UNIVERSITÄT
BERN

Privacy Concerns in Public Web APIs

SCG Seminar - Marc-Andrea Tarnutzer

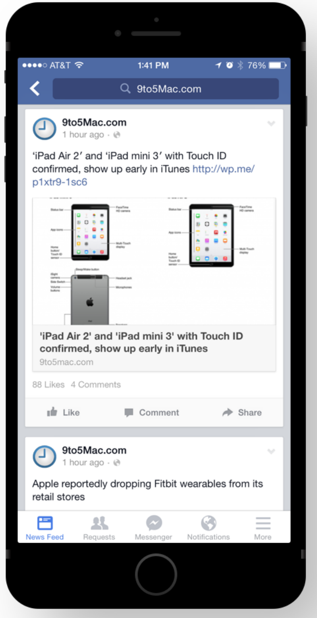
Agenda

- Introduction

- Implementation & Analysis
- Results
- Demo

- Lessons Learned
- Future Work

Web APIs are Everywhere



9to5Mac.com
1 hour ago ·

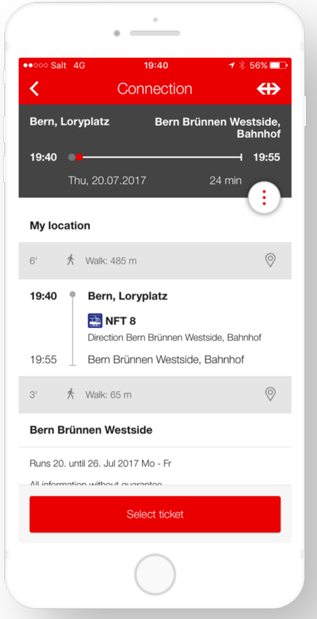
'iPad Air 2' and 'iPad mini 3' with Touch ID confirmed, show up early in iTunes http://wp.me/p1xtr9-1sc6

'iPad Air 2' and 'iPad mini 3' with Touch ID confirmed, show up early in iTunes
9to5mac.com

88 Likes 4 Comments

9to5Mac.com
1 hour ago ·

Apple reportedly dropping Fitbit wearables from its retail stores



Bern, Loryplatz **Bern Brünnen Westside, Bahnhof**

19:40 19:55

Thu, 20.07.2017 24 min

My location

6' Walk: 485 m

19:40 **Bern, Loryplatz**

NFT 8
Direction Bern Brünnen Westside, Bahnhof

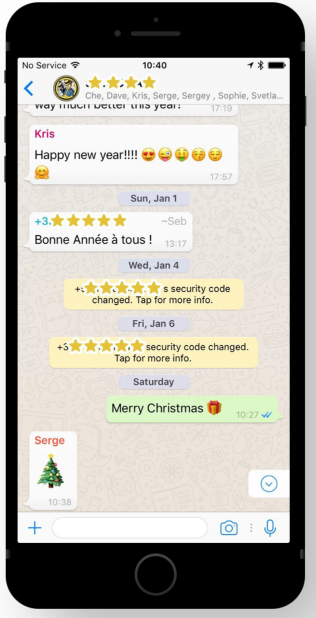
19:55 Bern Brünnen Westside, Bahnhof

3' Walk: 65 m

Bern Brünnen Westside

Runs 20. until 26. Jul 2017 Mo - Fr

All information without guarantee



[redacted]
Che, Dave, Kris, Serge, Sergey , Sophie, Svetla...

way much better this year! 17:19

Kris
Happy new year!!!! 😍😜🤑😚😌🤗 17:57

Sun, Jan 1

+3.[redacted] ~Seb
Bonne Année à tous ! 13:17

Wed, Jan 4

+[redacted]s security code changed. Tap for more info.

Fri, Jan 6

+3[redacted] security code changed. Tap for more info.

