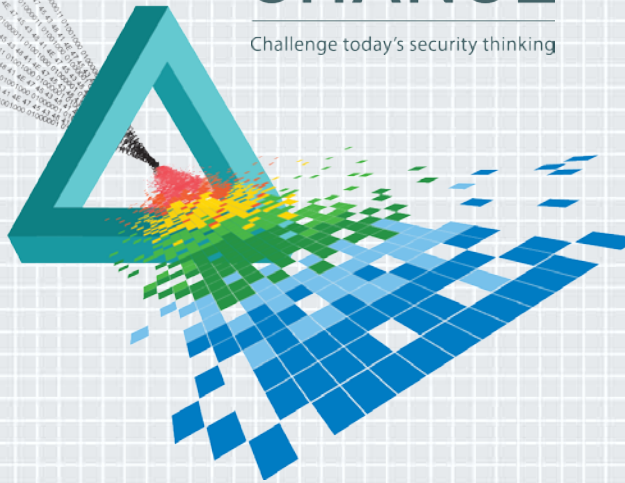
RSAConference2015
San Francisco | April 20-24 | Moscone Center

CHANGE
Challenge today's security thinking



SESSION ID: HTA-T08

How We Discovered Thousands of Vulnerable Android Apps in 1 Day

Joji Montelibano
Vulnerability Analysis Technical Manager
CERT
@certcc

Will Dormann
Vulnerability Analyst
CERT
@wdormann

Copyright

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM-0002136

What is CERT?

- Center of Internet security expertise
- Established in 1988 by the US Department of Defense on the heels of the Morris worm that created havoc on the ARPANET, the precursor to what is the Internet today
- Located in the Software Engineering Institute (SEI)
  - Federally Funded Research & Development Center (FFRDC)
  - Operated by Carnegie Mellon University (Pittsburgh, Pennsylvania)

CERT Vulnerability Analysis

Mission: Make Software Safer

Vulnerability Coordination

Vulnerability Discovery

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Vulnerability Coordination

Is easy?

ActiveX

- Dranzer + HijackThis logs + Automation = Lots of Vulnerabilities
- Vulnerability Detection in ActiveX Controls through Automated Fuzz Testing (Jan 2008)http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=53466

ActiveX

- Thousands of vulnerabilities discovered.
- Manual coordination of important/popular ones.
- Many ignored.

ffmpeg

- ffmpeg + BFF = lots of uniquely-crashing testcases

msg6282 (view) **Author: WD** **Date: 2009-06-30.18:28:54**

Attached is a zip file with multiple (73) files that cause ffmpeg to crash. The crashers are in a subset of various codecs. Included with each codec/directory are:
1) The seed/good file
2) Variations of the file that cause crashes (basename.x.y)
3) GDB output for the crashing testcases
4) Valgrind output for the crashing testcases
5) tabriffdump output for the crashing testcases
6) A diff summary of what is different between the crashing testcase and the original file, RIFF-header-wise.

About half of the crashers are something that is in a RIFF header for the file (e.g. ImageHeight, ImageWidth, dsScale, etc.) The other half appear to be something specific decoding of the codec.

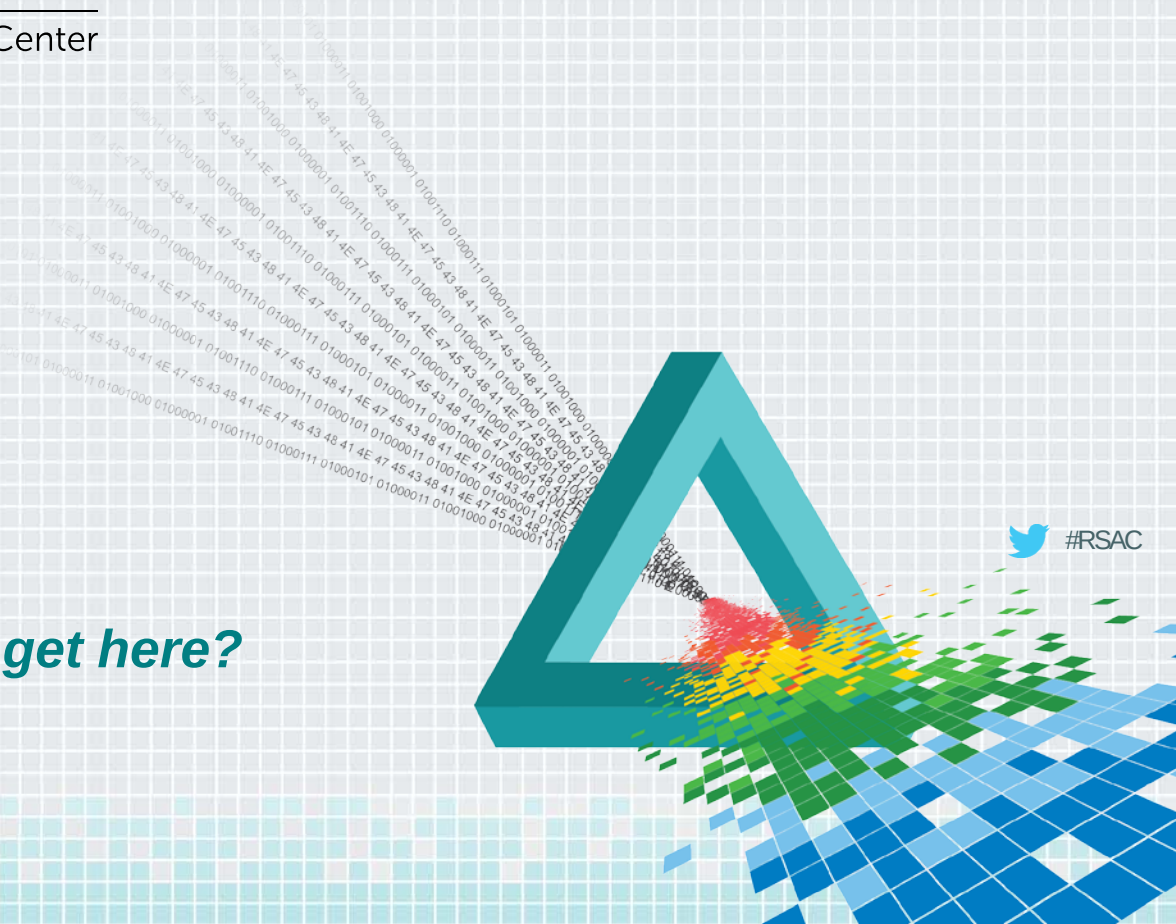
ffmpeg response

msg6333 (view) **Author: reimar** **Date: 2009-07-03.11:55:02**

```
On Tue, Jun 30, 2009 at 06:28:54PM +0000, WD wrote:
> Attached is a zip file with multiple (73) files that cause ffmpeg to crash.

A lot of these file crash no longer with SVN, please get rid of those
that work now, 73 files are simply too much to handle.
```

RSAConference2015

San Francisco | April 20-24 | Moscone Center



Background

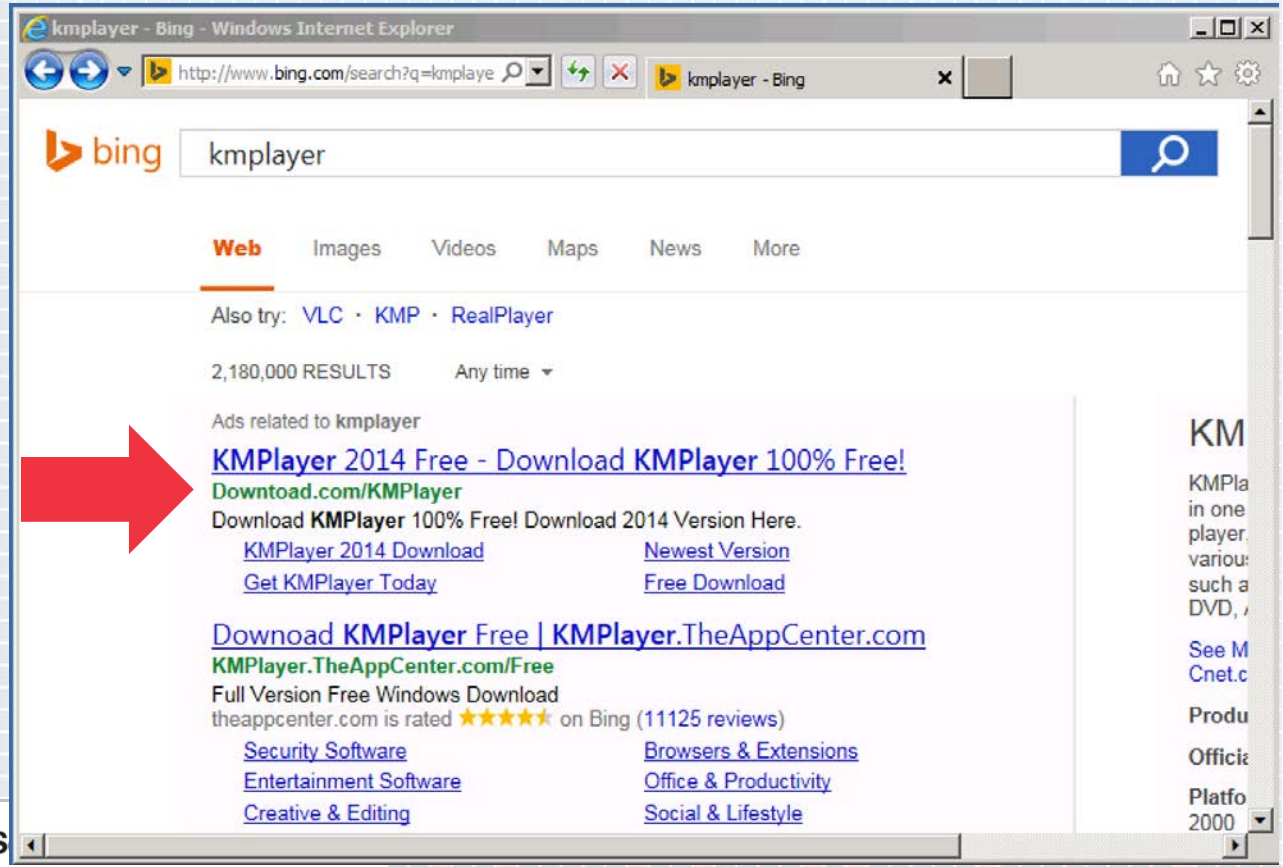
Where am I and how did I get here?

History

- Download.com

http://www.cert.org/blogs/certcc/post.cfm?EntryID=199

The internet is horrible



Identical installers

- Installers from Download.com are the same:

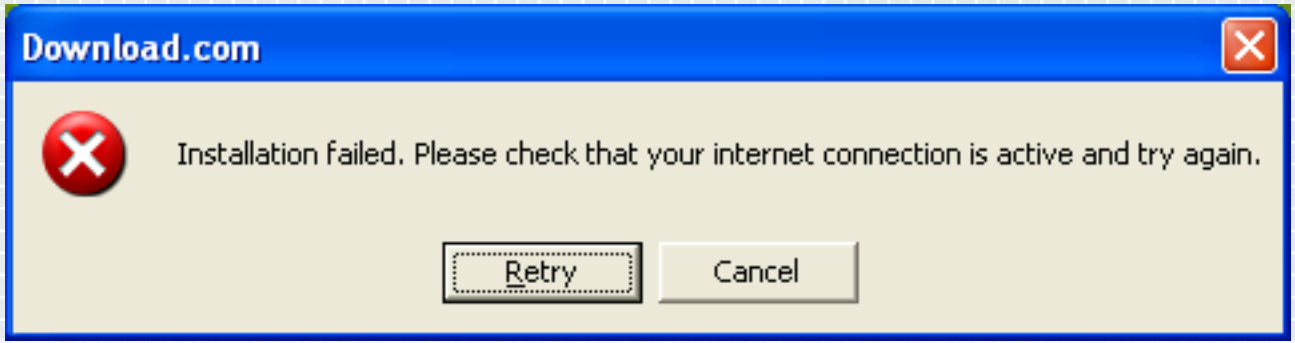
- `5a275a569dce6e2f2f0284d82d31310b *cbsidlm-cbsi213-Enable__Disable_Registry_Tool-SEO-75812481.exe`
- `5a275a569dce6e2f2f0284d82d31310b *cbsidlm-cbsi213-KMPlayer-SEO-10659939.exe`

Software retrieval

```
GET /rest/v1.0/softwareProductLink?productSetId=10659939&partTag=dlm&path=SEO&build=213 HTTP/1.1
Host: api.cnet.com

HTTP/1.1 200 OK

<?xml version="1.0" encoding="utf-8"?>

<CNETResponse xmlns="http://api.cnet.com/restApi/v1.0/ns"
xmlns:xlink="http://www.w3.org/1999/xlink" version="1.0"><SoftwareProductLink id="13819308"
setId="10659939" appVers="1.0"><Name><![CDATA[KMPlayer -
3.9.1.129]]></Name><ProductName><![CDATA[KMPlayer]]></ProductName><ProductVersion><![CDATA[3.9.1.
129]]></ProductVersion><FileName><![CDATA[KMPlayer_3.9.1.129.exe]]></FileName><FileSize><![CDATA[
35872504]]></FileSize><FileMd5Checksum><![CDATA[5d0e7d17fc4ef0802a9332c83075047c]]></FileMd5Check
sum><PublishDate><![CDATA[2014-10-
06]]></PublishDate><CategoryId><![CDATA[13632]]></CategoryId><Category><![CDATA[Downloads^Video
Software^Video
Players]]></Category><License><![CDATA[Free]]></License><DownloadLink>http://software-files-
a.cnet.com/s/software/13/81/93/08/KMPlayer_3.9.1.129.exe?token=1413054436_d56f7814cd5af230f782dd2
8550e185a</DownloadLink><TrackedDownloadLink>http://dw.cbsi.com/redir?edId=1174&amp;siteId=4&amp;
lop=feed.dl&amp;ontId=13632&amp;tag=tdw_dlman&amp;pid=13819308&amp;destUrl=http%3A%2F%2Fsoftware-
files-
a.cnet.com%2Fs%2Fsoftware%2F13%2F81%2F93%2F08%2FKMPlayer_3.9.1.129.exe%3Ftoken%3D1413054436_2defb
65a1350a3b035964c18f30fb06e%26fileName%3DKMPlayer_3.9.1.129.exe
```

