DISSECTING GOOGLE BOUNCER
Lecture 14b

COMPSCI 702
Security for Smart-Devices

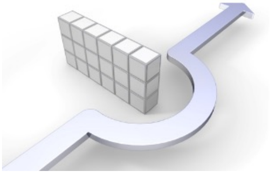
Nalin Asanka Gamagedara Arachchilage

Slides from Muhammad **Rizwan** Asghar

April 1, 2021

THE UNIVERSITY OF AUCKLAND NEW ZEALAND

BOUNCER WAS EASILY BYPASSED



- No surprise
- Google is trying to solve a very difficult problem
- Story of how Bouncer was analysed

GETTING STARTED

- How to proceed for dissecting Bouncer?
- There are lots of unanswered questions

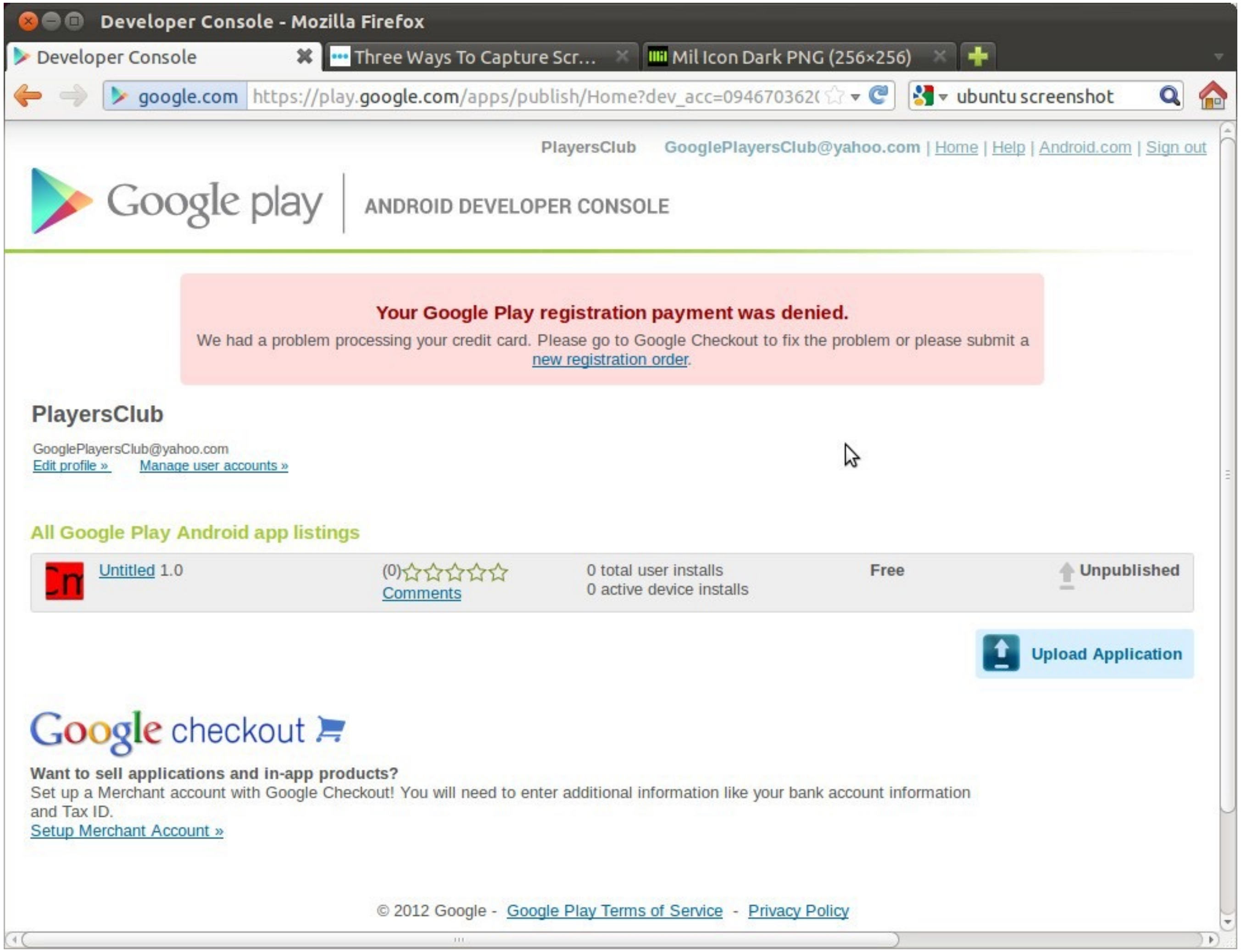
SOME UNANSWERED QUESTIONS

- Does Bouncer use static or dynamic analysis?
- When does Bouncer analyse the app?
- Are all apps analysed?
- Network access: is it open, filtered, or emulated?
- Environment: what is the system execution environment?
- Timing: how long does our app run?
- Input: is there any artificial input to the app?

