App Revocation Checking

Why is this still so hard?

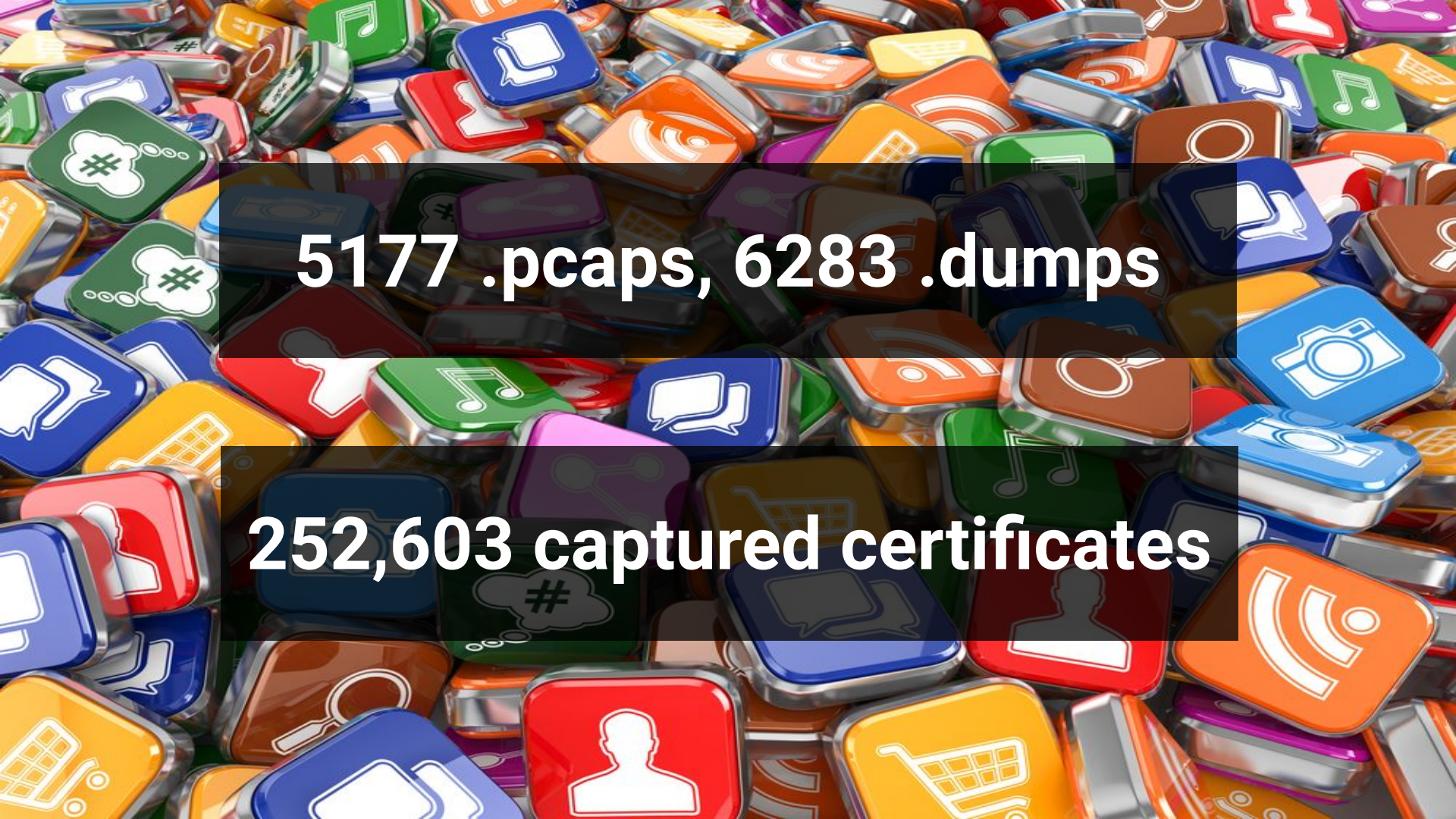
Kevin Bock • Dave Levin • Jingjing Ren • Dave Choffnes • Alan Mislove


Secure | https://www.usenix.org/conference/hotsec18
usenix ASSOCIATION
HotSec '18
ATTEND
ACTIVITIE
HotSec '18
2018 USENIX Su
AUGUST 14, 2018
BALTIMORE, MD, USA
Co-located with USENIX Security '18
DST Root CA X3
Let's Encrypt Authority X3
5767409591910400-fe4.pantheonsite.io
Certificate Standard
5767409591910400-fe4.pantheonsite.io
Issued by: Let's Encrypt Authority X3
Expires: Sunday, September 30, 2018 at 4:59:20 PM Eastern Daylight Time
This certificate is valid
Details
Subject Name
Common Name 5767409591910400-fe4.pantheonsite.io
Issuer Name
Country US
Organization Let's Encrypt
Common Name Let's Encrypt Authority X3
Serial Number 03 93 7F 7D FA DC B7 04 2F F1 52 D0 04 11 8F F4
OK


REVOKED


REVOKED
?


400+ Unique Apps


5177 .pcaps, 6283 .dumps
252,603 captured certificates


HELP

0


Revocations
0

Google's senior staff software engineer's take:
https://www.imperialviolet.org/2014/04/19/revchecking.html

Android’s TrustManagerImpl:

```
try {
    PKIXParameters params = new PKIXParameters(trustAnc
    params.setRevocationEnabled(false);
    params.addCertPathChecker(new ExtendedKeyUsagePKIXC
```

*“The details… of the revocation checking policy are **deliberately not documented** because they are subject to change.”*

- Still fails soft at least up to iOS 10.3

See https://forums.developer.apple.com/thread/24298

See https://github.com/square/okhttp/issues/2348


server
SSL
certificate
APP
trusted
root CA's

App Store


No Shame


SOLUTIONS
NEW