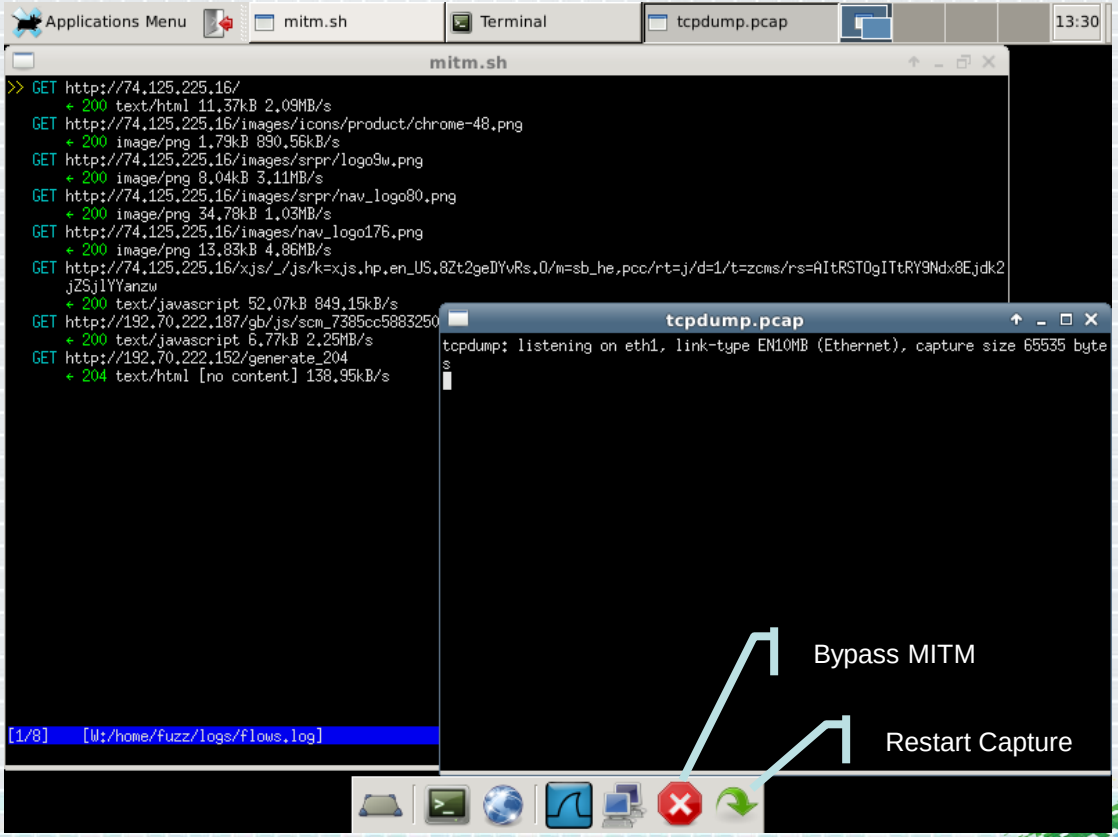
Just MITM it!

- Set up a proxy to modify content as it's transferred
- Problem: Installer isn't proxy-aware!



Solution: CERT Tapioca

- Transparent Proxy Capture Appliance
- UbuFuzz + iptables + mitmproxy



CERT Tapioca

CERT Tapioca

CERT Tapioca is a network-layer man-in-the-middle (MITM) proxy VM that is based on UbuFuzz and is preloaded with mitmproxy. CERT Tapioca is available in OVA format, which should be compatible with a range of virtualization products, including VMware, VirtualBox, and others.

The primary modes of operation are

1) Checking for apps that fail to validate certificates:
Simply associate device to access point or connect to network and perform the activity. Any logged https traffic is from software that fails to check for a valid SSL chain.

2) Investigating traffic of any http/https traffic:
Install the root CA of the MITM software that you are using into the OS of the device that you are testing.

Download CERT Tapioca.

Download

Related Blog Posts

Finding Android SSL Vulnerabilities with CERT Tapioca

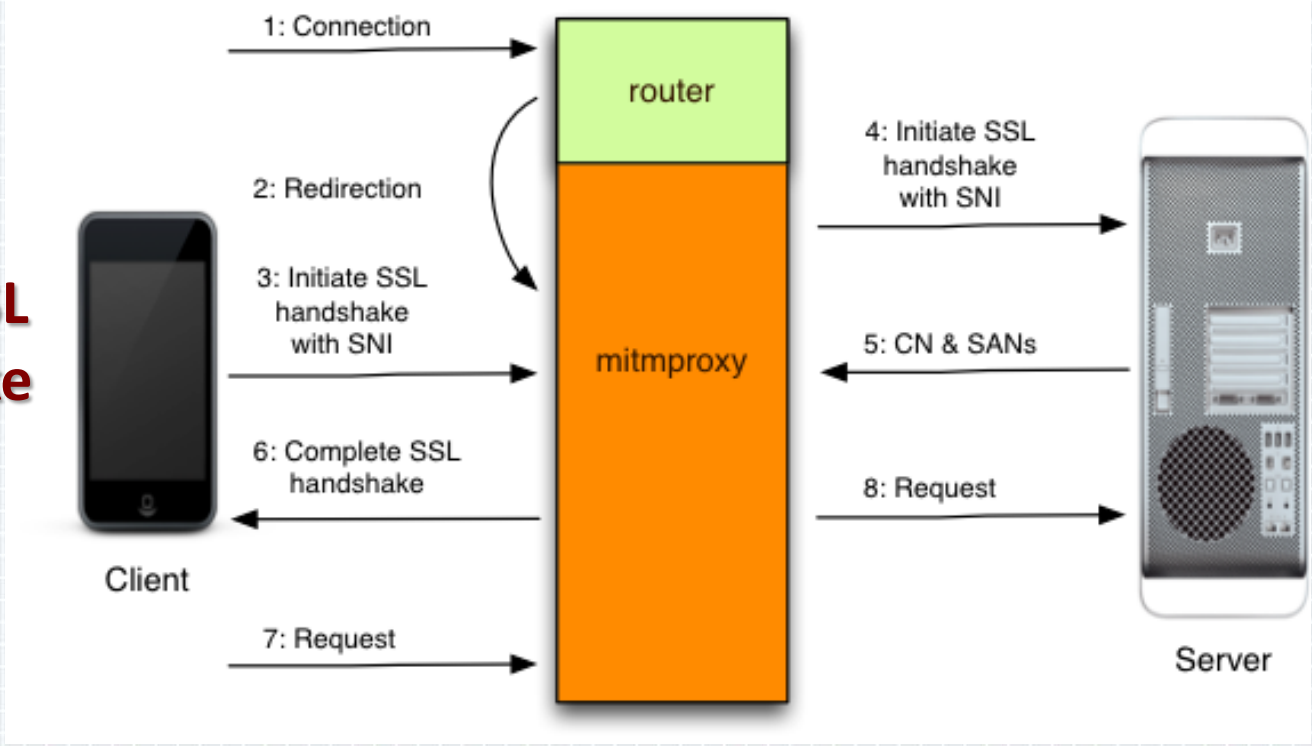
Announcing CERT Tapioca for MITM Analysis

http://www.cert.org/vulnerability-analysis/tools/cert-tapioca.cfm

How it works

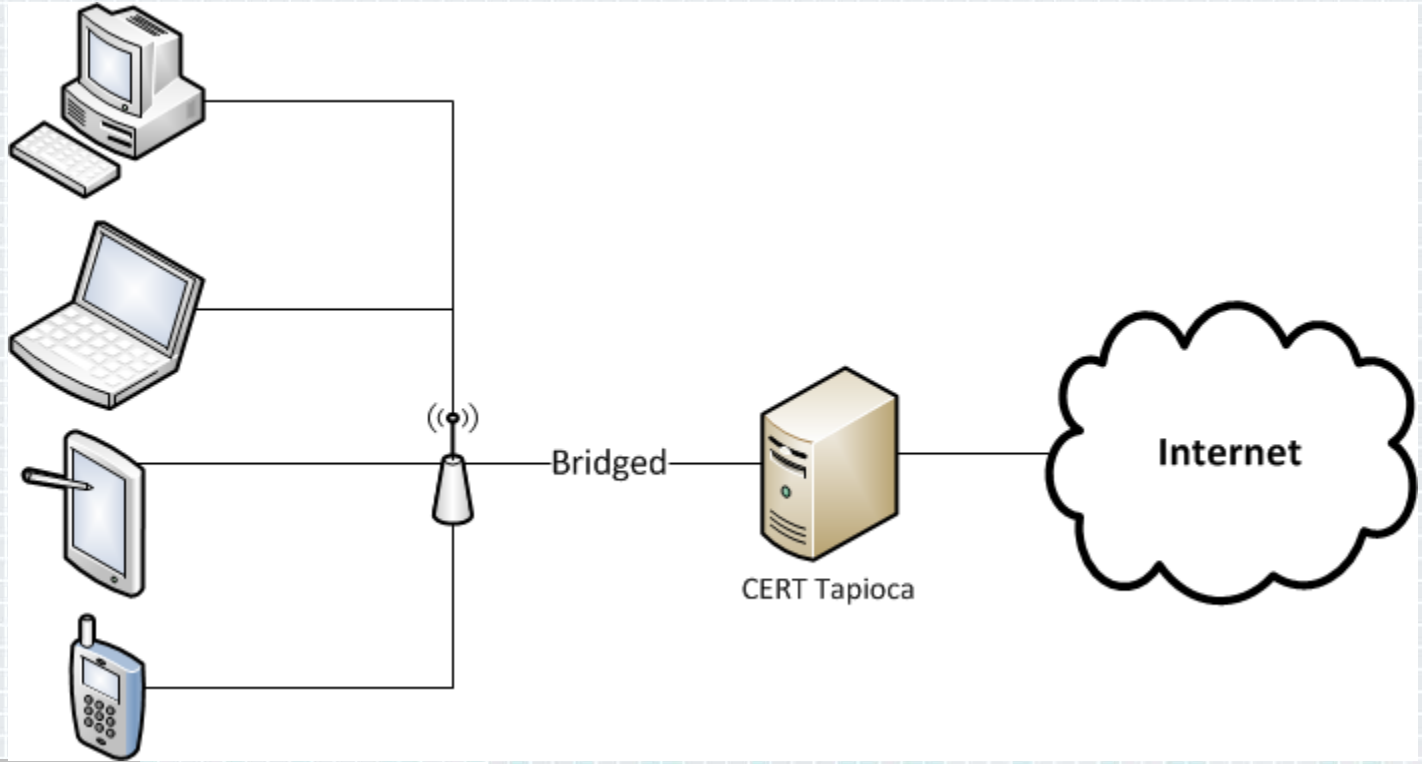
I can see everything if the client doesn't validate SSL

