EECS 448 Smartphone Security

Xusheng Xiao

Electrical Engineering and Computer Science
Case Western Reserve University

Instructor and Lectures

Instructor: Xusheng Xiao, xusheng.xiao@case.com, 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

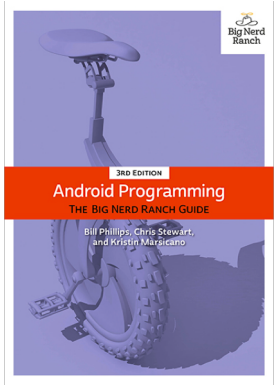
- **Mixed with lectures, labs, and paper presentations/discussions**
- **Project-oriented course**
  - You can learn a set of state-of-the-art Android analysis tools
  - You will build your own tools with innovative analysis on Android apps
- Start installing Java and Android Studio right away
  - https://developer.android.com/studio/index.html

Syllabus

https://docs.google.com/document/d/17gOYOlDY_nowxfL69mhYqUGx4eRVLGvdIXj3vpe1ueQ

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

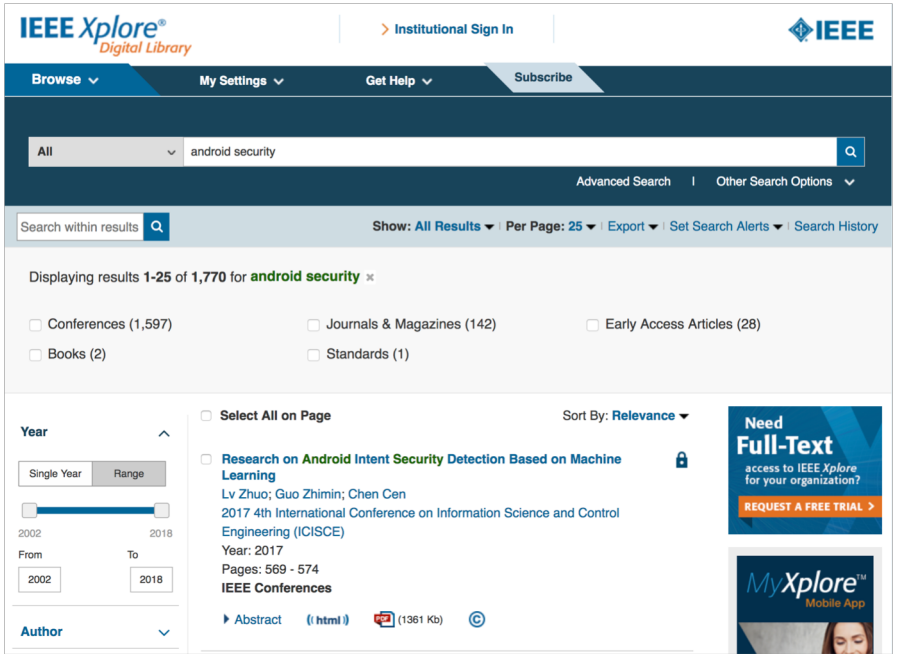
- Paper presentation and discussions
  - Each team is assigned a direction (totally 5 directions, introduced later)
  - Besides recommended papers, you may find related papers to present
  - You may download slides, or make your own!
  - You will write summary of other students' presentations in class

