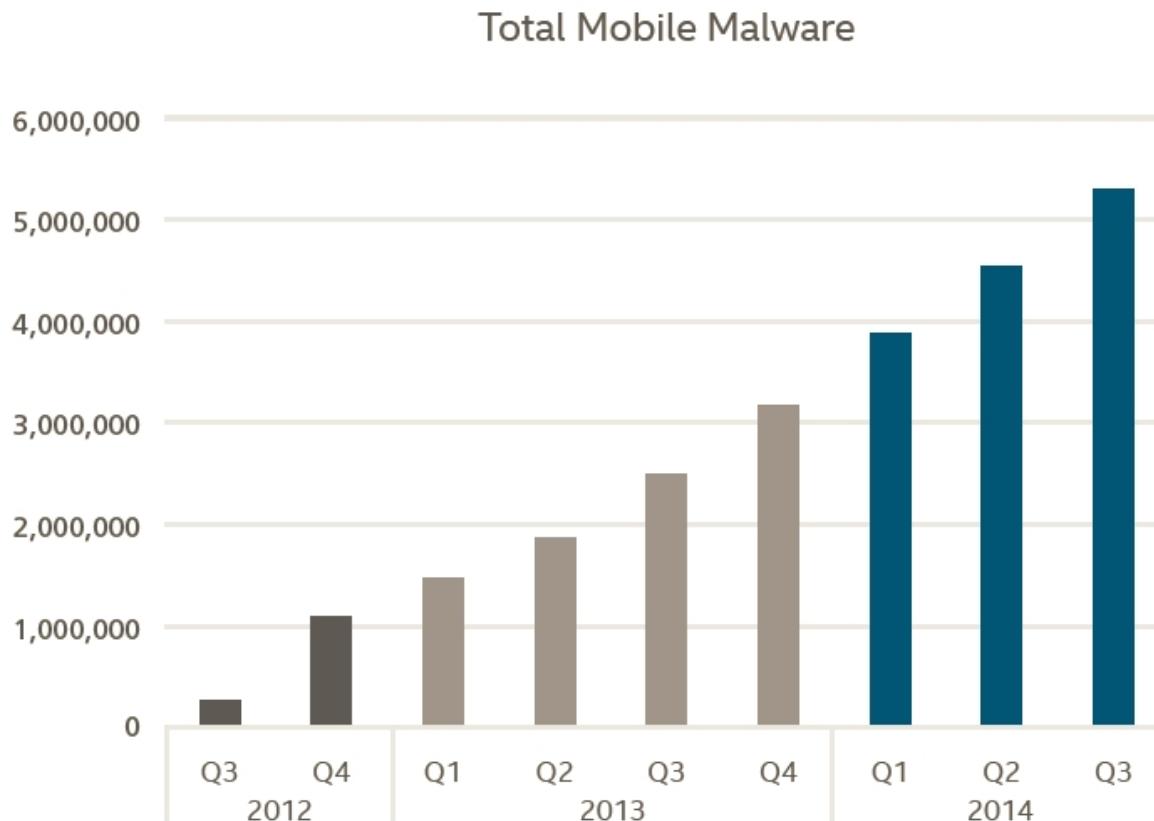
- 2017: 3 million Android apps!
- Growth rate: 1,300+ apps a day
- Everywhere in life: social, navigation, email, etc.

# Usage of Personal information

Permission	What for
Device ID & call info	Lets apps know if you are taking a call
Identity	Authorizes apps to sign in using other accounts
Contacts	Allows apps to read information on all contacts
Camera	Apps can control camera
SMS	Apps can read, send messages
Storage	Lets apps access entire memory and read, edit and delete data
Device & app history	Gives apps access to phone data—sites you browse, bookmarks, other apps
Phone	Lets apps control phone calls
Photo/Media /Files and Microphone	Gives access to photos, files, recordings on your phone
Location	Shows apps your precise location

- Customized services
  - Accounts
  - Phone calls
  - Location
  - SMS
- Potential risks
  - Account info leakage
  - Paid calls
  - Location-based ads or attacks
  - Illegitimate or Premium-rate SMS