Invalid SSL handshake

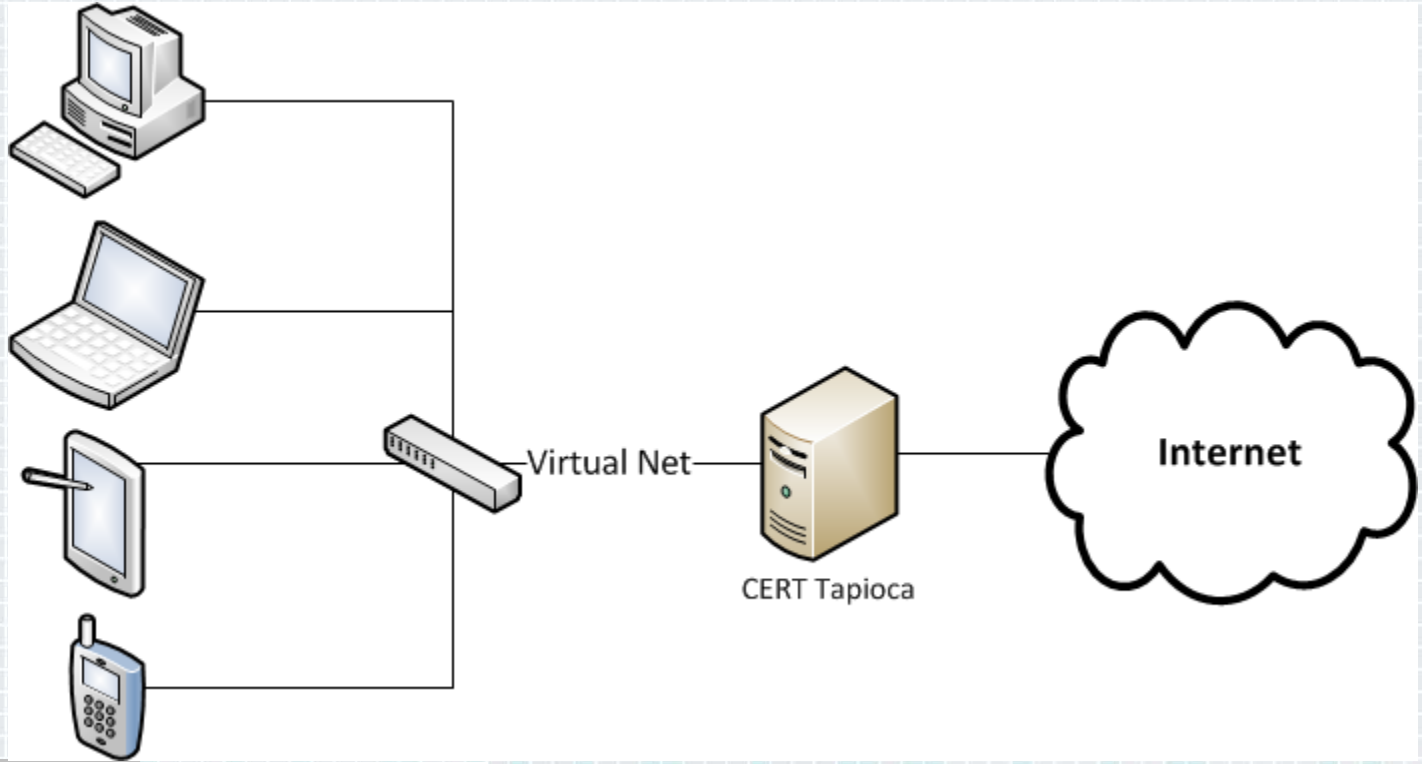


Valid SSL handshake

Tapioca architecture



Tapioca architecture



Investigating Android

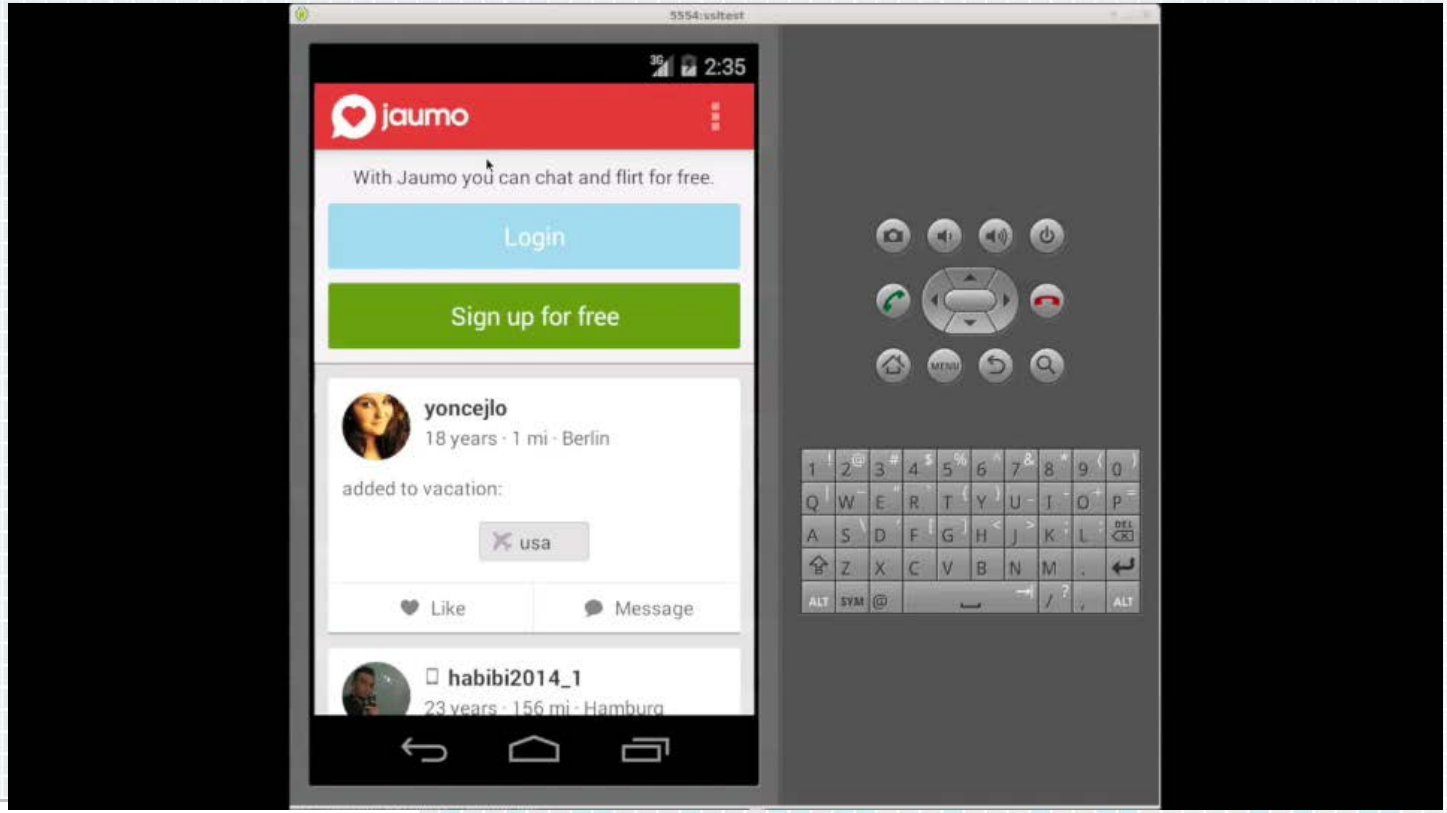
- Use a phone and a wireless access point

Improvement #1

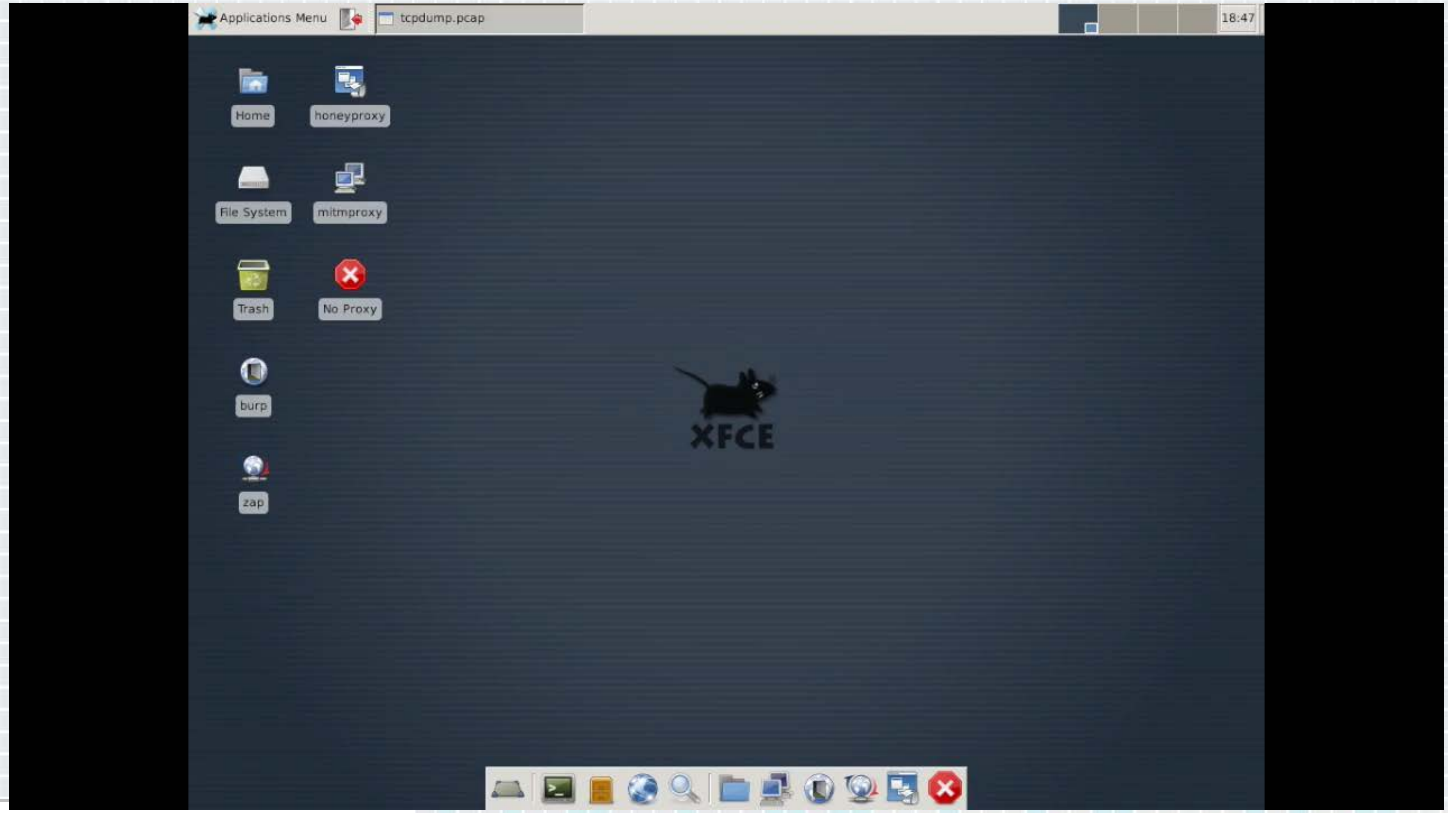
- Virtualization and Automation
  - google-play-crawler
  - VMware
  - Android SDK
  - AVD
  - Monkeyrunner
  - Monkey
- Now I can test when I sleep!

https://github.com/Akdeniz/google-play-crawler
http://developer.android.com/tools/help/monkeyrunner_concepts.html
http://developer.android.com/tools/help/monkey.html
http://www.cert.org/blogs/certcc/post.cfm?EntryID=204

Automated Android



CERT Tapioca



Improvement #2

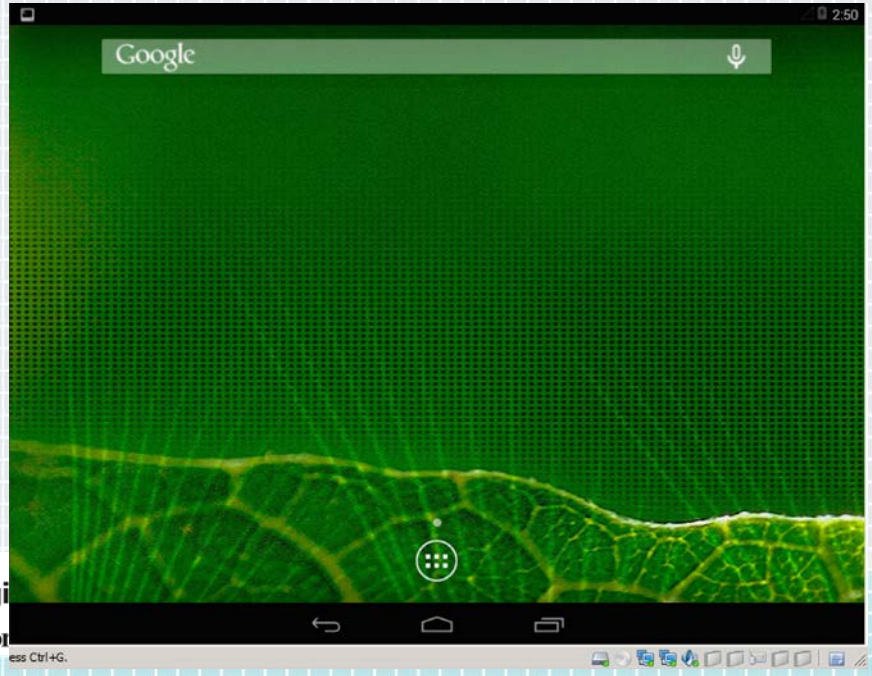
- Parallelization
- Rather than 1 Android VM and 1 Tapioca VM, what about 20 of each?
- Now I can test 20x faster!

Android emulation annoyance

- ARM Android emulation is slow. Very slow.
- x86 Android emulation is fast (~15x faster), IFF you have a KVM-enabled Linux kernel.

