

ANDROID APP DISTRIBUTION

Lecture 14a

COMPSCI 702

Security for Smart-Devices

Nalin Asanka Gamagedara Arachchilage

Slides from Muhammad **Rizwan** Asghar

March 31, 2021



THE UNIVERSITY OF
AUCKLAND
NEW ZEALAND

GOOGLE PLAY STORE



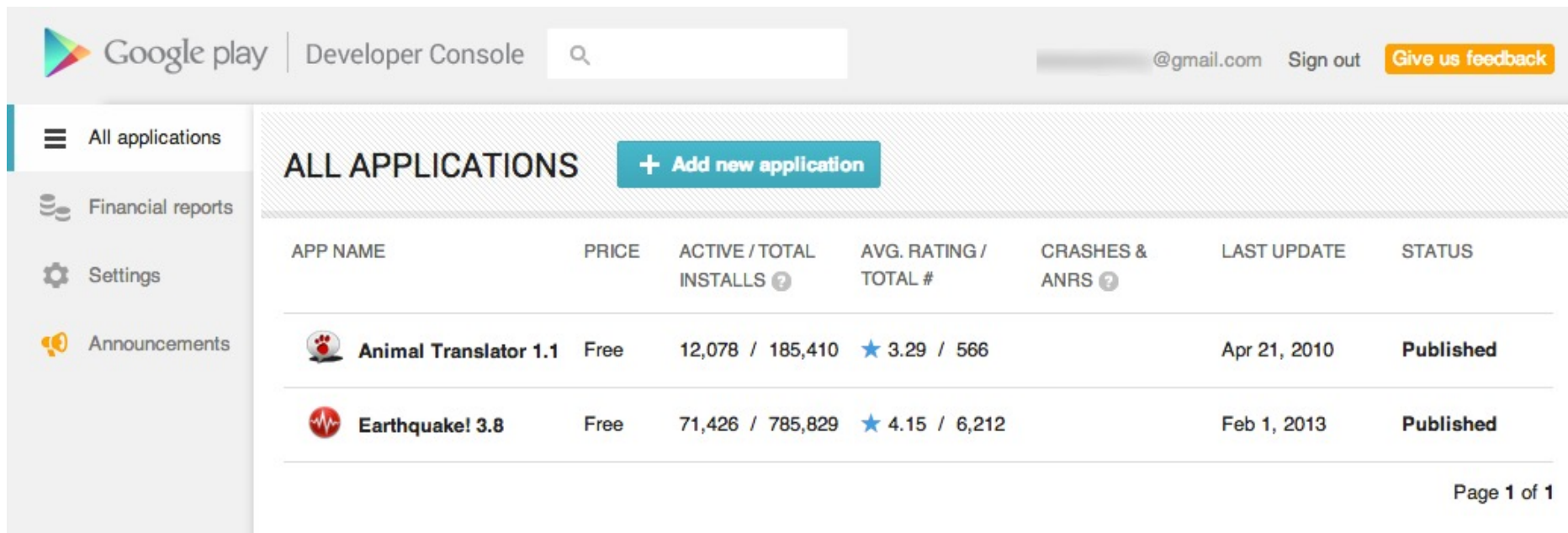
- An app distribution platform operated by Google
- It was introduced on October 22, 2008
- It serves as the official app store for Android
- Apps are available either free of charge or at a cost
- As of April 27, 2020, the Google Play store has reached over **2.885 million apps**
- Over 84.3 billion downloads in 2019 (release January 2020)

GOOGLE PLAY STORE





- To distribute apps, developers have to pay USD 25 as registration fee for a Google Play Developer Console account
- Developers receive **70%** of the app price, while the remaining **30%** goes to the distribution partner and operating fees
- The Play Store apps are not open-source
- Only Android devices that comply with Google's compatibility requirements may install and access apps

DEVELOPER CONSOLE



The screenshot shows the Google Play Developer Console interface. At the top, there is a header with the Google Play logo, the text "Developer Console", a search bar, and user information including "@gmail.com", "Sign out", and a "Give us feedback" button. On the left side, there is a navigation menu with icons and labels for "All applications", "Financial reports", "Settings", and "Announcements". The main content area is titled "ALL APPLICATIONS" and includes a "+ Add new application" button. Below this is a table listing applications with columns for App Name, Price, Active / Total Installs, Avg. Rating / Total #, Crashes & ANRS, Last Update, and Status.

APP NAME	PRICE	ACTIVE / TOTAL INSTALLS ?	AVG. RATING / TOTAL #	CRASHES & ANRS ?	LAST UPDATE	STATUS
 Animal Translator 1.1	Free	12,078 / 185,410	★ 3.29 / 566		Apr 21, 2010	Published
 Earthquake! 3.8	Free	71,426 / 785,829	★ 4.15 / 6,212		Feb 1, 2013	Published

Page 1 of 1

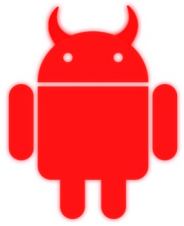
Are these apps benign?