# Potentially Unwanted Apps

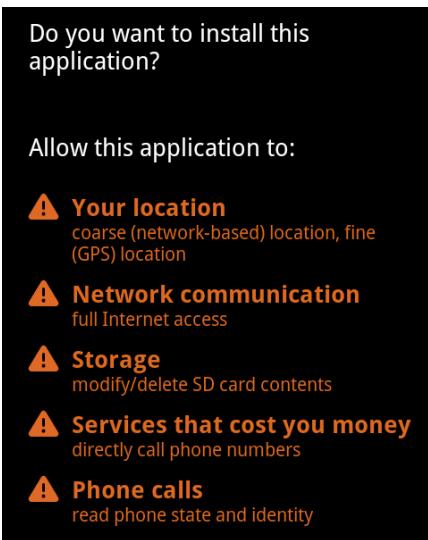


Protection mechanism based on permission system

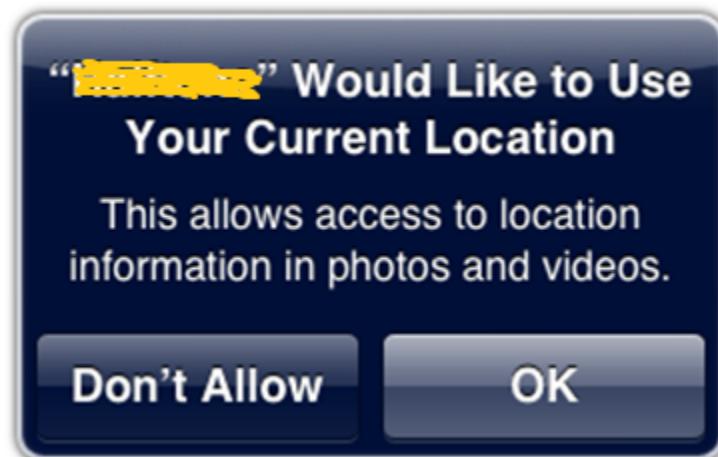
Source: McAfee Labs

# Privacy Control in Mobile Platforms

## Permission List



## Popup Dialog

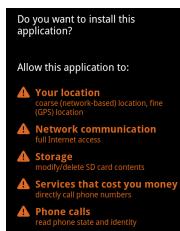


- These approaches report **what** permissions to use, not **how** or **why** permissions are used
- Users simply install applications **without questioning** the requested permissions

# Major Challenges

- Limited assistance for permission granting

Permission List



Popup Dialog



- Limited differentiations of permission uses



- Limited protection of sensitive user inputs

Comment:

Submit

Credit card type

Select Card Type

Card number

15 or 16 digit

Expiration date

MM - YYYY

# Course Objectives

- In-depth understanding of basic concepts in Android programming including Android UI, Android components
- In-depth knowledge of the Android Permission System
- In-depth knowledge of smartphone security techniques
  - Analysis on app descriptions, reviews, code, and UI
- General knowledge of program analysis techniques
- General knowledge of UI analysis techniques

# Course Objectives (2)

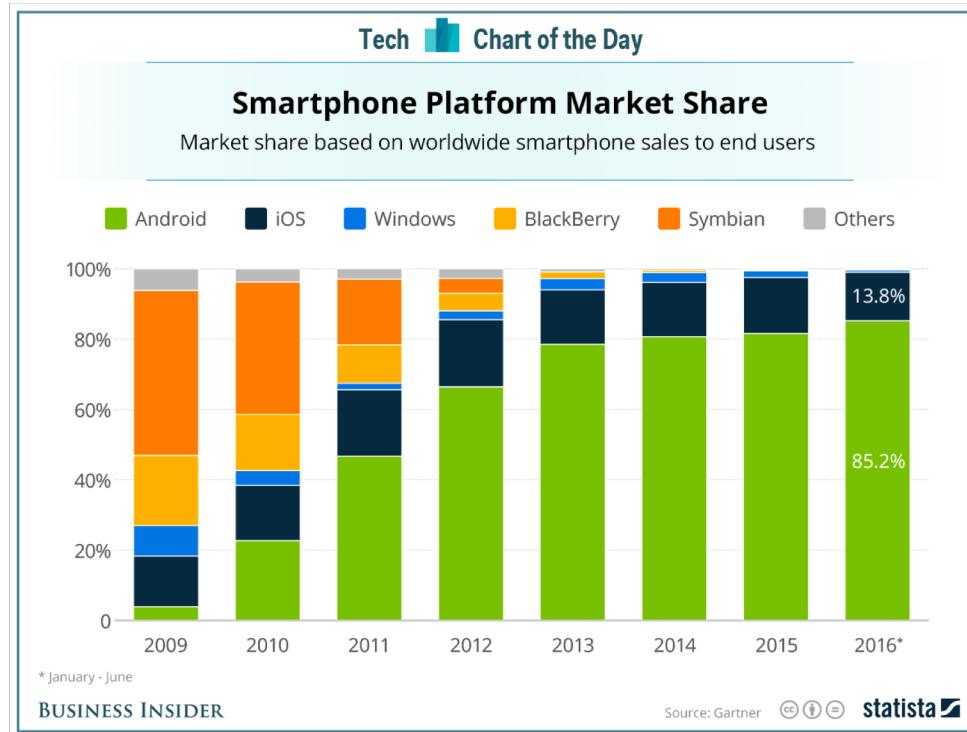
- Hands-on experience on building an app analysis tool that involves:
  - Designing an innovative analysis,
  - Building upon (open source) app analysis tools to analyze apps,
  - Project: Building an app analysis tool that can directly analyze Android apps for security purposes
- Experience in
  - Report writing (project proposal and final project report are required),
  - Project design, demonstration and presentation,
  - Experience in working in a project team

