

SESSION ID: HTA-T08

How We Discovered Thousands of Vulnerable Android Apps in 1 Day

Joji Montelibano

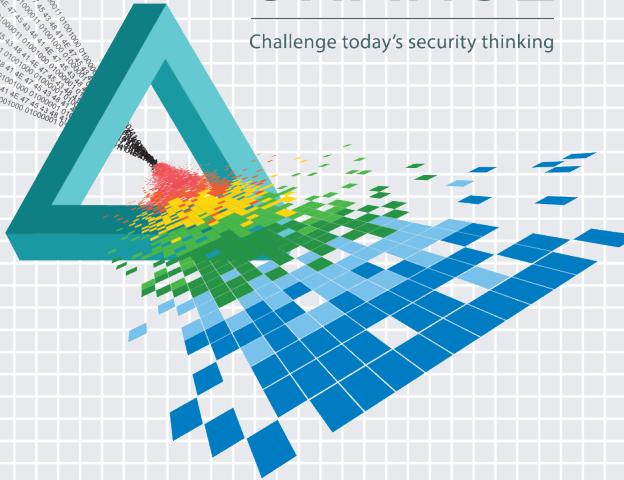
Vulnerability Analysis Technical Manager
CERT
@certcc

Will Dormann

Vulnerability Analyst
CERT
@wdormann

CHANGE

Challenge today's security thinking



Copyright

Copyright 2015 Carnegie Mellon University

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.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

CERT® and CERT Coordination Center® are registered marks of Carnegie Mellon University.

DM-0002136



Software Engineering Institute
Carnegie Mellon



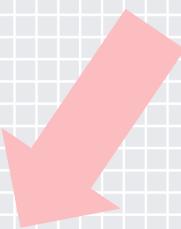
What is CERT?

- ◆ 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)

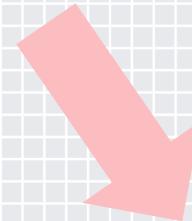


CERT Vulnerability Analysis

Mission: Make Software Safer



Vulnerability
Coordination



Vulnerability
Discovery

RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

Vulnerability Coordination

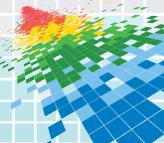
Is easy?



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.



RSA® Conference 2015

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

kmplayer - Bing - Windows Internet Explorer
http://www.bing.com/search?q=kmplaye

bing kmplayer

Web Images Videos Maps News More

Also try: VLC · KMP · RealPlayer

2,180,000 RESULTS Any time ▾

Ads related to kmplayer

[KMPlayer 2014 Free - Download KMPlayer 100% Free!](#)
[Download.com/KMPlayer](#)
Download KMPlayer 100% Free! Download 2014 Version Here.
[KMPlayer 2014 Download](#) [Newest Version](#)
[Get KMPlayer Today](#) [Free Download](#)

[Download KMPlayer Free | KMPlayer.TheAppCenter.com](#)
[KMPlayer.TheAppCenter.com/Free](#)
Full Version Free Windows Download
theappcenter.com is rated ★★★★☆ on Bing (11125 reviews)
[Security Software](#) [Browsers & Extensions](#)
[Entertainment Software](#) [Office & Productivity](#)
[Creative & Editing](#) [Social & Lifestyle](#)