Saturday

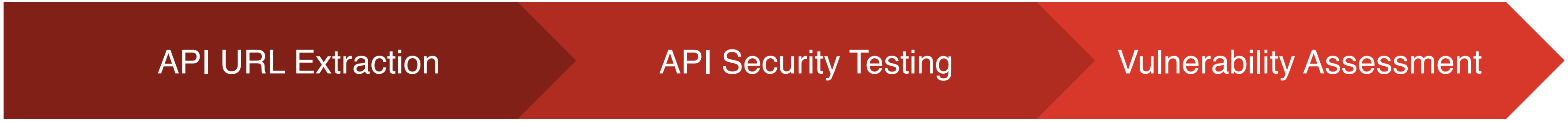
Merry Christmas 🎁 10:27 ✓✓

Serge
🎄 10:38

WeChat Team Sponsored
它是什么?
Details
1 hour ago
♡ Alex, Sun Nan , Elliott Ng , Raine
Alex: 占位占位!

Amber Wu
这就是晚餐了😁
1 hour ago

Project Overview

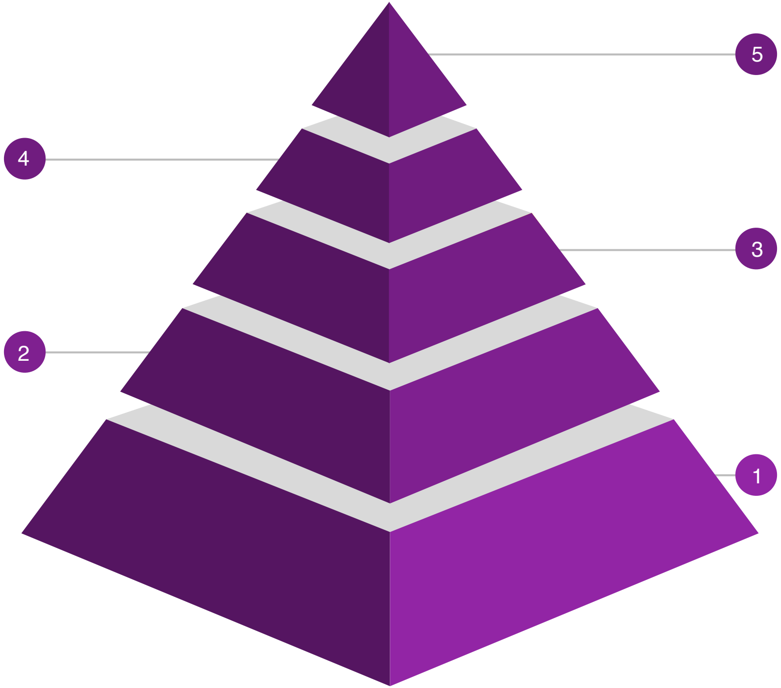


API URL Extraction

API Security Testing

Vulnerability Assessment

Approach



5 **Hand crafted exploits**

4 **App decompilation**
E.g. for further analysis of parameters, JSON structure, ...

3 **API is-alive tests**

2 **Purification of found URLs**
Parsing and purification of URLs found in 100k log files

1 **API URL extraction**
Extract URLs from APK corpus (100k apps, size: 750 GB)