# Course Topics

- Five segments
  - Lectures for basic concepts
  - Labs for tools
  - Paper presentation and discussions
- Segment 1: Android Basics
- Segment 2: Android Permission System
- Segment 3: Textual Artifacts in Android
- Segment 4: Malicious Behaviors
- Segment 5: UI Analysis

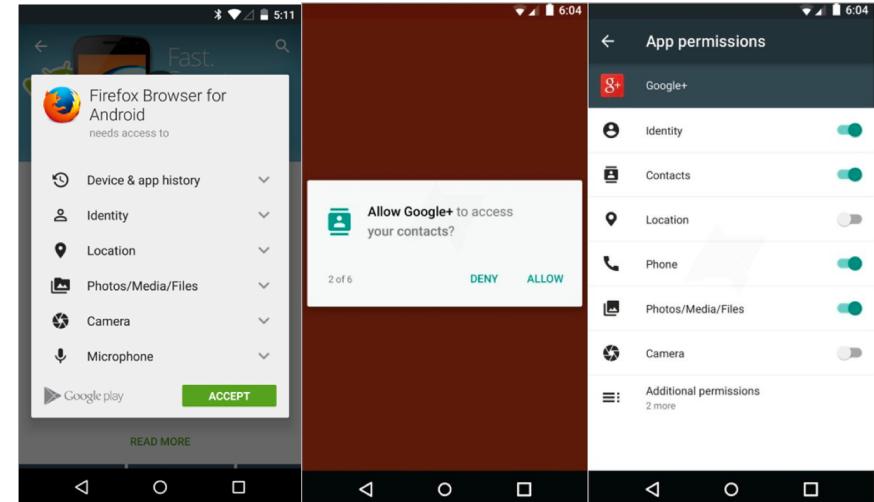
# Android Basics

- Architecture
- Components
- Activity Lifecycle
- Inter-Component Communications



# Android Permission Systems

- Permission System



- Permission Studies:

- PScout: Analyzing the Android Permission Specification
- Android Permissions Demystified
- Understanding the Purpose of Permission Use in Mobile Apps

# Textual Artifacts in Android

← Privacy Policy

If your organization signed a Dropbox for Business Agreement with Dropbox, that Agreement may have modified the privacy policy below. Please [contact your organization's Admin](#) for details.

### Dropbox Privacy Policy

Posted: February 13, 2015

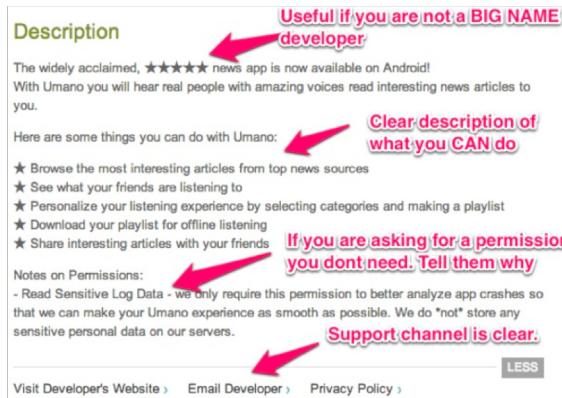
Thanks for using Dropbox! Here we describe how we collect, use and handle your information when you use our websites, software and services ("Services").