Identical installers

- ◆ Installers from Download.com are the same:
 - ◆ 5a275a569dce6e2f2f0284d82d31310b *cbsid1m-cbsi213-
Enable_Disable_Registry_Tool-SEO-75812481.exe
 - ◆ 5a275a569dce6e2f2f0284d82d31310b *cbsid1m-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]]></FileMd5Checksum><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_d56f7814cd5af230f782dd28550e185a</  
DownloadLink><TrackedDownloadLink>http://dw.cbsi.com/redir?  
edId=1174&siteId=4&lop=feed.dl&ontId=13632&tag=tdw_dlman&pid=13819308&dest  
Url=http%3A%2F%2Fsoftware-files-a.cnet.com%2Fs%2Fsoftware  
%2F13%2F81%2F93%2F08%2FKMPlayer_3.9.1.129.exe%3Ftoken  
%3D1413054436_2defb65a1350a3b035964c18f30fb06e%26fileName%3DKMPlayer_3.9.1.129.exe
```

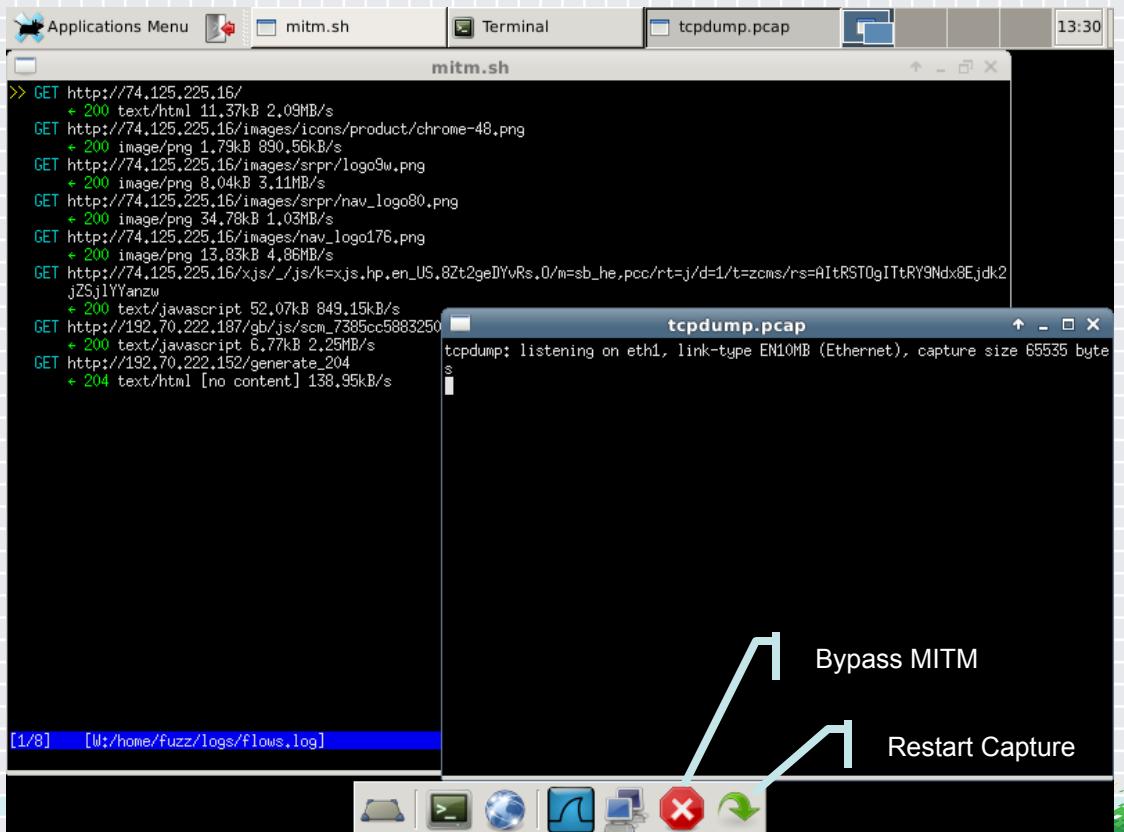
Just MITM it!

- ◆ 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

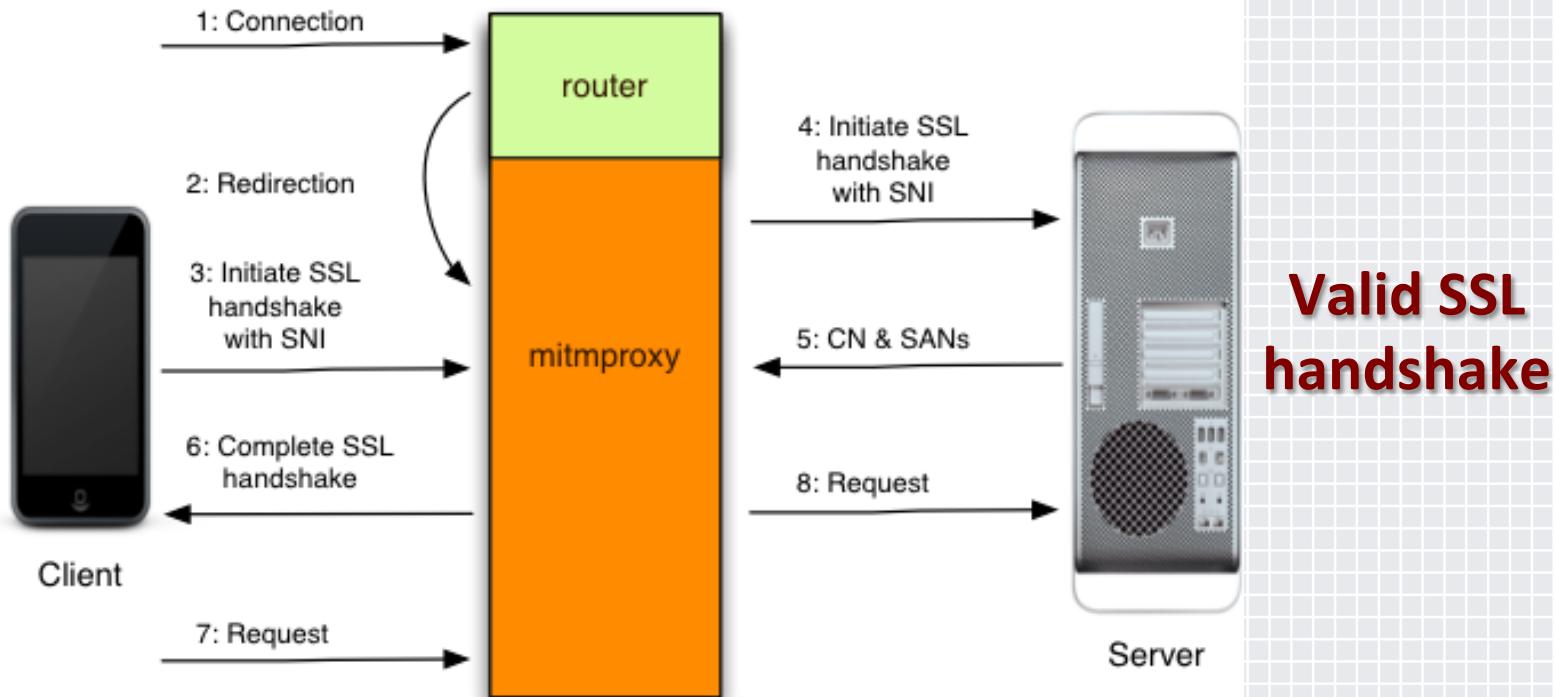
[Finding Android SSL Vulnerabilities with CERT Tapioca](#)

[Announcing CERT Tapioca for MITM Analysis](#)

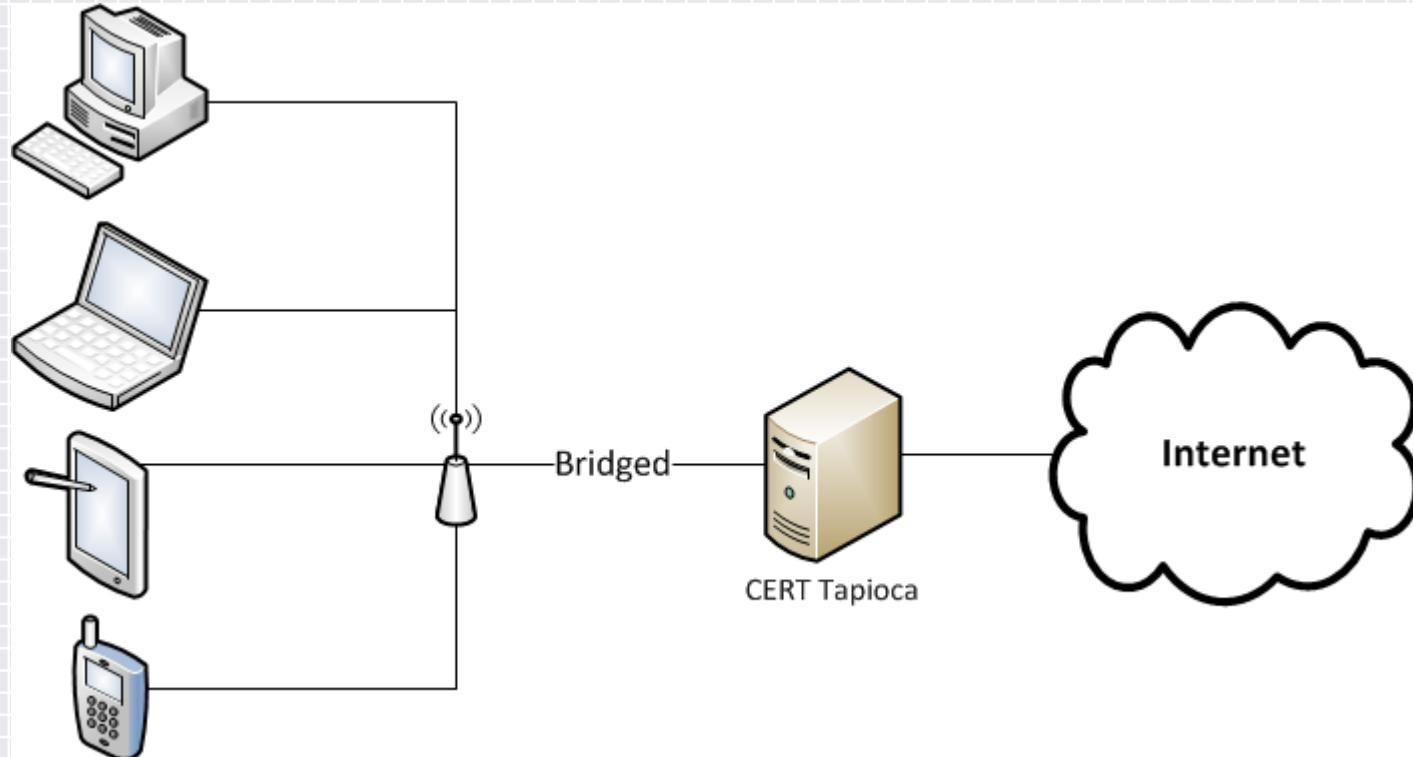
