TRAIL OF BITS Defense Guided by Experience

NYU·poly POLYTECHNIC INSTITUTE OF NEW YORK UNIVERSITY

Executive Overview
NYU-Poly & Mobile Security

Dan Guido

Hacker in Residence, NYU-Poly
Co-Founder & CEO, Trail of Bits

CSAW 2012

Who am I?

@dguido

NYU·poly

POLYTECHNIC INSTITUTE OF NEW YORK UNIVERSITY

CSAW

Academics

System updates:
OOB bundle download

- Available bundle versions
- "X-Encryption-Id"
- package_get.py
- Brute-forcing unreleased versions!

```
orange-qcfm_parse bnull$ python package_get.py -b [illegible] | grep qcfm
http://[illegible].blackberry.com/[illegible]
[illegible]qcfm.os.factory.[illegible].signed.bar
```

Voight-Kampff'ing
The BlackBerry PlayBook

Zach Lanier and Ben Nell

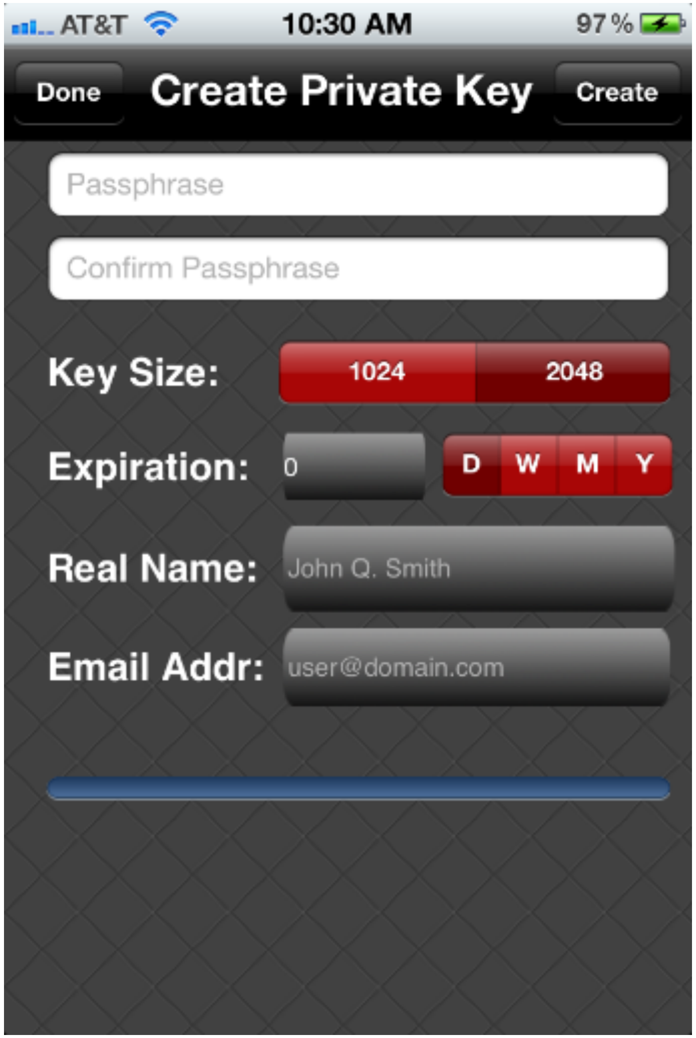
- Hack Night
- AppSec/PenTest
- Mobile Dev