#### What & Why

We collect and use the following information to provide, improve and protect our Services:

**Account.** We collect, and associate with your account, information like your name, email address, phone number, payment info, and physical address. Some of our services let you access your accounts and your information with other service providers.

**Services.** When you use our Services, we store,



## App descriptions

## App privacy policy

### User reviews

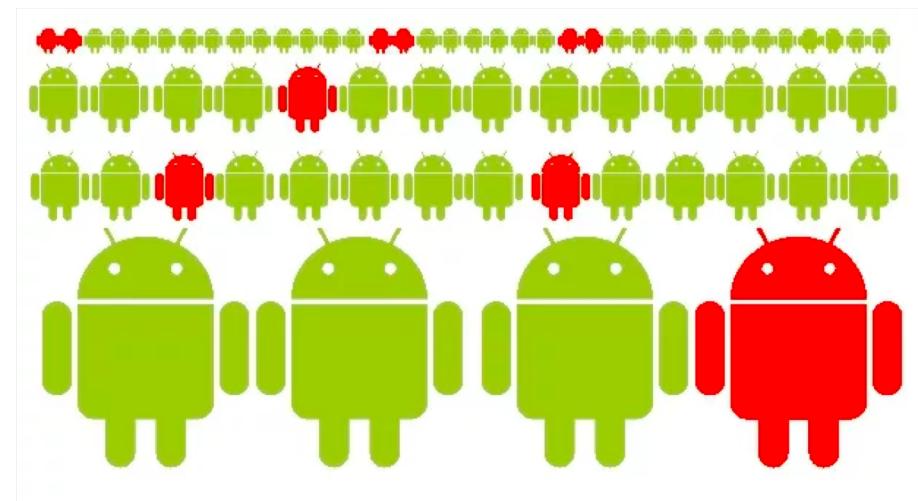
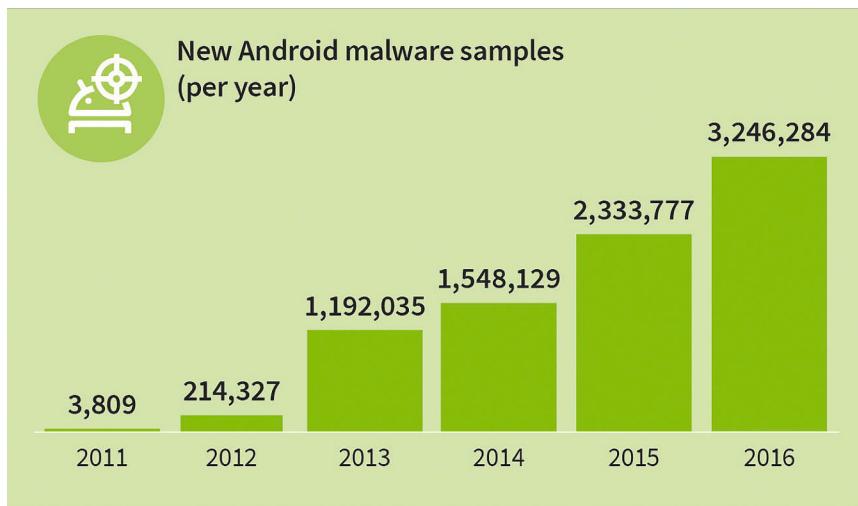
Lavanya Ganta 10 June 2017  
★ ★ ★ ★ ★  
Not interested in this

sampa pattanayak 7 June 2017  
★ ★ ★ ★ ★  
Worst app

Gurmukh Singh 6 June 2017  
★ ★ ★ ★ ★  
Ridiculous

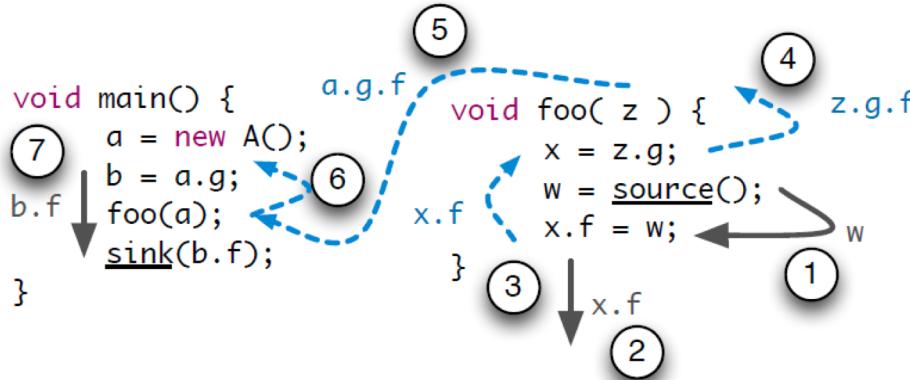
## App reviews

# Potentially Harmful Behavior



- A Study of Android Application Security
- Dissecting Android Malware: Characterization and Evolution