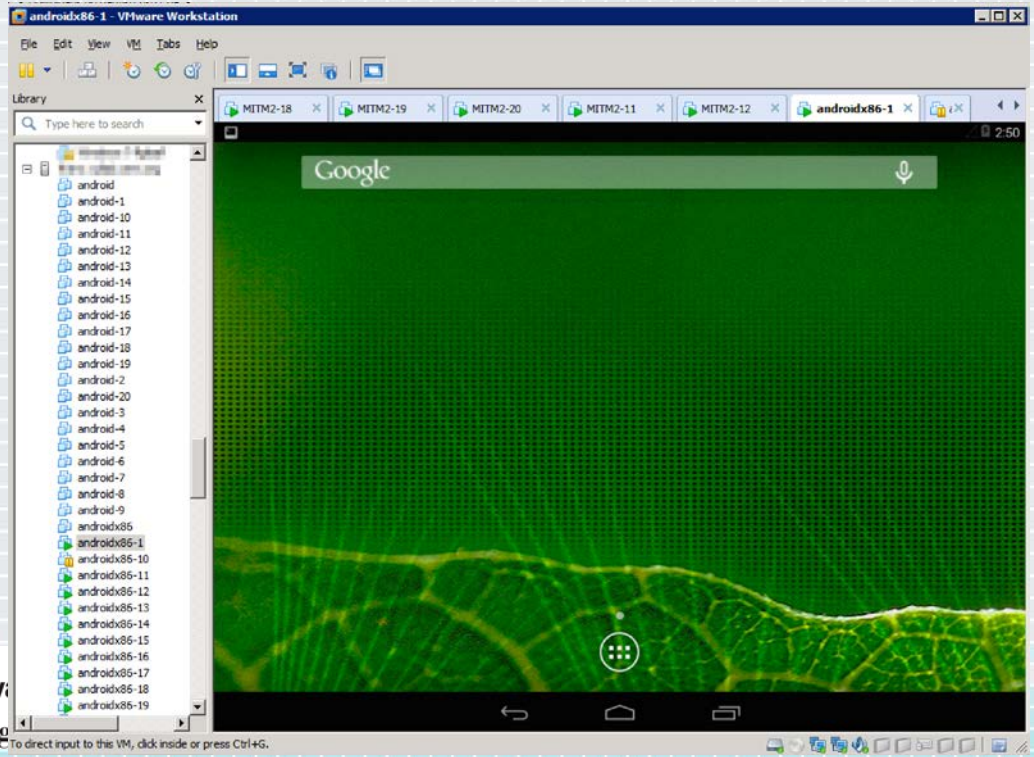
Improvement #3

- Solution: x86 Android in a VM (not an emulator):
- http://www.android-x86.org/

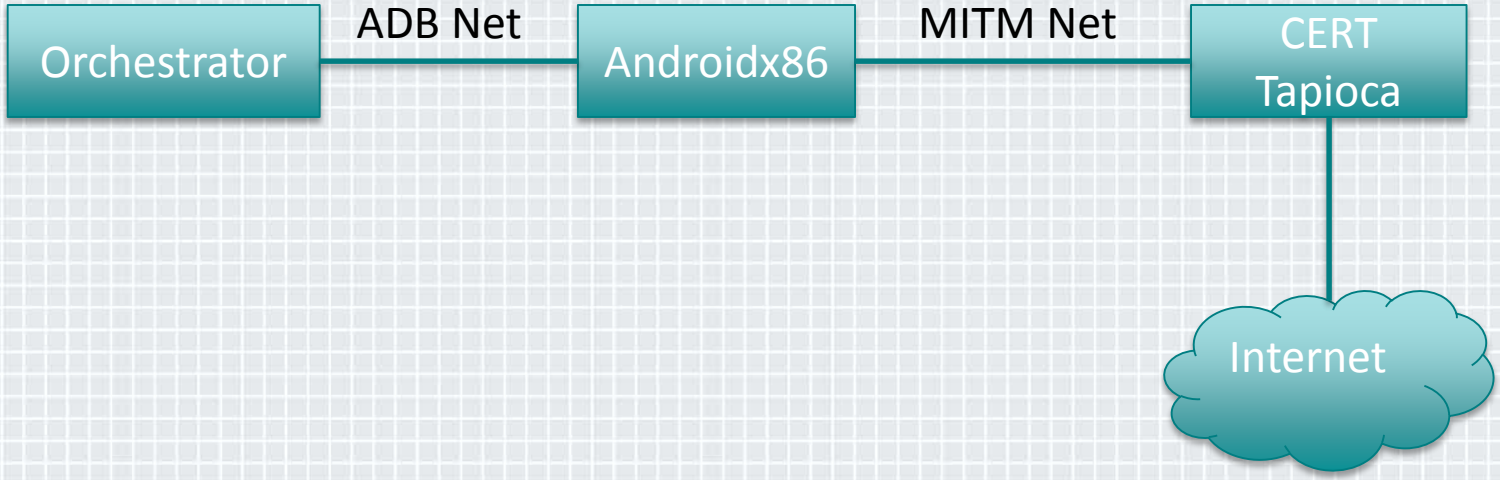


Improvement #4

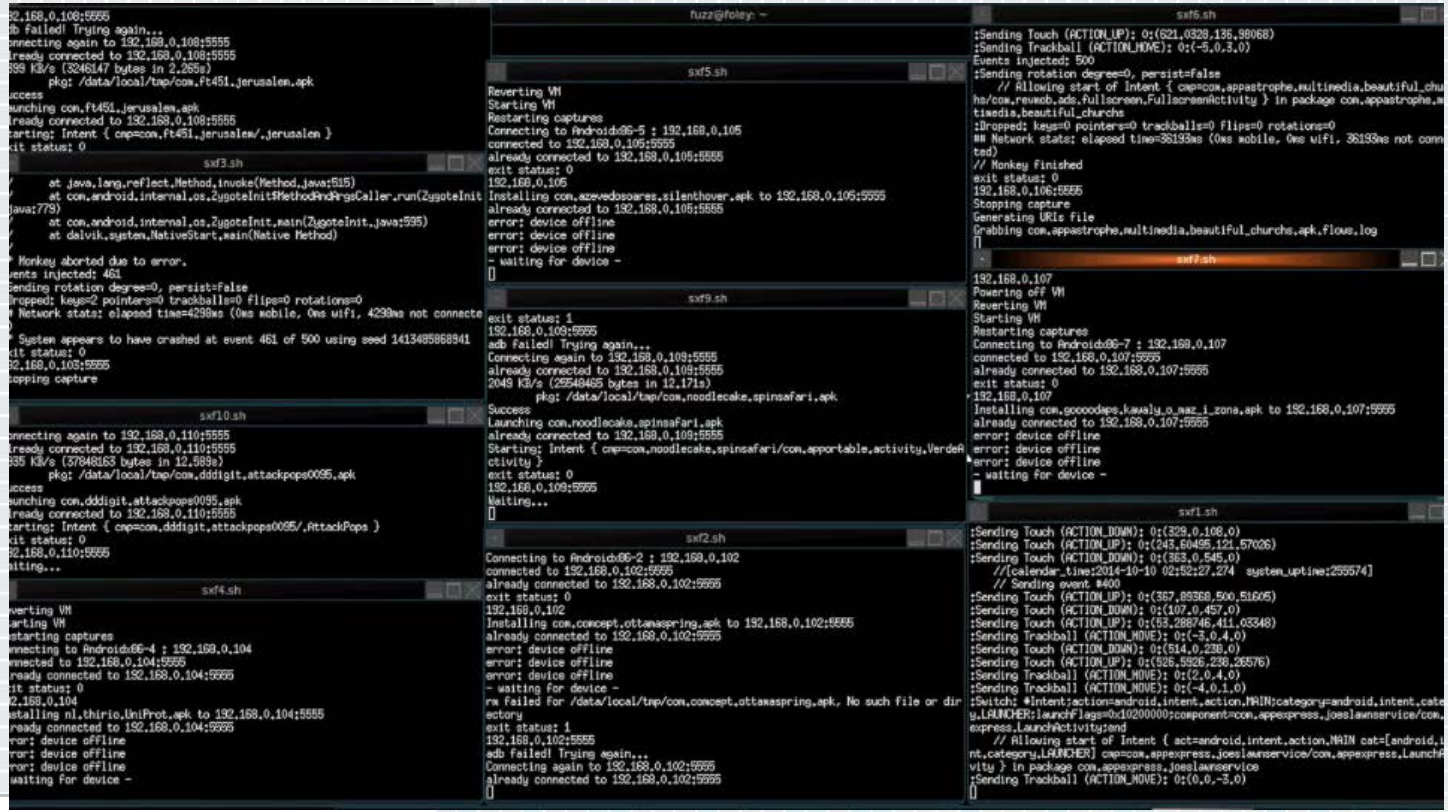
- Let’s make 20 of them!



Androidx86 SSL Test Architecture



Automation of 20 VMs



RSAConference2015

San Francisco | April 20-24 | Moscone Center

#RSAC

Android SSL Coordination

This one's optimistic

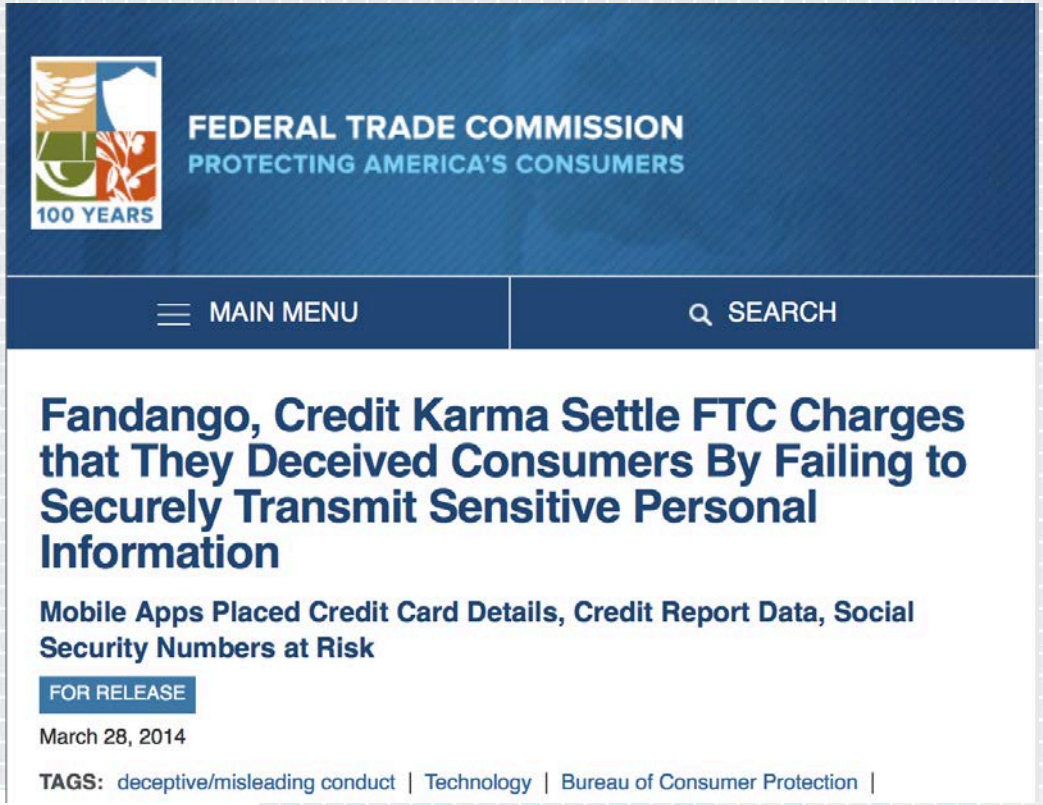
Prior SSL Investigations

- Why Eve and Mallory Love Android: An Analysis of Android SSL (In)Security
- October 18, 2012 - Sascha Fahl, Marian Harbach, Thomas Muders, Matthew Smith, Lars Baumgärtner, Bernd Freisleben
- http://android-ssl.org/files/p50-fahl.pdf
- “To evaluate the state of SSL use in Android apps, we downloaded 13,500 popular free apps from Google’s Play Market and studied their properties with respect to the usage of SSL.”
- No app authors contacted?

Prior SSL Investigations

- SSL Vulnerabilities: Who listens when Android applications talk?
- August 20, 2014 - Adrian Mettler, Vishwanath Raman, Yulong Zhang
- https://www.fireeye.com/blog/threat-research/2014/08/ssl-vulnerabilities-who-listens-when-android-applications-talk.html
- “We reviewed the 1,000 most-downloaded free applications in the Google Play store as of July 17, 2014.”
- No app authors contacted?

Prior SSL Investigations



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS
100 YEARS

MAIN MENU | SEARCH

Fandango, Credit Karma Settle FTC Charges that They Deceived Consumers By Failing to Securely Transmit Sensitive Personal Information

Mobile Apps Placed Credit Card Details, Credit Report Data, Social Security Numbers at Risk

FOR RELEASE

March 28, 2014

TAGS: deceptive/misleading conduct | Technology | Bureau of Consumer Protection |

Notify Affected Authors

Hello,

This is Will Dormann with the CERT Coordination Center, which is part of Carnegie Mellon University. <http://www.cert.org/about>

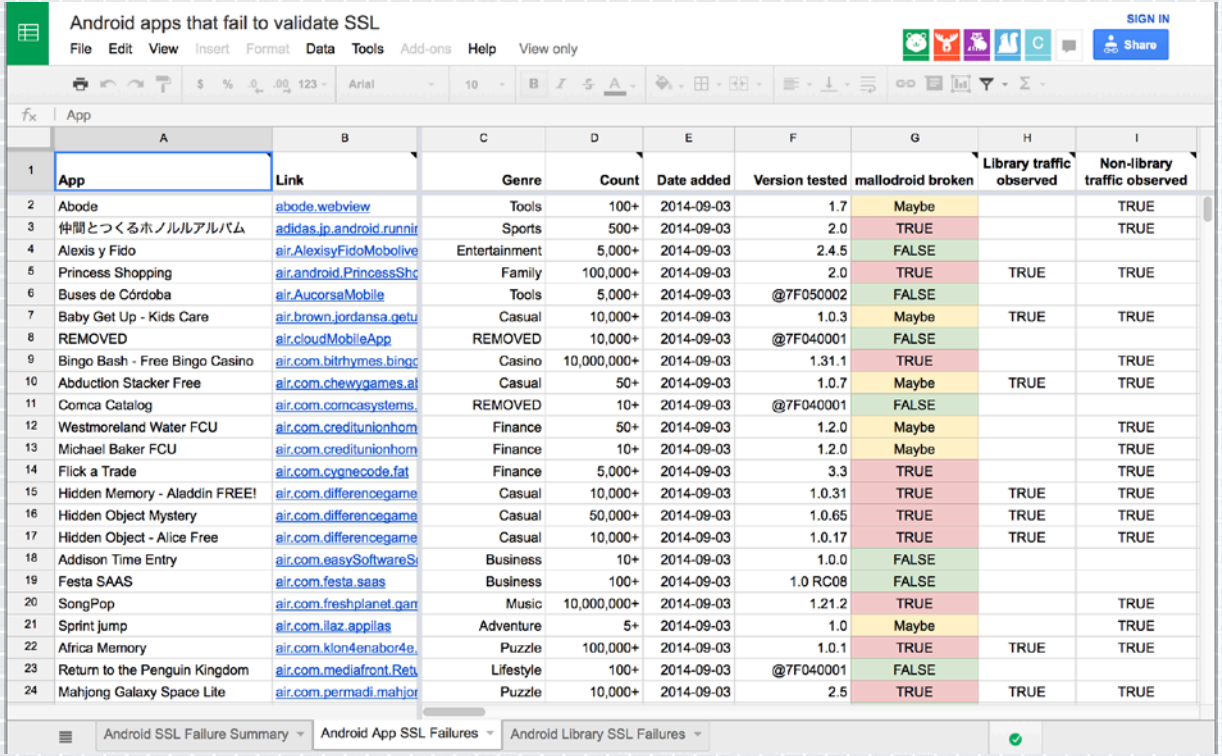
We've recently been evaluating with CERT Tapioca <http://www.cert.org/blogs/certcc/post.cfm?EntryID=204> the use of SSL by Android apps. Through automated testing, we are logging apps that cause traffic to be sent or received over an HTTPS connection that has an invalid SSL certificate chain.