Academics

NYU·poly
POLYTECHNIC INSTITUTE OF NEW YORK UNIVERSITY

Security Research

Assessment



Create Private Key

Passphrase

Confirm Passphrase

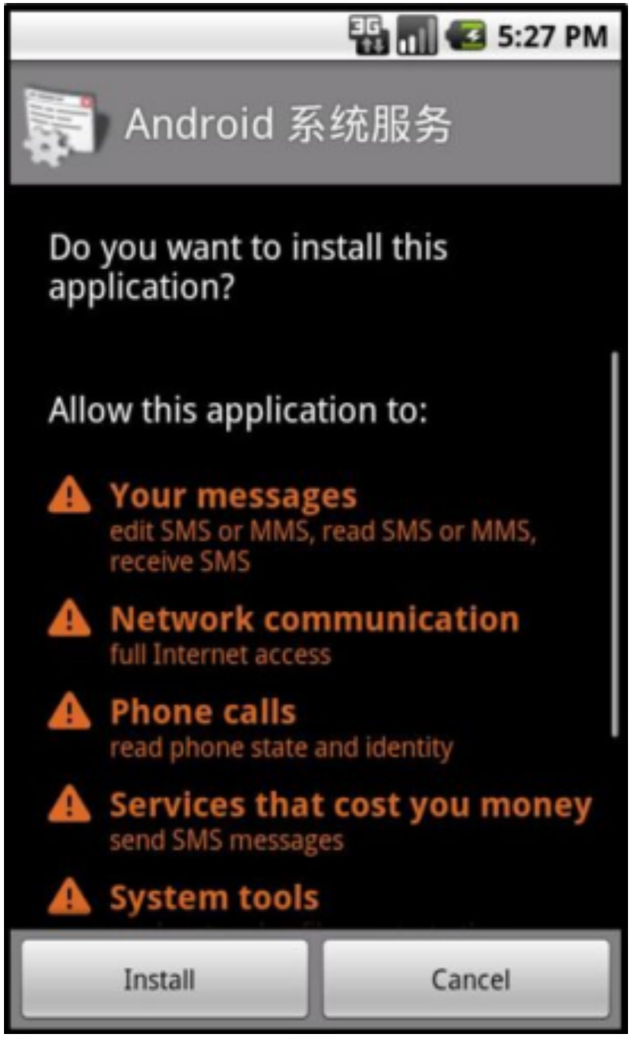
Key Size: 1024 2048

Expiration: 0 D W M Y

Real Name: John Q. Smith

Email Addr: user@domain.com

Remediation



Android 系统服务

Do you want to install this application?

Allow this application to:

⚠ **Your messages**
edit SMS or MMS, read SMS or MMS, receive SMS

⚠ **Network communication**
full Internet access

⚠ **Phone calls**
read phone state and identity

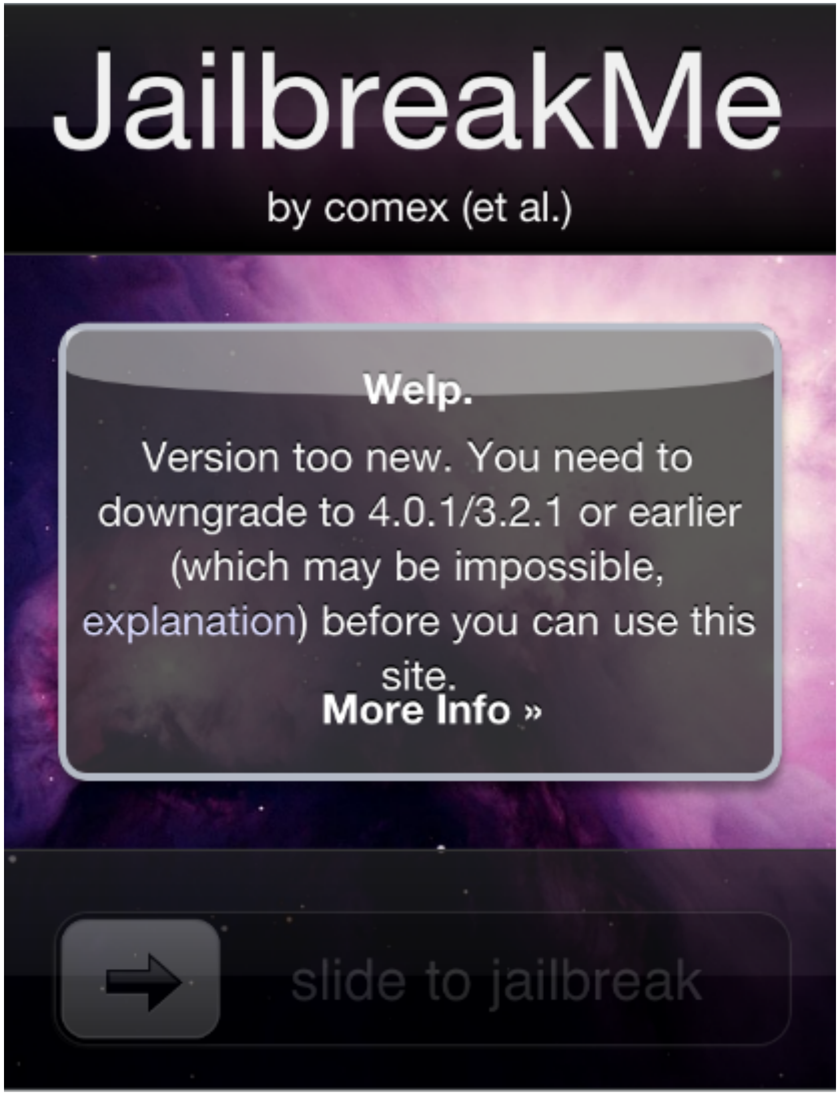
⚠ **Services that cost you money**
send SMS messages

⚠ **System tools**

THREADS

- Connect with Industry
- Pragmatic & Practical
- Latest Discoveries
- Broadened Exposure

iOS Jailbreak Analysis



JailbreakMe

by comex (et al.)