<http://www.cert.org/vulnerability-analysis/tools/cert-tapioca.cfm>

How it works

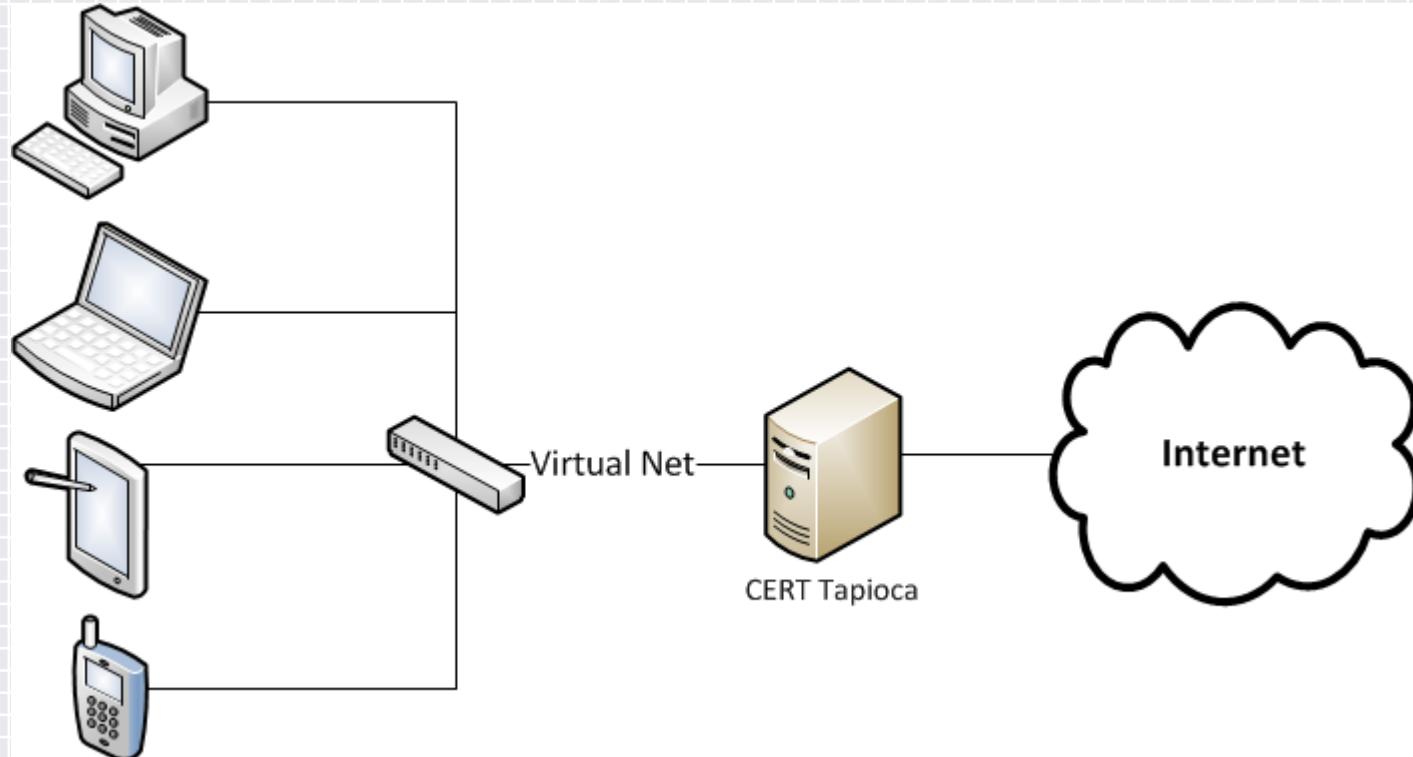
I can see everything if the client doesn't validate SSL



Tapioca architecture



Tapioca architecture



Investigating Android

- ◆ Use a phone and a wireless access point

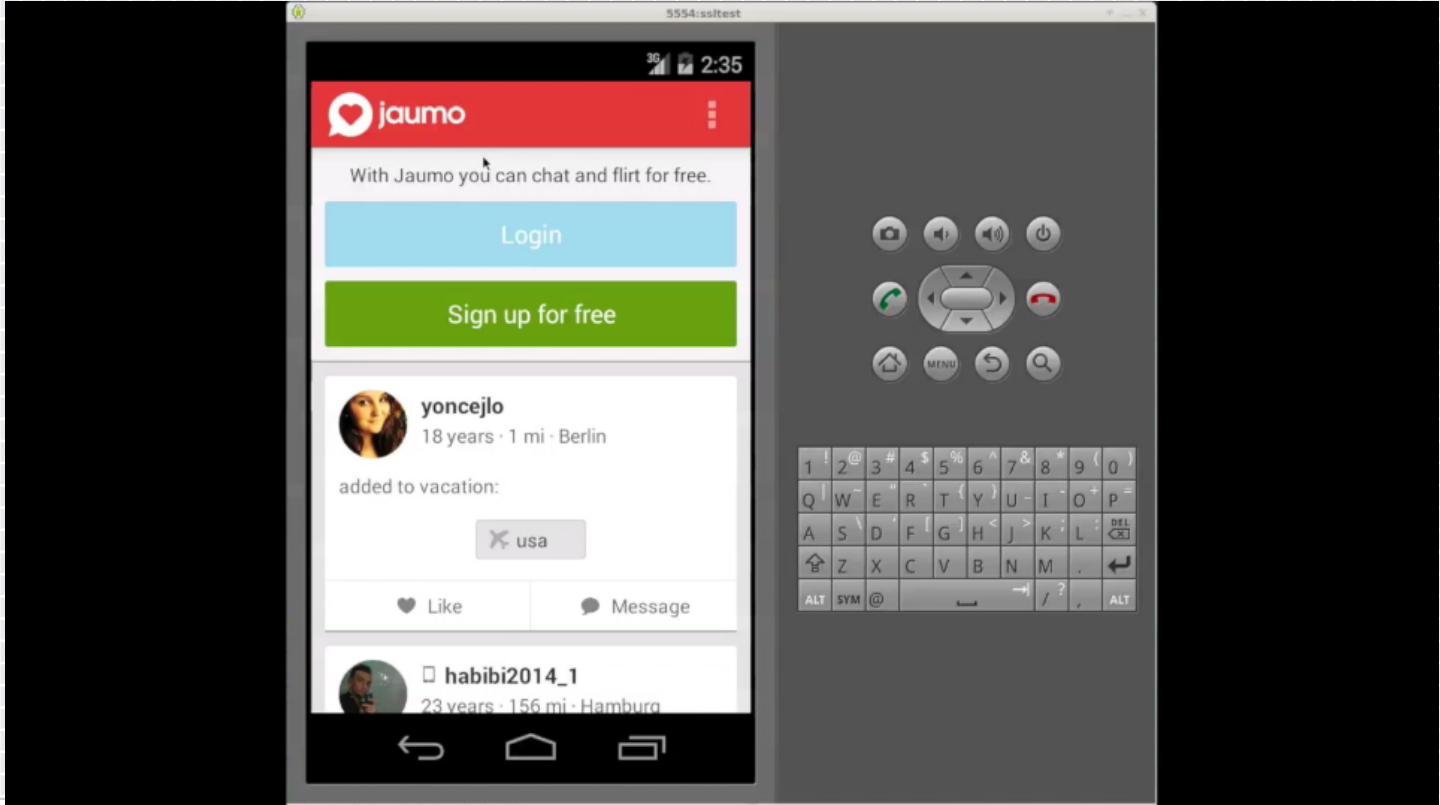


Improvement #1

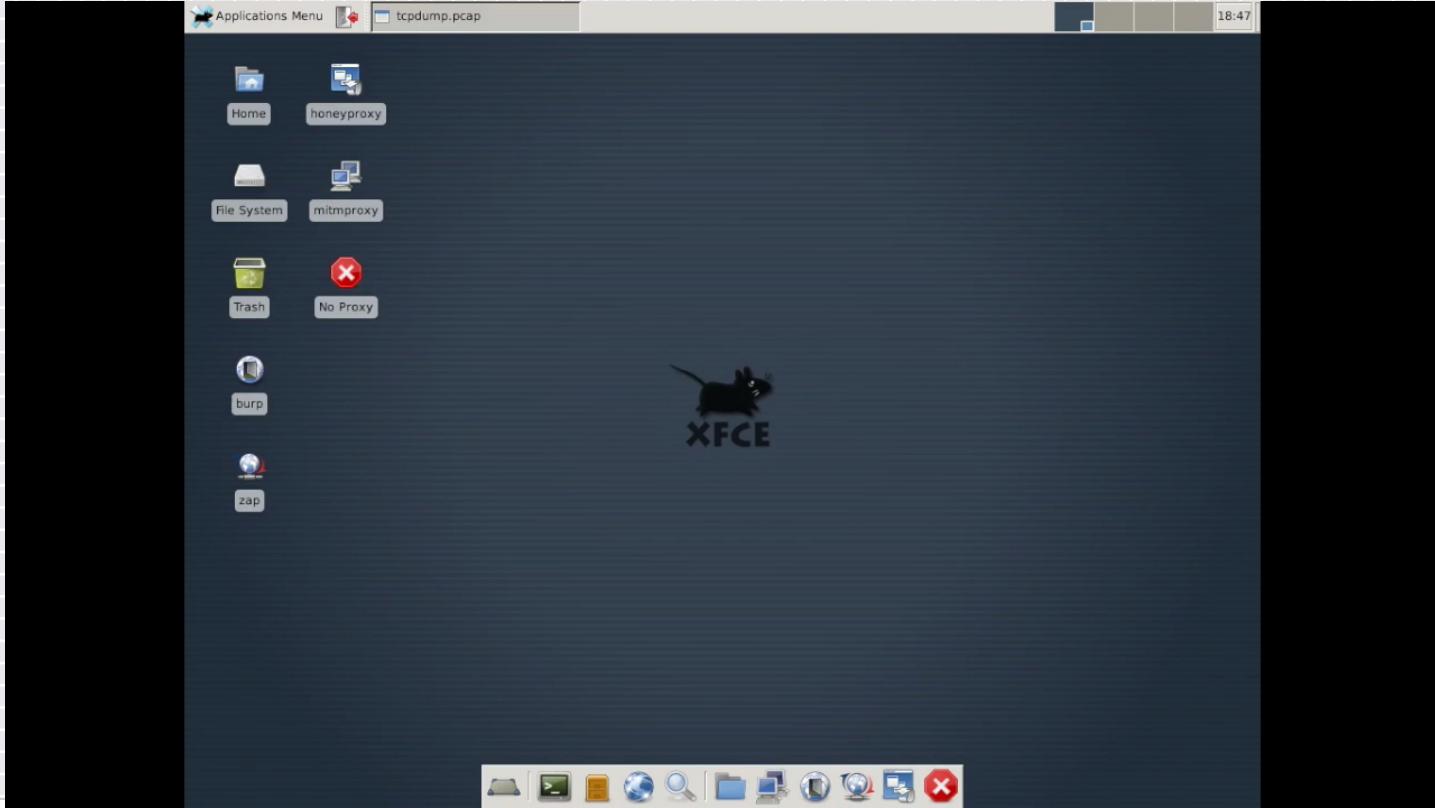
- ◆ Virtualization and Automation
 - google-play-crawler
 - VMware
 - Android SDK
 - AVD
 - Monkeyrunner
 - Monkey
- ◆ Now I can test when I sleep!

<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

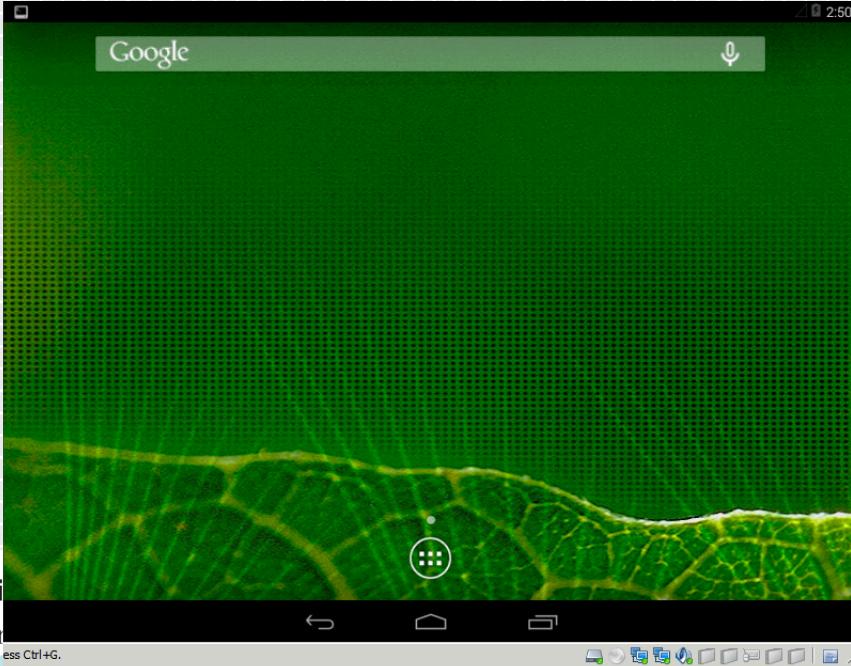
- ◆ Parallelization
- ◆ Rather than 1 Android VM and 1 Tapioca VM, what about 20 of each?
- ◆ Now I can test 20x faster!

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.

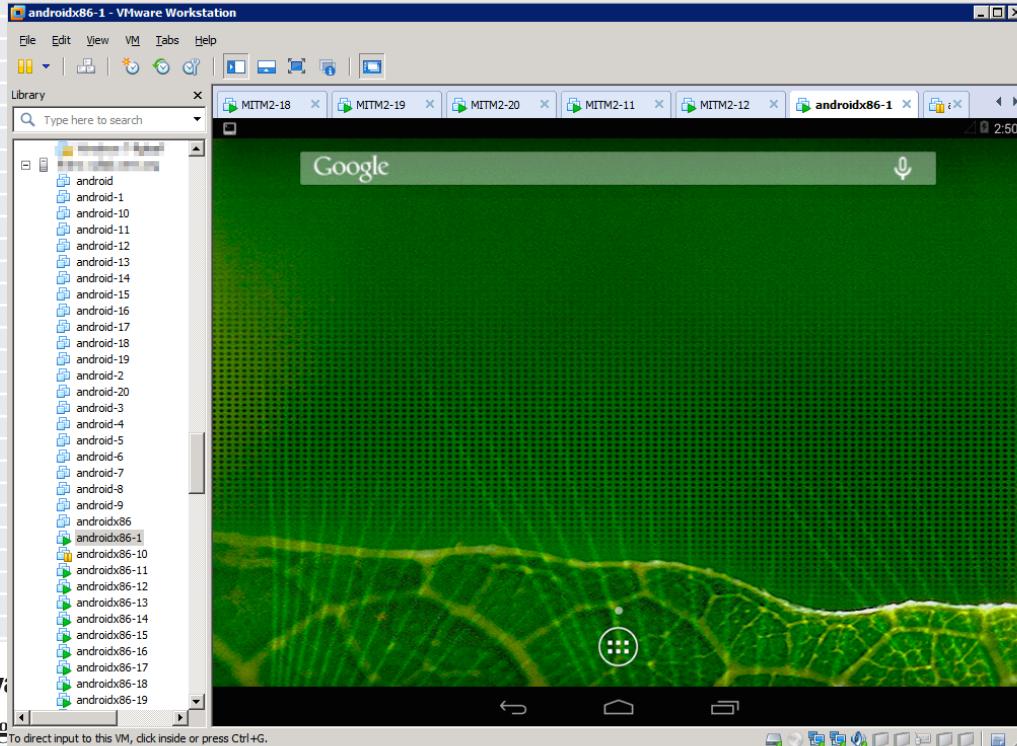
Improvement #3

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

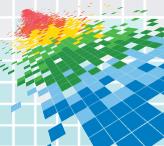


Improvement #4

- ◆ Let's make 20 of them!



Androidx86 SSL Test Architecture



Automation of 20 VMs

