ANDROID APP INSTALLATION AND SCANNING

Lecture 15a

COMPSCI 702

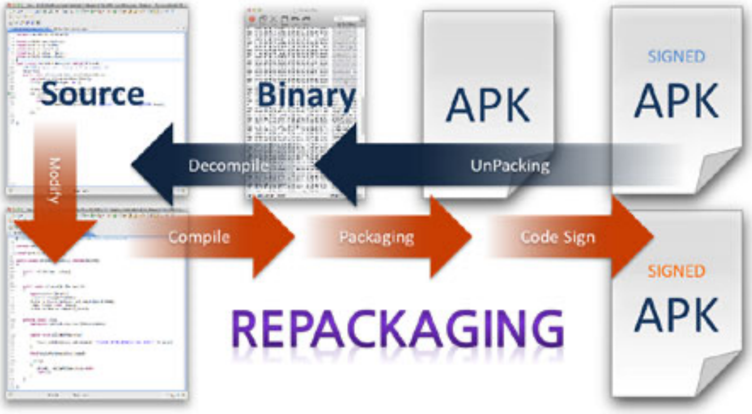
Security for Smart-Devices

Nalin Asanka Gamagedara Arachchilage

Slides from Muhammad **Rizwan** Asghar

April 1, 2021

APP REPACKAGING



- A major attack vector
- Attackers cannot forge signatures
- However, they can remove the original signature and sign the repackaged app using a new certificate
  - Repackaged app encloses a malicious payload
- Android prevents malicious updates but breaks trust on the first time install
- Attracts users to download popular apps that are repackaged

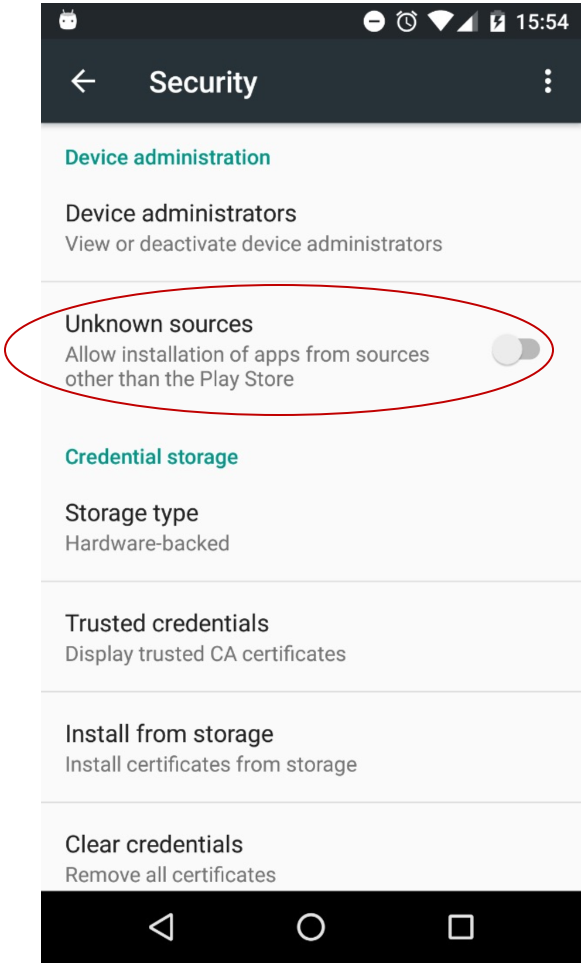
WAYS TO INSTALL ANDROID APPS

- Google Play Store
  - A common way for the most of users
- Sideloading
  - Installing apps from any other source

SIDELOADING

- Sideloading refers to the process of downloading apps from a source other than Google Play Store
- Sideloading is only possible if installation from *"Unknown Sources"* in Security Settings is enabled

ENABLING SIDELOADING



Device administration

Device administrators
View or deactivate device administrators

Unknown sources
Allow installation of apps from sources other than the Play Store