The following application has demonstrated this incorrect behavior:
APP_ID
https://play.google.com/store/apps/details?id=APP_ID

Due to the sheer volume of affected applications, we are currently unable to manually inspect every affected application. However, we are sending notifications to the application authors for further

Investigation.
<SNIP>

Publish the offending apps



Android apps that fail to validate SSL

File Edit View Insert Format Data Tools Add-ons Help View only

SIGN IN Share

App

	A	B	C	D	E	F	G	H	I
1	App	Link	Genre	Count	Date added	Version tested	mallodroid broken	Library traffic observed	Non-library traffic observed
2	Abode	abode.webview	Tools	100+	2014-09-03	1.7	Maybe		TRUE
3	仲間とつくるホノルルアルバム	adidas.jp.android.runnir	Sports	500+	2014-09-03	2.0	TRUE		TRUE
4	Alexis y Fido	air.AlexisyFidoMobolive	Entertainment	5,000+	2014-09-03	2.4.5	FALSE		
5	Princess Shopping	air.android.PrincessShc	Family	100,000+	2014-09-03	2.0	TRUE	TRUE	TRUE
6	Buses de Córdoba	air.AucorsaMobile	Tools	5,000+	2014-09-03	@7F050002	FALSE		
7	Baby Get Up - Kids Care	air.brown.jordansa.getu	Casual	10,000+	2014-09-03	1.0.3	Maybe	TRUE	TRUE
8	REMOVED	air.cloudMobileApp	REMOVED	10,000+	2014-09-03	@7F040001	FALSE		
9	Bingo Bash - Free Bingo Casino	air.com.bitrhymes.bingc	Casino	10,000,000+	2014-09-03	1.31.1	TRUE		TRUE
10	Abduction Stacker Free	air.com.chewygames.al	Casual	50+	2014-09-03	1.0.7	Maybe	TRUE	TRUE
11	Comca Catalog	air.com.comcasystems.	REMOVED	10+	2014-09-03	@7F040001	FALSE		
12	Westmoreland Water FCU	air.com.creditunionhom	Finance	50+	2014-09-03	1.2.0	Maybe		TRUE
13	Michael Baker FCU	air.com.creditunionhom	Finance	10+	2014-09-03	1.2.0	Maybe		TRUE
14	Flick a Trade	air.com.cygnecode.fat	Finance	5,000+	2014-09-03	3.3	TRUE		TRUE
15	Hidden Memory - Aladdin FREE!	air.com.differencegame	Casual	10,000+	2014-09-03	1.0.31	TRUE	TRUE	TRUE
16	Hidden Object Mystery	air.com.differencegame	Casual	50,000+	2014-09-03	1.0.65	TRUE	TRUE	TRUE
17	Hidden Object - Alice Free	air.com.differencegame	Casual	10,000+	2014-09-03	1.0.17	TRUE	TRUE	TRUE
18	Addison Time Entry	air.com.easySoftwareS	Business	10+	2014-09-03	1.0.0	FALSE		
19	Festa SAAS	air.com.festa.saas	Business	100+	2014-09-03	1.0 RC08	FALSE		
20	SongPop	air.com.freshplanet.gan	Music	10,000,000+	2014-09-03	1.21.2	TRUE		TRUE
21	Sprint jump	air.com.ilaz.appilas	Adventure	5+	2014-09-03	1.0	Maybe		TRUE
22	Africa Memory	air.com.klon4enabor4e.	Puzzle	100,000+	2014-09-03	1.0.1	TRUE	TRUE	TRUE
23	Return to the Penguin Kingdom	air.com.mediafront.Retu	Lifestyle	100+	2014-09-03	@7F040001	FALSE		
24	Mahjong Galaxy Space Lite	air.com.permadi.mahjor	Puzzle	10,000+	2014-09-03	2.5	TRUE	TRUE	TRUE

Android SSL Failure Summary | Android App SSL Failures | Android Library SSL Failures

https://docs.google.com/spreadsheets/d/1t5GXwjw82SyunALVJb2w0zi3FoLRIkfGPc7AMjRF0r4/edit?usp=sharing

Listed Applications

- An app is listed in the spreadsheet when it fails dynamic analysis with CERT Tapioca.

- If an app isn't listed:
  - It was not tested
  - Automation did not trigger HTTPS network traffic
  - It is not vulnerable

RSAConference2015

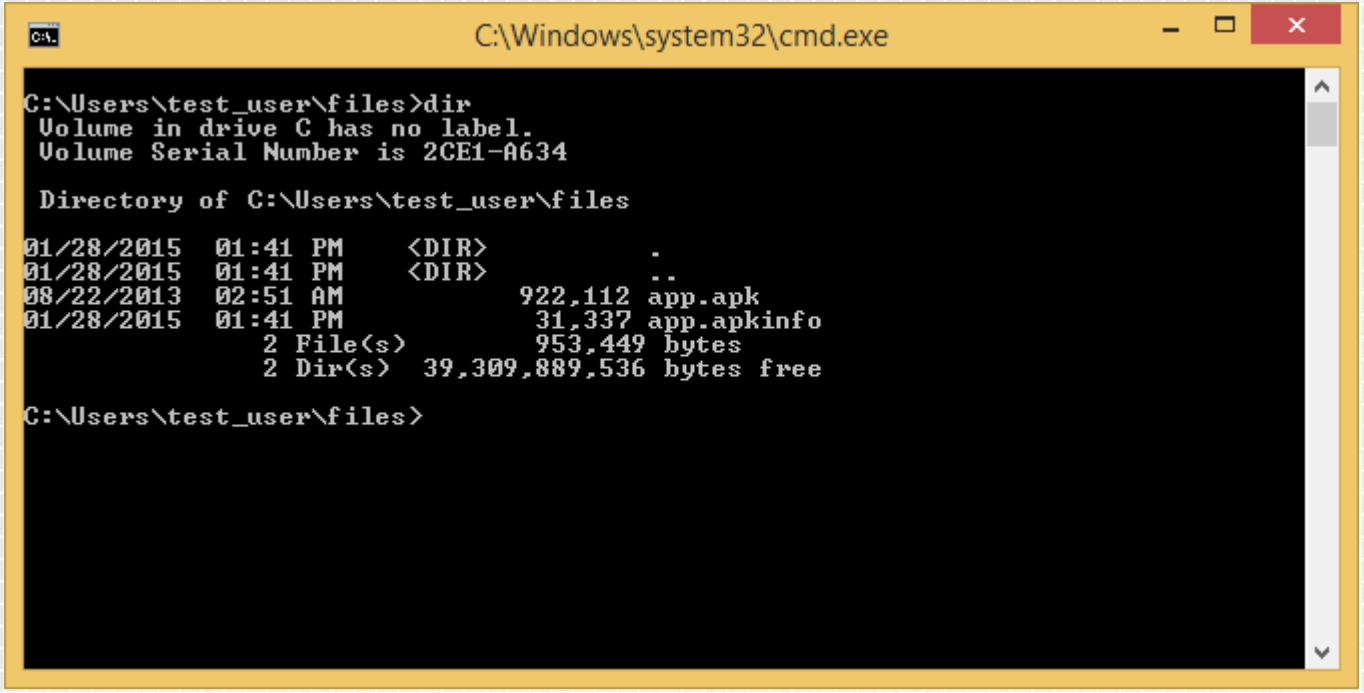
San Francisco | April 20-24 | Moscone Center

Issues Encountered

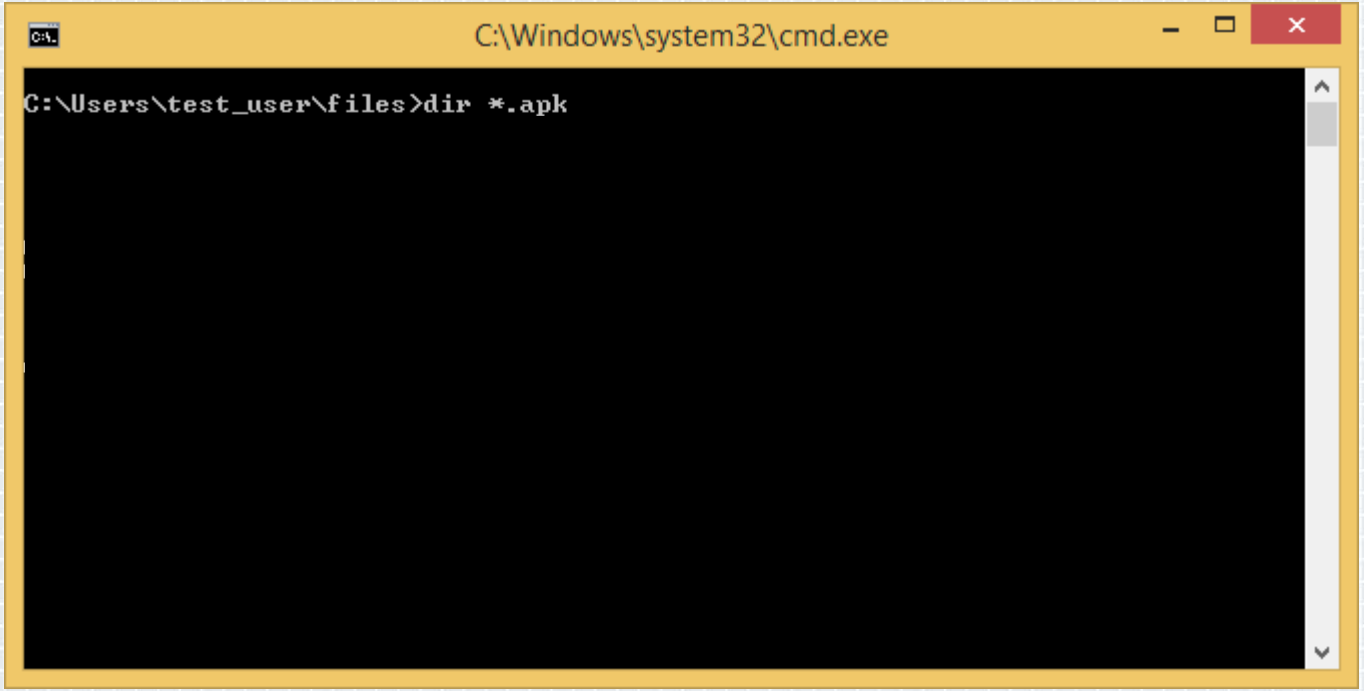
So you've got a million APK files?

#RSAC

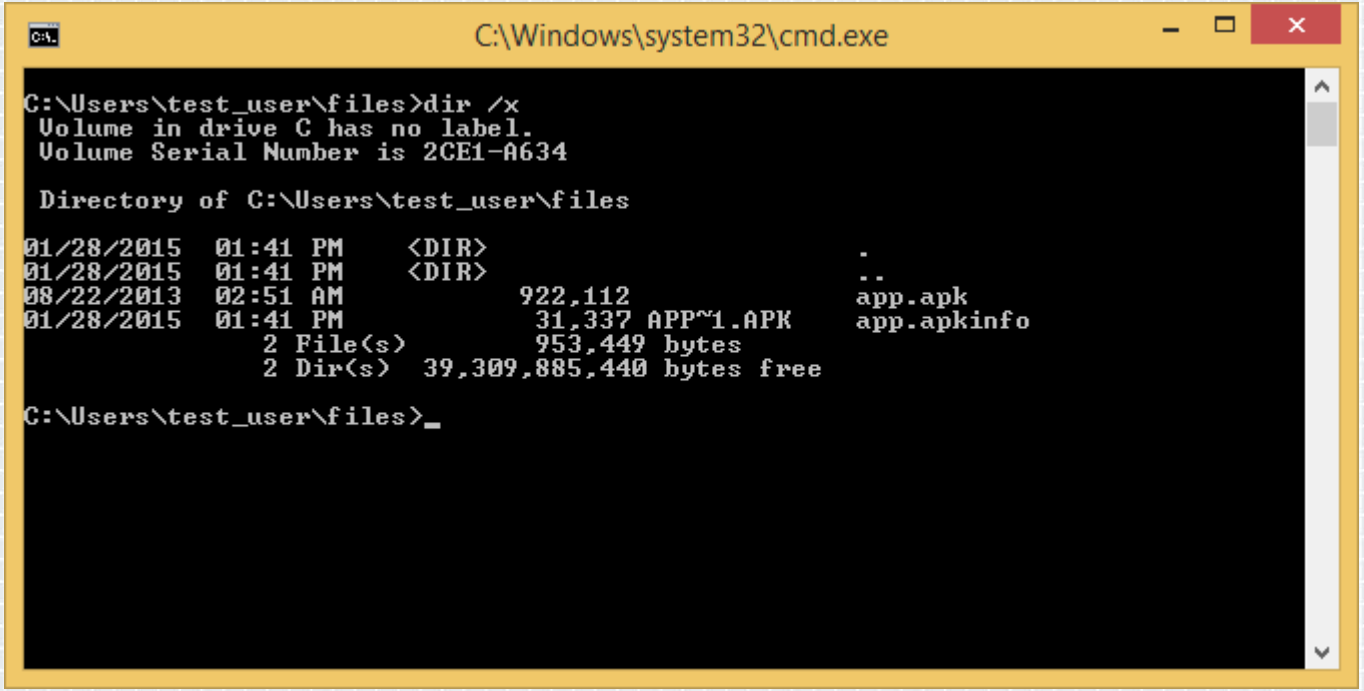
Windows CMD.EXE



Windows CMD.EXE

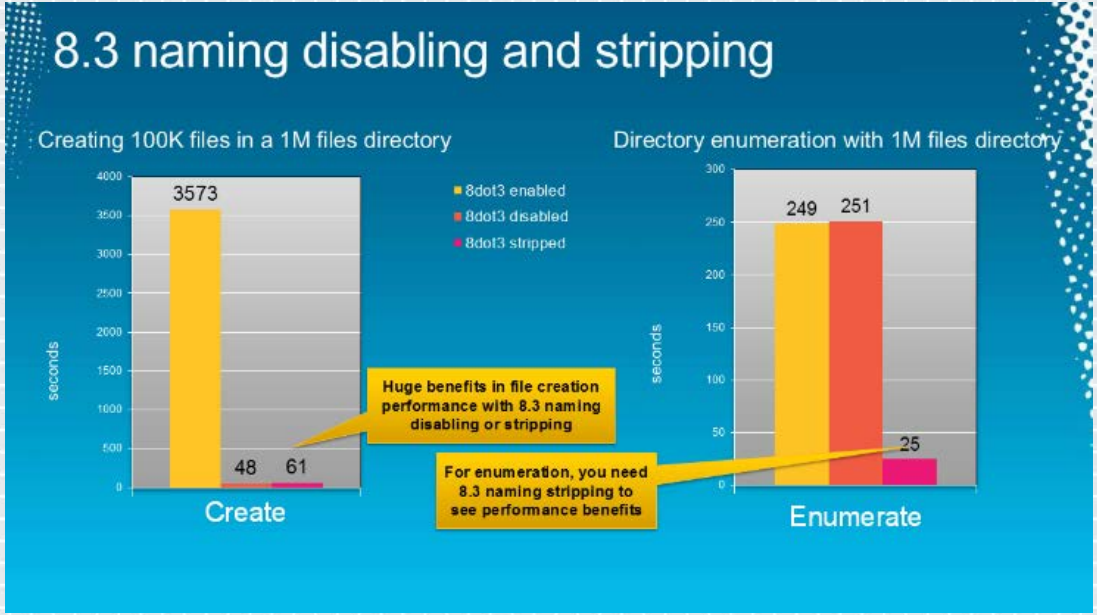


Windows CMD.EXE



THANKS MICROS~1 !!!1!