```

192.168.0.108:5555
adb failed! Trying again...
connecting again to 192.168.0.108:5555
already connected to 192.168.0.108:5555
599 Kb/s (3245147 bytes in 2.269s)
    pkg: /data/local/tmp/cow.Ft451.jerusalem.apk
success
launching com.ft451.jerusalem.apk
already connected to 192.168.0.108:5555
starting Intent { cmp=com.ft451.jerusalem/.jerusalem }
exit status: 0
    sxf3.sh
        at java.lang.reflect.Method.invoke(Method.java:515)
        at com.android.internal.os.ZygoteInit$MethodAndArgsCaller.run(ZygoteInit.java:779)
        at com.android.internal.os.ZygoteInit.main(ZygoteInit.java:595)
        at dalvik.system.NativeStart.main(Native Method)

Monkey aborted due to error.
events injected: 481
sending rotation degrees=0, persist=false
dropped: keys=2 pointers=0 trackballs=0 flips=0 rotations=0
Network state: elapsed time=429ms (ms mobile, 0ms wifi, 429ms not connected)
System appears to have crashed at event 461 of 500 using seed 1413485868941
exit status: 0
192.168.0.108:5555
capping capture

    sxf10.sh
        connecting again to 192.168.0.110:5555
        already connected to 192.168.0.110:5555
        555 Kb/s (37848163 bytes in 12.589s)
            pkg: /data/local/tmp/cow.attackpops005.apk
success
launching com.attackpops005.apk
already connected to 192.168.0.110:5555
starting Intent { cmp=com.attackpops005/.AttackPops }
exit status: 0
192.168.0.110:5555
witing...
    sxf4.sh
        reverting VM
        starting VM
        starting captures
        connecting to Android:00-4 : 192.168.0.104
        connected to 192.168.0.104:5555
        ready connected to 192.168.0.104:5555
        exit status: 0
        192.168.0.104
        installing nl.chirio.UniProt.apk to 192.168.0.104:5555
        already connected to 192.168.0.104:5555
        error: device offline
        error: device offline
        error: device offline
        waiting for device -
        rm failed for /data/local/tmp/com.concept.ottawaspring.apk. No such file or directory
        exit status: 1
        192.168.0.104:5555
        adb failed! Trying again...
        connecting again to 192.168.0.104:5555
        already connected to 192.168.0.104:5555
    sxf7.sh
        Reverting VM
        Starting VM
        Restarting captures
        Connecting to Android:00-5 : 192.168.0.105
        connected to 192.168.0.105:5555
        already connected to 192.168.0.105:5555
        exit status: 0
        192.168.0.105
        Installing com.acevedosilva.silenthover.apk to 192.168.0.105:5555
        already connected to 192.168.0.105:5555
        error: device offline
        error: device offline
        error: device offline
        - waiting for device -
    sxf9.sh
        exit status: 1
        192.168.0.109:5555
        adb failed! Trying again...
        connecting again to 192.168.0.109:5555
        already connected to 192.168.0.109:5555
        2049 Kb/s (29549465 bytes in 12.171s)
            pkg: /data/local/tmp/cow.noodlecake.spinsafari.apk
success
        launching com.noodlecake.spinsafari.apk
        already connected to 192.168.0.109:5555
        Starting Intent { cmp=com.noodlecake.spinsafari/com.eportable.activity.VerdeActivity }
        exit status: 0
        192.168.0.109:5555
        Waiting...
    sxf2.sh
        connecting to Android:00-2 : 192.168.0.102
        connected to 192.168.0.102:5555
        already connected to 192.168.0.102:5555
        exit status: 0
        192.168.0.102
        installing com.concept.ottawaspring.apk to 192.168.0.102:5555
        already connected to 192.168.0.102:5555
        error: device offline
        error: device offline
        error: device offline
        - waiting for device -
        rm failed for /data/local/tmp/com.concept.ottawaspring.apk. No such file or directory
        exit status: 1
        192.168.0.102:5555
        adb failed! Trying again...
        connecting again to 192.168.0.102:5555
        already connected to 192.168.0.102:5555
    sxf6.sh
        :Sending Touch (ACTION_UP): 0:(621,0328,135,38068)
        :Sending Trackball (ACTION_NONE): 0:(-5,0,3,0)
        Events injected: 500
        :Dropping: keys=0 pointers=0 trackballs=0 Flips=0 rotations=0
        ## Network state: elapsed time=36139ms (0ms mobile, 0ms wifi, 36139ms not connected)
        // Monkey Finished
        exit status: 0
        192.168.0.106:5555
        Stopping capture
        Generating URLs file
        grabbing com.appastrophe.multimedia.beautiful_churche.apk.flows.log
    sxf8.sh
        192.168.0.107
        Powering off VM
        Reverting VM
        Starting VM
        Restarting captures
        Connecting to Android:00-7 : 192.168.0.107
        connected to 192.168.0.107:5555
        already connected to 192.168.0.107:5555
        exit status: 0
        192.168.0.107
        Installing com.spooncode.kawaly_o.waz_i_zone.apk to 192.168.0.107:5555
        already connected to 192.168.0.107:5555
        error: device offline
        error: device offline
        error: device offline
        - waiting for device -
    sxf1.sh
        :Sending Touch (ACTION_DOWN): 0:(329,0,108,0)
        :Sending Touch (ACTION_UP): 0:(423,50495,121,57026)
        :Sending Touch (ACTION_DOWN): 0:(363,0,545,0)
        //Calendar_time=2014-10-10 02:52:27.274 system_uptime=255574
        // Sending event #400
        :Sending Touch (ACTION_UP): 0:(367,89368,500,51605)
        :Sending Touch (ACTION_DOWN): 0:(107,0,457,0)
        :Sending Touch (ACTION_UP): 0:(53,288746,411,03348)
        :Sending Touch (ACTION_DOWN): 0:(-5,0,4,0)
        :Sending Trackball (ACTION_MOVE): 0:(514,0,23,0)
        :Sending Touch (ACTION_UP): 0:(528,5926,238,26576)
        :Sending Trackball (ACTION_MOVE): 0:(2,0,4,0)
        :Sending Trackball (ACTION_MOVE): 0:(-4,0,0,0)
        :Setuid Intent{ android.intent.action.MRIN;category=android.intent.category.LAUNCHER } flags=0x200000 component=com.appexpress.joeslawnservice/com.appexpress.LaunchActivity
        // Allowing start of Intent { actions=android.intent.action.MRIN cat=[android.intent.category.LAUNCHER] cmp=com.appexpress.joeslawnservice/com.appexpress.LaunchActivity }
        :Sending Trackball (ACTION_MOVE): 0:(0,0,-3,0)
    