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

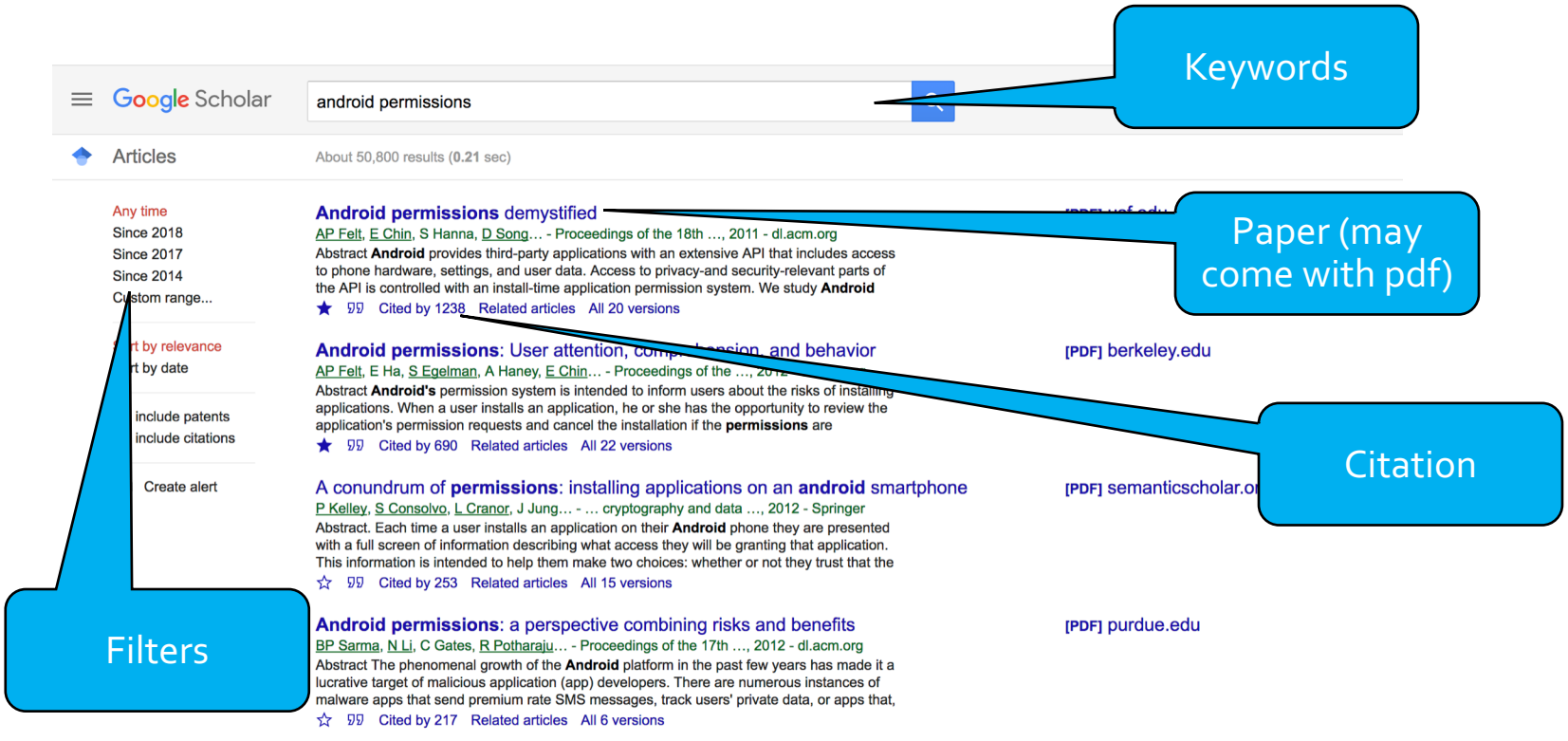
ACM/IEEE Digital Library



http://ieeexplore.ieee.org/

https://dl.acm.org

Google Scholar



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

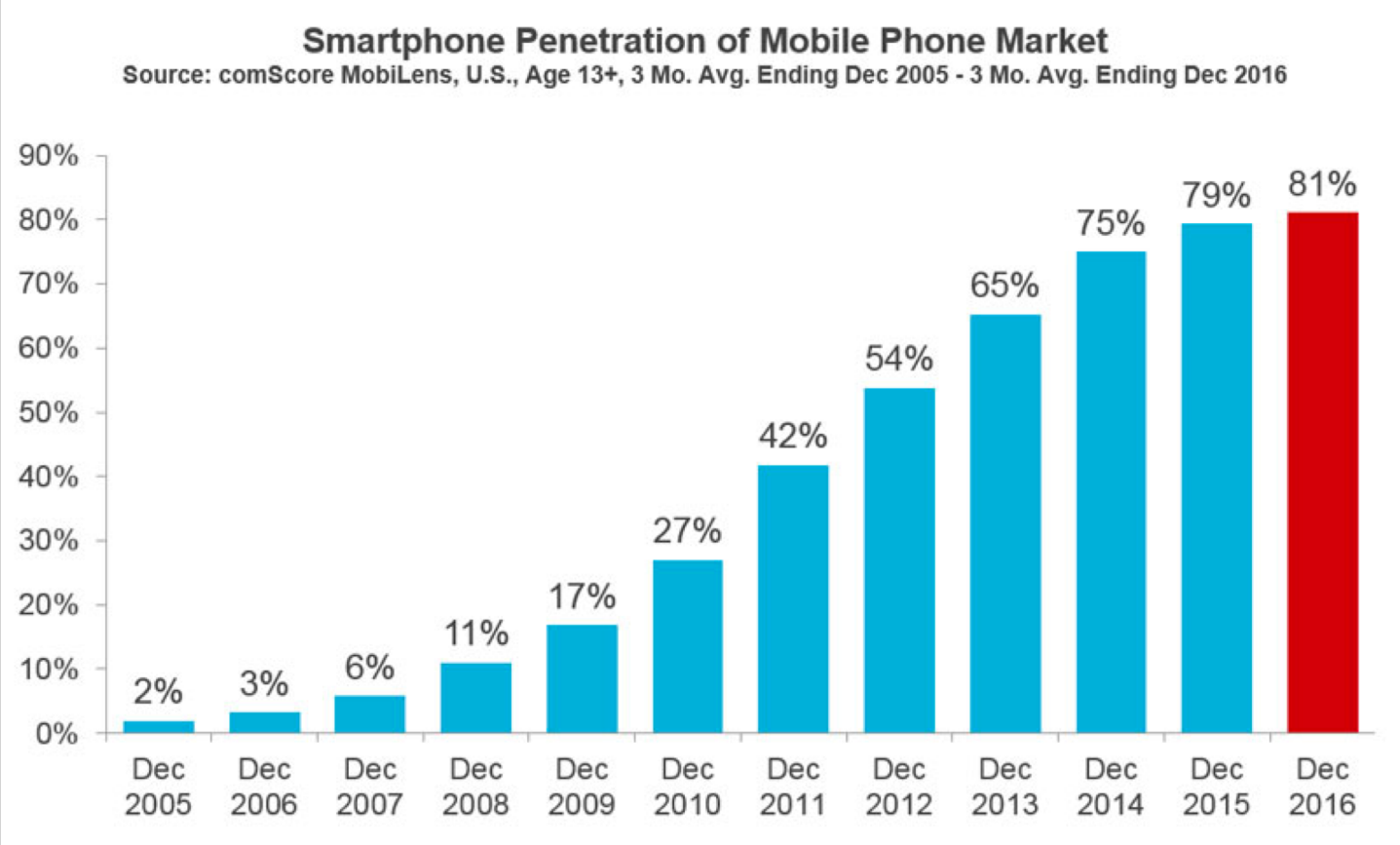
Grading