# Static Analysis



## Application analysis workflow

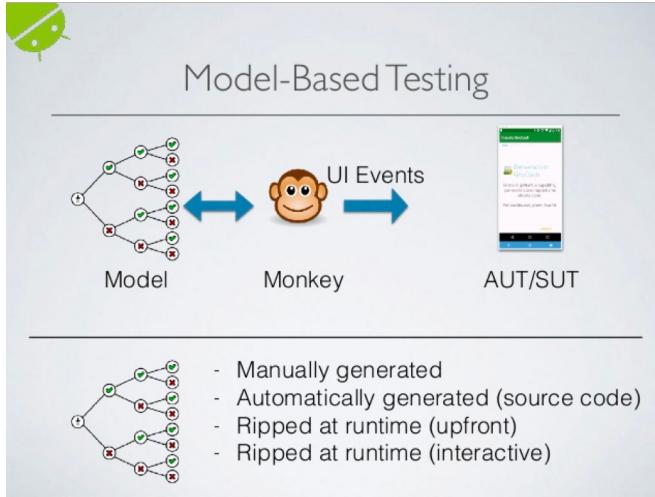
### ■ Static Analysis Tools for Android Apps

TOOL	DESCRIPTION	URL
Dexter	Static android application analysis tool	<a href="https://dexter.bluebox.com/">https://dexter.bluebox.com/</a>
Androguard	Analysis tool (.dex, .apk, .xml, .arsc)	<a href="https://code.google.com/p/androguard/">https://code.google.com/p/androguard/</a>
smali/baksmali	Assembler/disassembler (dex format)	<a href="https://code.google.com/p/smali/">https://code.google.com/p/smali/</a>
apktool	Decode/rebuild resources	<a href="https://code.google.com/p/android-apktool/">https://code.google.com/p/android-apktool/</a>
JD-GUI	Java decompiler	<a href="http://java.decompiler.free.fr/?q=jdgui">http://java.decompiler.free.fr/?q=jdgui</a>
Dex2jar	Disassembler tool for DEX files	<a href="http://dex2jar.sourceforge.net/">http://dex2jar.sourceforge.net/</a>
AXMLPrinter2.jar	Prints XML document from binary XML	<a href="http://code.google.com/p/android4me/">http://code.google.com/p/android4me/</a>
dex2jar	Analysis tool (.dex and .class files)	<a href="https://code.google.com/p/dex2jar/">https://code.google.com/p/dex2jar/</a>
apkinspector	Analysis functions	<a href="https://code.google.com/p/apkinspector/">https://code.google.com/p/apkinspector/</a>
Understand	Source code analysis and metrics	<a href="http://www.scitools.com/">http://www.scitools.com/</a>
Agnitio	Security code review	<a href="http://sourceforge.net/projects/agnitiotool/">http://sourceforge.net/projects/agnitiotool/</a>

OWASP

- <https://securityonline.info/android-malware-analysis-tools/>
- FlowDroid
- AppContext: Differentiating Malicious and Benign Mobile App Behaviors Under Context
- CHEX: Statically Vetting Android Apps for Component Hijacking Vulnerabilities
- Semantics-Aware Android Malware Classification Using Weighted Contextual API Dependency Graphs
- Collaborative verification of information flow for a high-assurance app store

# Dynamic Analysis



- TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones
- Vetting Undesirable Behaviors in Android Apps with Permission Use Analysis
- DroidScope: Seamlessly Reconstructing the OS and Dalvik Semantic Views for Dynamic Android Malware Analysis

# UI Analysis

Credit card type

Select Card Type

Card number

15 or 16 digits

Sensitive

Expiration date

MM - YYYY

Comment:

Insensitive

Submit

- SUPOR: Precise and Scalable Sensitive User Input Detection for Android Apps
- UIPicker: User-Input Privacy Identification in Mobile Applications
- PERUIM: Understanding Mobile Application Privacy With Permission-UI Mapping

# Thank You !



## Questions ?