```



RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

Android SSL Coordination

This one's optimistic



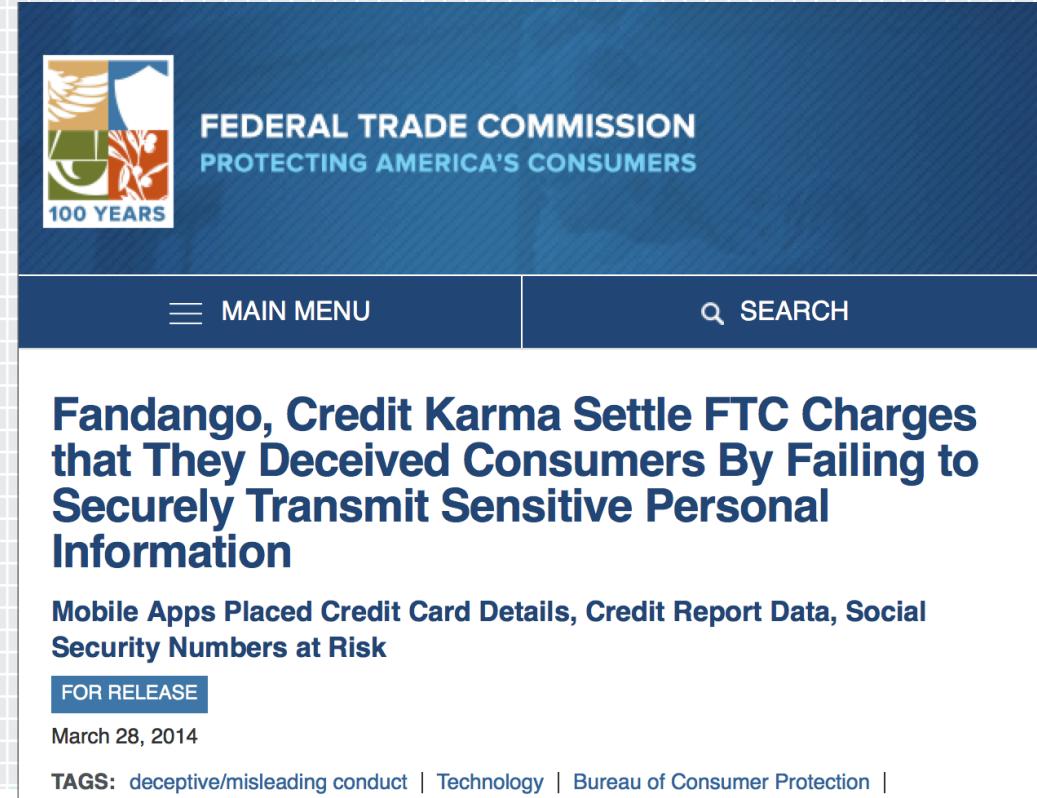
Prior SSL Investigations

- ◆ 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



The screenshot shows the official website of the Federal Trade Commission (FTC). The header features the FTC logo with four stylized icons (a shield, a scale, a key, and a torch) and the text "FEDERAL TRADE COMMISSION" and "PROTECTING AMERICA'S CONSUMERS". Below the logo is a "100 YEARS" anniversary graphic. The navigation bar includes a "MAIN MENU" button and a "SEARCH" bar. The main content area displays a news article titled "Fandango, Credit Karma Settle FTC Charges that They Deceived Consumers By Failing to Securely Transmit Sensitive Personal Information". A subtitle below the title reads "Mobile Apps Placed Credit Card Details, Credit Report Data, Social Security Numbers at Risk". A "FOR RELEASE" button, the date "March 28, 2014", and a "TAGS" section with terms like "deceptive/misleading conduct", "Technology", and "Bureau of Consumer Protection" are also visible.

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:

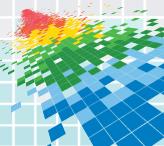
APP_ID

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

SIGN IN Share

App	Link	Genre	Count	Date added	Version tested	mallodroid broken	Library traffic observed	Non-library traffic observed
Abode	abode.webview	Tools	100+	2014-09-03	1.7	Maybe		TRUE
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
Alexis y Fido	air.AlexisyFidoMobolive	Entertainment	5,000+	2014-09-03	2.4.5	FALSE		
Princess Shopping	air.android.PrincessSh	Family	100,000+	2014-09-03	2.0	TRUE	TRUE	TRUE
Buses de Córdoba	air.AucorsaMobile	Tools	5,000+	2014-09-03	@7F050002	FALSE		
Baby Get Up - Kids Care	air.brown.jordansa.getu	Casual	10,000+	2014-09-03	1.0.3	Maybe	TRUE	TRUE
REMOVED	air.cloudMobileApp	REMOVED	10,000+	2014-09-03	@7F040001	FALSE		
Bingo Bash - Free Bingo Casino	air.com.bithymes.bingc	Casino	10,000,000+	2014-09-03	1.31.1	TRUE		TRUE
Abduction Stacker Free	air.com.chewygames.at	Casual	50+	2014-09-03	1.0.7	Maybe	TRUE	TRUE
Comca Catalog	air.com.comcasystems.	REMOVED	10+	2014-09-03	@7F040001	FALSE		
Westmoreland Water FCU	air.com.creditunionhom	Finance	50+	2014-09-03	1.2.0	Maybe		TRUE
Michael Baker FCU	air.com.creditunionhom	Finance	10+	2014-09-03	1.2.0	Maybe		TRUE
Flick a Trade	air.com.cygnecode.fat	Finance	5,000+	2014-09-03	3.3	TRUE		TRUE
Hidden Memory - Aladdin FREE!	air.com.differencegame	Casual	10,000+	2014-09-03	1.0.31	TRUE	TRUE	TRUE
Hidden Object Mystery	air.com.differencegame	Casual	50,000+	2014-09-03	1.0.65	TRUE	TRUE	TRUE
Hidden Object - Alice Free	air.com.differencegame	Casual	10,000+	2014-09-03	1.0.17	TRUE	TRUE	TRUE
Addison Time Entry	air.com.easySoftwareS	Business	10+	2014-09-03	1.00	FALSE		
Festa SAAS	air.com.festa.saas	Business	100+	2014-09-03	1.0 RC08	FALSE		
SongPop	air.com.freshplanet.gar	Music	10,000,000+	2014-09-03	1.21.2	TRUE		TRUE
Sprint jump	air.com.ilaz.applas	Adventure	5+	2014-09-03	1.0	Maybe		TRUE
Africa Memory	air.com.klon4enabor4e.	Puzzle	100,000+	2014-09-03	1.0.1	TRUE	TRUE	TRUE
Return to the Penguin Kingdom	air.com.mediafront.Retu	Lifestyle	100+	2014-09-03	@7F040001	FALSE		
Mahjong Galaxy Space Lite	air.com.permadi.mahjor	Puzzle	10,000+	2014-09-03	2.5	TRUE	TRUE	TRUE

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

Listed Applications

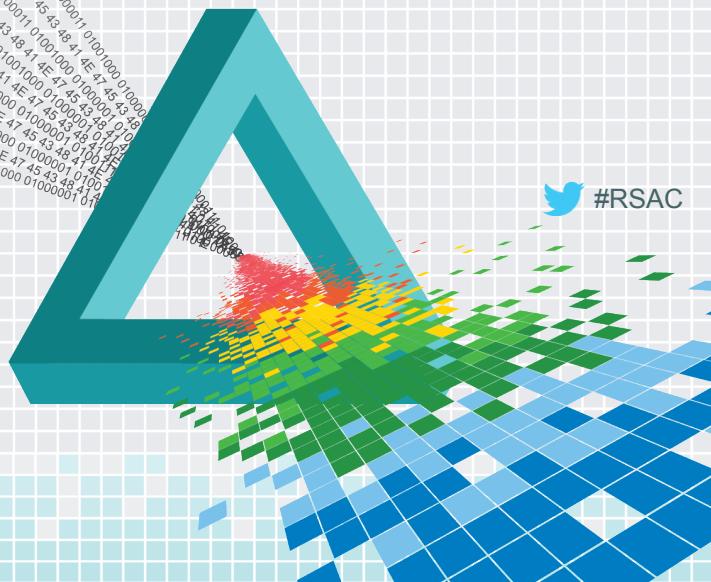
- ◆ An app is listed in the spreadsheet when it fails dynamic analysis with CERT Tapioca.
- ◆ If an app isn't listed:
 - It was not tested
 - Automation did not trigger HTTPS network traffic
 - It is not vulnerable

RSA® Conference 2015

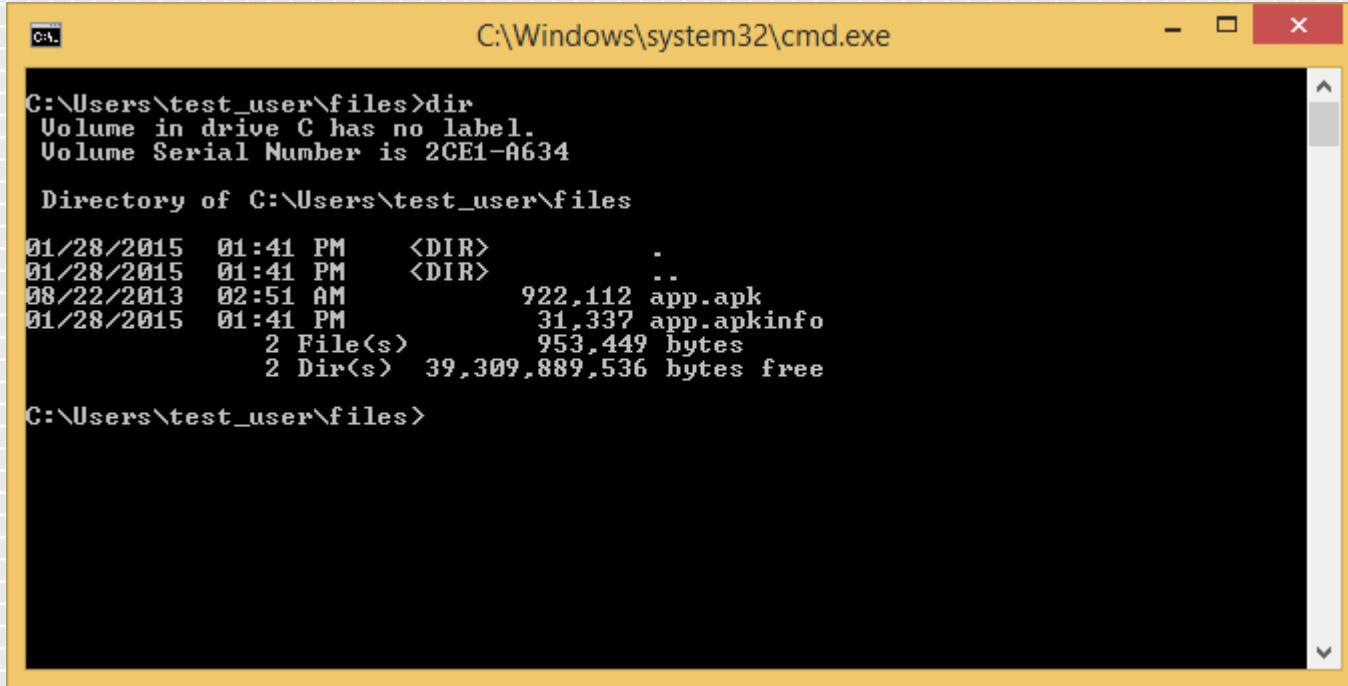
San Francisco | April 20-24 | Moscone Center

Issues Encountered

So you've got a million APK files?



Windows CMD.EXE



C:\Windows\system32\cmd.exe

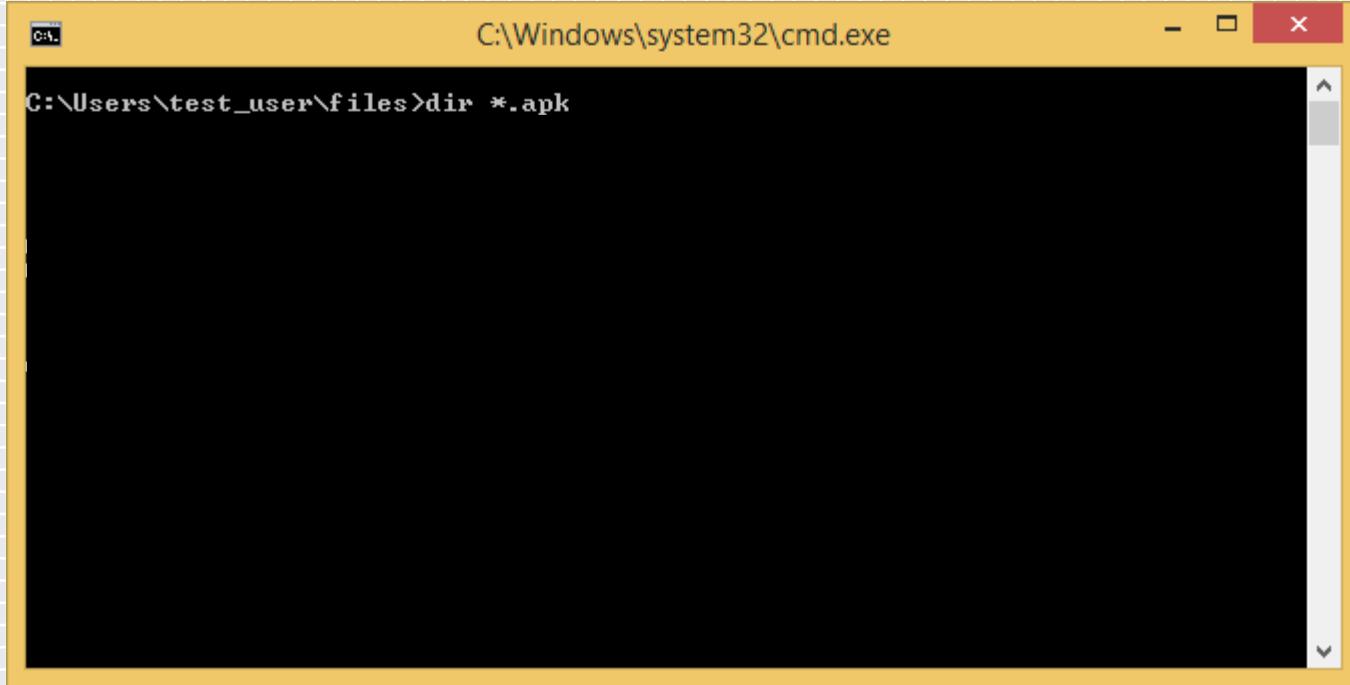
```
C:\Users\test_user\files>dir
 Volume in drive C has no label.
 Volume Serial Number is 2CE1-A634

 Directory of C:\Users\test_user\files

01/28/2015  01:41 PM    <DIR>    .
01/28/2015  01:41 PM    <DIR>    ..
08/22/2013  02:51 AM           922,112 app.apk
01/28/2015  01:41 PM           31,337 app.apkinfo
                  2 File(s)      953,449 bytes
                  2 Dir(s)   39,309,889,536 bytes free

