SafeBreach LABS

The Price of Convenience

How Security Vulnerabilities in Global Transportation Payment Systems Can Cost You

Omer Attias

DEF CON

Omer Attias

Security Researcher

- 6 years of experience in cyber security
- Main focus in low level & vulnerability research
- Technology and Science enthusiast

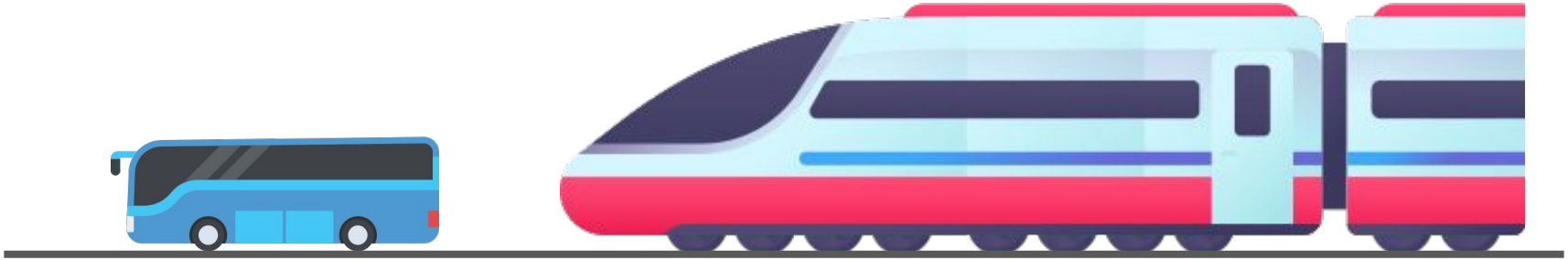


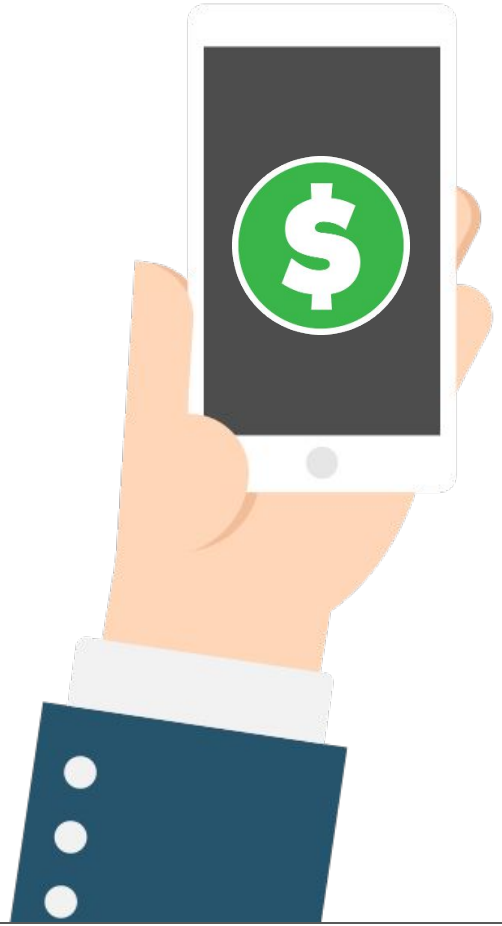
SafeBreach LABS

Agenda

- Introduction
- Mobile Payment Solution
- Train Tickets & Hole In The Logs
- Moovit
- API & Implementation Benefits
- Closure and Q&A

Public Transportation





MaaS & MaaS Operator

What is MaaS?

MaaS & MaaS Operator

Mobility as a service (MaaS) is a type of service that enables users to plan, book, and pay for multiple types of mobility services - all in one mobile application.

A **MaaS Operator** is a company that hosts a variety of transport options.