WHAT IS MALWARE?



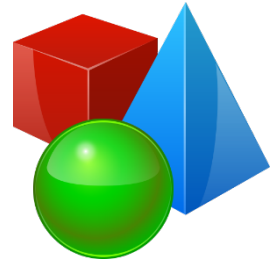
- Malware is an abbreviated term meaning **Malicious Software**
- Any software that can disrupt normal activities
- Any software that does not behave as declared
- Any software that compromises
 - Privacy
 - Confidentiality
 - Reliability
 - ...

ANDROID UNDER ATTACK



- **99%** of mobile malware is on Android
 - Source: [F-SECURE State of Cyber Security](#) (2017)
- On March 17, 2017, Nokia reported a **400% increase** in the past 12 months
 - Source: [nokia.com](#)
- Android malware targeting **NZ and Aus bank apps**
 - Source: [netguide.co.nz](#) (March 10, 2016)

MALWARE TYPES

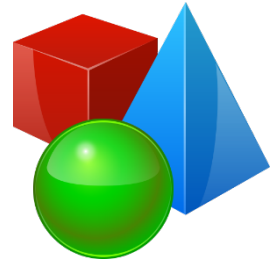


- **Spyware**
 - Collect sensitive information and upload to remote servers
 - E.g., FakeNetflix collects user name and password from Netflix users

- **Destructive trojans**
 - Modify content on the devices
 - E.g., Android.Elite.1.origin (a fake angry bird game)

- **Financial charges**
 - SMS trojan for sending SMS to premium numbers
 - E.g., FakePlayer uses a hard-coded message “798657” and sends it to several premium numbers in Russia

MALWARE TYPES (2)



- Ransomware
 - Stealing data and asking for money to get it back
 - E.g., Police

- Mobile botnets
 - Receive commands from remote Command and Control (C&C) servers
 - E.g., DroidKungFu

- Root-kit exploit
 - All the above and much more!
 - E.g., DroidKungFu

GOOGLE BOUNCER



- Google uses an in-house automated anti-malware system called *Google Bouncer*
- A first line of defence against Android malware
- Google Bouncer aims at filtering out malicious apps
- The Bouncer service emulates Android apps on Google's cloud and looks for anomalies that may be an indicative of malware

ANDROID BOUNCER (2012)

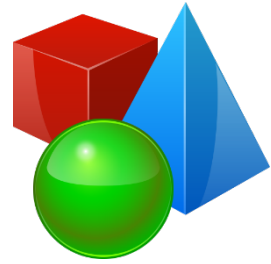


*“Today we’re revealing a service we’ve developed, codenamed Bouncer, which provides **automated scanning** of Android Market for potentially malicious software without disrupting the user experience of Android Market or requiring developers to go through an application approval process.*”

*The service performs a set of analyses on new applications, applications already in Android Market, and developer accounts. Here’s how it works: once an application is uploaded, the service immediately **starts analyzing it for known malware, spyware and trojans**. It also looks for behaviors that indicate an **application might be misbehaving**, and compares it against previously analyzed apps to detect possible red flags. We actually run every application on Google’s cloud infrastructure and **simulate how it will run on an Android device to look for hidden, malicious behavior.**”*

Source: <http://googlemobile.blogspot.co.nz/2012/02/android-and-security.html>

WHAT KIND OF ANALYSIS?



- **Static analysis**
 - It does not require code execution
 - Typically, a static analysis tool will inspect the program for all possible runtime behaviours to seek out potentially malicious code
 - It offers full coverage, but less reliable
- **Dynamic analysis**
 - It requires code execution to determine flow of the program
 - Typically, a dynamic analysis tool examines runtime behaviour of the app only on given inputs
 - It is more reliable, but lacks coverage
- **Hybrid analysis**
 - A mix of static and dynamic analysis

GOOGLE ANNOUNCEMENT (2015)



*“Several months ago, we **began reviewing apps before they are published** on Google Play to better protect the community and improve the app catalog. This new process **involves a team of experts** who are responsible for identifying violations of our developer policies earlier in the app lifecycle. We value the rapid innovation and iteration that is unique to Google Play, and will continue to help developers get their products to market within a matter of hours after submission, rather than days or weeks. In fact, there has been no noticeable change for developers during the rollout.*

To assist in this effort and provide more transparency to developers, we’ve also rolled out improvements to the way we handle publishing status. Developers now have more insight into why apps are rejected or suspended, and they can easily fix and resubmit their apps for minor policy violations.”

Source:

<http://android-developers.blogspot.co.nz/2015/03/creating-better-user-experiences-on.html>



Questions?

Thanks for your attention!