WHAT WE NEED

- Money
- Prepaid phones
- Prepaid credit cards

PAYMENT LOOPHOLE


Developer Console - Mozilla Firefox
Developer Console
Three Ways To Capture Scr...
Mil Icon Dark PNG (256×256)
google.com https://play.google.com/apps/publish/Home?dev_acc=094670362(
ubuntu screenshot

PlayersClub GooglePlayersClub@yahoo.com | Home | Help | Android.com | Sign out

Google play | ANDROID DEVELOPER CONSOLE

Your Google Play registration payment was denied.

We had a problem processing your credit card. Please go to Google Checkout to fix the problem or please submit a new registration order.

PlayersClub

GooglePlayersClub@yahoo.com
Edit profile » Manage user accounts »

All Google Play Android app listings

Untitled 1.0	(0)☆☆☆☆☆ Comments	0 total user installs 0 active device installs	Free	Unpublished

Upload Application

Google checkout

Want to sell applications and in-app products?
Set up a Merchant account with Google Checkout! You will need to enter additional information like your bank account information and Tax ID.
Setup Merchant Account »

© 2012 Google - Google Play Terms of Service - Privacy Policy

It was possible to submit apps without paying!

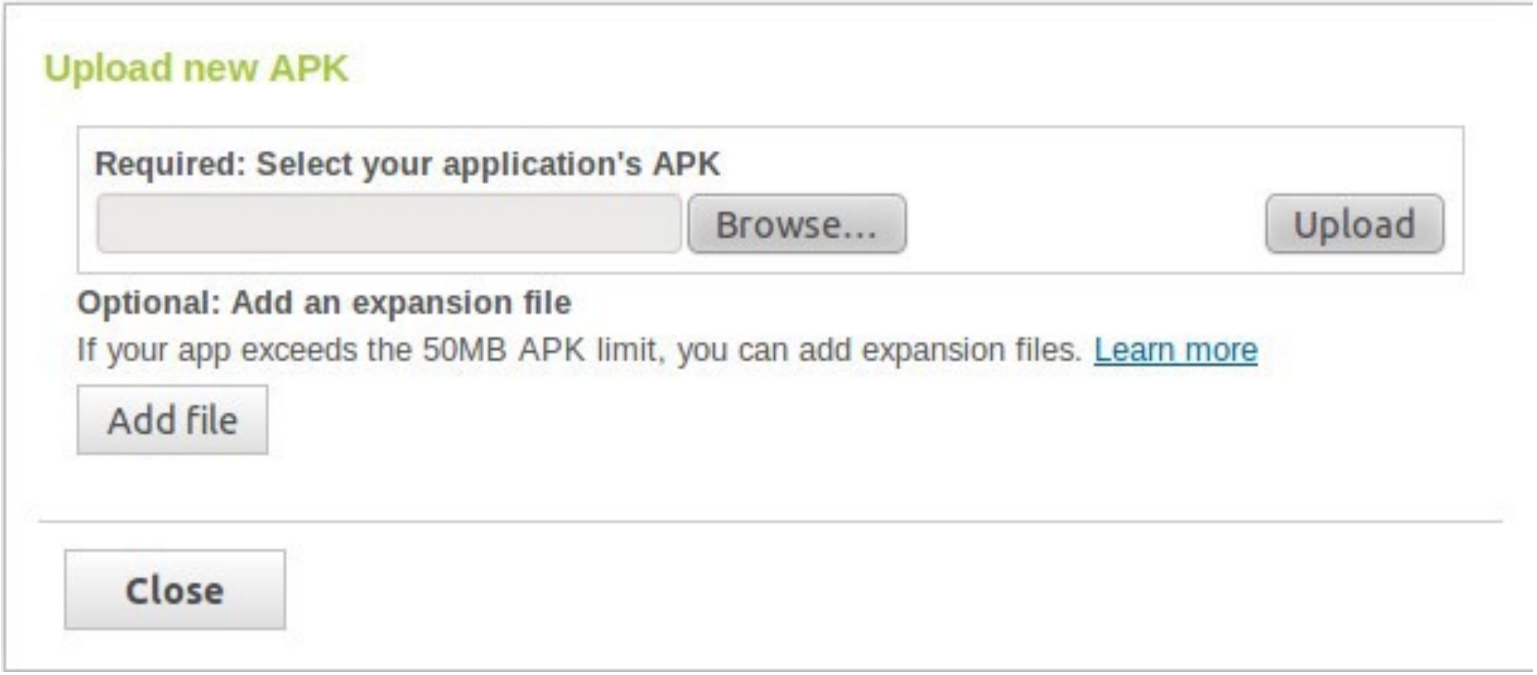
HOW TO PROCEED

- Submit a sample app that connects to the Command and Control (C&C) server

- First do not do any harm

- See what happens

SUBMISSION STEP 1



Upload new APK

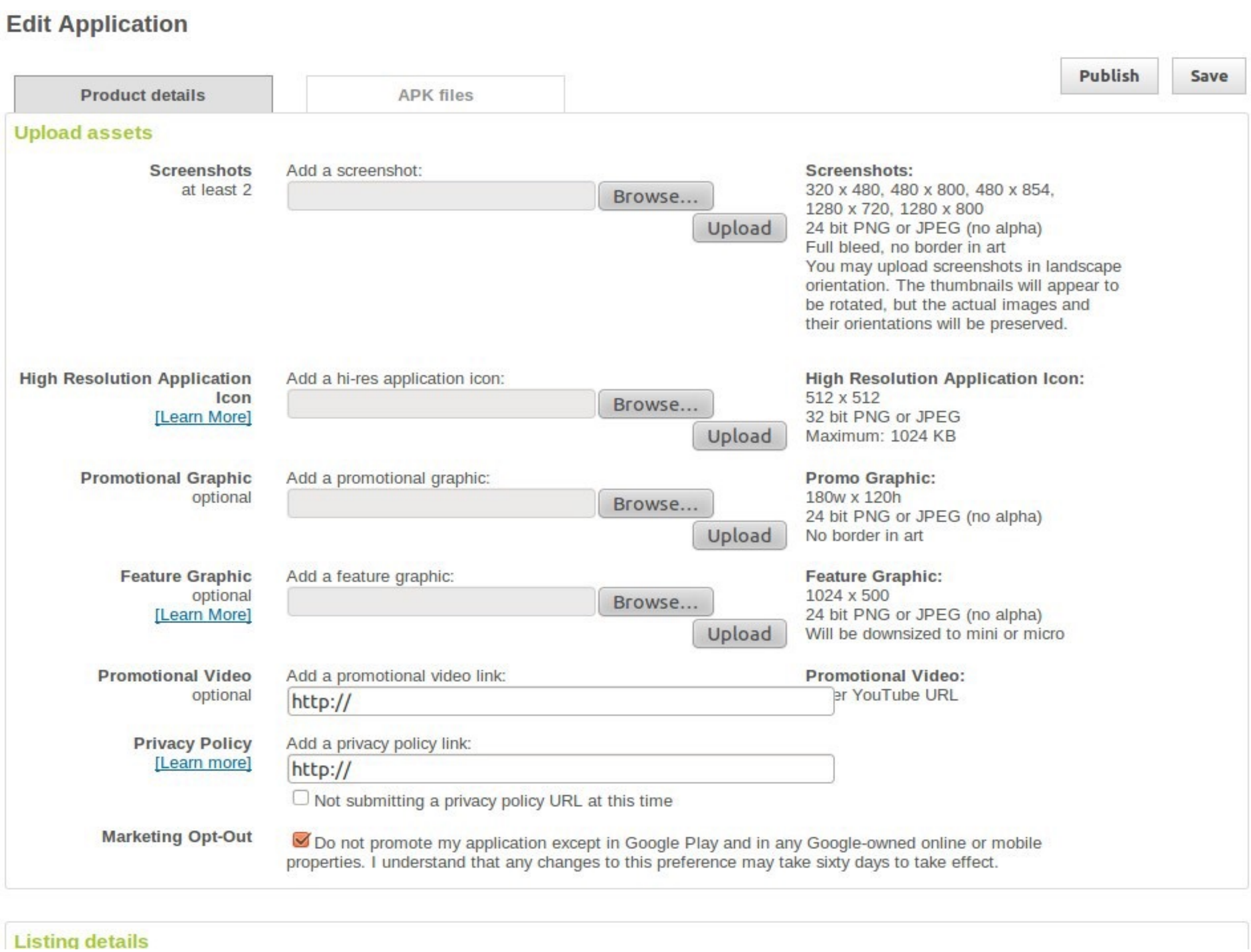
Required: Select your application's APK

Optional: Add an expansion file

If your app exceeds the 50MB APK limit, you can add expansion files. Learn more

Upload your APK

SUBMISSION STEP 2



Edit Application

Upload assets

Screenshots
at least 2

Add a screenshot:

Screenshots:
320 x 480, 480 x 800, 480 x 854,
1280 x 720, 1280 x 800
24 bit PNG or JPEG (no alpha)
Full bleed, no border in art
You may upload screenshots in landscape orientation. The thumbnails will appear to be rotated, but the actual images and their orientations will be preserved.

High Resolution Application Icon
[Learn More]

Add a hi-res application icon:

High Resolution Application Icon:
512 x 512
32 bit PNG or JPEG
Maximum: 1024 KB

Promotional Graphic
optional

Add a promotional graphic:

Promo Graphic:
180w x 120h
24 bit PNG or JPEG (no alpha)
No border in art

Feature Graphic
optional
[Learn More]

Add a feature graphic:

Feature Graphic:
1024 x 500
24 bit PNG or JPEG (no alpha)
Will be downsized to mini or micro

Promotional Video
optional

Add a promotional video link:
http://

Promotional Video:
er YouTube URL

Privacy Policy
[Learn more]

Add a privacy policy link:
http://

☐ Not submitting a privacy policy URL at this time

Marketing Opt-Out

☑ Do not promote my application except in Google Play and in any Google-owned online or mobile properties. I understand that any changes to this preference may take sixty days to take effect.

Listing details

Fill in the app metadata

SUBMISSION STEP 3

- Press ‘Save’ button

-
  ```
  74.125.19.84 - - [08/Apr/2012:23:33:05 -0400]
  "GET /?id=9774d56d682e549c HTTP/1.1" 200 5 "-"
  "Apache-HttpClient/UNAVAILABLE    (java 1.4)" "-"
  ```

- Looks like Bouncer ran the app!
  - Before it was actually published to the market!

BOUNCER IN A NUTSHELL

- Runtime analysis of app
- Emulated Android environment
- Runs for 5 minutes
- On Google's infrastructure
- Allows external network access

FINGERPRINT CLASSIFICATION

- Underlying system
  - Linux, QEMU emulator, system properties, etc.
- Android framework
  - Sensors: camera, accelerometer, GPS, etc.
  - Data sources: address book, SMS, photos, files, etc.
- Environment and behaviour
  - IP addresses, timing attacks, input automation, etc.

SYSTEM/QEMU IDENTIFIERS

- Lots of information
  - *\/proc/cpuinfo*: goldfish
  - Obvious QEMU stuff: */sys/qemu_trace*, etc.
  - And much more …
- Fingerprinting QEMU
  - Based on emulation discrepancies
  - Using the following technique, it was possible to fingerprint the exact QEMU version (and exploit)
    - Paleari, Roberto, Lorenzo Martignoni, Giampaolo Fresi Roglia, and Danilo Bruschi. "A fistful of red-pills: How to automatically generate procedures to detect CPU emulators." In Proceedings of the USENIX Workshop on Offensive Technologies (WOOT), vol. 41, p. 86. 2009.
    - Link: http://static.usenix.org/event/woot09/tech/full_papers/paleari.pdf

SYSTEM VITAL SIGNS

	Galaxy Nexus	Bouncer*
Brand	Google	Tmobile
CPUABI	arbeabi-v7a	armeabi
CPUABI2	armeabi	unknown
Host	vpbs3.mtv.corp.google.com	android-test-2.mtv.corp.google.com
Manufacturer	Samsung	HTC
Model	Galaxy Nexus	T-Mobile myTouch 3G
Product	yakju	opal
Serial	01469107030XXXXX	unknown

*May be a version dependent on requested the SDK version of submitted app

INVASIVE VITAL SIGNS

	Galaxy Nexus	Emulator	Bouncer*
Phone number	1248760XXXX	15555215554	15555215504
Phone device	358350040XXXXXX	000000000000000	112358132134559
Phone serial	8901260362485XXXXXX	89014103211118510720	89014103211118510720
SIM name	T-Mobile	Android	T-Mobile
Network name	T-Mobile	Android	T-Mobile