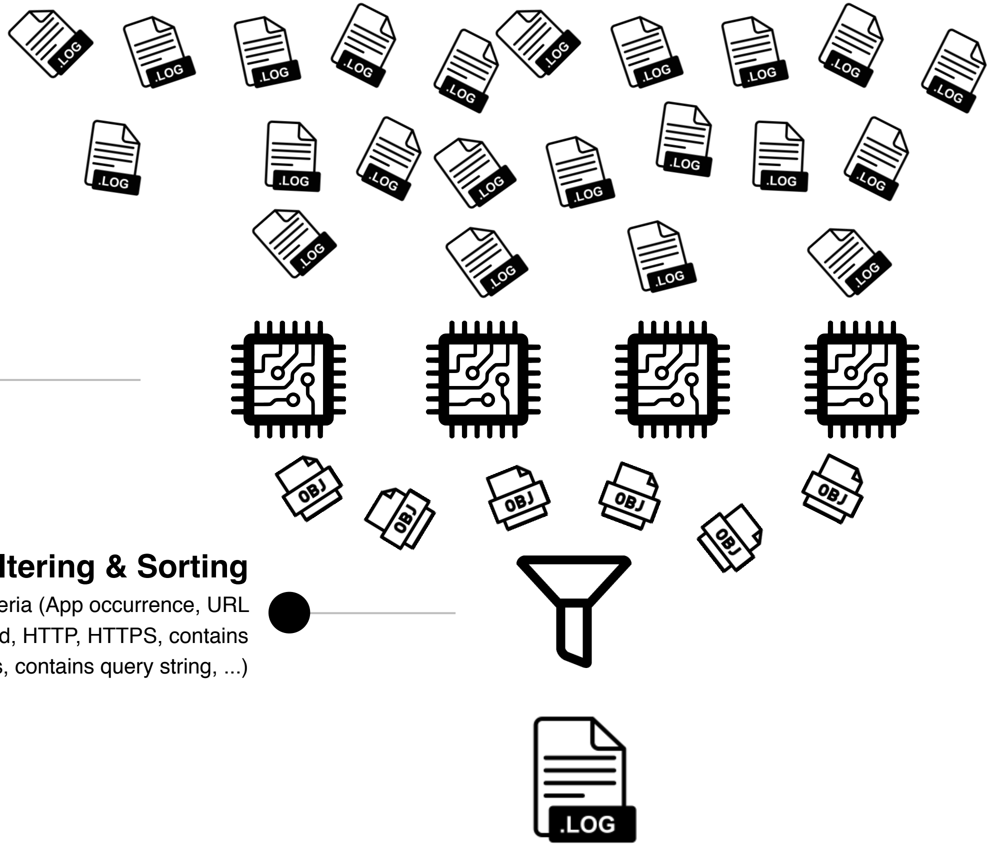
APK

- Android Package (APK)
- Package file format
- Used for app distribution and installation on the Android OS
- APK contains compiled source code, assets, resources, certificates, … of a program

JSON

- JavaScript Object Notation (JSON)
- Open-standard file format
- Used to transmit data objects
- Key-value pairs
- Often used in APIs to send and receive data

API URL Parser



Parsing

Concurrent parsing of URLs
found in 100k log files (4 GB)