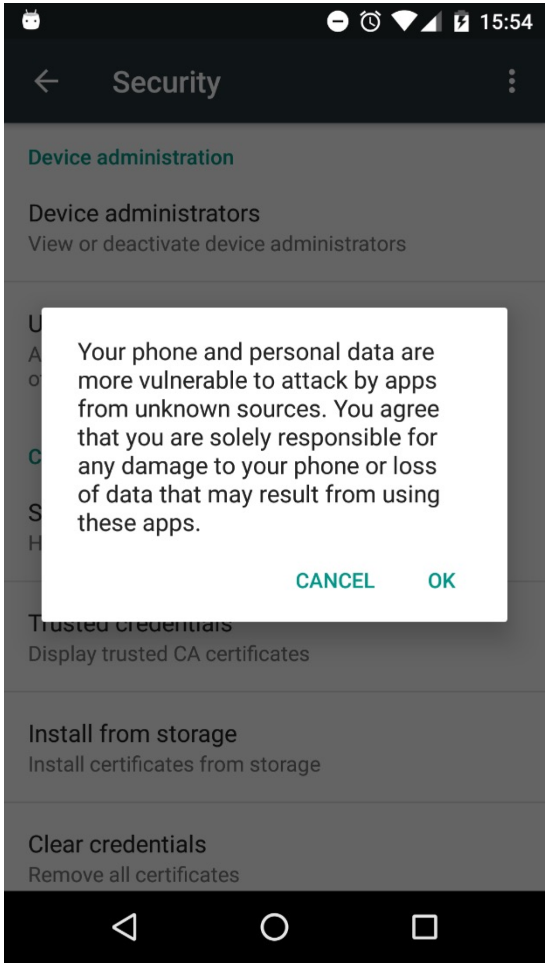
Credential storage

Storage type
Hardware-backed

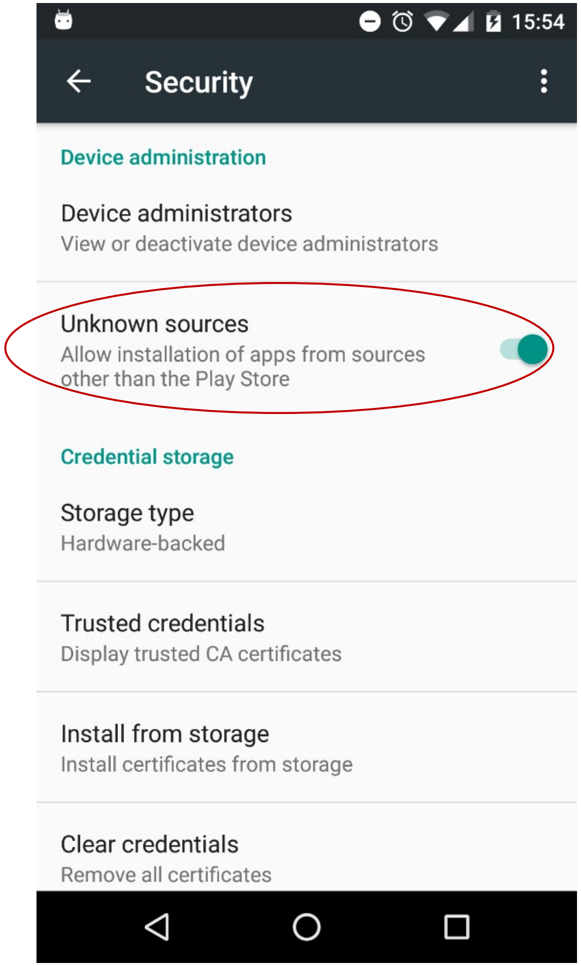
Trusted credentials
Display trusted CA certificates

Install from storage
Install certificates from storage

Clear credentials
Remove all certificates



Your phone and personal data are more vulnerable to attack by apps from unknown sources. You agree that you are solely responsible for any damage to your phone or loss of data that may result from using these apps.