*May be a version dependent on requested the SDK version of submitted app

MORE VITALS

- Android ID: 9774d56d682e549c
  - Emulators return this ID
  - Some older phones return this as well
  - Link: http://stackoverflow.com/questions/6106681/android-ho

- More recent tests indicate this ID may be changing or dynamic

BOUNCER’S OWNER

- Google account associated with the Bouncer device:
  - base64.b64decode('OyBtaWxlcy5rYXJsc29uQGdtYWlsLmNvbSwgY29tLmdvb2dsZQ==');
  - miles.karlson@gmail.com

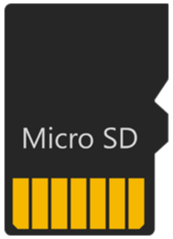
CONTACT DATABASE

- Who does Miles Karlson hang out with?
  - Check out the Android contact list

- 74.125.184.94 [10/May/2012:09:34:19 0500] "GET
  /index.html?
  q=TWljaGVsbGUgTGV2aW4gbWljaGVsbGUuay5sZXZ
  p bkBnbWFpbC5jb20= HTTP/1.1" 200 44

- michelle.k.levin@gmail.com

SDCARD CONTENTS



- download/cat.jpg
- download/lady-gaga-300.jpg
- DCIM/Camera/IMG_20120302_142816.jpg
- android/data/passwords.txt

BOUNCER IP RANGE

- Bouncer allows Internet access
- So what IPs does it come from?
  - 74.125.0.0/16
  - Also in recent tests: 209.85.128.0/17
  - Manual review: 173.194.99.0/16
-
  ```
  $ whois 74.125.19.84 | grep OrgName
  OrgName: Google Inc.
  ```
-
  ```
  $ whois 173.194.99.18 | grep OrgName
  OrgName: Google Inc.
  ```