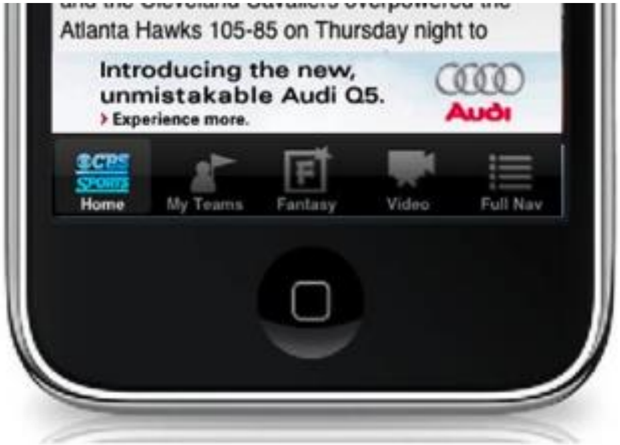
Welp.

Version too new. You need to downgrade to 4.0.1/3.2.1 or earlier (which may be impossible, explanation) before you can use this site.

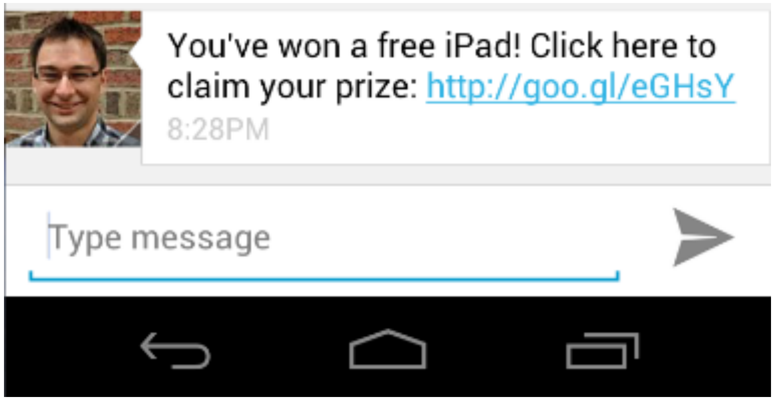
More Info »

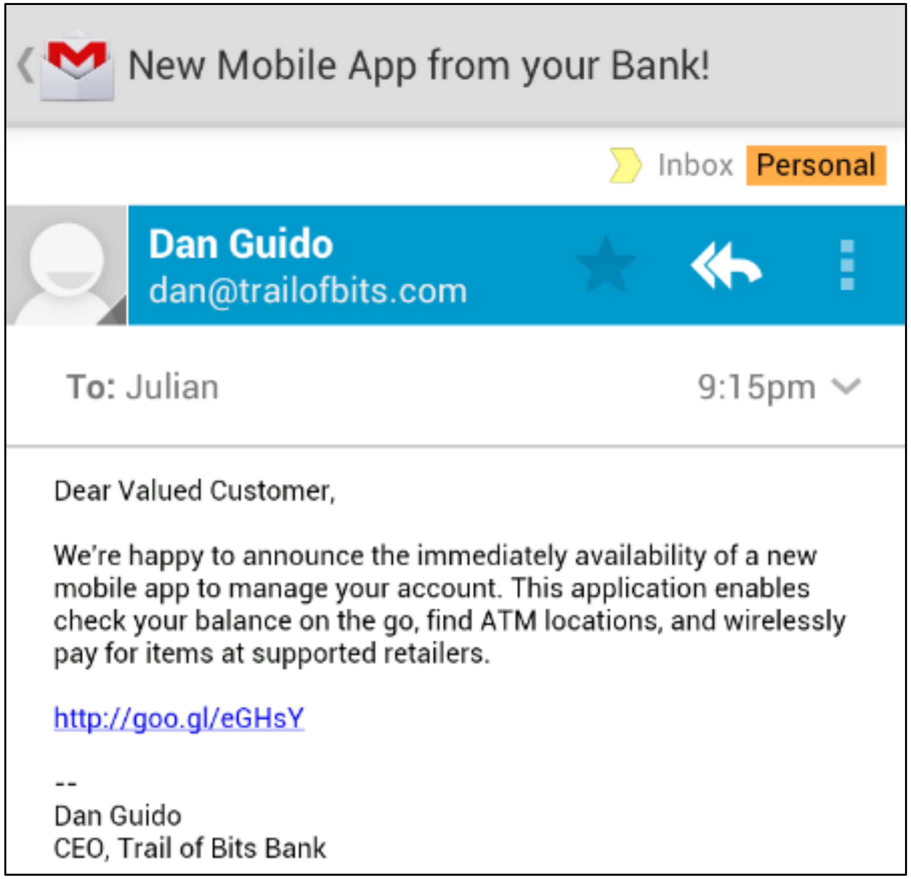
- Attacker Strategy
- Possible vs Actual
- Optimized Defense