- 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

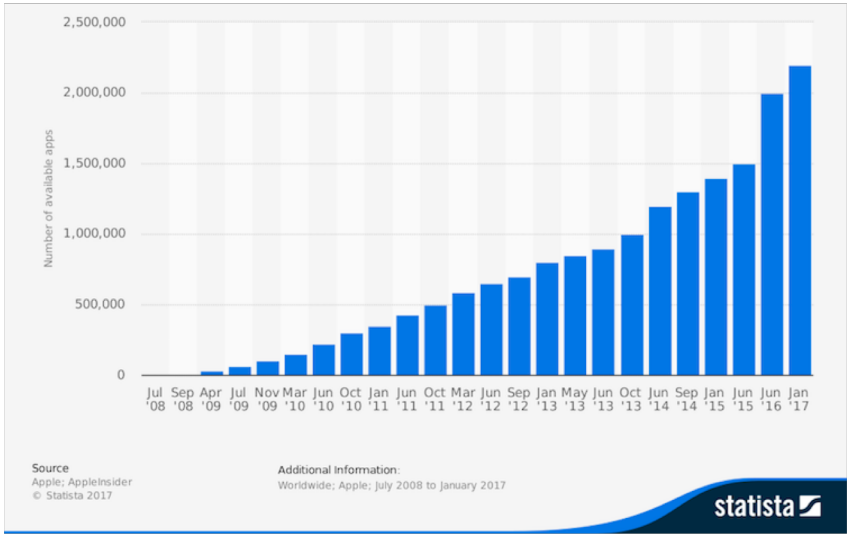
Modern mobile-device platforms provide a central place for distributing software

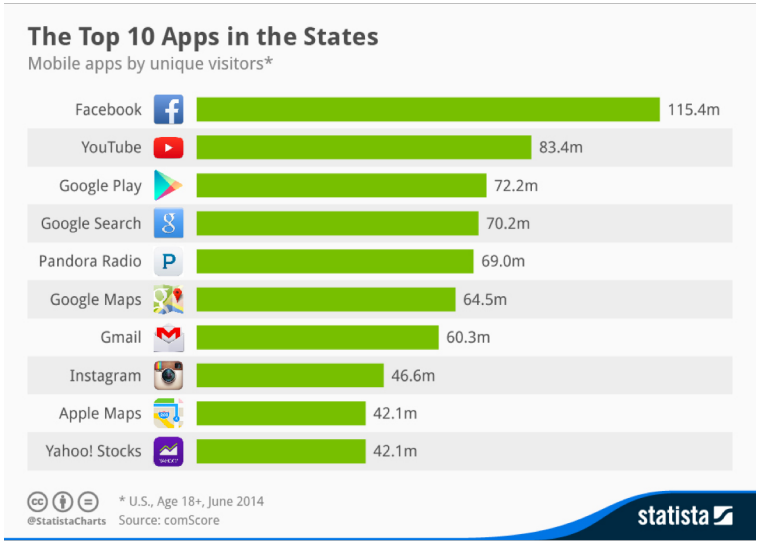
- App Store (iOS) and Google Play
- Third-party applications (apps)