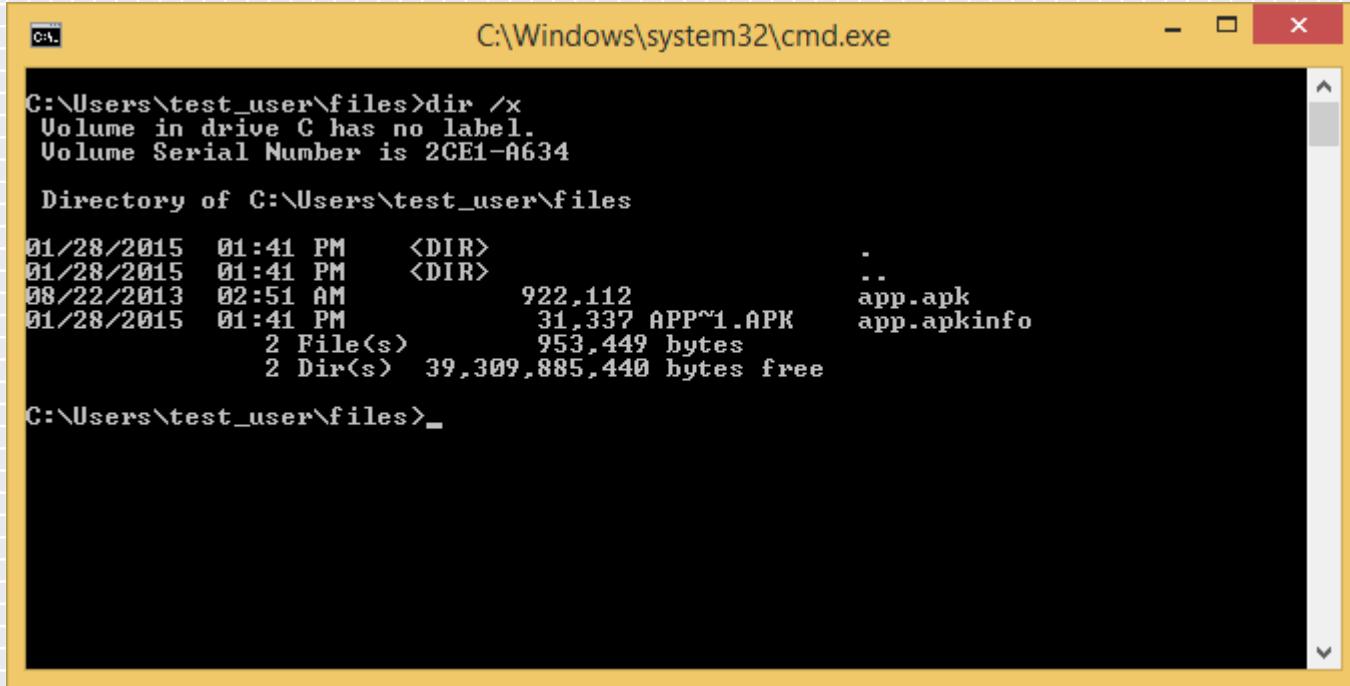
C:\Users\test_user\files>
```

Windows CMD.EXE



A screenshot of a Windows Command Prompt window titled "C:\Windows\system32\cmd.exe". The window is yellow with a black background. The command "dir *.apk" is typed in the prompt at the top. The output area is completely black, indicating no files were found.

Windows CMD.EXE



C:\Windows\system32\cmd.exe

```
C:\Users\test_user\files>dir /x
Volume in drive C has no label.
Volume Serial Number is 2CE1-A634

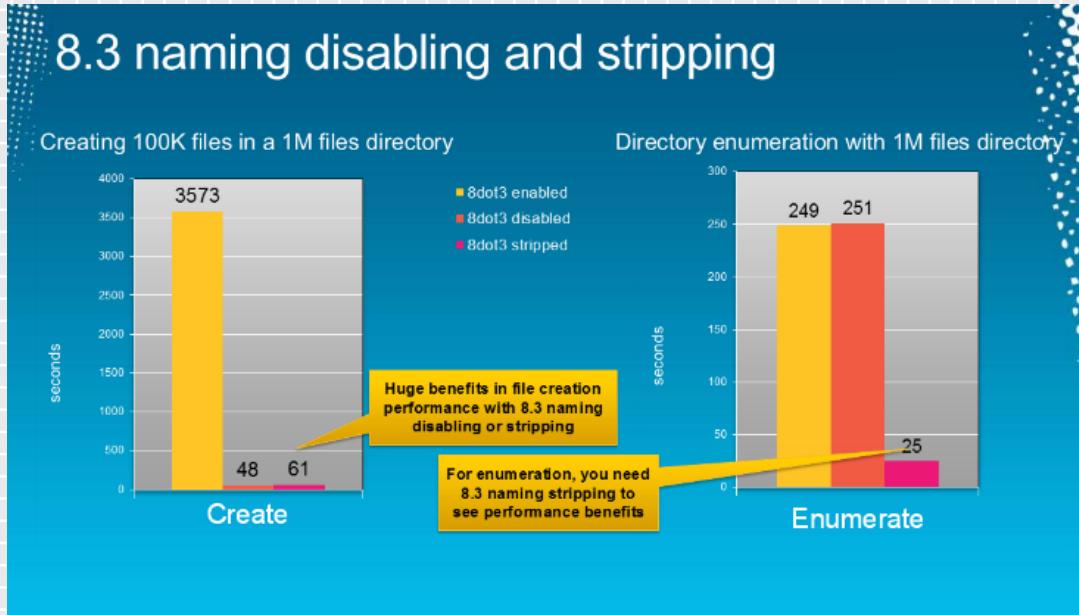
Directory of C:\Users\test_user\files

01/28/2015  01:41 PM    <DIR>
01/28/2015  01:41 PM    <DIR>
08/22/2013  02:51 AM            922,112      app.apk
01/28/2015  01:41 PM            31,337 APP~1.APK    app.apkinfo
                           2 File(s)       953,449 bytes
                           2 Dir(s)   39,309,885,440 bytes free

