



openHPI – Internet Security Mobile Apps and Malware

Prof. Dr. Christoph Meinel
Hasso Plattner Institute, Potsdam, Germany

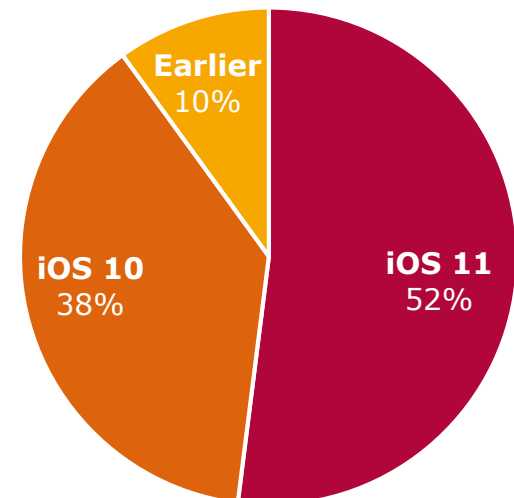
Mobile Platforms

With the widespread use of the mobile operating systems **Android** and **iOS**, the corresponding app stores - **Google Play** and **Apple's App Store** have also grown in importance

- March 2017
 - 2.800.000 Apps in Google Play Store
 - 2.200.000 Apps in Apple App Store

Android Version	Name	Percentage
2.3.X	Gingerbread	0,5%
4.0.X	Ice Cream Sandwich	0,5%
4.1 – 4.3	Jelly Bean	6,2%
4.4	KitKat	13,8%
5.0 – 5.1	Lollipop	27,2%
6.0	Marshmallow	30,9%
7.0 – 7.1	Nougat	20,6%
8.0	Oreo	0,3%

Nov.
2017



Nov.
2017

Basic Concepts (1/2)

Publication of apps

- Developer must log in to the respective store
- Apps are electronically signed by the developer to prevent unintentional changes
- Store operators will review apps for malicious behavior or functionality

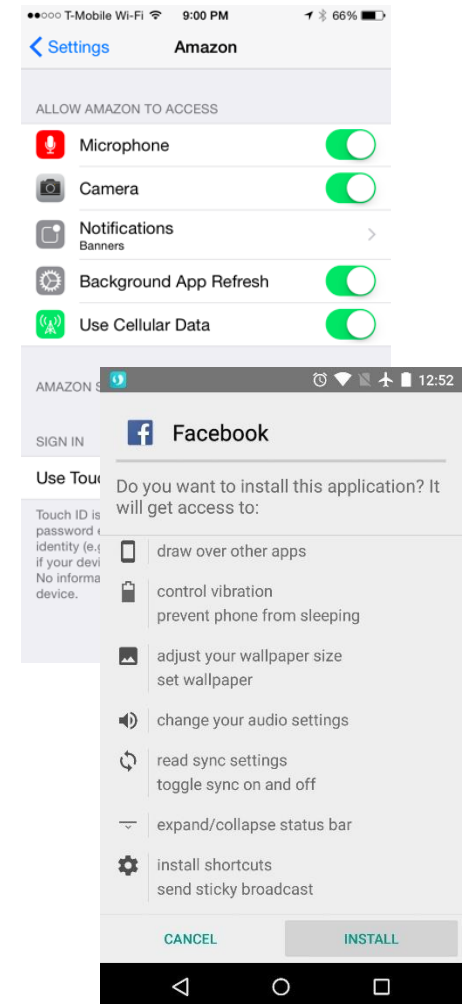
Apps are run in separate environments

- Unauthorized access to the data of other apps is thus prevented
- Information exchange is enabled (e.g., access to contacts in the address book) through defined interfaces and corresponding access rights

Basic Concepts (2/2)