Apple App Store

Google Play

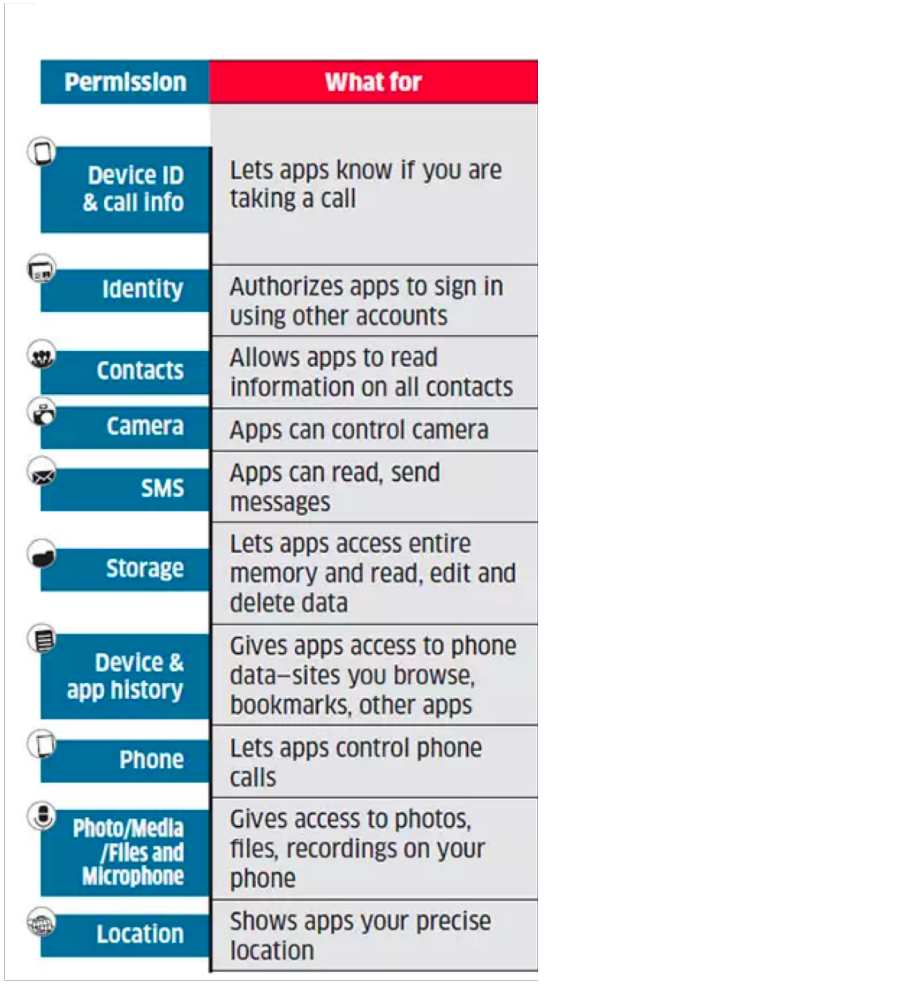
Popularity of Mobile Apps





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

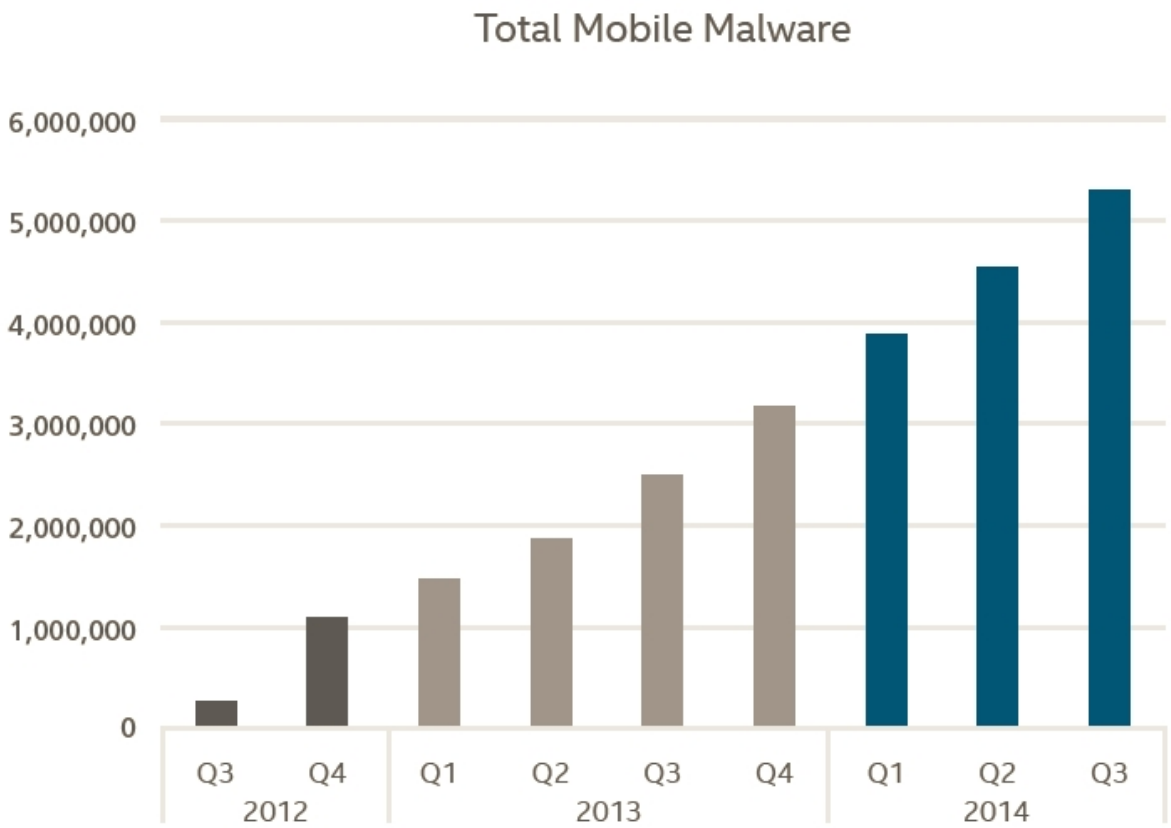
Usage of Personal information



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

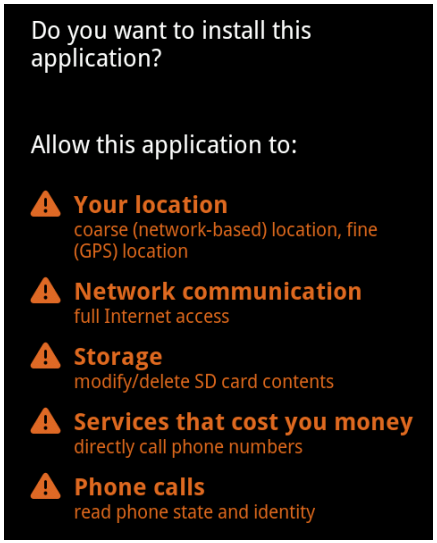


Protection mechanism based on permission system