Mobile EIP


Atlanta Hawks 105-85 on Thursday night to

Introducing the new, unmistakable Audi Q5.
› Experience more.


You've won a free iPad! Click here to claim your prize: http://goo.gl/eGHsY
8:28PM


New Mobile App from your Bank!

Dan Guido
dan@trailofbits.com

To: Julian 9:15pm

Dear Valued Customer,

We're happy to announce the immediately availability of a new mobile app to manage your account. This application enables check your balance on the go, find ATM locations, and wirelessly pay for items at supported retailers.

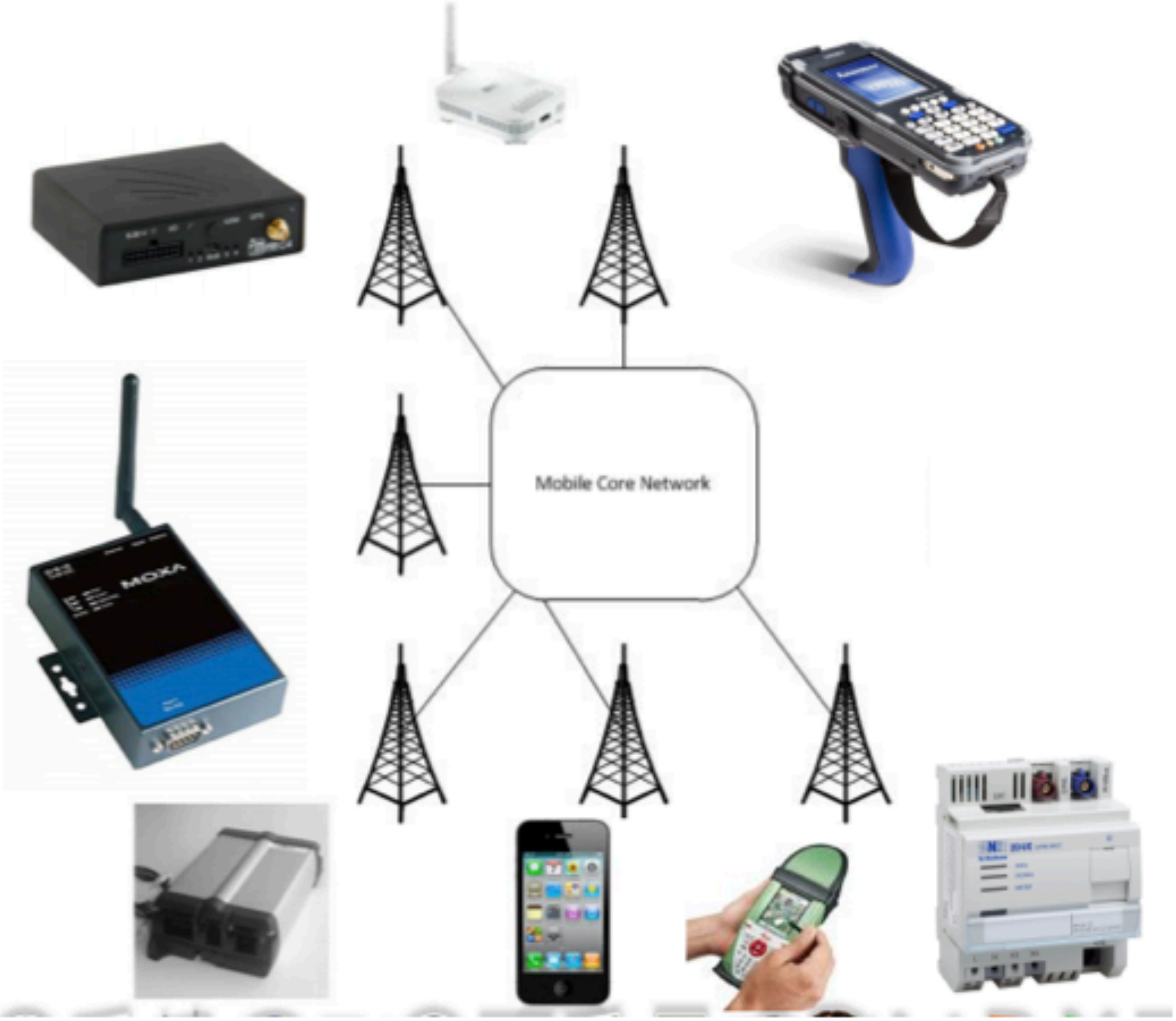
http://goo.gl/eGHsY

--
Dan Guido
CEO, Trail of Bits Bank

When good jailbreaks, *go bad*

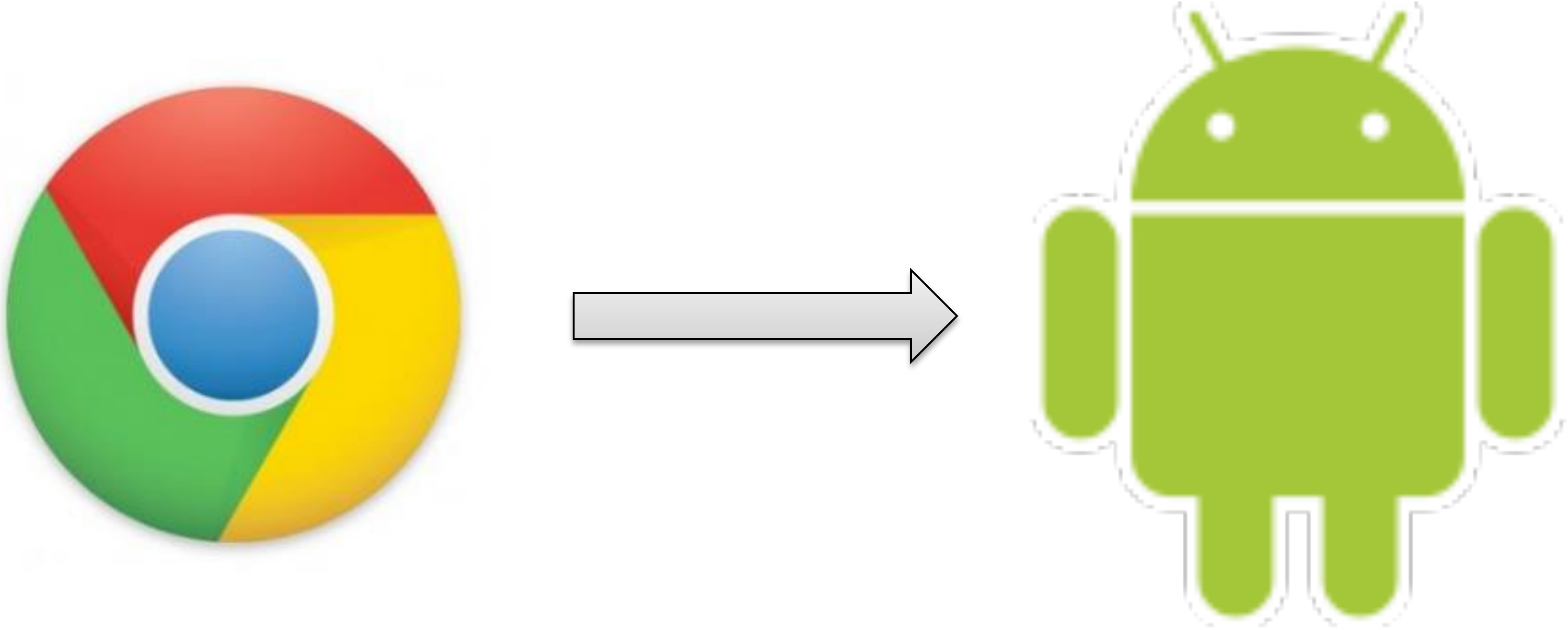
Probing Operator Networks

Probing Operator Networks

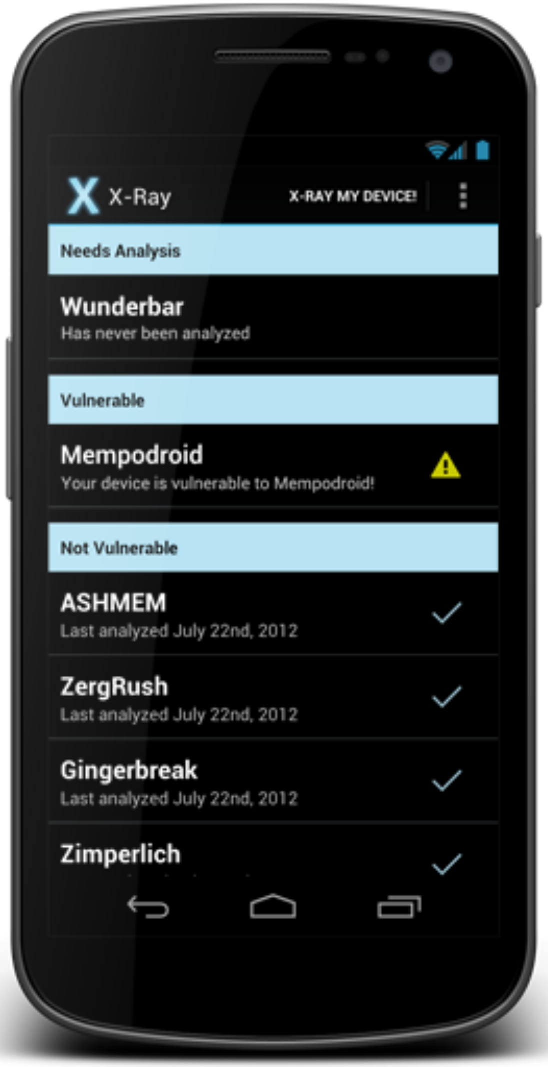


A Tale of Mobile Threats

Native Client



X-Ray



X X-Ray X-RAY MY DEVICE!

Needs Analysis

Wunderbar
Has never been analyzed

Vulnerable

Mempodroid ⚠