Bird



Moovit

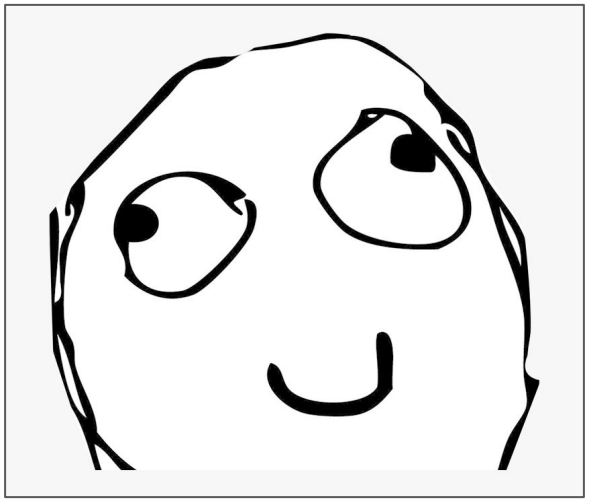
Disclosure



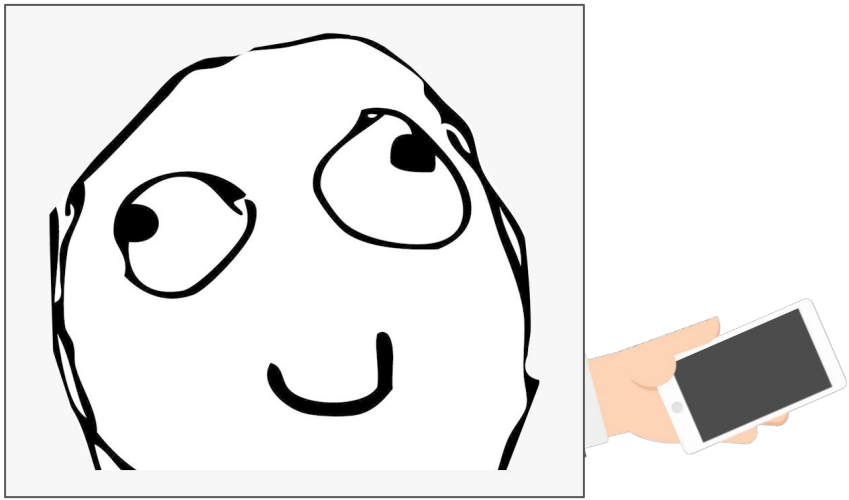


The Mobile Solution

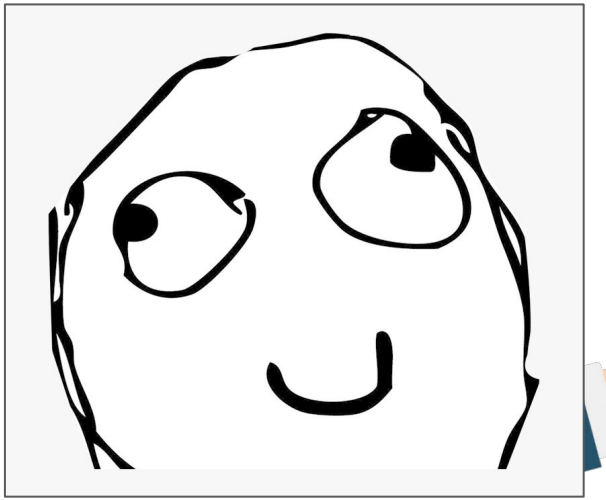
Meet Mike

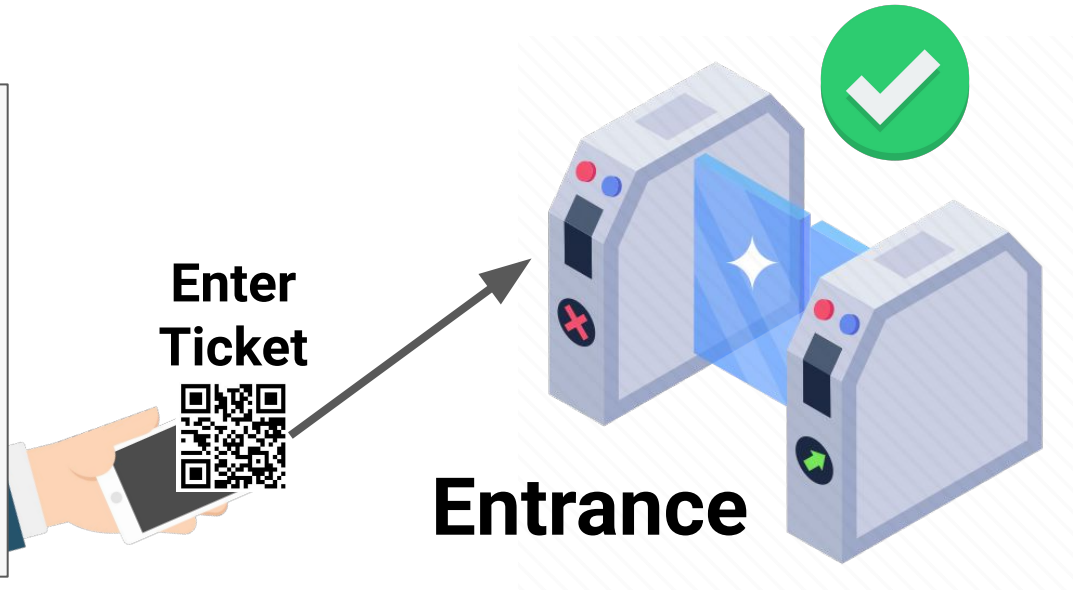


Paying With The Smartphone

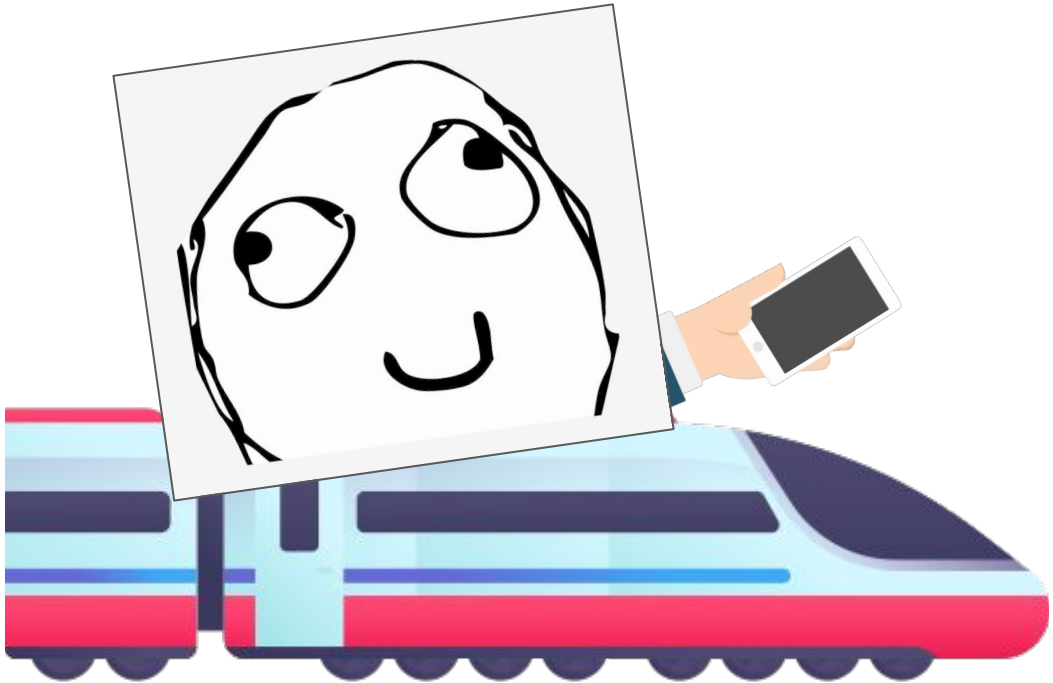


Entering The Train Station

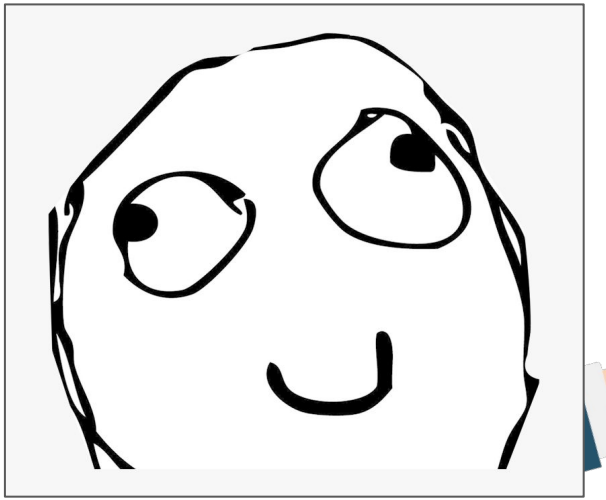




Having Fun Ride

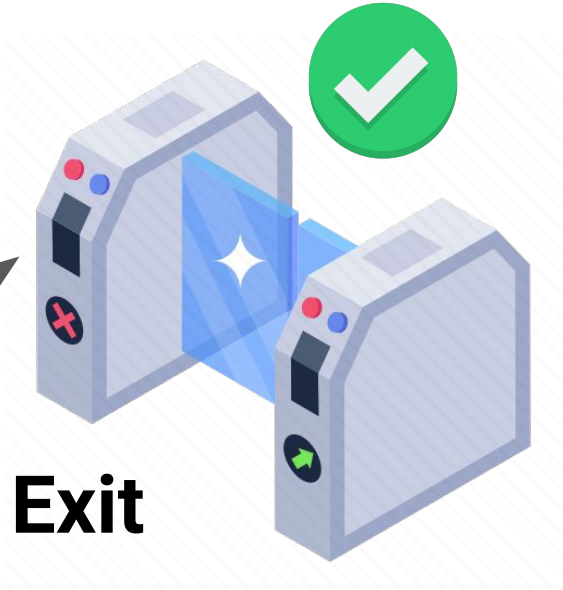


Exiting The Train Station



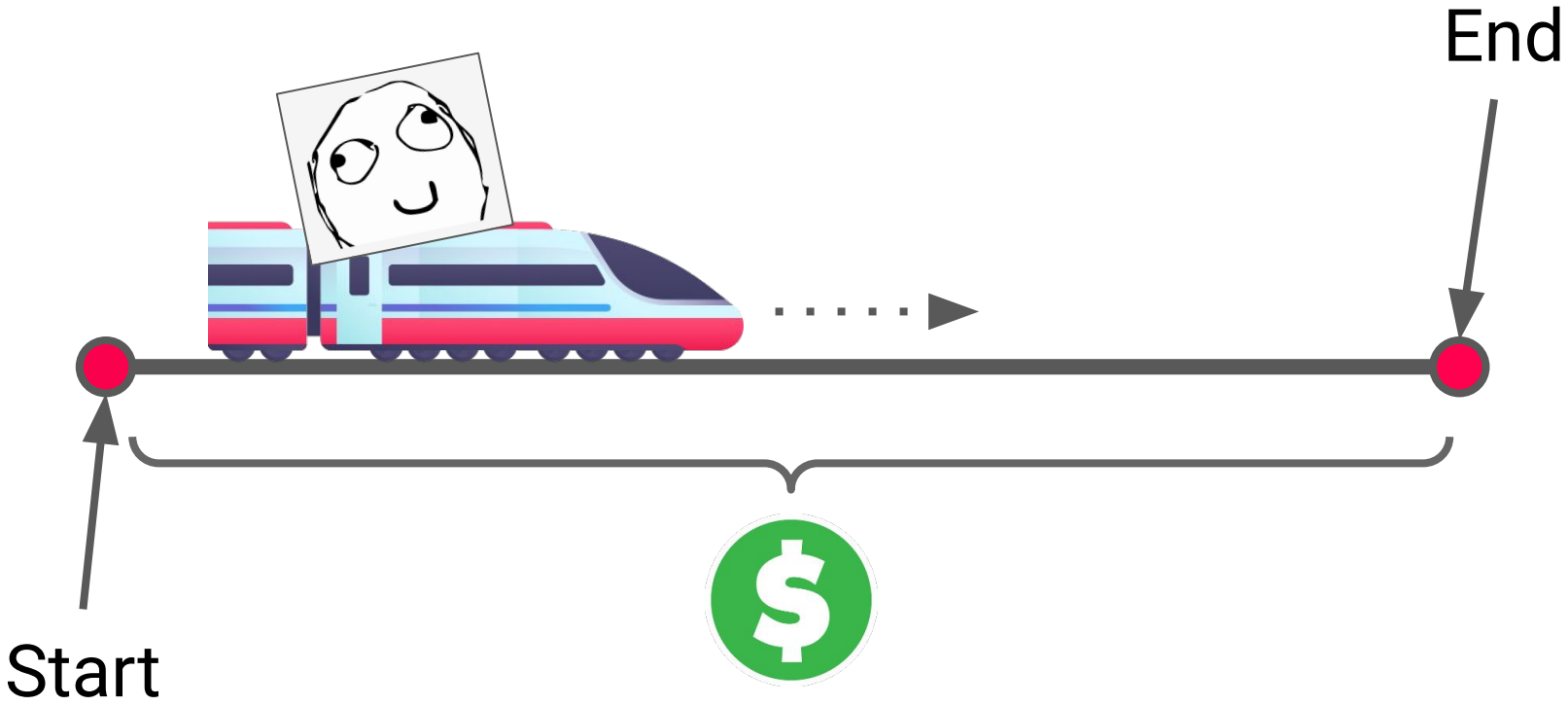


Exit
Ticket



Exit

Fare Calculation



What The Ticket Contains?



Ticket Format

Ticket Example



1103111228148713604081111039120515963892513201

Collecting Samples

```
------------------------------------------------------------
#1
Date: 12.06.2022
Entered station: Merkazit Ha-Miphratz    Time: 9:01
Exited station: Tel Aviv Ha-Shalom       Time: 10:40
Ticket: 10111141113013101317413141310147412123511371101214201
------------------------------------------------------------
```

```
------------------------------------------------------------
#2
Date: 09.06.2022
Etnter Station: Tel Aviv Ha-Shalom       Time: 19:31
Exited Station: Merkazit Ha-Miphratz     Time: 21:11
Ticket: 11576101622113547128961313151441021211450 201
------------------------------------------------------------
```

```
------------------------------------------------------------
#3
Date: 06.06.2022
Entered Station: Merkazit Ha-Miphratz    Time: 08:53
Exited Station: Tel Aviv Ha-Shalom       Time: 10:40
Ticket: 10111412714121312412154313121121371384823151294313201
------------------------------------------------------------
```