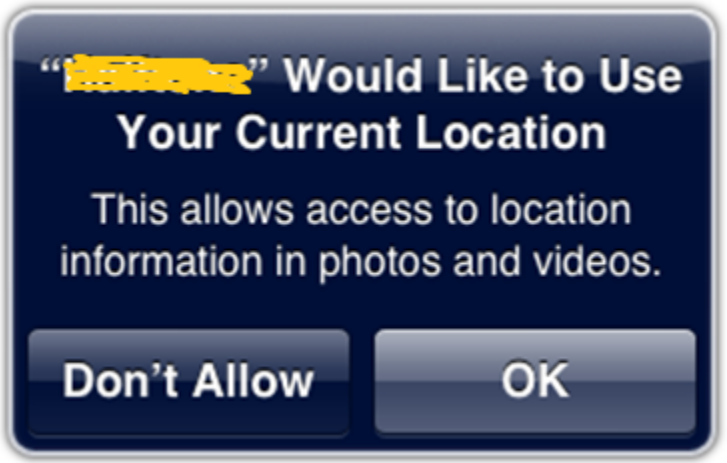
Source: McAfee Labs

Privacy Control in Mobile Platforms

Permission List



Popup Dialog

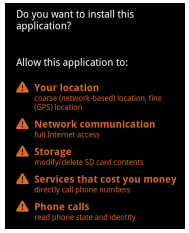


- These approaches report ***what*** permissions to use, not ***how*** or ***why*** permissions are used
- Users simply install applications without questioning the requested permissions