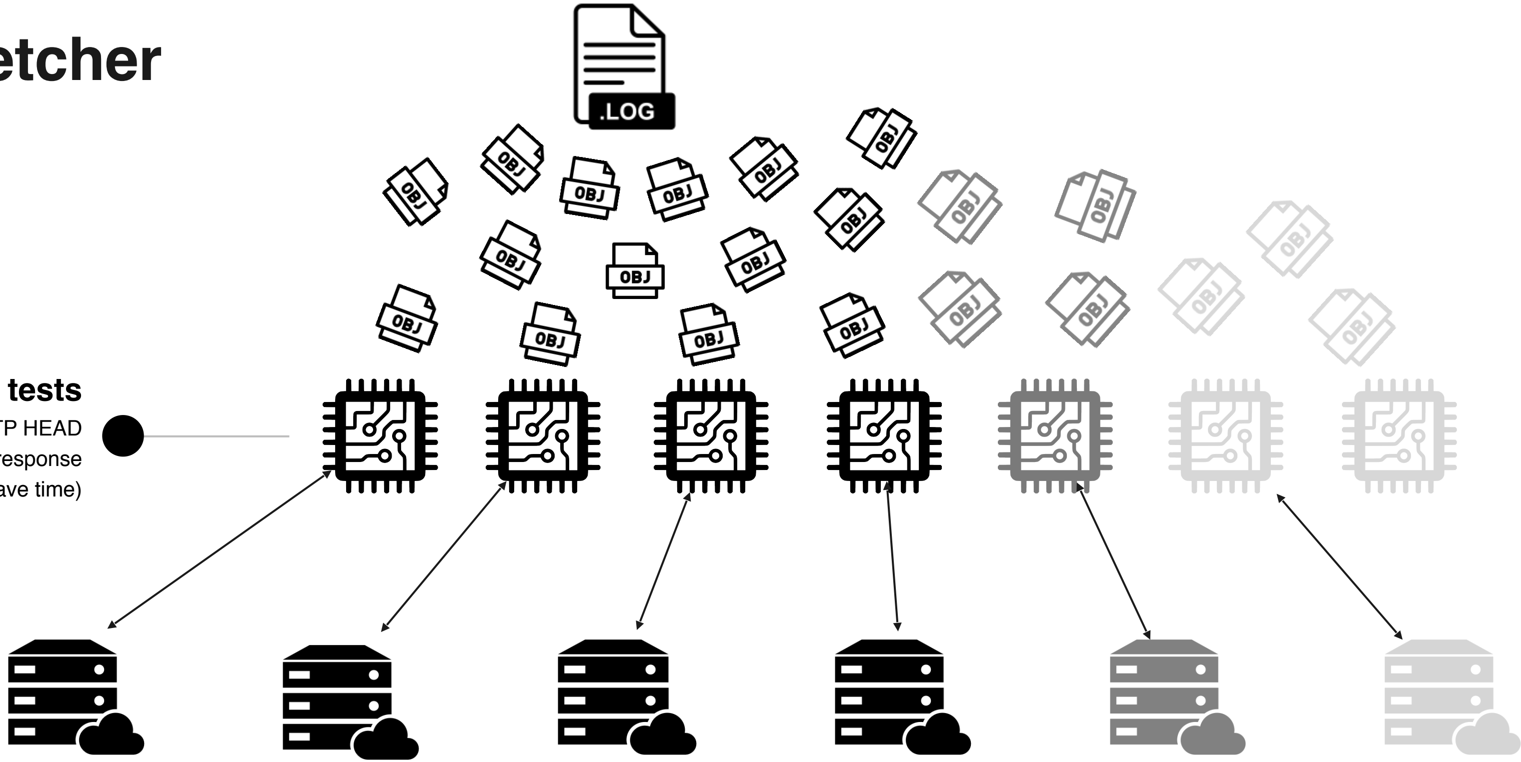
Filtering & Sorting

Filter URLs for certain criteria (App occurrence, URL occurrence, API keyword, HTTP, HTTPS, contains credentials, contains query string, ...)