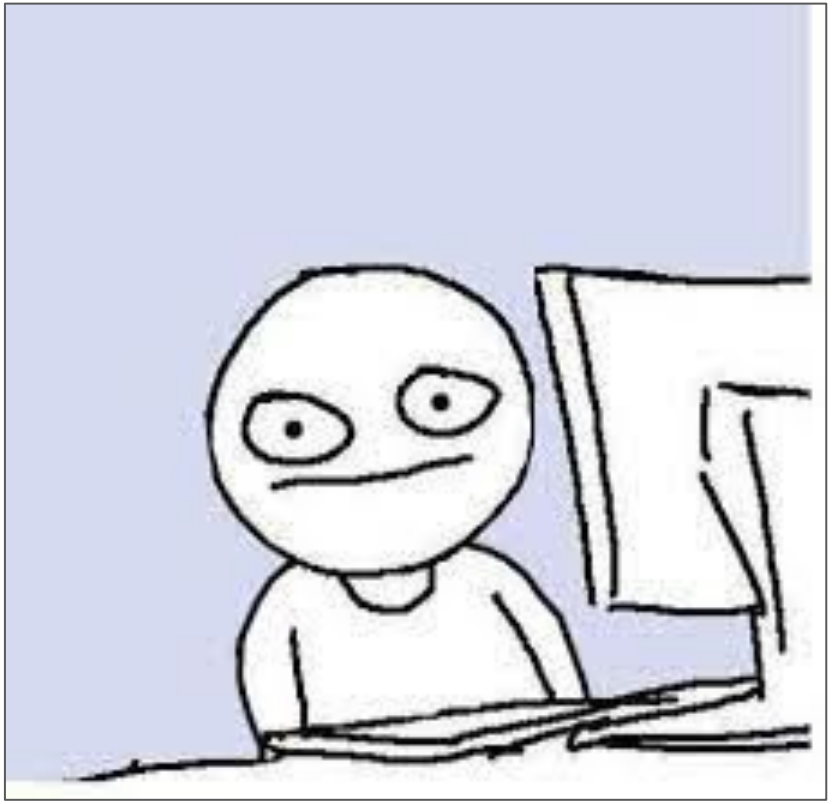
Quick Search On Google

Found the following API:

https://ravkavonline.co.il/api/ravkav/lookups/



Well.. Now What?



The Experiment

Valid Ticket:

11031112281487136040811110391205159638925132 01

Moovit-Pango Operator

To

IDF Operator



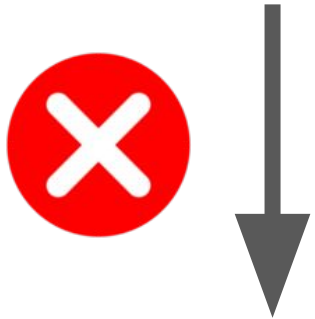
Fake Ticket:

11031112281487136040811110391205159638925132 50

The Experiment

Valid Ticket:

110311122814871360408111103912051596389251320 1



Fake Ticket:

110311122814871360408111103912051596389251325 0

Conclusion



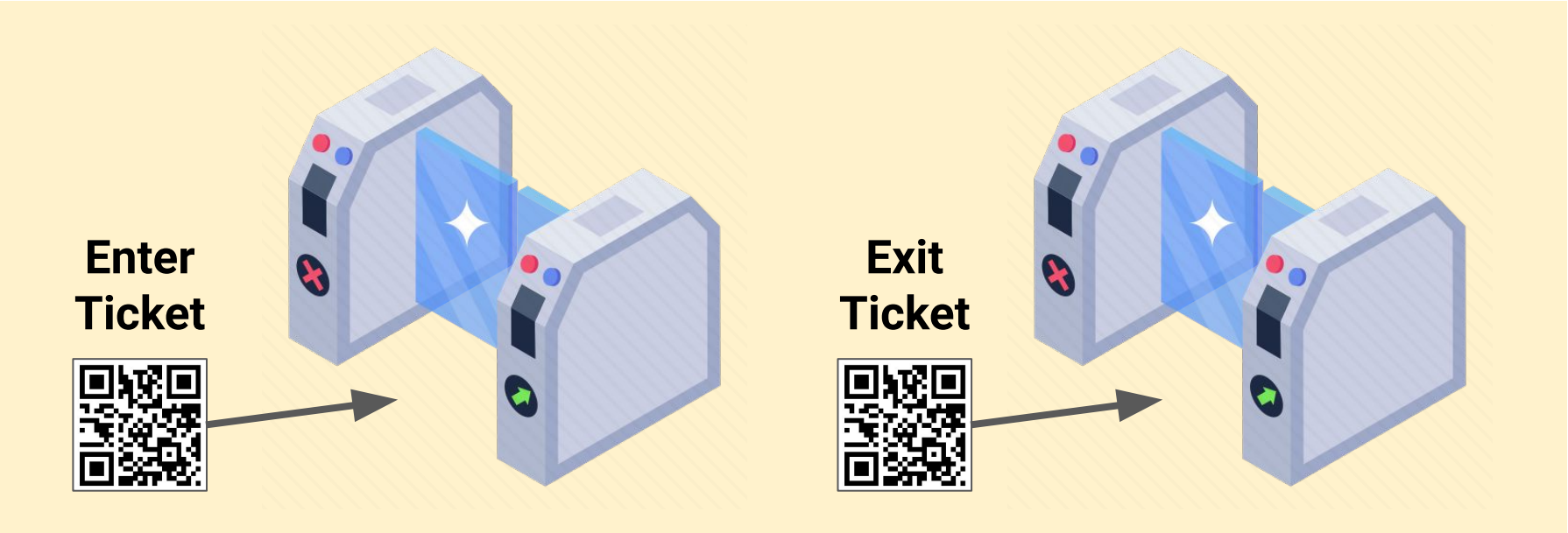
The Gates

(Behind the Scenes)

Logical Vulnerability



Reminder



Diffing Entrance & Exit Tickets

Enter Ticket



=

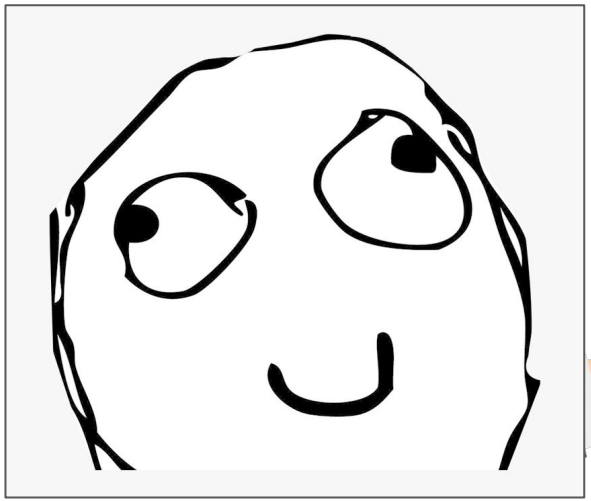
Exit Ticket



Hmm...