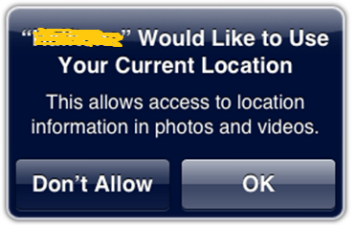
Major Challenges

- Limited assistance for permission granting

Permission List



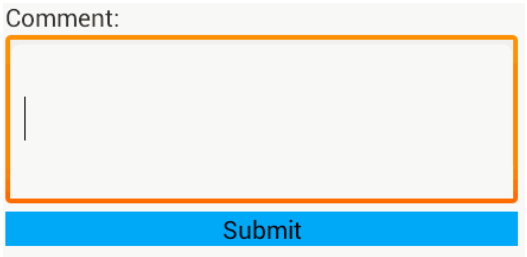
Popup Dialog

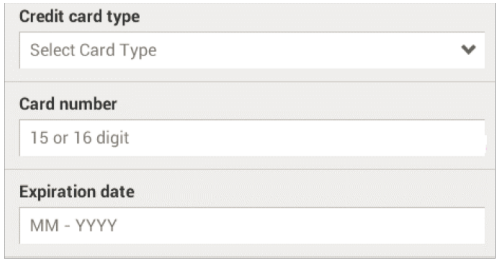


- Limited differentiations of permission uses

Signal Changed

- Limited protection of sensitive user inputs





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

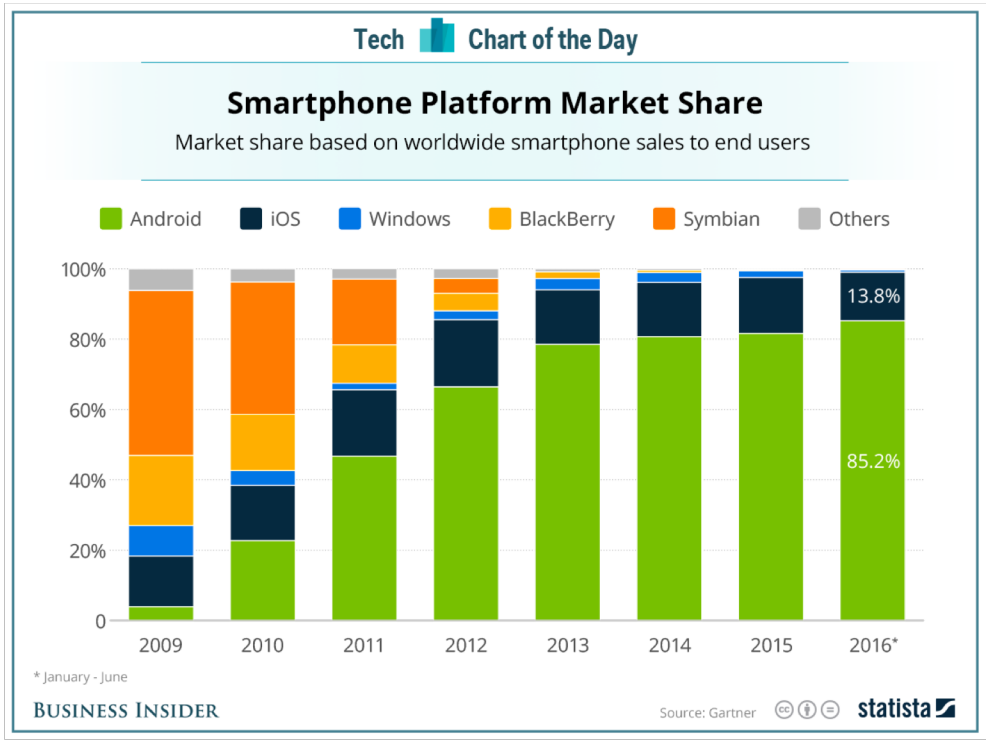
Course Topics

- 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

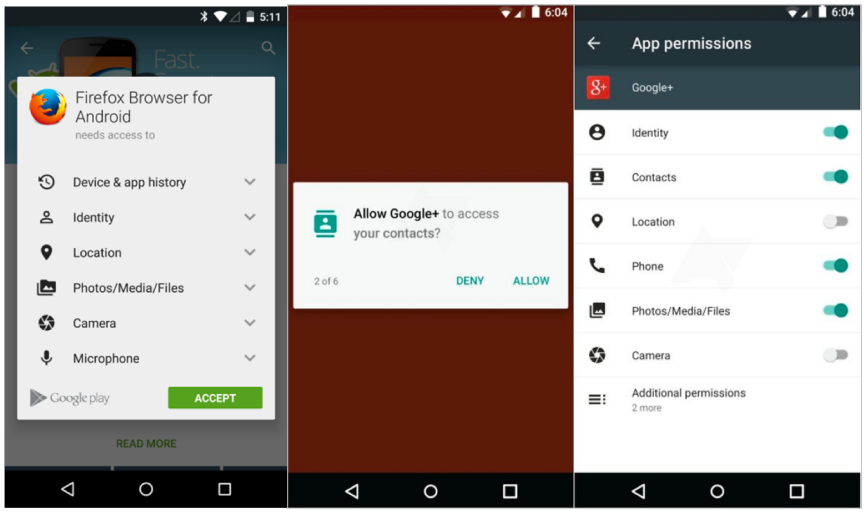
Android Basics

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



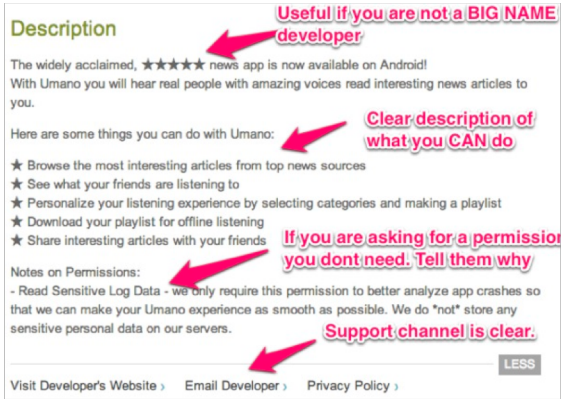
Android Permission Systems

- Permission System

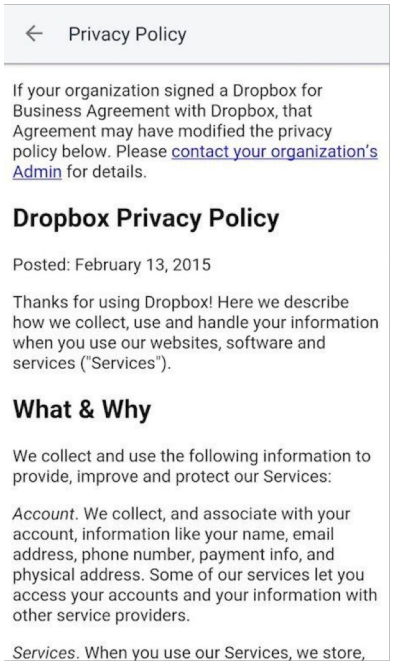


- Permission Studies:
  - PScout: Analyzing the Android Permission Specification
  - Android Permissions Demystified
  - Understanding the Purpose of Permission Use in Mobile Apps