C:\Users\test_user\files>_
```

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](#)

RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

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



KIM KARDASHIAN HOLLYWOOD

Glu - January 14, 2015

Adventure

In-app purchases

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

4.5 stars (510,970)

8+1

+27307 Recommend this on Google

Developer



What Makes an App Important?

1-5 installs



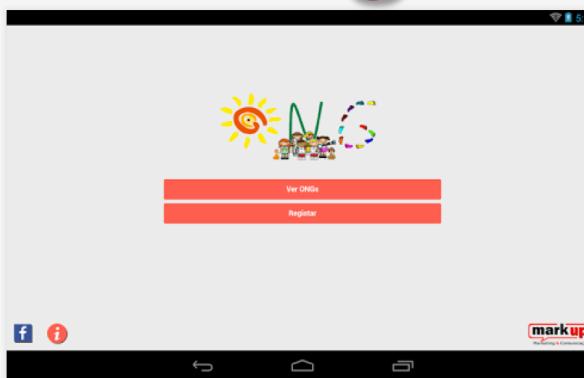
Diretório CNG.PT
Markup, Up Lda - January 14, 2015
Social

This app is compatible with all of your devices.

g+1 Recommend this on Google

Insecurely uses paypal

No CVE assigned



What Makes an App Important?



5-10 million installs

TweetCaster for Twitter

OneLouder Apps - January 16, 2015

5,663,788 46,340 Following
Add to Wish List

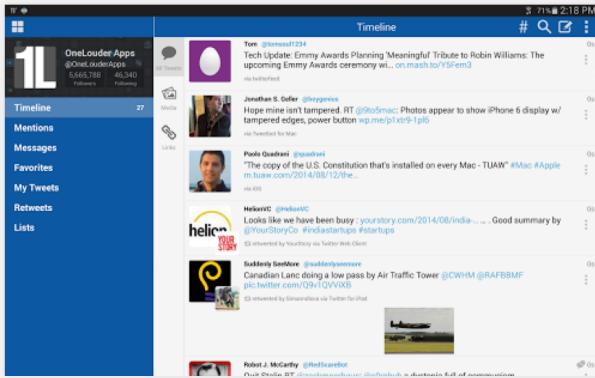
Offers in-app purchases

502,879
The developer

8+1 +71768 Recommend this on Google

Sends user/password

No CVE assigned



CVE10K



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.

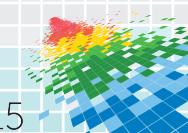
📍 Everywhere

🔗 cve.mitre.org/cve/identifier...

 Tweet to CVE10K



 Software Engineering Institute
Carnegie Mellon

RSA Conference 2015 

CVE Assignment

- ◆ Are Android applications CVE-worthy?

CVE Assignment

- ◆ Are Android applications CVE-worthy?
- ◆ No*

* Maybe, but stop assigning CVEs

RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

What Makes an Android Developer?

A pulse



#RSAC

AppsGeyser



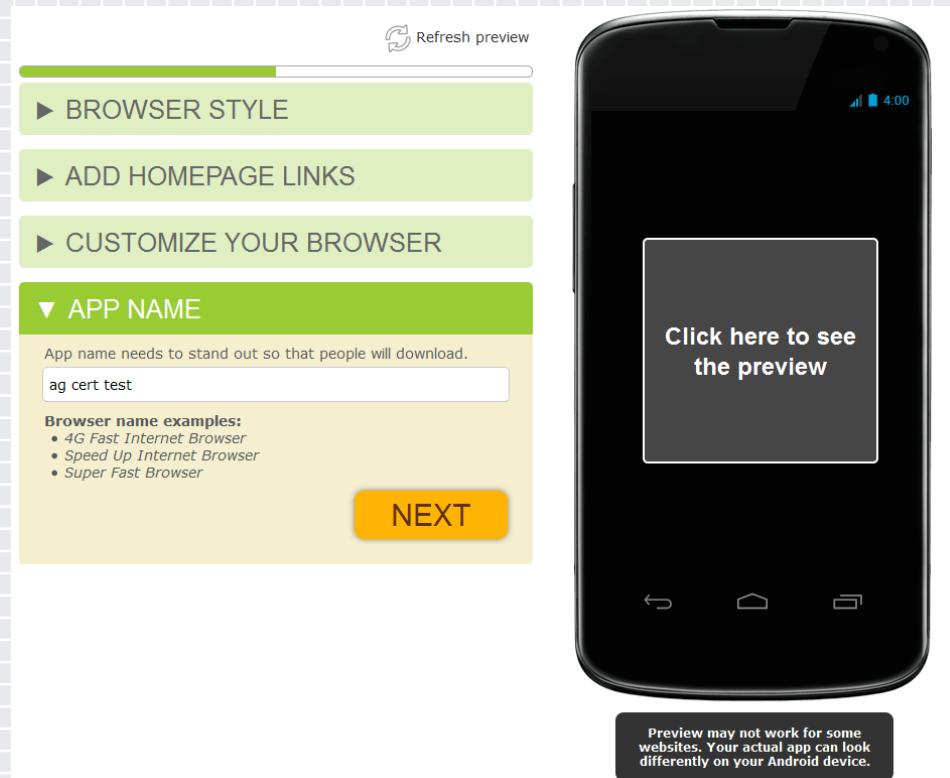
Create an Android App for
FREE!

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



The image shows the AppsGeyser web-based application interface on the left and a preview of the generated mobile application on the right.

Left Side (App Creation Interface):

- Top right: Refresh preview button.
- Section: BROWSER STYLE
- Section: ADD HOMEPAGE LINKS
- Section: CUSTOMIZE YOUR BROWSER
- Section: APP NAME (Collapsed)
- Text: App name needs to stand out so that people will download.
- Input field: ag cert test
- Text: Browser name examples:
 - 4G Fast Internet Browser
 - Speed Up Internet Browser
 - Super Fast Browser
- Large yellow button: NEXT

Right Side (Mobile Preview):

An Android smartphone displays a dark screen with a central white rectangular box containing the text: "Click here to see the preview".

Bottom Center:

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 COMMUNIT	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+



San Francisco | April 20-24 | Moscone Center

Apps That Exist *And also fail to validate SSL*



Mobile Network Signal Booster



Mobile Network Signal Booster

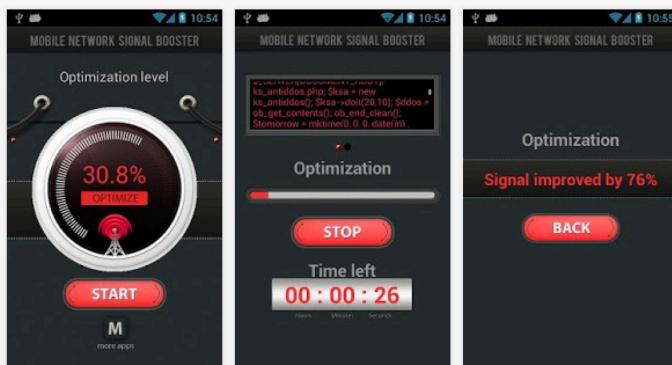
Slovak Creative Studio - April 25, 2013

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.

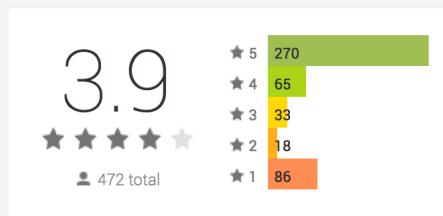
=====

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](#)



AMAZING Out of the multitude of apps that I have tried to strengthen my network signal, this is the only one that wor

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 signals fine with th

Anthony Kasowski ★★★★★



Mobile Network Signal Booster

Additional information

Updated

April 25, 2013

Size

13M

Installs

50,000 - 100,000

Current Version

1.0

Requires Android

2.2 and up

Content Rating

Everyone

Contact Developer[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

★★★★★ (459,875)

Top Developer

8+ 79,665 Recommend this on Google

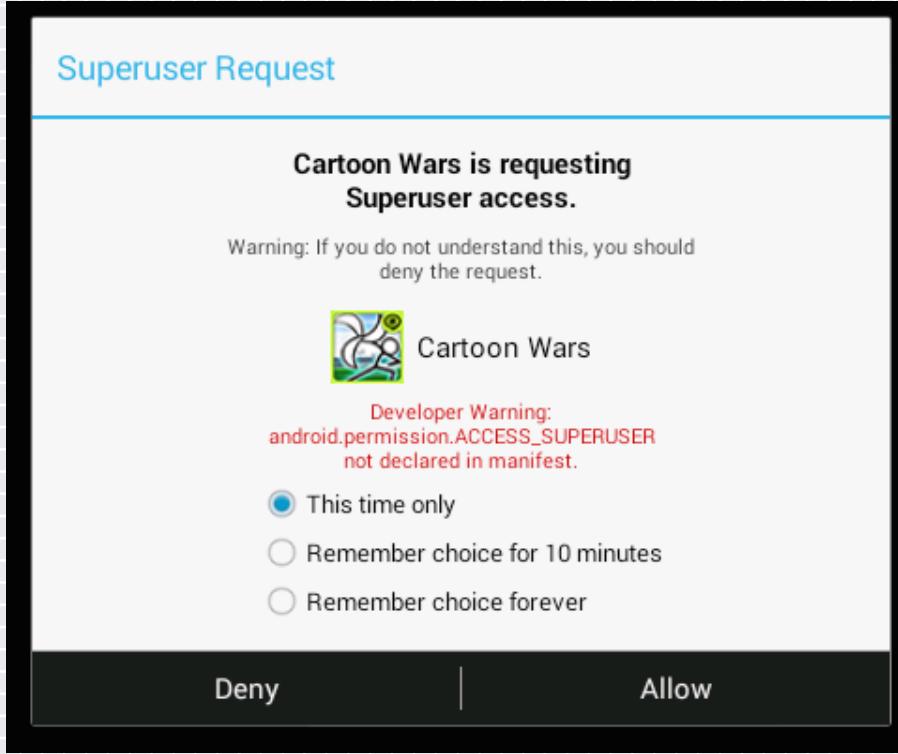


Cartoon Wars

Additional information

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

Cartoon Wars