8.3 Filenames



"**Note**: Although disabling 8.3 file name creation increases file performance under Windows, some applications (16-bit, 32-bit, or 64-bit) may not be able to find files and directories that have long file names."

http://blogs.technet.com/b/josebda/archive/2012/11/13/windows-server-2012-file-server-tip-disable-8-3-naming-and-strip-those-short-names-too.aspx
http://support.microsoft.com/kb/121007

Busybox

- **recursive_action (and thus find) slow due to [l]stat()**
- Rich Felker Tue, 28 May 2013 21:13:18 -0700
- Conceptually, the find utility need not perform lstat on each filename unless it's needed for matching criteria. However, find is implemented based on libbb's recursive_action, which always performs stat or lstat. This makes busybox's find excruciatingly slow compared to GNU find.

Solution

- Real fileserver with ZFS.

Bug 197336 - find command cannot see more than 32765 subdirectories when using ZFS (edit)

Save Changes

Status: New (edit)

Reported: 2015-02-04 23:19 UTC by Will Dormann

CVE Fun

You keep using that word. I do not think it means what you think it means.

How to track Vulnerabilities?

- CVE is the de facto standard for tracking vulnerabilities in applications.
- MITRE, who operates CVE, does not attempt to track all applications with CVE.

What Makes an App Important?

5-10 million installs

Insecurely retrieves ads

No CVE assigned

What Makes an App Important?

1-5 installs

Insecurely uses paypal

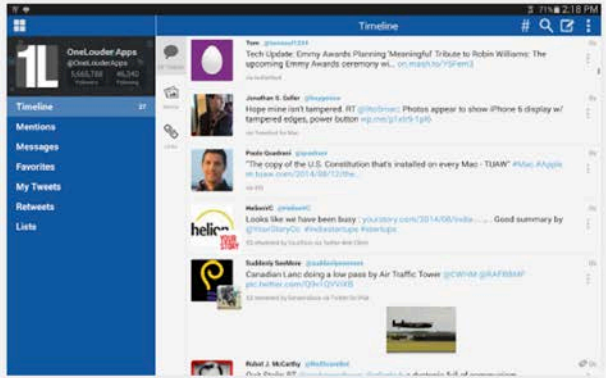
No CVE assigned

What Makes an App Important?

5-10 million installs

Sends user/password

No CVE assigned



CVE10K


Celebrating 15 Years
CVE10K
@CVE10K
We released 5-digit CVE-2014-10001 and 6-digit CVE-2014-100001 IDs on January 13, 2015, plus 90 others. Issues, compliments, or concerns welcome.
Everywhere
cve.mitre.org/cve/identifier…
Tweet to CVE10K

CVE Assignment

- Are Android applications CVE-worthy?

CVE Assignment

- Are Android applications CVE-worthy?

- No*

* Maybe, but stop assigning CVEs

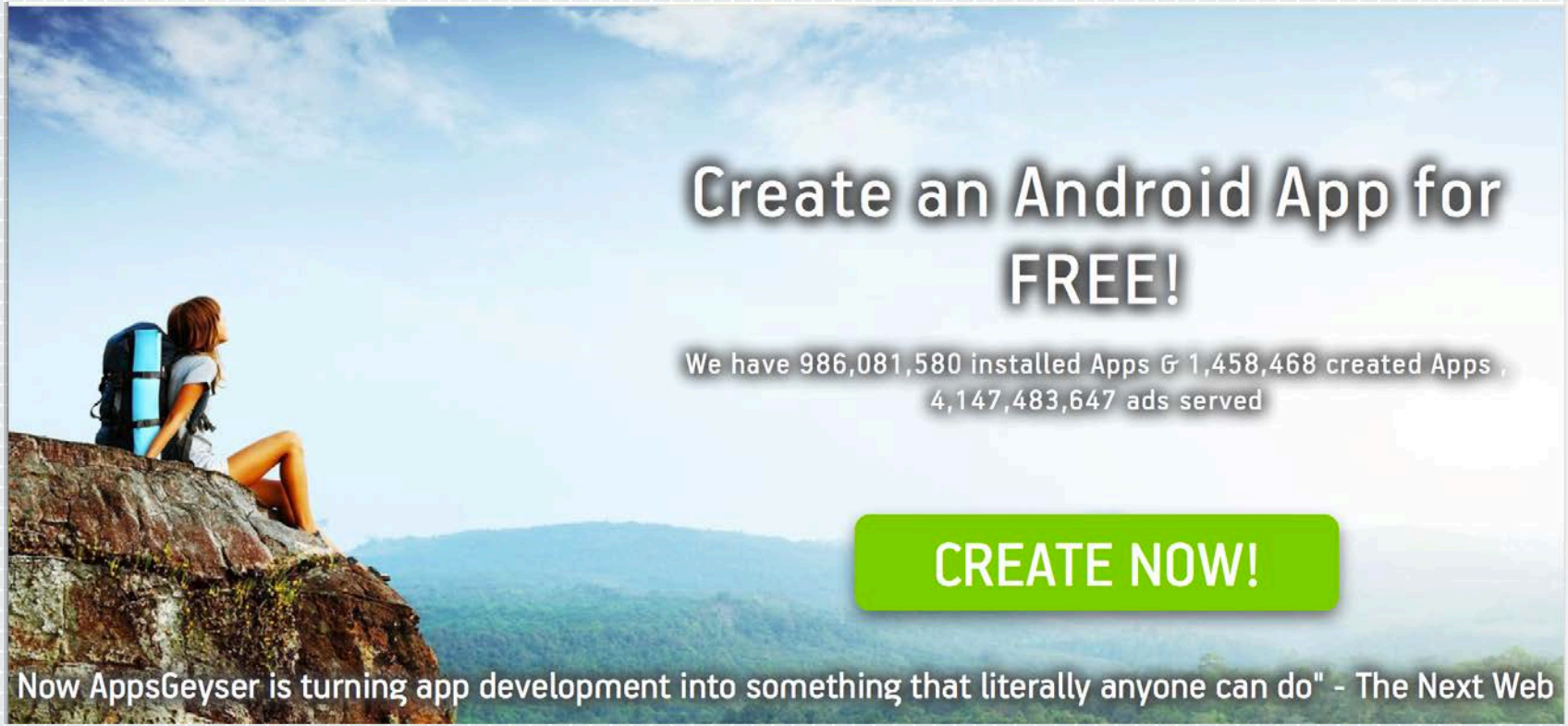
RSAConference2015

San Francisco | April 20-24 | Moscone Center

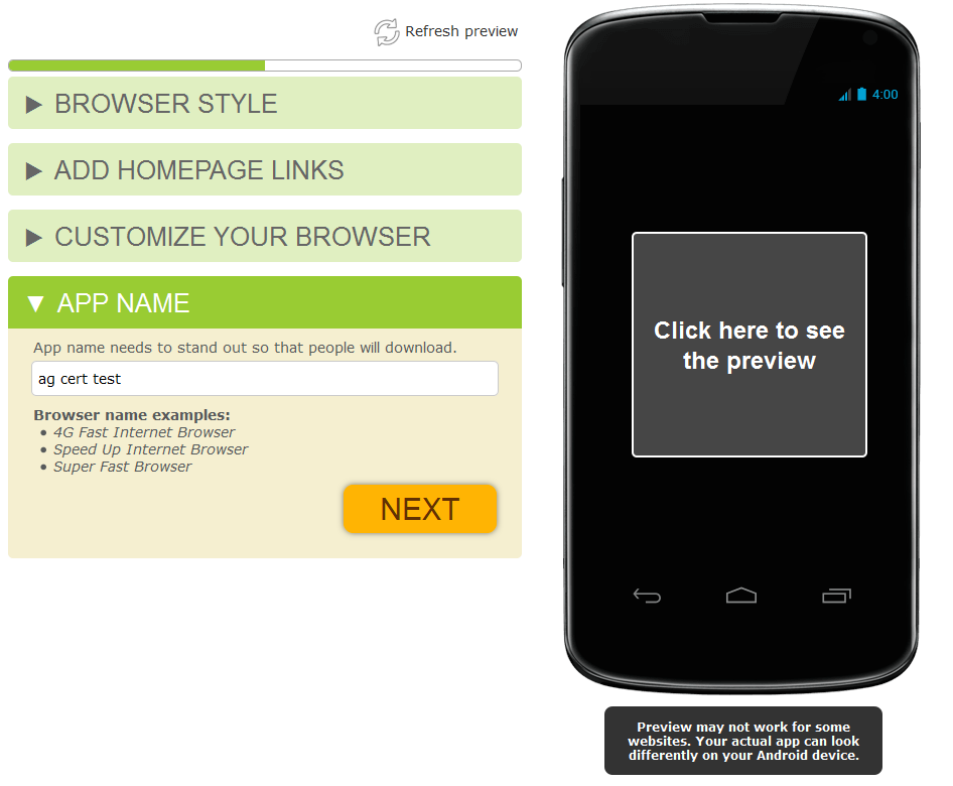
What Makes an Android Developer?

A pulse

AppsGeyser


Create an Android App for FREE!
We have 986,081,580 installed Apps & 1,458,468 created Apps , 4,147,483,647 ads served
CREATE NOW!
Now AppsGeyser is turning app development into something that literally anyone can do" - The Next Web

AppsGeyser


Refresh preview
▶ BROWSER STYLE
▶ ADD HOMEPAGE LINKS
▶ CUSTOMIZE YOUR BROWSER
▼ APP NAME
App name needs to stand out so that people will download.
ag cert test
Browser name examples:
• 4G Fast Internet Browser
• Speed Up Internet Browser
• Super Fast Browser
NEXT
4:00
Click here to see the preview
Preview may not work for some websites. Your actual app can look differently on your Android device.

VulsGeyser

Vulnerability Note VU#1680209

AppsGeyser generates Android applications that fail to properly validate SSL certificates

Original Release date: 19 Dec 2014 | Last revised: 07 Jan 2015

Print Tweet Send Share

Overview

AppsGeyser generates applications that fail to properly validate SSL certificates.

Description

AppsGeyser is an online tool that generates Android applications. At the time of publication of this vulnerability note, the AppsGeyser website claims to have generated over 1.3 million Android applications. The applications that are generated by AppsGeyser include code that disables SSL certificate validation for HTTPS traffic.

AppsGeyser Fixed

Impact

When a victim is using an application generated by AppsGeyser, an attacker on the same network as the Android device may be able to view or modify network traffic that should have been protected by HTTPS. The impact varies based on what the application is doing. Possible outcomes include credential stealing or arbitrary code execution.

Solution

Regenerate affected Android applications

The AppsGeyser application generator has been updated to correctly validate SSL certificates. Any applications that were created before December 24, 2014 should be regenerated.

Vendor Information (Learn More)

Vendor	Status	Date Notified	Date Updated
AppsGeyser	Affected	12 Dec 2014	19 Dec 2014

AppsGeyser Apps

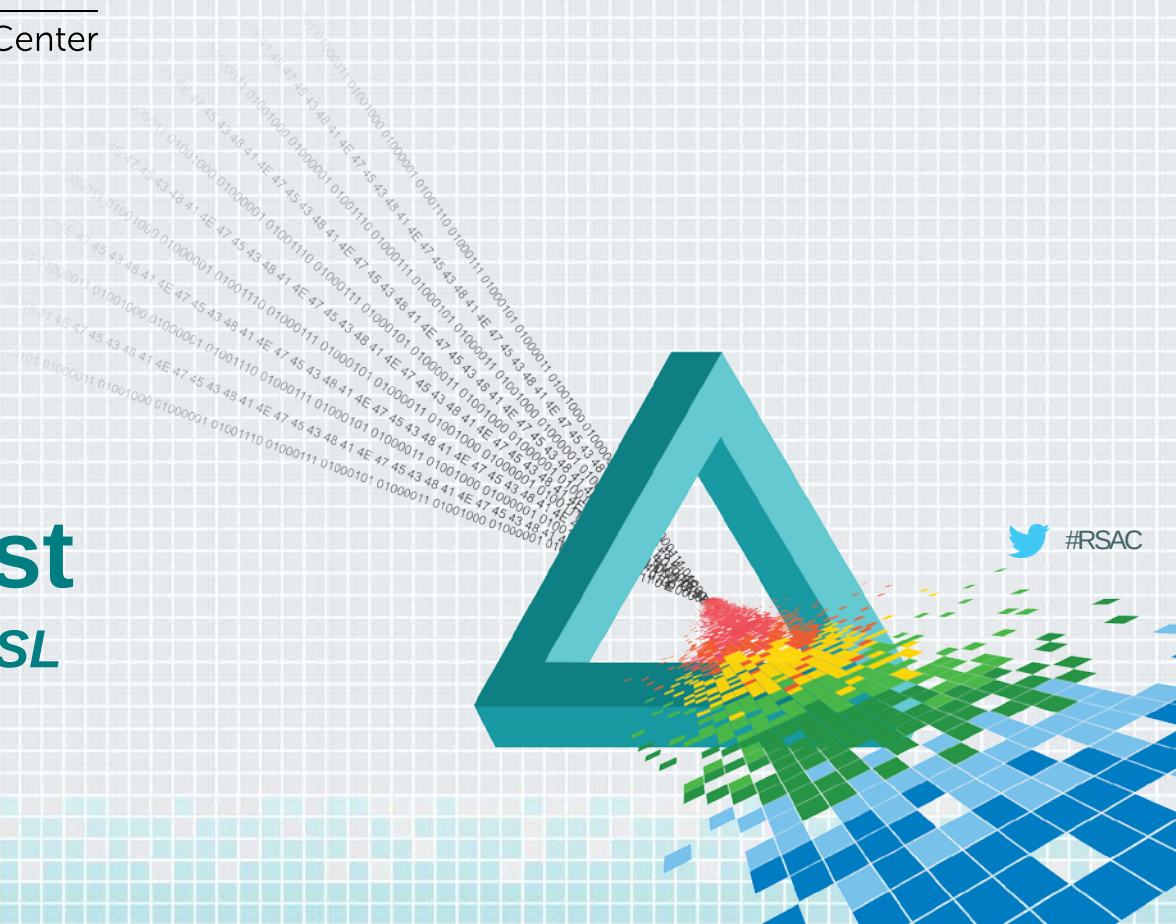
Fred Fuller Oil & Propane	com.wFredFuller	Business	100+
Free 2 Browse	com.wFree2Browse	Tools	10+
Free Classifieds Pensacola	com.wFreeAds	Shopping	100+
Free Animations Sharing	com.wFreeAnimationsSharing	Entertainment	1,000+
Freebies Junction	com.wFreebiesJunction	Social	100+
FREE Binary Options Signals	com.wFREEBinaryOptionsSignals	Finance	1,000+
FREE Binary Options Strategy	com.wFREEBinaryOptionsStrategy	Finance	1,000+
Free Career Advice	com.wFreeCareerAdvisor	Business	100+
FREE COPIER SUPPORT COMMUNI	com.wFREECOPIERSUPPORT	Tools	1,000+
FREE Craft and Hobby KINDLES	com.wFREECraftandHobbyKINDLEBOOKS	Books & Reference	1,000+
REMOVED	com.wFreeCreditMonitoringTarget	REMOVED	REMOVED
Freedom1	com.wFreedom1	News & Magazines	10+
FreedomOutpost	com.wFreedomOutpost	News & Magazines	100+
Freedom Wireless	com.wFreedomWireless1	Shopping	1,000+
EURUSD Forex Trading Signals	com.wFREEEURUSDForexTradingSignals	Finance	1,000+
FREE Forex Signals	com.wFREEForexSignals	Finance	10,000+
FREE GBPUSD Trading Signals	com.wFREEGBPUSDTradingSignals	Finance	500+
Free Gift Cards Palace	com.wFreeGiftCardsPalace	Shopping	1,000+
Free Hermes Bag- Get yours now	com.wFreeHermesBag	Shopping	500+
Latest Hindi Ringtone Free	com.wFreeHindiMovieLatestRingtone	Music & Audio	10,000+
Free Insta Likes And Followers	com.wFreeInstaFollowersAndLikes	Social	500+
Free Keywords Suggestion Tool	com.wFreeKeywordsSuggestionTool	Tools	100+
Freelanced	com.wFreelanced	Business	100+