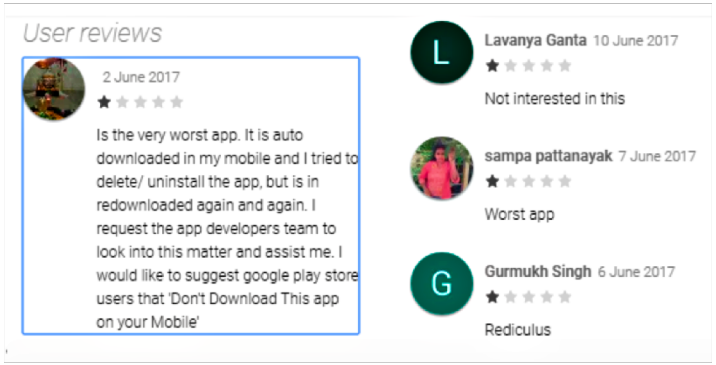
Textual Artifacts in Android



App descriptions

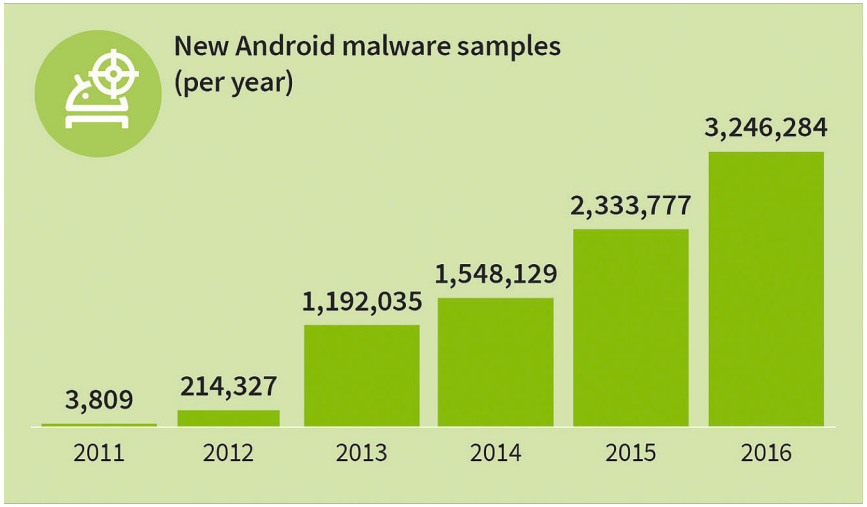


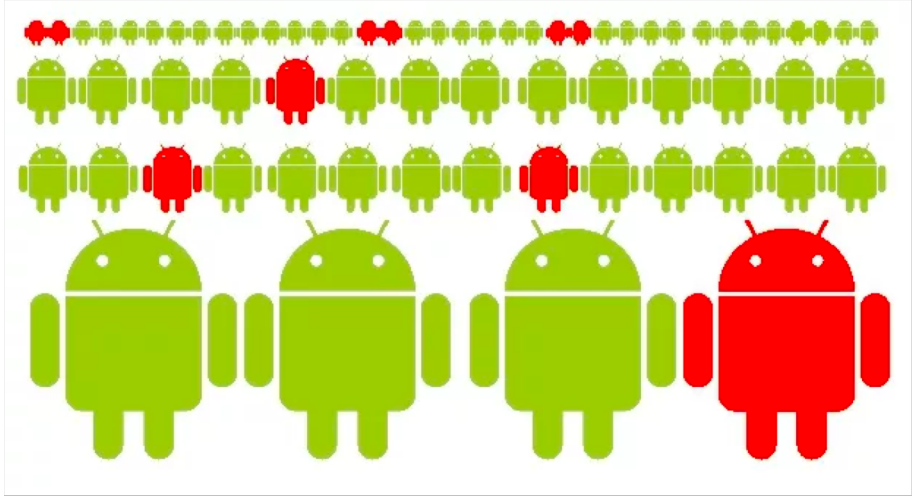
App privacy policy



App reviews

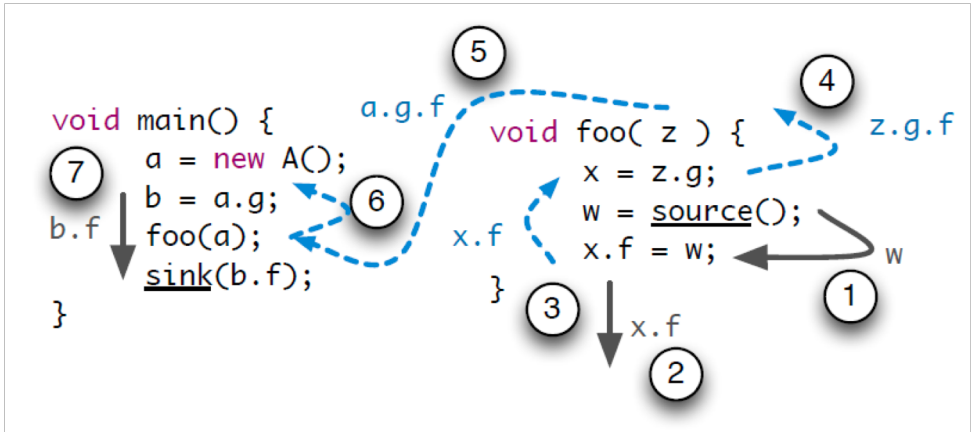
Potentially Harmful Behavior

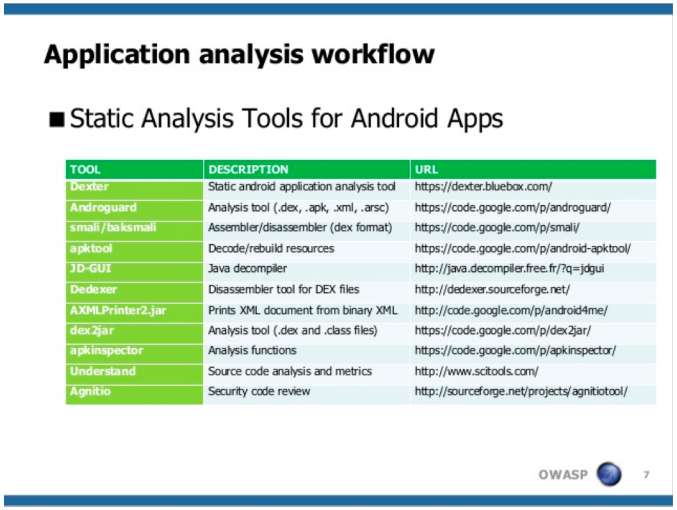




- A Study of Android Application Security
- Dissecting Android Malware: Characterization and Evolution

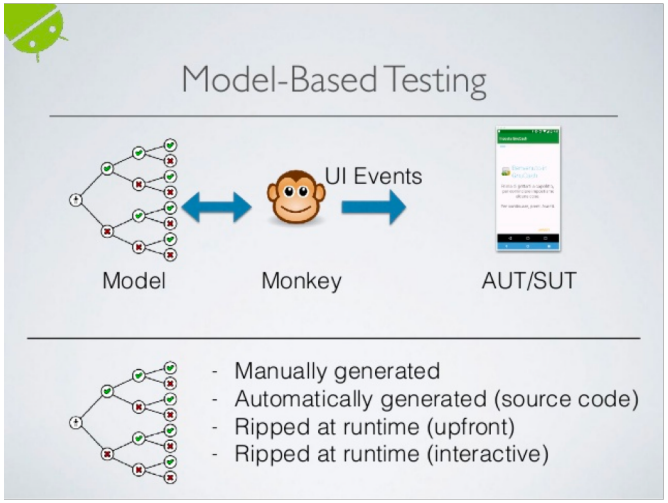