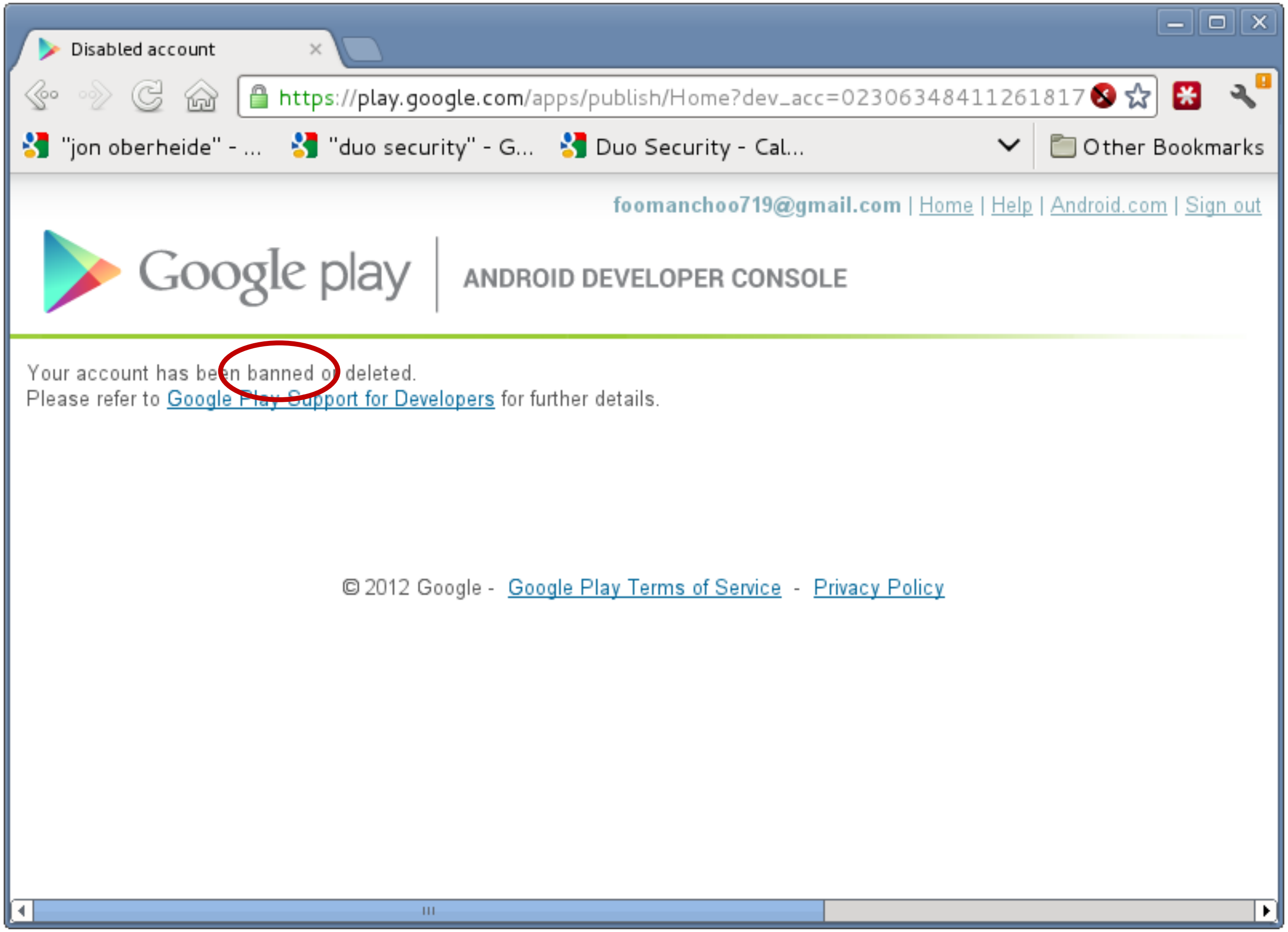
TIME CONSIDERATIONS

- Bouncer runs your app for 5 minutes
- Do not do anything bad for 5 minutes!
- Bouncer is not a physical device, QEMU is SLOW!

INPUT EMULATION

- Bouncer explores the app by emulating input, clicking, etc.
- 74.125.184.81   [10/May/2012:10:41:10 0500]
  "GET /foo?**q=opened** HTTP/1.1" 200 413
- 74.125.184.89 [10/May/2012:10:41:11 0500]
  "GET /foo?**q=after_alert** HTTP/1.1" 200 413
- 74.125.184.32 [10/May/2012:10:41:41 0500]
  "GET /foo?**q=clicked_ok** HTTP/1.1" 200 413
- 74.125.184.89 [10/May/2012:10:41:48 0500]
  "GET /foo?**q=clicked** HTTP/1.1" 200 413
- Predictable input actions can be used to fingerprint vs real user

LICENSE ISSUES



foomanchoo719@gmail.com | Home | Help | Android.com | Sign out

Your account has been banned or deleted.
Please refer to Google Play Support for Developers for further details.

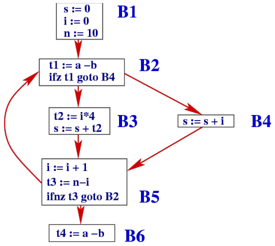
© 2012 Google - Google Play Terms of Service - Privacy Policy

Got caught a couple times in early experiments doing some stupid stuff

GETTING CAUGHT

- What happens when you get flagged?
- Inferred Bouncer process
  - Dynamic analysis of submitted app
  - If flagged, manual analysis by human operator
  - If deemed malicious, goodbye account!
- Manual analysis originated from different IP range (173.194.99.0/16)

STATIC ANALYSIS



```
s := 0
i := 0
n := 10

t1 := a –b
ifz t1 goto B4

t2 := i*4
s := s + t2

s := s + i

i := i + 1
t3 := n–i
ifnz t3 goto B2

t4 := a –b
```

- Unexplored
- Sometimes the APK never calls back
- Presumably, this means it was not dynamically tested

WHAT CAN GOOGLE DO?

- Some easy stuff
  - E.g., hide strings, emulator identifiers, etc.
- Some medium stuff
  - E.g., diversify IP ranges
- Some hard stuff
  - E.g., prevent a sufficiently convincing model of a real user's Android device

FINAL THOUGHTS

- Dynamic analysis is hard!
- Bouncer does not have to be perfect to be useful
  - It will catch crappy malware
  - It might not catch sophisticated malware
  - It is not different from anti-viruses or an Intrusion Detection System (IDS)

RESOURCES

- Zhou, Yajin, and Xuxian Jiang
  Dissecting android malware: Characterization and evolution
  In Security and Privacy (SP), 2012 IEEE Symposium on, pp. 95-109. IEEE, 2012.

ACKNOWLEDGEMENT

- This lecture is based on the following presentation
  Jon Oberheide and Charlie Miller
  Dissecting the Android Bouncer
  SummerCon 2012

Questions?

Thanks for your attention!