Device administration

Device administrators
View or deactivate device administrators

Unknown sources
Allow installation of apps from sources other than the Play Store

Credential storage

Storage type
Hardware-backed

Trusted credentials
Display trusted CA certificates

Install from storage
Install certificates from storage

Clear credentials
Remove all certificates

SIDELOADING METHODS

- USB
  - adb install MyApp.apk
  - This method is used mostly by app developers
- Bluetooth/WiFi
- Memory card
  - SD card
- Third party app stores
  - E.g., Chinese stores
- Website
- Email

ABOUT DOWNLOADING APPS

- Are you safe as long as you download apps from Google Play Store?

- Will you get hacked when you download apps from any other source?

SECURITY SERVICES BY GOOGLE PLAY

- There are currently two types of security services provided by Google Play for all Android users
  - Protection within Google Play Store
  - Google Play Protect

- There are over 2 billion devices protected by Google Play
  - Source: Google Report, Android Security 2017 Year in Review

PROTECTION WITHIN GOOGLE PLAY STORE

- Google Play Store is Android's app distribution platform that **protects users** from potentially harmful apps

- It has **policies in place** to protect users from attackers trying to distribute potentially harmful apps

- Within Google Play, developers are validated in two stages:
  - Developers are first reviewed when they create their Google Play developer account based on their **profile and credit card**
  - Developers are then reviewed further with additional signals upon app **submission**

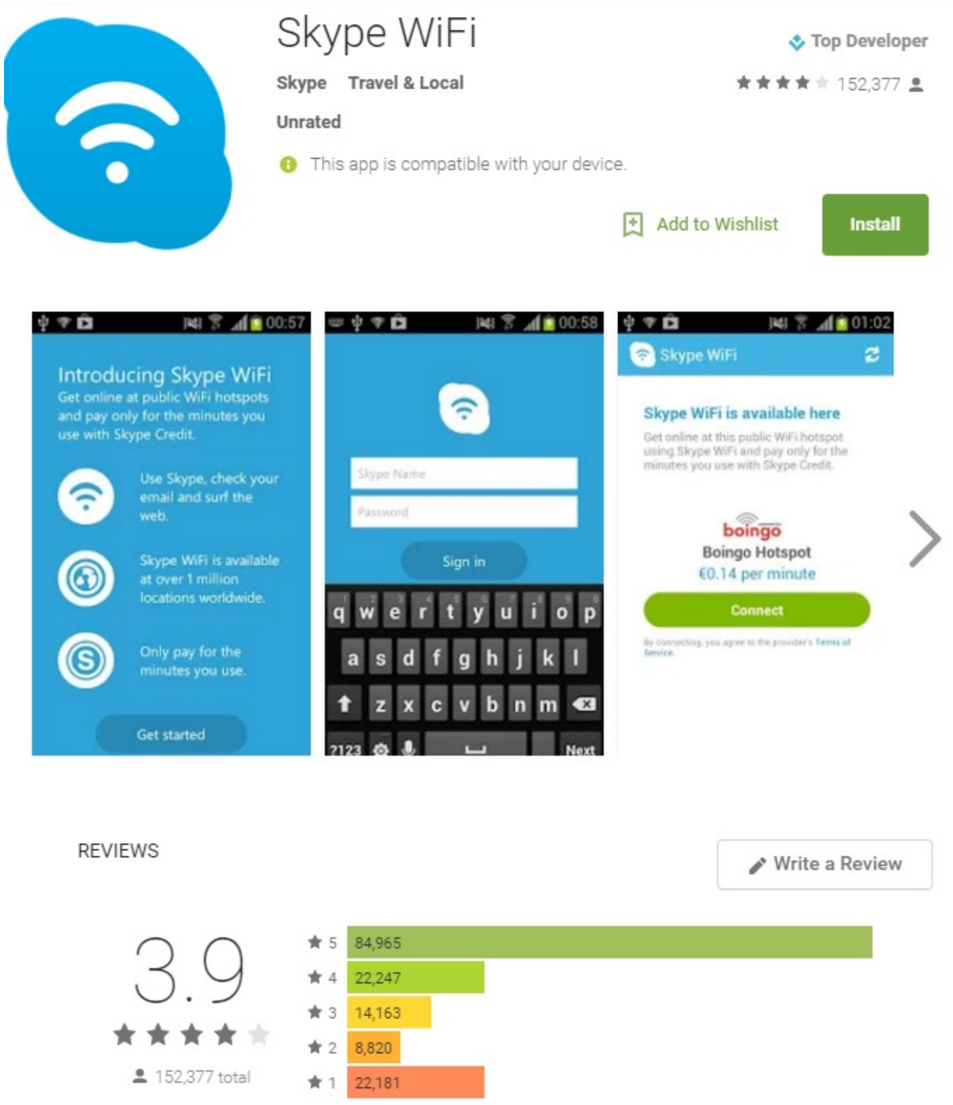
- Google Play **regularly scans** apps for malware and other vulnerabilities