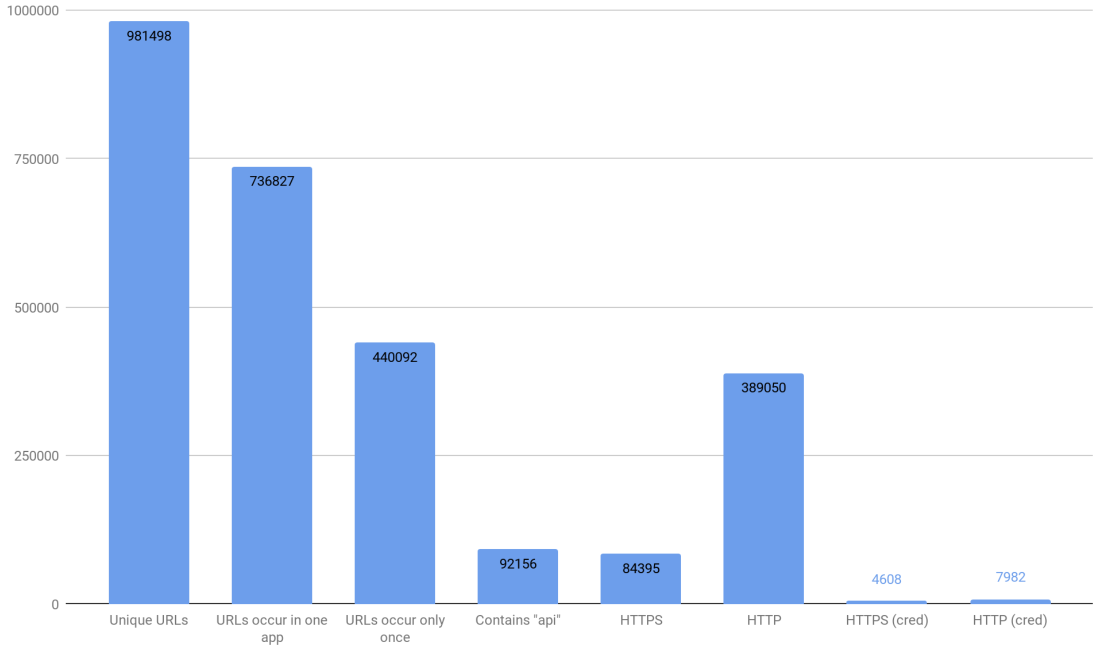
API Fetcher

API is-alive tests

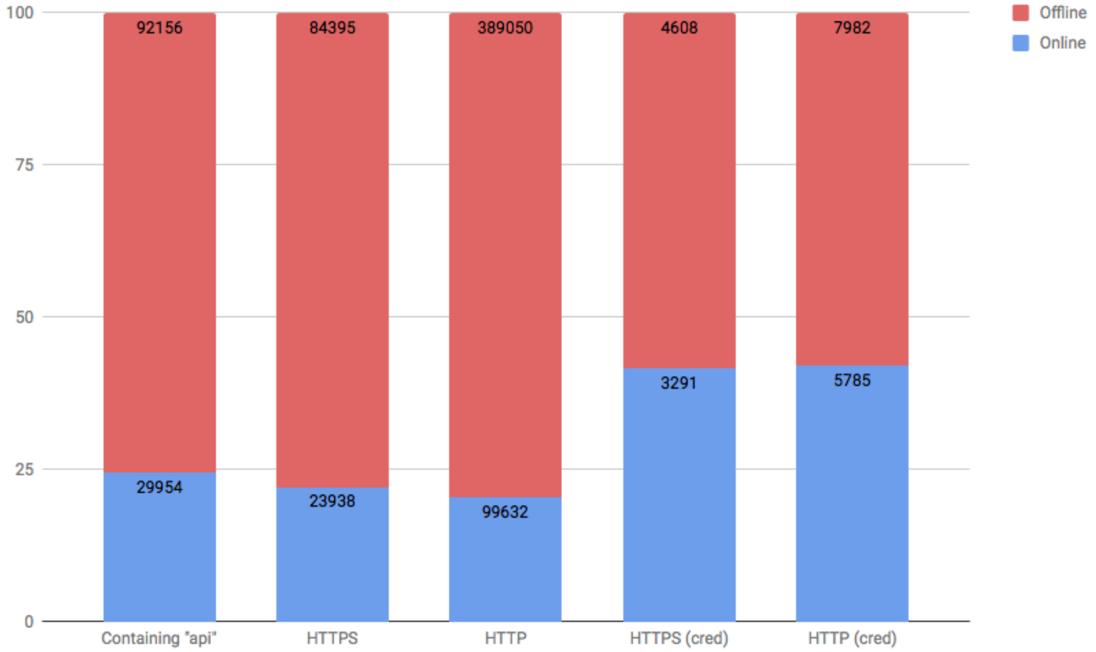
Concurrently send HTTP HEAD requests (don’t request response body to save time)



Results I


1000000
750000
500000
250000
0
981498
736827
440092
92156
84395
389050
4608
7982
Unique URLs
URLs occur in one app
URLs occur only once
Contains "api"
HTTPS
HTTP
HTTPS (cred)
HTTP (cred)

Results II

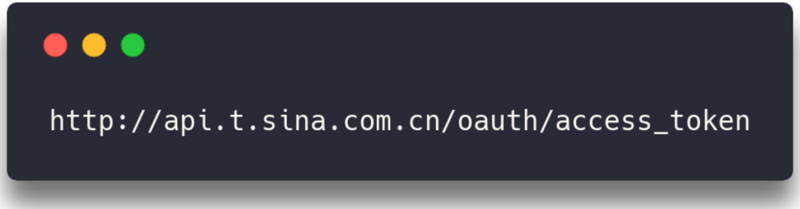


100
75
50
25
0
92156
29954
84395
23938
389050
99632
4608
3291
7982
5785
Containing "api"
HTTPS
HTTP
HTTPS (cred)
HTTP (cred)
🟥 Offline
🟦 Online

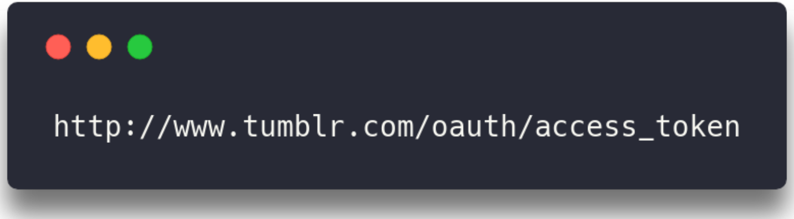
Manual API Analysis

- API analysis with Postman / CocoaRestClient & JADX
- Findings
  - Hardcoded credentials / API keys / authentication tokens / ...
  - Insecure query strings / account management
  - HTTP for sensitive data
  - Missing authentication