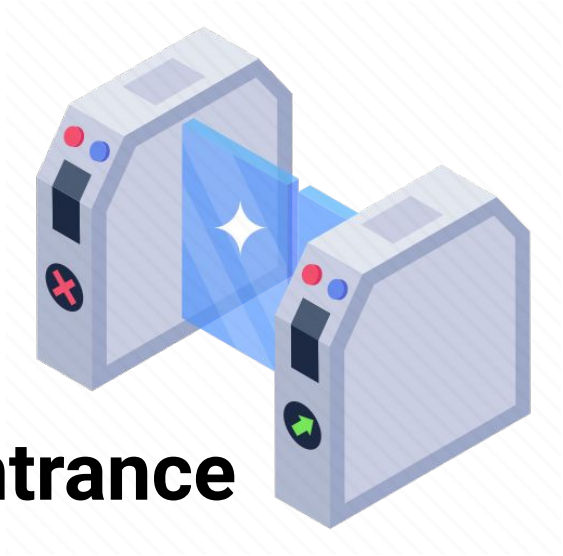


Cancel & Use



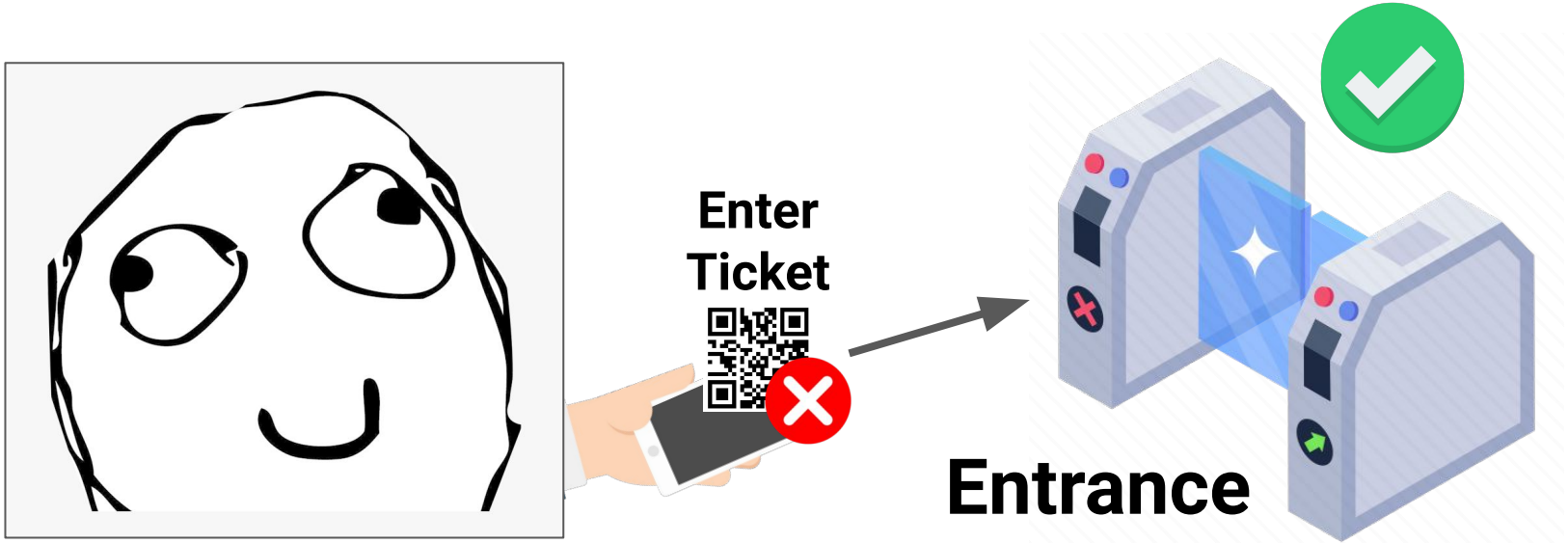
Enter
Ticket



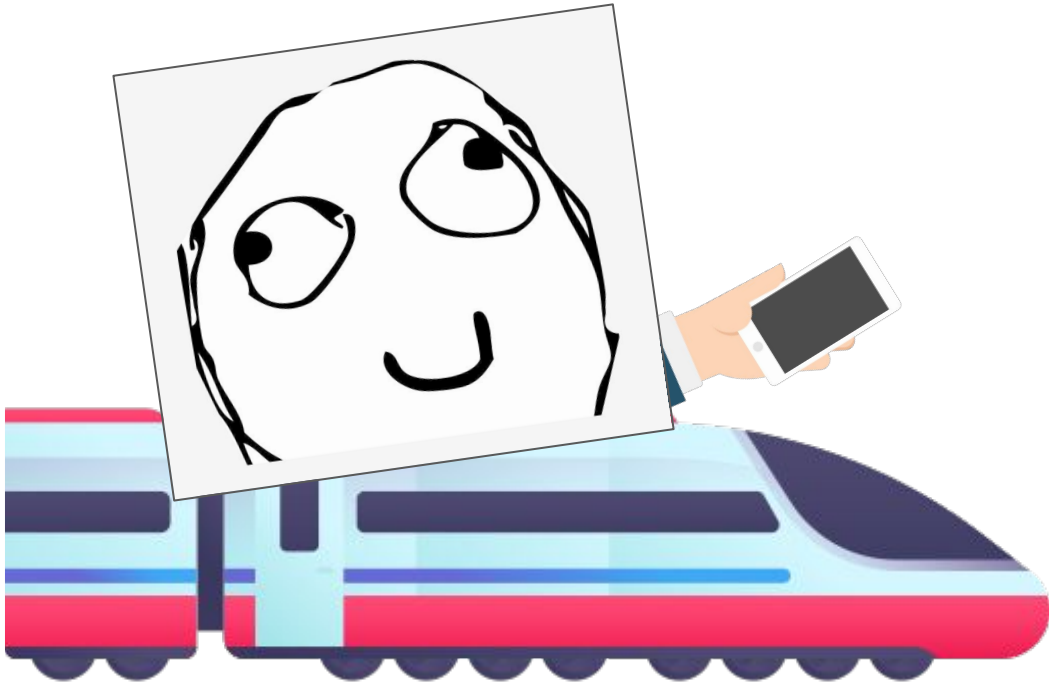


Entrance

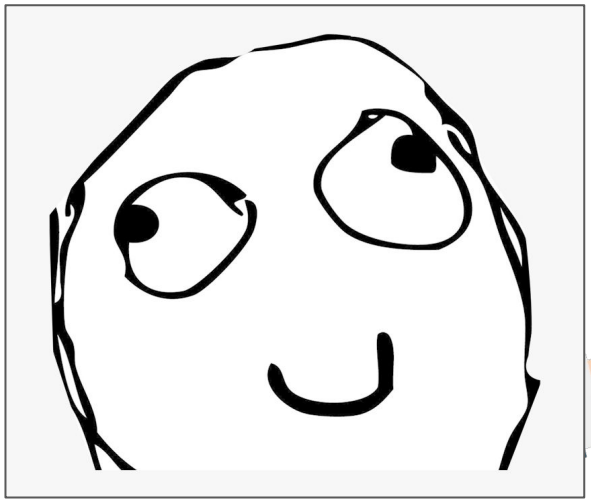
Cancel & Use

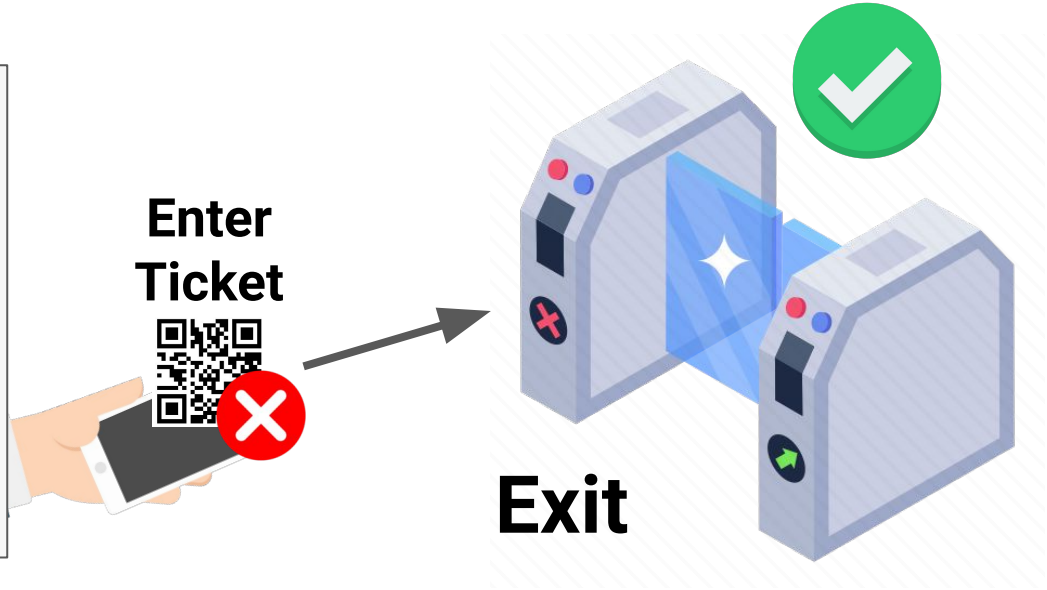


Having Fun Ride