Brightest LED Flashlight



Brightest LED Flashlight

Intellectual Flame Co., Ltd. - September 2, 2014

Tools

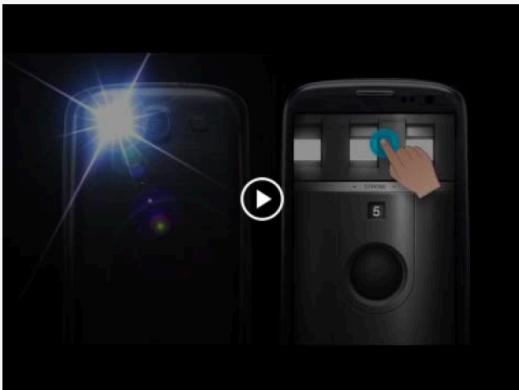
Install

Add to Wishlist

This app is compatible with all of your devices.

★★★★★ (575,802)

8+1 +141458 Recommend this on Google



RSA® Conference 2015

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 merely a notification mechanism to tell the server the communication channel is being tampered with. As such, it is a feature that our application to continue to communicate with the backend even though 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

RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

Public Reception

Fighting the battle of who could care less



Reddit



reddit ANDROIDDEV comments related

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,
    certutilis.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.

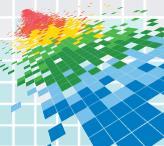
[permalink](#) [save](#) [parent](#) [report](#) [give gold](#) [reply](#)

[–] **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

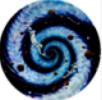
forums.makingmoneywithandroid.com C Search S D Home ABP > >

I just received email from
CERT Coordination Center , I
don't know what is happen ????

Reply With Quote

2014-12-08, 10:04 AM #2

A1ka1inE Senior Member



Join Date: Jan 2013
Posts: 1,612
[Post Thanks / Like](#) (0)
Mentioned: 72 Post(s)

Yeah I had one of these for an app that gets hardly any downloads. I don't think their affiliated with Google though and the e-mail seems quite arbitrary anyway.
No big deal if you ask me.

[Sign up with mobileCore here for \\$100 bonus when reaching 100k impressions!](#)
[Attractive Interstitial Ads \(and other ad units\) that perform well in both apps in games and on a global scale. Weekly payments too!](#)

[Sign up with StartApp here for \\$15 when you hit 100k ad impressions!](#)
[They run a great range of Interstitial Ads for apps and games on a global scale, with banners available too.](#)

DO NOT USE inMobi. Check out this thread.

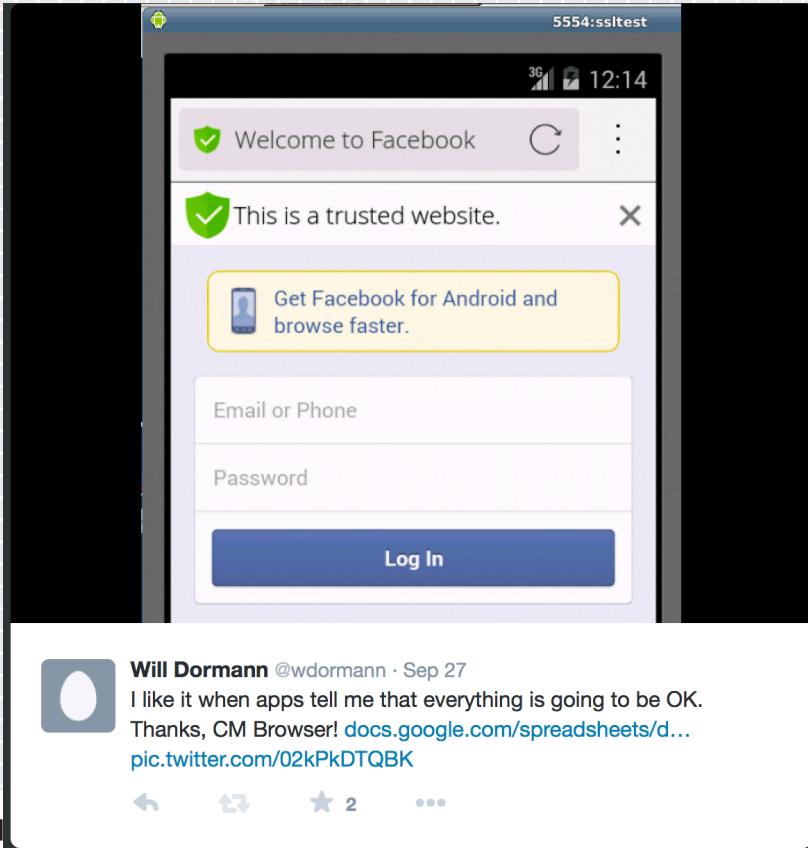
Reply With Quote

2014-12-10, 05:31 AM #3

javaexp

I also got one yesterday. I ignore it unless it is sent by google.

Twitterverse #1 (warmup)



Four Months Later



CM Browser - Fast & Secure

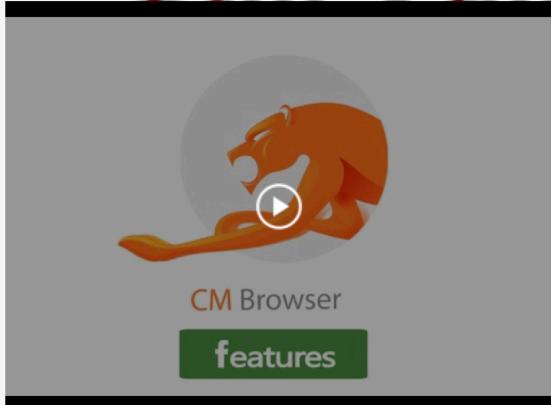
Cheetah Mobile Inc. - January 27, 2015

Communication

Install Add to Wishlist

★★★★★ (1,131,825)

Still Vulnerable



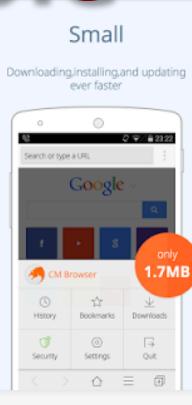
Speedy

Browsing acceleration gets you browsing faster than ever



Small

Downloading, installing, and updating ever faster



Twitterverse #2 (Getting interesting)



Coles Supermarkets

@Coles



Follow

@wdormann privacy & security is of the upmost importance to us & our credit card app has never experienced a security vulnerability.



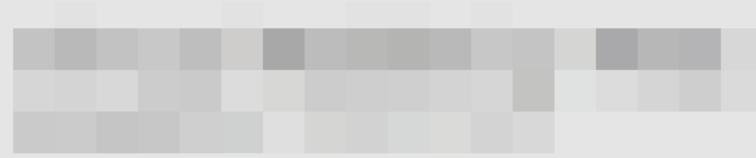
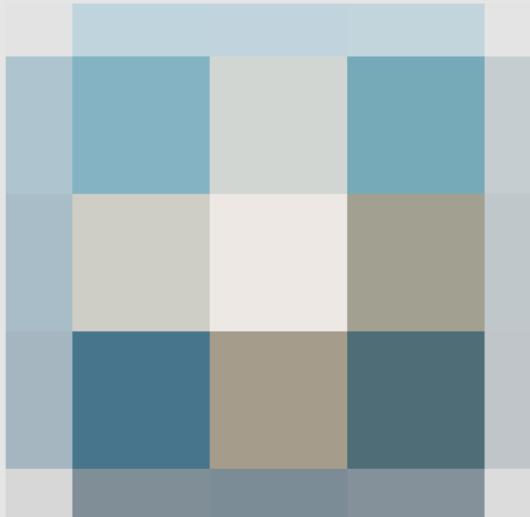
Reality-distortion field

"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



Finance

Install



Add to Wishlist

★★★★★ (5,939)

Vendor Reaction



RSA® Conference 2015

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,



Software Engineering Institute
Carnegie Mellon

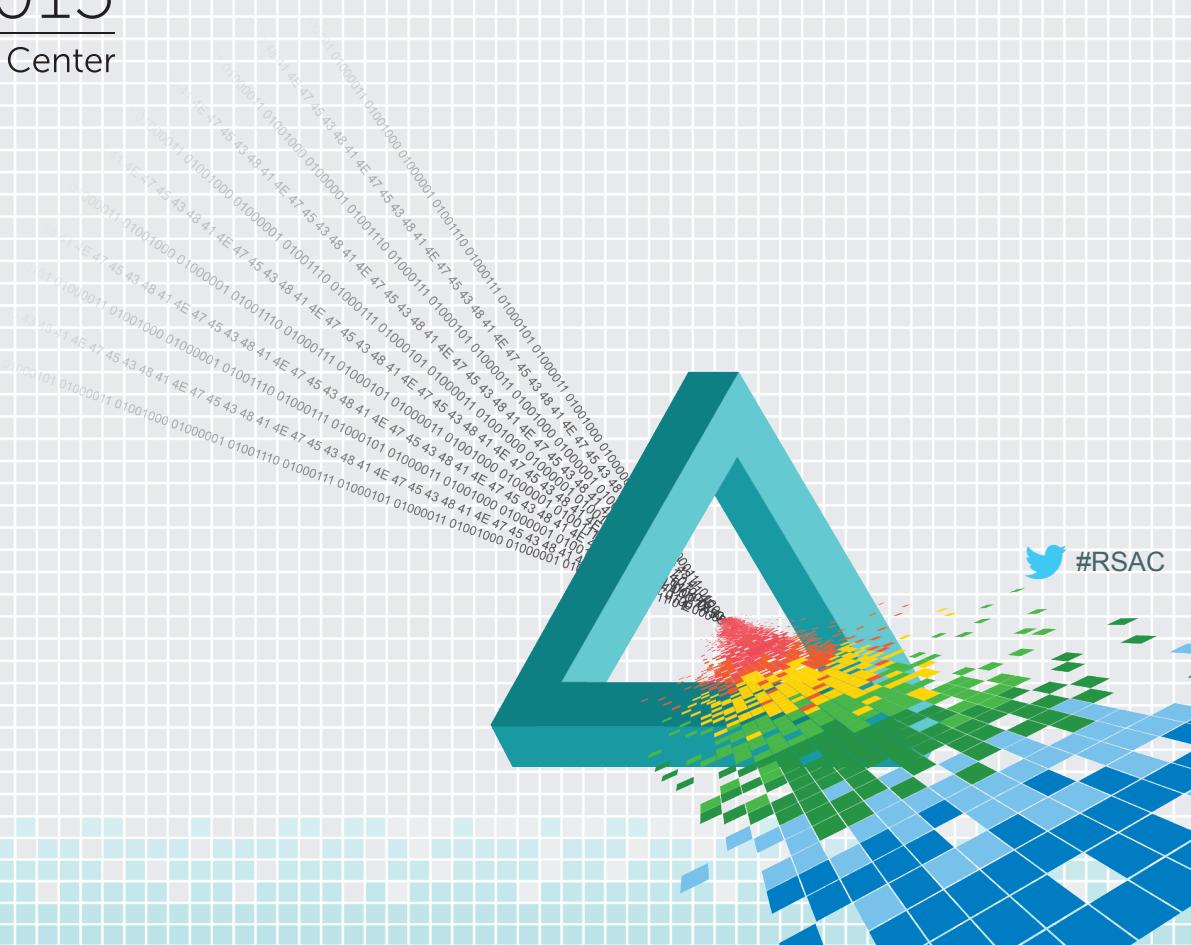


RSA® Conference 2015

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/>

RSA® Conference 2015

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

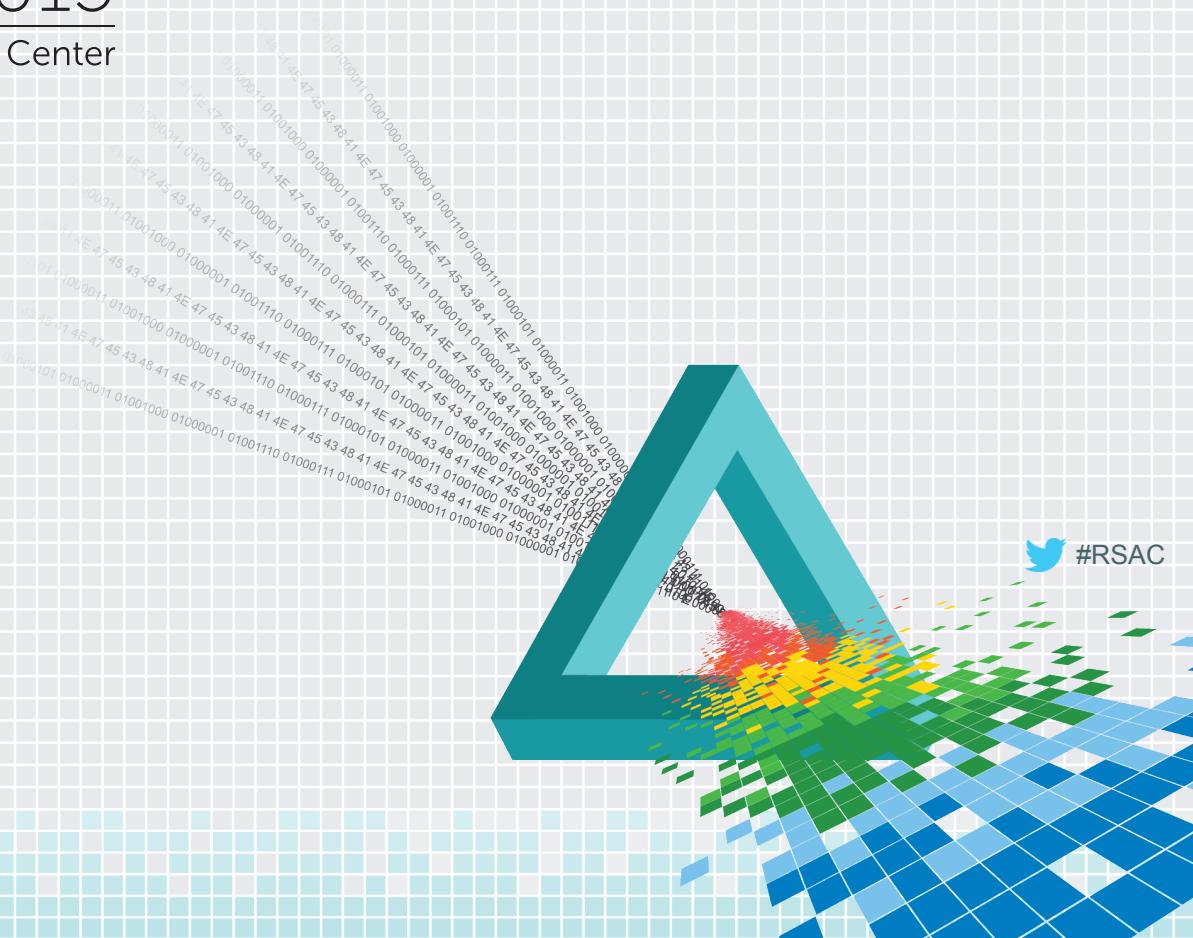
Apply What You Have Learned Today

- ◆ 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

RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

Appendix



Android SSL Testing Architecture