Findings - Examples I

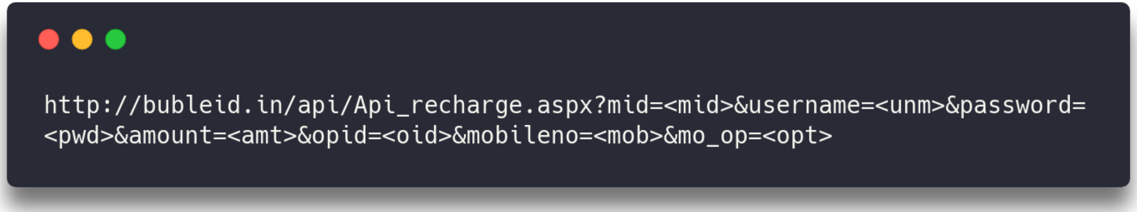


```
http://api.t.sina.com.cn/oauth/access_token
```

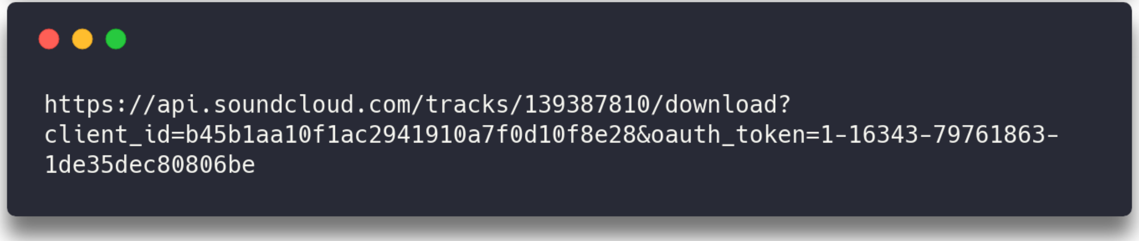


```
http://www.tumblr.com/oauth/access_token
```

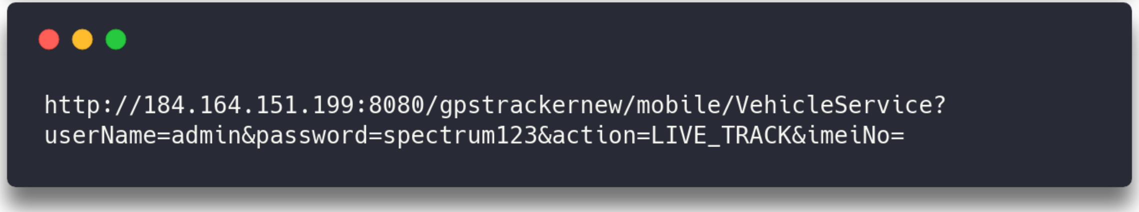
Findings - Examples II



```
http://bubleid.in/api/Api_recharge.aspx?mid=<mid>&username=<unm>&password=
<pwd>&amount=<amt>&opid=<oid>&mobileno=<mob>&mo_op=<opt>
```



```
https://api.soundcloud.com/tracks/139387810/download?
client_id=b45b1aa10f1ac2941910a7f0d10f8e28&oauth_token=1-16343-79761863-
1de35dec80806be
```



```
http://184.164.151.199:8080/gpstrackernew/mobile/VehicleService?
userName=admin&password=spectrum123&action=LIVE_TRACK&imeiNo=
```

Demo

Lessons Learned

- **Communication security is a problem**
  - HTTP vs. HTTPS
  - Query strings instead of HTTP headers and HTTP message body for sensitive information
- **Omnipresent issues**
  - Hardcoding
  - Vulnerable Chinese apps
  - Offline API URLs
  - Ad services
- **Also popular services have security problems**

Future Work

- SSL certificate checking
- Automated search of API parameters
- SQL injection
- DoS attacks and boundary checks

Summary

- Introduction
- Implementation & Analysis
    - API URL Parser & API Fetcher
- Results & Examples
- Demo
- Lessons Learned
- Future Work