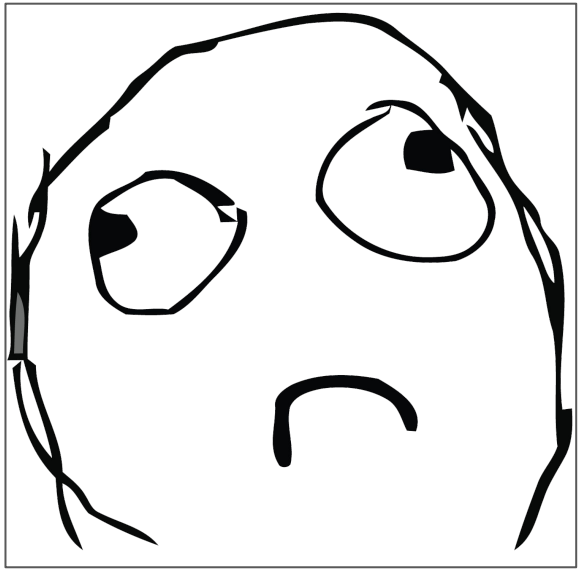
Cancel & Use



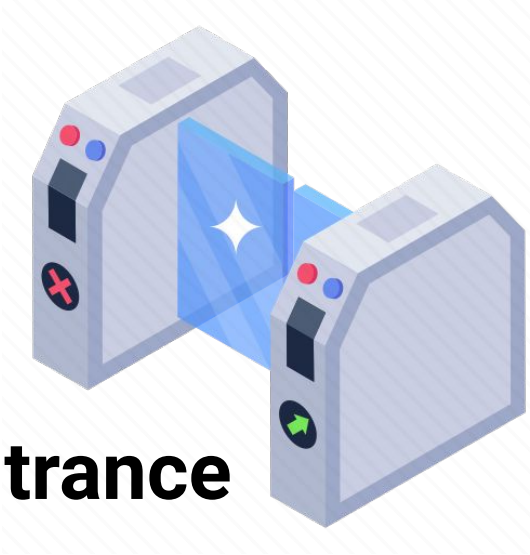


Cancel & Use

The fare from your 08/05/2023 08:30 ride has been updated, according to the information from the Ministry of Transport. Check My Rides for the updated fare.



What Probably Happened?