Static Analysis





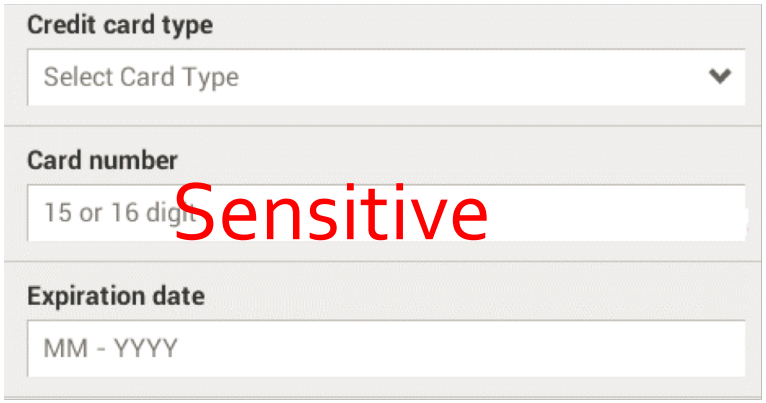
- https://securityonline.info/android-malware-analysis-tools/
- FlowDroid
- AppContext: Differentiating Malicious and Benign Mobile App Behaviors Under Context
- CHEX: Statically Vetting Android Apps for Component Hijacking Vulnerabilities
- Semantics-Aware Android Malware Classification Using Weighted 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



- 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 ?