Metova Credit Union Apps

Apex Federal Credit Union	com.metova.cuae.afcu	Finance	100+
ATL Federal Credit Union	com.metova.cuae.atlfcu	Finance	100+
Bloomington Postal ECU App	com.metova.cuae.bloomingtonpostal	Finance	10+
Community Credit Union Mobile	com.metova.cuae.ccu	Finance	500+
Day Air Credit Union	com.metova.cuae.dayair	Finance	1,000+
Education Personnel FCU	com.metova.cuae.educationpersonnel	Finance	100+
Enrichment Federal CU	com.metova.cuae.efcu	Finance	1,000+
Forest Area FCU Mobile	com.metova.cuae.fafcu	Finance	500+
Farm Bureau Family CU	com.metova.cuae.fbfcu	Finance	50+
Gulf Coast Educators FCU	com.metova.cuae.gcefcu	Finance	1,000+
GeoVista Credit Union Mobile	com.metova.cuae.gvcu	Finance	1,000+
Honor Credit Union Mobile	com.metova.cuae.hcu	Finance	1,000+
La Terre Federal Credit Union	com.metova.cuae.laterrefcu	Finance	100+
Magnify Credit Union	com.metova.cuae.magcu	Finance	100+
Mountain Credit Union	com.metova.cuae.mcu	Finance	1,000+
Memorial Credit Union Mobile	com.metova.cuae.memorial	Finance	500+
Notre Dame FCU	com.metova.cuae.ndfcu	Finance	1,000+
Partnership Financial CU	com.metova.cuae.ntscu	Finance	100+
Oak Trust CU App	com.metova.cuae.oaktrustcu	Finance	100+
Postal Family FCU App	com.metova.cuae.postalfamily	Finance	100+

RSAConference2015

San Francisco | April 20-24 | Moscone Center



Apps That Exist

And also fail to validate SSL

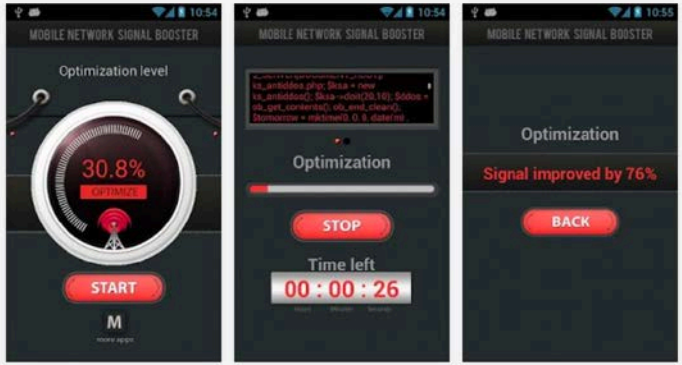
Mobile Network Signal Booster

Mobile Network Signal Booster

Slovak Creative Studio - April 25, 2013
Tools

Install | Add to Wishlist

★★★★☆ (472)



Description

Mobile Network Signal Booster allows you to optimize the level of the signal in your phone and use the nearest stations to significantly improve signal reception and the Internet!
Optimizes signal your phone in one click.
==========
Features of the application:
√ Very easy-to-use
√Optimizes signal not only a phone, but also the work of the Internet in your handset.
√For more effective optimization it is recommended to repeat optimization for several days

Reviews

Write a Review

3.9
★★★★☆
472 total

★ 5	270
★ 4	65
★ 3	33
★ 2	18
★ 1	86

AMAZING Out of the multitude of apps that I have tried to strengthen my netw ork signal, this is the only one that wo

Nanci M. LambCranford ★★★★★

Wooow Idk if this app really works for t he evo 4g when im outside my house i n the open area my signels fine with th

Anthony Kasowski ★☆☆☆☆

Mobile Network Signal Booster

Additional information

Updated	Size	Installs	Current Version
April 25, 2013	13M	50,000 - 100,000	1.0

Requires Android	Content Rating	Contact Developer
2.2 and up	Everyone	Email Developer

Cartoon Wars

Cartoon Wars

GAMEVIL Inc. - August 26, 2014

Arcade

Install | Add to Wishlist

This app is compatible with all of your devices. **Offers in-app purchases**

★★★★½ (459,875)

+1 +79665 Recommend this on Google

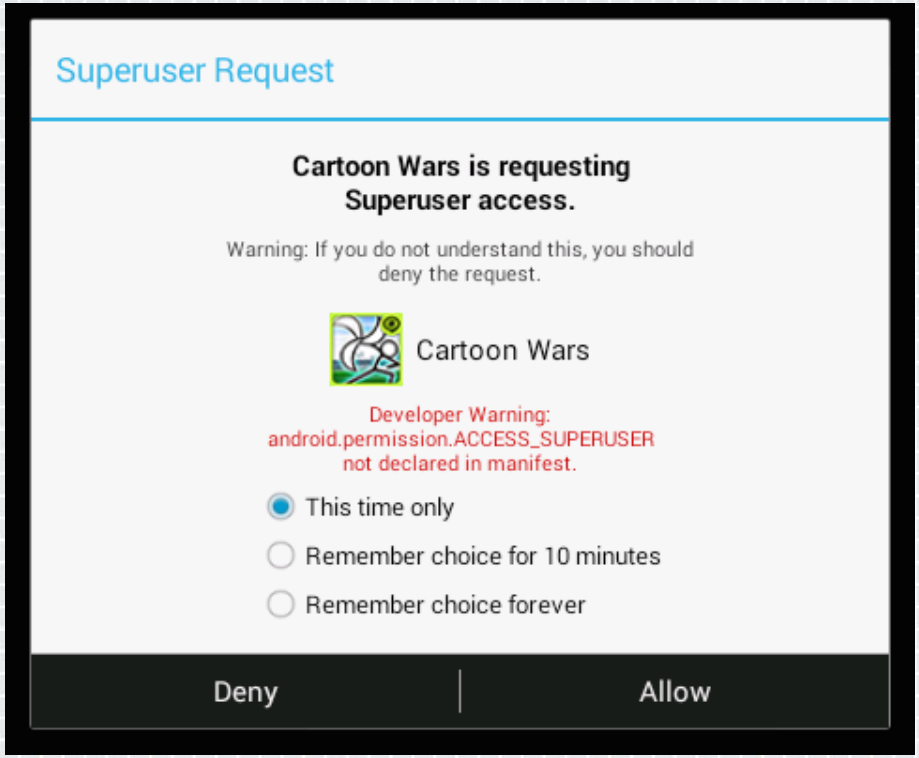
Top Developer

Cartoon Wars

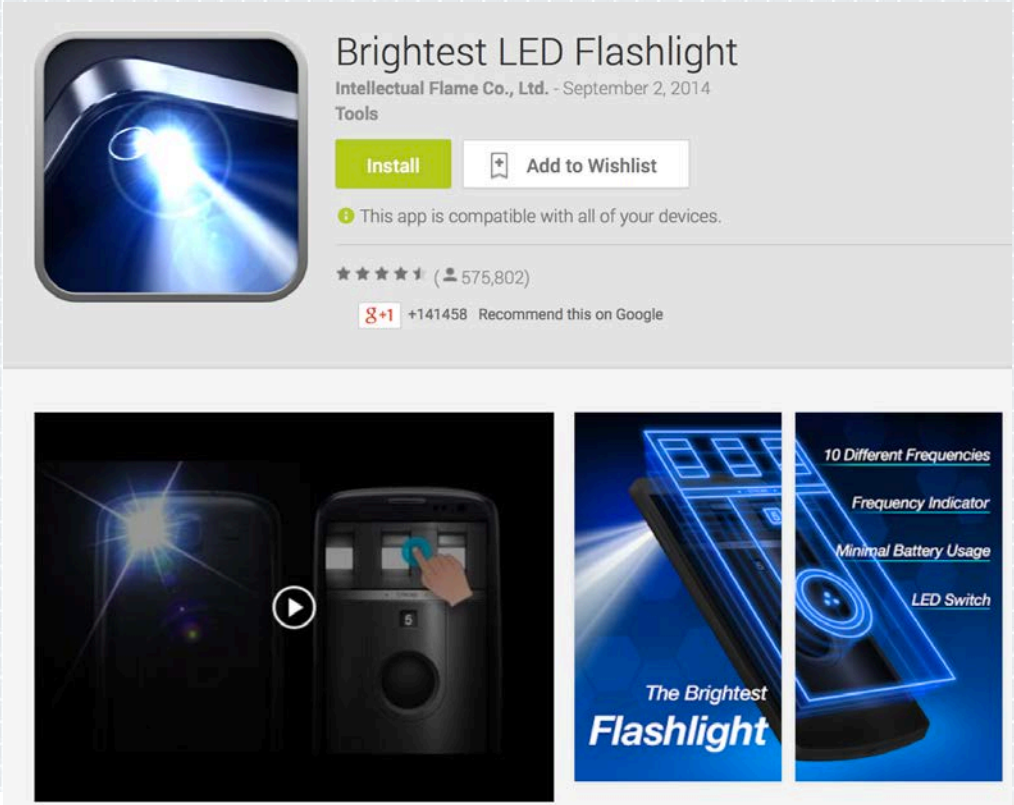
Additional information

Updated August 26, 2014	**Size** 15M	**Installs** 10,000,000 - 50,000,000	**Current Version** 1.1.1
Requires Android 2.2 and up	**Content Rating** Medium Maturity	**In-app Products** $0.99 - $99.99 per item	**Permissions** View details
Report Flag as inappropriate	**Offered By** GAMEVIL Inc.	**Developer** Visit Website Email contact@gamevilusa.com Privacy Policy 999 N Sepulveda Blvd, Ste 150, El Segundo, CA, United States	

Cartoon Wars



Brightest LED Flashlight



RSAConference2015

San Francisco | April 20-24 | Moscone Center

Selected Developer Responses

Still optimistic?

Application author response

Hello,

Thank you for your e-mail! The app that you have in mind is not created or related to us or [REDACTED]. We recently found out about it and we are looking for a way to take it down as it's made by a person trying to exploit [REDACTED]'s name. Is there a way to report this app and take it down? We would really appreciate help in this.

Application author response

I understand, i was consuming a service the generates real random numbers based on measurements of quantum phenomena.

So i just didnt cared about the ssl config on the http request since it was a very trivial.

Application author response

I don't know what the hell you're talking about, my application does not include any SSL connection !!!

Application author response

Remove

Application author response

What????

Application author response

I want to thank you very much fix for SSL, but Google Play Store my suspends, I want to fix bugs, I want to get back my application, please help

Application author response

Mr. Will

Thanks alot for your analysis. We checked everything in the app. There is not even a single bug. Your mail is type a type of spam which is of no use. If you really have something then work practically.

Application author response

Hi CERT Coordination Center,

Our application is an authentication application and has among other features a backend where there is a Risk Engine present, the communication taking place when connecting with a faulty certificate is to merly a notification mechanism to tell the server the communication channel is beeing tampered with. As such, it is a feature that our application to continue to communicate with the backend even even thought the channel is compromised by usage of a faulty certificate.

Application author response

Well I’m not sure how a SSL Vulnerability can be present in an application when I don’t take any payments through the application for any product. Looks like you have much more testing to do. Can you please stop sending me emails.