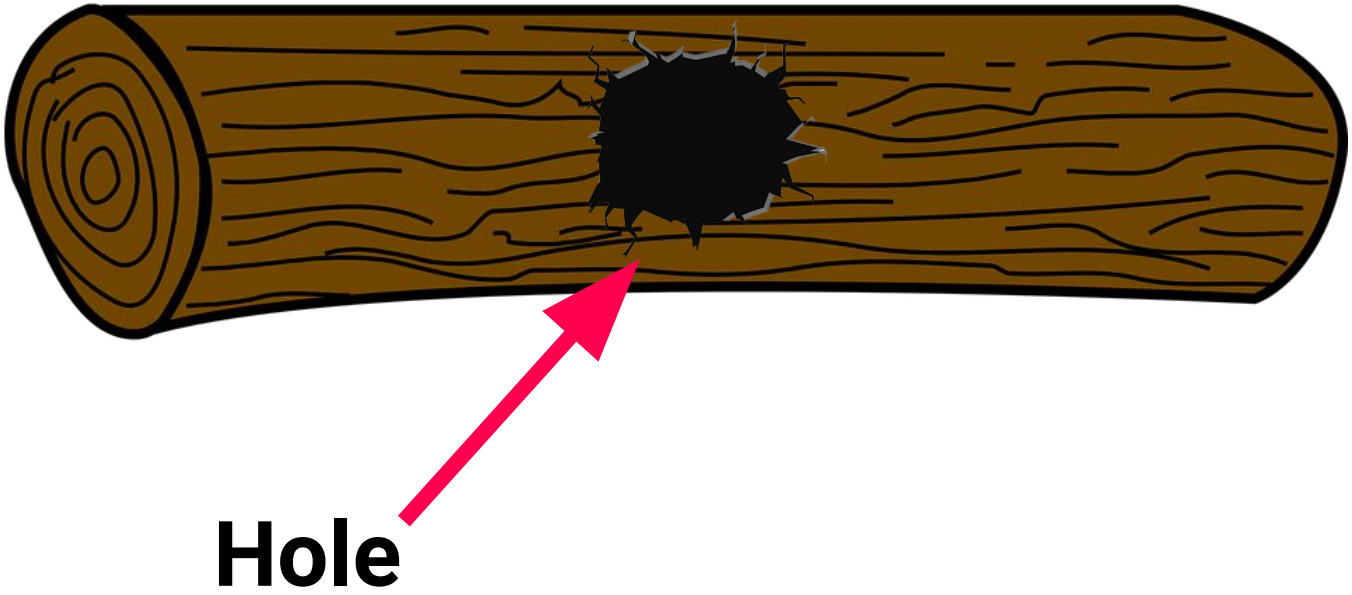


Entrance

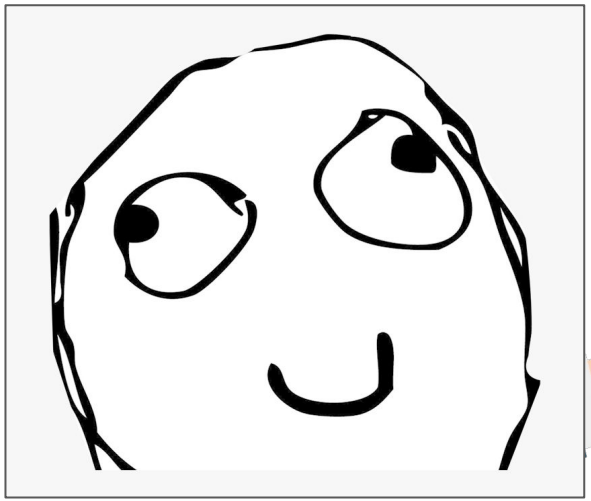


Exit

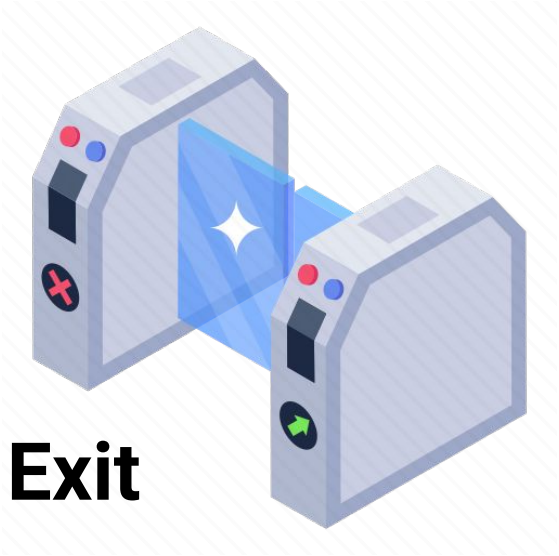
Hole In The Log



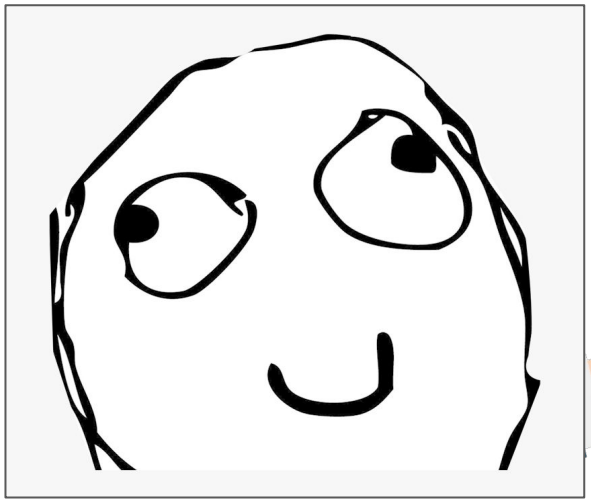
Hole In The Log

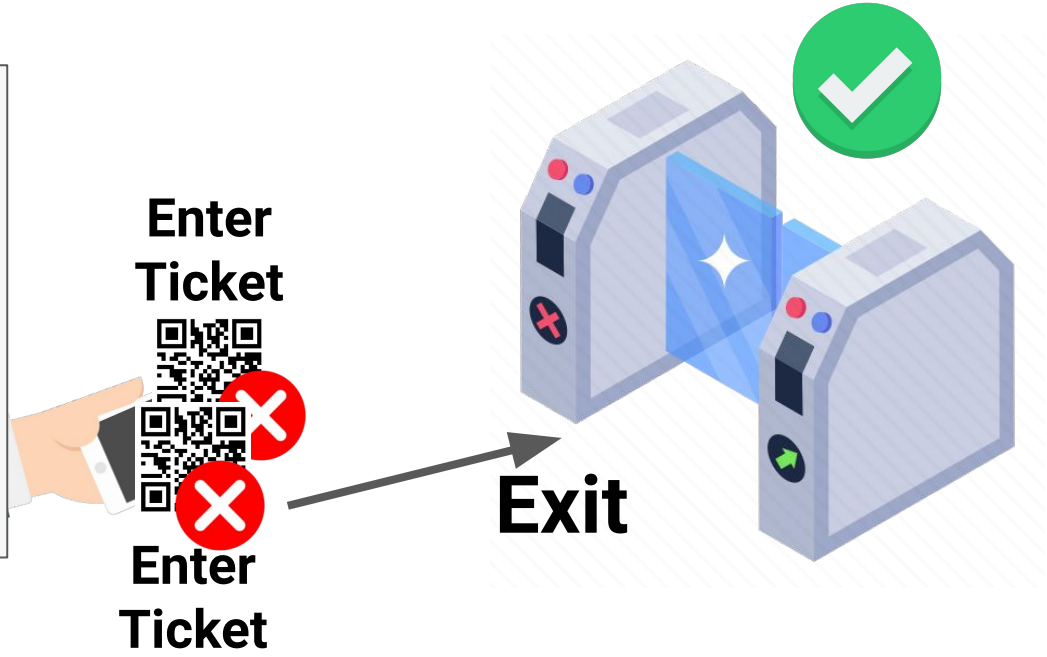






Hole In The Log





Summarize

- How mobile solution works 
- How to trick the gates 

Moovit

(MaaS Operator)