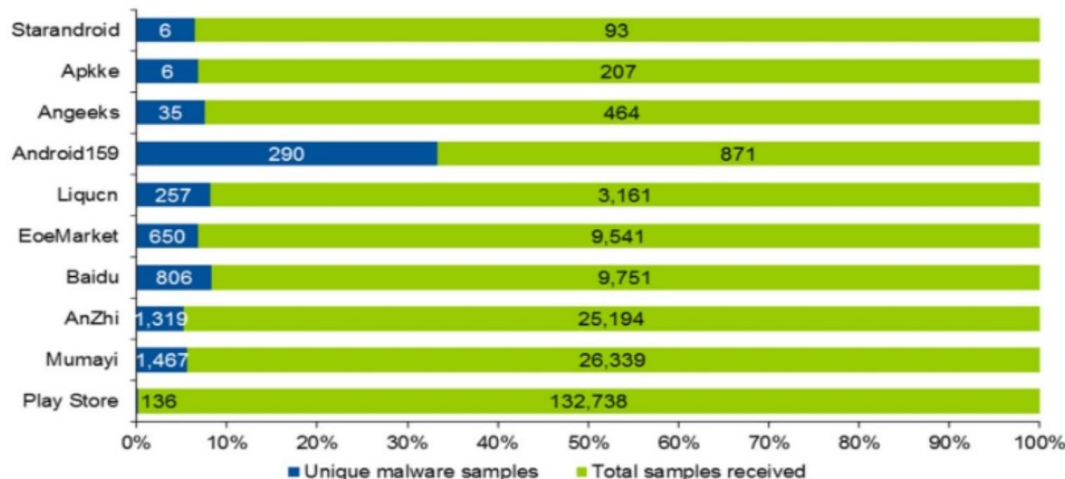
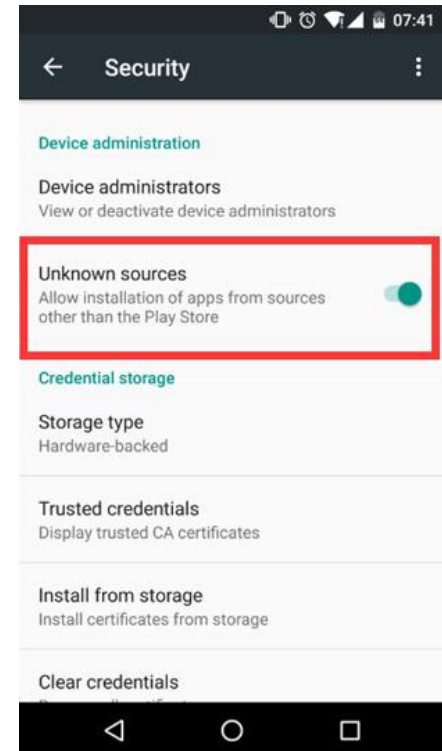
Authorizations

- Allow the user to determine what information an app is allowed to access
- Commonly requested authorizations:
 - ☐ Location
 - ☐ Camera
 - ☐ Address book
 - ☐ ...
- The authorizations requested by an app should be checked and limited if necessary
 - ☐ However, some functionality of the app may be affected if permissions are disabled



Alternative App Stores

- There are a variety of alternative sources through which apps can be downloaded, especially for the Android operating system
- To be able to use alternative app stores, one must allow the installation from unknown sources
- Usually, no extensive checks are carried out in such alternative stores



IBM Security 2016

Mobile Malware

Mobile malware is mainly used for stealing money

- The following methods are often used:
 - Sending premium SMS
 - Performing click fraud
 - Stealing login data for online banking
 - ...
- More malicious functions:
 - Location tracking
 - Theft of private data and information, e.g. pictures or contacts
 - Automatic downloading of other apps

Mobile Malware Examples: Dendroid

Dendroid is an application for remote maintenance that can be used with malicious intent

- Dendroid was developed with the intention of bypassing the "Google Play Store" security check
- Malware can be embedded and distributed over benign apps
- The app contains the following functions:
 - Intercepting and blocking SMS
 - Capturing photos, videos and sound
 - Recording telephone conversations
 - ...



Mobile Malware Examples: ExpensiveWall

ExpensiveWall is a new variant of a malware family that trojanizes various apps

- In September 2017, security researchers identified 50 different infected apps, which were downloaded between 1 million and 4.2 million times
- Malware uses different obfuscation techniques to evade Google Play's built-in anti-malware protections
- Objective of the malware is to register victims to premium services and to send premiums SMS messages

Vulnerabilities in Mobile Operating Systems

Not only malware apps are a security risk, but also vulnerabilities in mobile operating systems

- Android is often customized by each smartphone maker, making it difficult to update the operating system
 - Therefore, most Android smartphones do not receive extensive updates to address weaknesses
- iOS usually only runs on Apple devices like iPhone and iPad, simplifying the development of updates
 - Most devices can receive regular updates as long as the device is still supported

Common Vulnerabilities in Android

- The **Stagefright** (2.0) vulnerability affects the multimedia server component in Android
 - Abuse possible via MMS message and any app supporting multimedia content
 - Enables the execution of malware and the extension of rights
- All Android versions prior to 5.1.1 were vulnerable - 1 billion affected devices (October 2015 estimation)
- Similar vulnerabilities are discovered and patched by Google every month up to now (2 years later)
- Phone manufacturers often does not apply security updates from Google



Protective Measures

- Protecting data in the case of theft of the device
 - Enabling of encryption
 - Use of a PIN, password, ... to unlock
- Updating apps and operating system
 - When purchasing devices ensure that the operating system is still supported and corresponding updates are available
- Install apps only from trustworthy sources
 - These are usually the official stores
- Look closely at authorizations requested by each app
 - Restriction of „unnecessary" authorizations
 - When in doubt, search for alternative apps