Your device is vulnerable to Mempodroid!

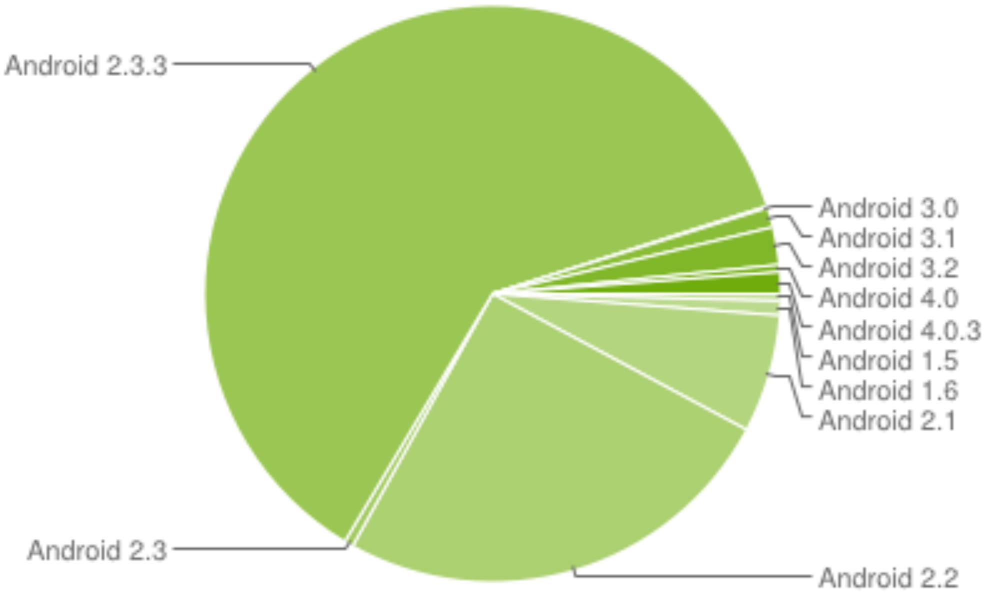
Not Vulnerable

ASHMEM ✓
Last analyzed July 22nd, 2012

ZergRush ✓
Last analyzed July 22nd, 2012

Gingerbreak ✓
Last analyzed July 22nd, 2012

Zimperlich ✓



Closing Thoughts

- “Mobile” doesn’t mean “smaller desktop”
- At the application-level, malware will be a bigger problem than exploitation (for now)
- Mobile is here and we might not be ready
  - When is the last time you integrity checked your baseband?