Thanks

–

Application author response

```
take me off your list
```

Application author response

Please contact the NSA.gov for this case because I am not the owner of this site

Thank you

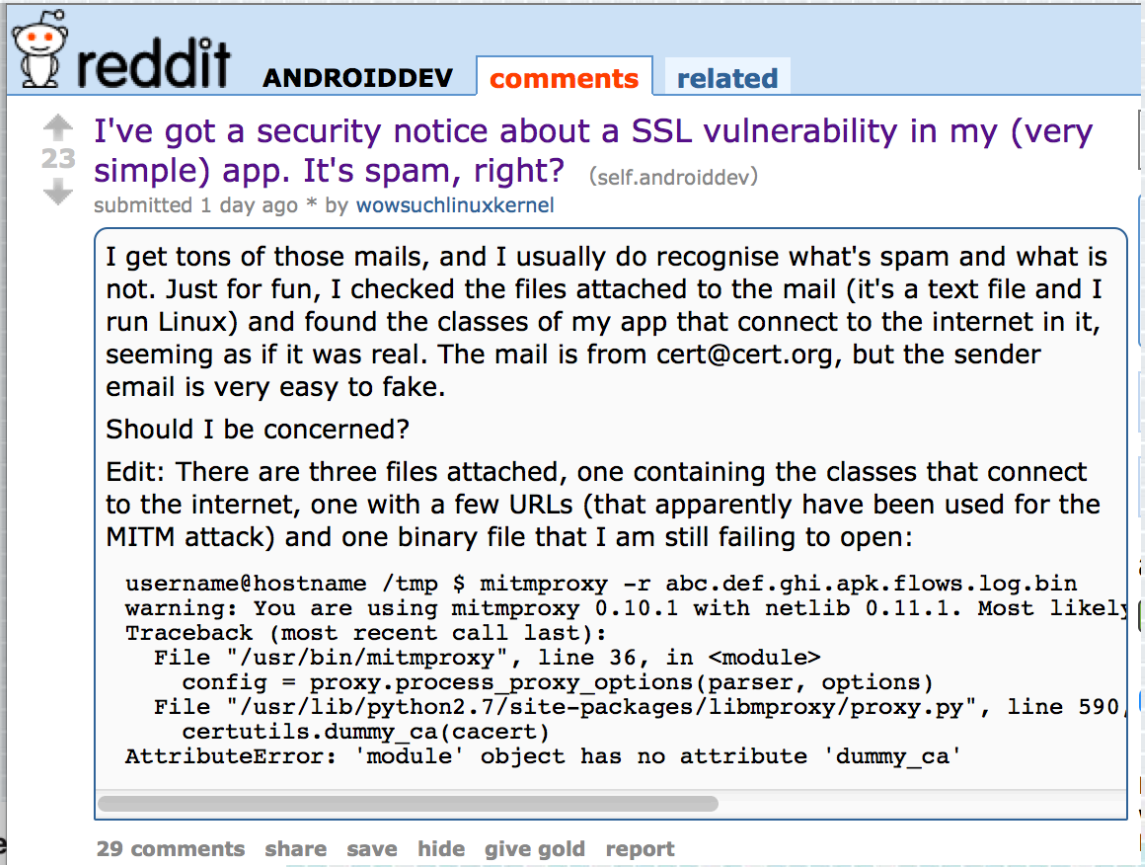
RSAConference2015

San Francisco | April 20-24 | Moscone Center

Public Reception

Fighting the battle of who could care less

Reddit



reddit ANDROIDDEV comments related

23

I've got a security notice about a SSL vulnerability in my (very simple) app. It's spam, right? (self.androiddev)

submitted 1 day ago * by wowsuchlinuxkernel

I get tons of those mails, and I usually do recognise what's spam and what is not. Just for fun, I checked the files attached to the mail (it's a text file and I run Linux) and found the classes of my app that connect to the internet in it, seeming as if it was real. The mail is from cert@cert.org, but the sender email is very easy to fake.

Should I be concerned?

Edit: There are three files attached, one containing the classes that connect to the internet, one with a few URLs (that apparently have been used for the MITM attack) and one binary file that I am still failing to open:

```
username@hostname /tmp $ mitmproxy -r abc.def.ghi.apk.flows.log.bin
warning: You are using mitmproxy 0.10.1 with netlib 0.11.1. Most likely
Traceback (most recent call last):
  File "/usr/bin/mitmproxy", line 36, in <module>
    config = proxy.process_proxy_options(parser, options)
  File "/usr/lib/python2.7/site-packages/libmproxy/proxy.py", line 590,
    certutils.dummy_ca(cacert)
AttributeError: 'module' object has no attribute 'dummy_ca'
```

29 comments share save hide give gold report

Reddit

[–] **flagrantaroma** 4 points 1 day ago

The issue would be that if you do not use SSL somebody using your app who is on a hostile network could have that publicly available file replaced with a malicious file without realizing it. The replacement could be filled with phishing links or exploit a vulnerability in the code that is processing that file.

permalink save parent report give gold reply

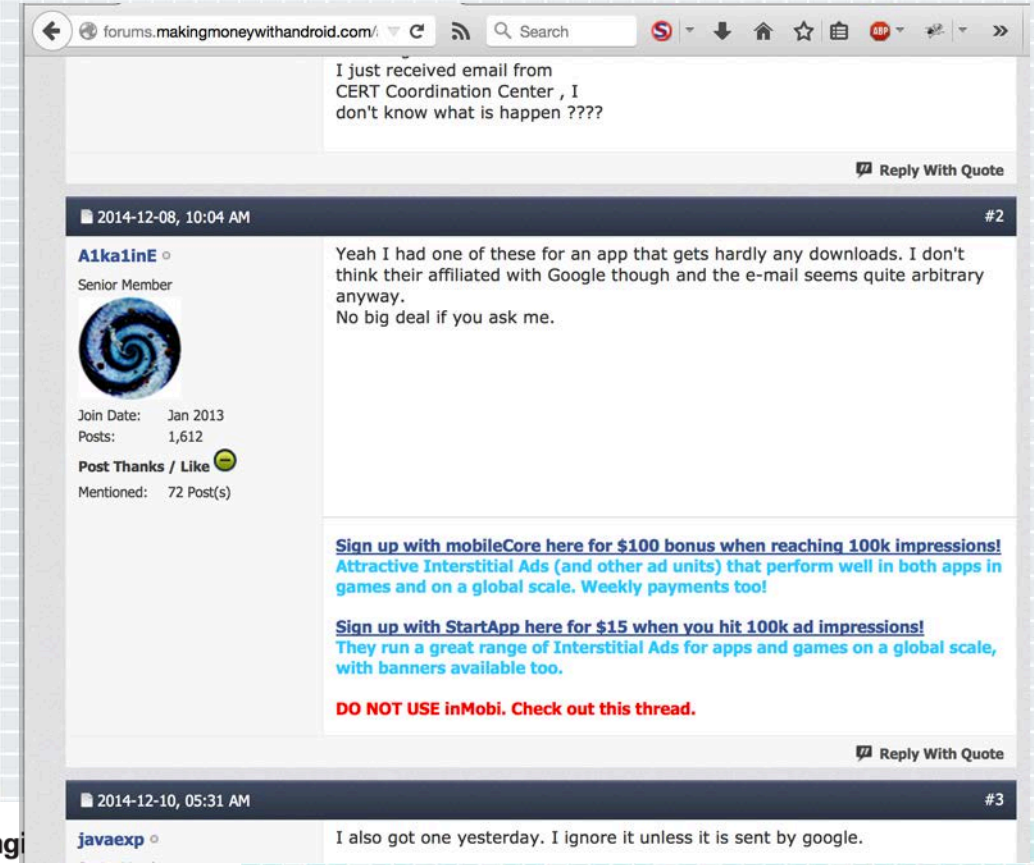
[–] **wowsuchlinuxkernel** [S] -8 points 1 day ago

Right! Thanks, I did not think about that. My app's audience are people who have much knowledge of computers so I think I can keep this "bug" unfixed.

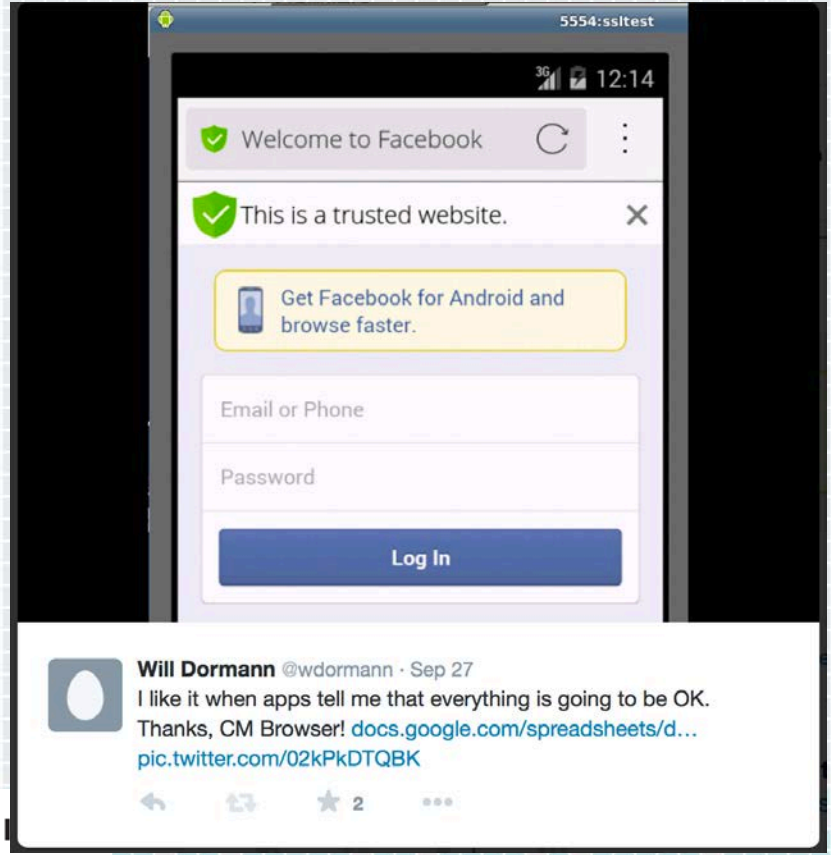
Thank you for your help.

permalink save parent report give gold reply

forums.makingmoneywithandroid.com



Twitterverse #1 (warmup)



Four Months Later

Twitterverse #2 (Getting interesting)

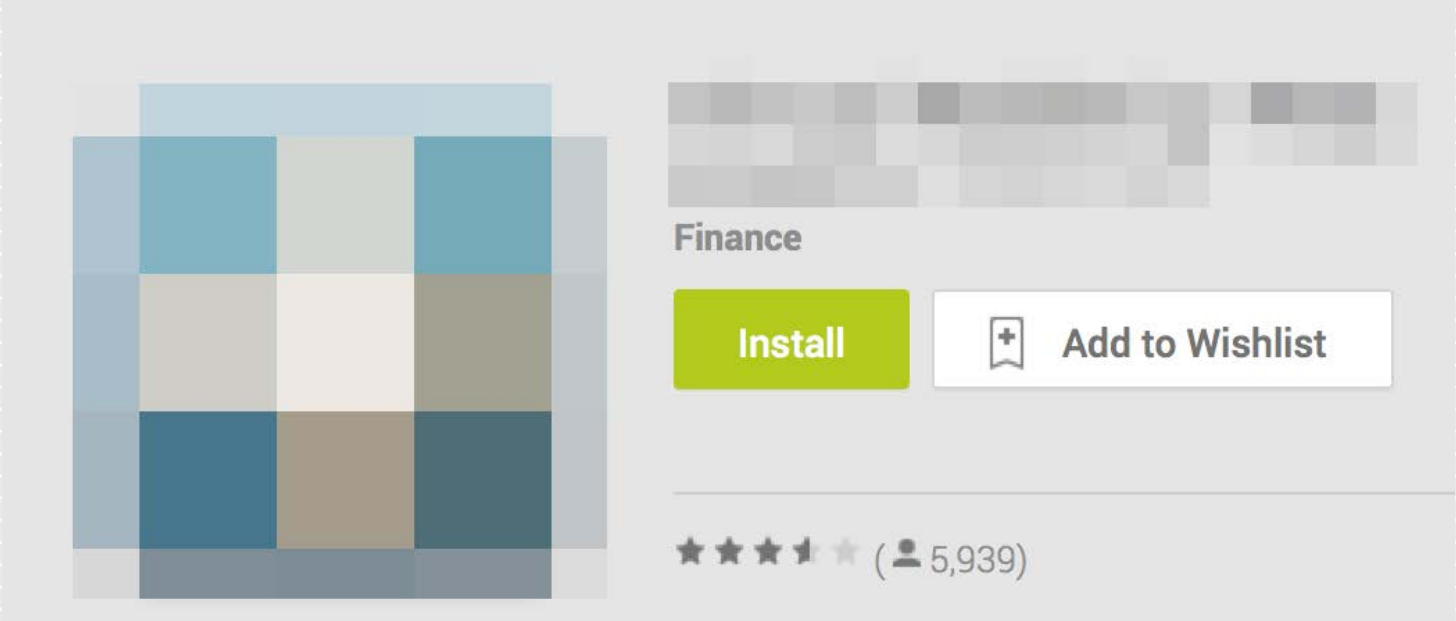
Reality-distortion field

"We have systems in place to immediately react to the ever-changing demands of the digital environment. Our credit card app has never experienced a security vulnerability."

The spokesperson added that the app is read only and all customer's money is protected under MasterCard's guarantee.

http://www.computerworld.com.au/article/554457/coles-responds-credit-card-app-vulnerability-reports/

Let's go nuclear



Vendor Reaction

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Not Everything is Bad

At least one

Somebody Cares!

Hello.

Thank you very much for the reply. I've confirmed that our record has been updated in the spreadsheet. And let me say thank you again for your hard efforts to investigate and report problems in large number of Android apps. Without your help, we'd have overlooked the issue much longer.

Best Regards,

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Statistics

Numbers don't lie?

The Numbers

	Total	Percent
Free Apps Tested	1,000,500	Most?
Vulnerable Apps Discovered	23,667	2.4%
Vulnerable App Authors Notified	23,301	98.5%
Email responses	1,593	6.8%
Email responses with fix details	25	0.1%

"There are now 1 million apps in the Google Play store."
July 24, 2013

http://mashable.com/2013/07/24/google-play-1-million/

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Where do we go from here?

Forward

Further Work

- Full SSL visibility (Root CA cert installed)
- Improved automation
- Other Platforms (IOS, Blackberry, Windows Phone)
- True Scalability

Conclusions

- Vulnerability coordination doesn’t scale easily
- CVE doesn’t scale easily
- There are plenty of horrible Android applications
- Application authors aren’t very responsive

Apply What You Have Learned Today

- Next week you should:
  - Download CERT Tapioca
  - Test using CERT Tapioca
- In the first three months following this presentation you should:
  - Use Tapioca to test applications used in your organization for SSL validation failures
    - Non-free applications
    - Non-Android applications
    - Report failures to CERT