- Google also **suspends developer accounts** that violate developer program policies

GOOGLE PLAY APP REVIEW

- Google Play also has ratings and reviews that provide information about an app before installing it

- If an app tries to mislead users, it is likely to have low star ratings and poor comments



Skype WiFi

Top Developer

Skype Travel & Local

★★★★☆ 152,377

Unrated

This app is compatible with your device.

Add to Wishlist

Install

Introducing Skype WiFi
Get online at public WiFi hotspots and pay only for the minutes you use with Skype Credit.

Use Skype, check your email and surf the web.

Skype WiFi is available at over 1 million locations worldwide.

Only pay for the minutes you use.

Get started

Skype Name

Password

Sign in

Skype WiFi

Skype WiFi is available here
Get online at this public WiFi hotspot using Skype WiFi and pay only for the minutes you use with Skype Credit.

boingo
Boingo Hotspot
€0.14 per minute

Connect

By connecting, you agree to the provider's Terms of Service.

REVIEWS

Write a Review

3.9
★★★★☆
152,377 total

★ 5	84,965
★ 4	22,247
★ 3	14,163
★ 2	8,820
★ 1	22,181

Source: Google Play Store

REMOTE APP REMOVAL BY GOOGLE

- Google removes malicious apps from Android Market
- In cases where users may have installed a malicious app that poses a threat, Google remotely removes that
- If an app is removed in this way, users might receive a notification on their phone

GOOGLE PLAY PROTECT

- Since 2017, Google Play is offering a service called Google Play Protect that provides **protection** from apps outside of Google Play

- Google Play Protect is enabled on over 2 billion devices running Android 4.3+
  - Source: Android Security 2017 Report

- Google Play Protect scans apps **when you install** them and constantly scans for potentially harmful apps

GOOGLE PLAY PROTECT

- By **default**, app verification is turned **on**
- Users can enable or disable Google Play Protect
  - Google > Security > Google Play Protect
- It is successor of Verify Apps
  - Verify Apps was offered in 2012, from Android 2.3+
- Do you think Google Play Protect can identify potentially harmful apps that employ obfuscation?
  - See the Android Security 2017 Report

RESOURCES

- **Chapter 3** of
  Android Security Internals: An In-Depth Guide to Android's Security Architecture
  Elenkov, Nikolay
  First Edition
  No Starch Press 2014
  ISBN:1593275811 9781593275815

- **Google Report, Android Security 2017 Year In Review**
  https://source.android.com/security/reports/Google_Android_Security_2017_Report_Final.pdf

- **Alternative Distribution Options**
  http://developer.android.com/distribute/tools/open-distribution.html

- **Exercising Our Remote Application Removal Feature**
  http://android-developers.blogspot.co.nz/2010/06/exercising-our-remote-application.html

Questions?

Thanks for your attention!