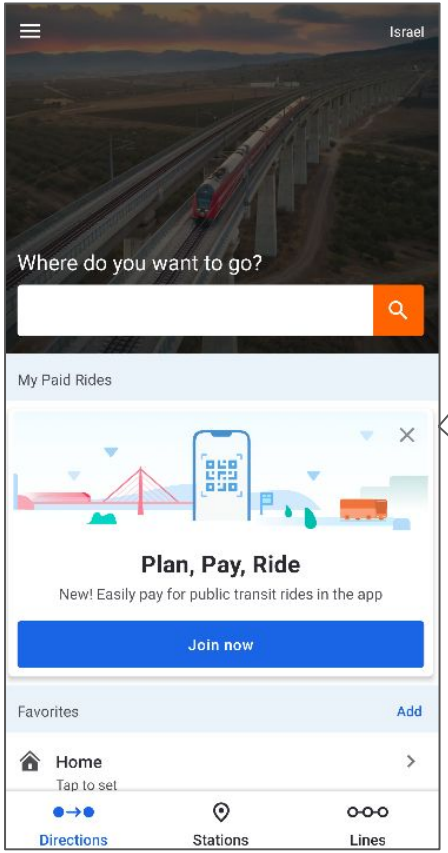


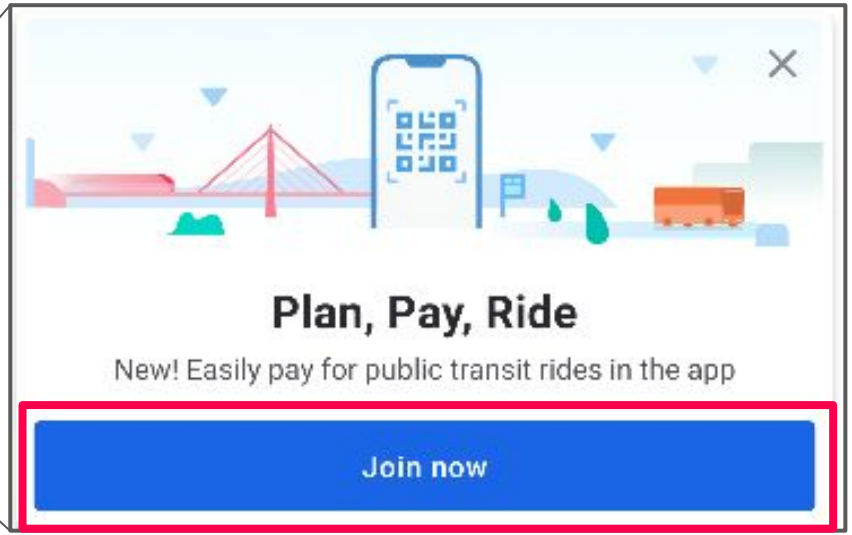
Moovit Overview

- Leading MaaS Operator
- Acquired by Intel at 900m $
- 1.4 Billion users
- 100 Countries
- 5000+ Cities

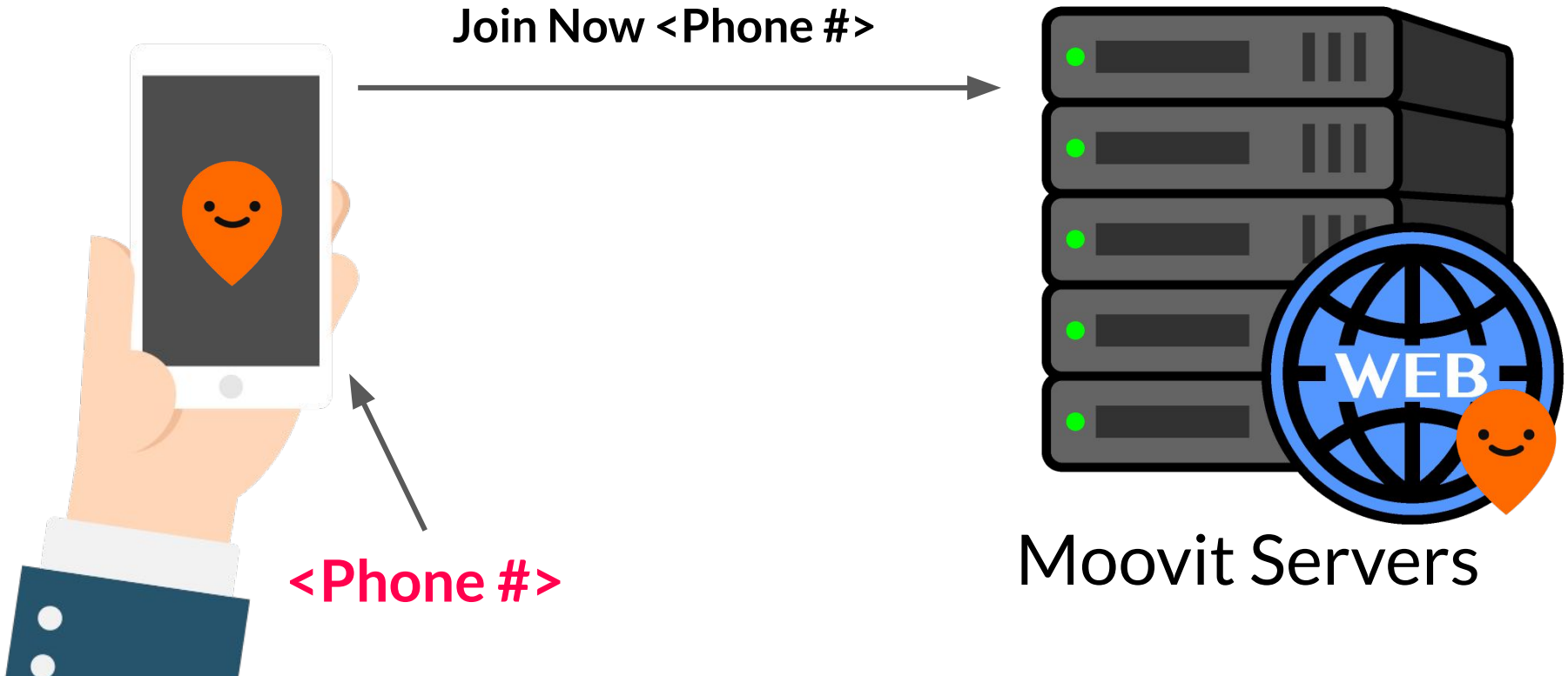


Moovit Interface

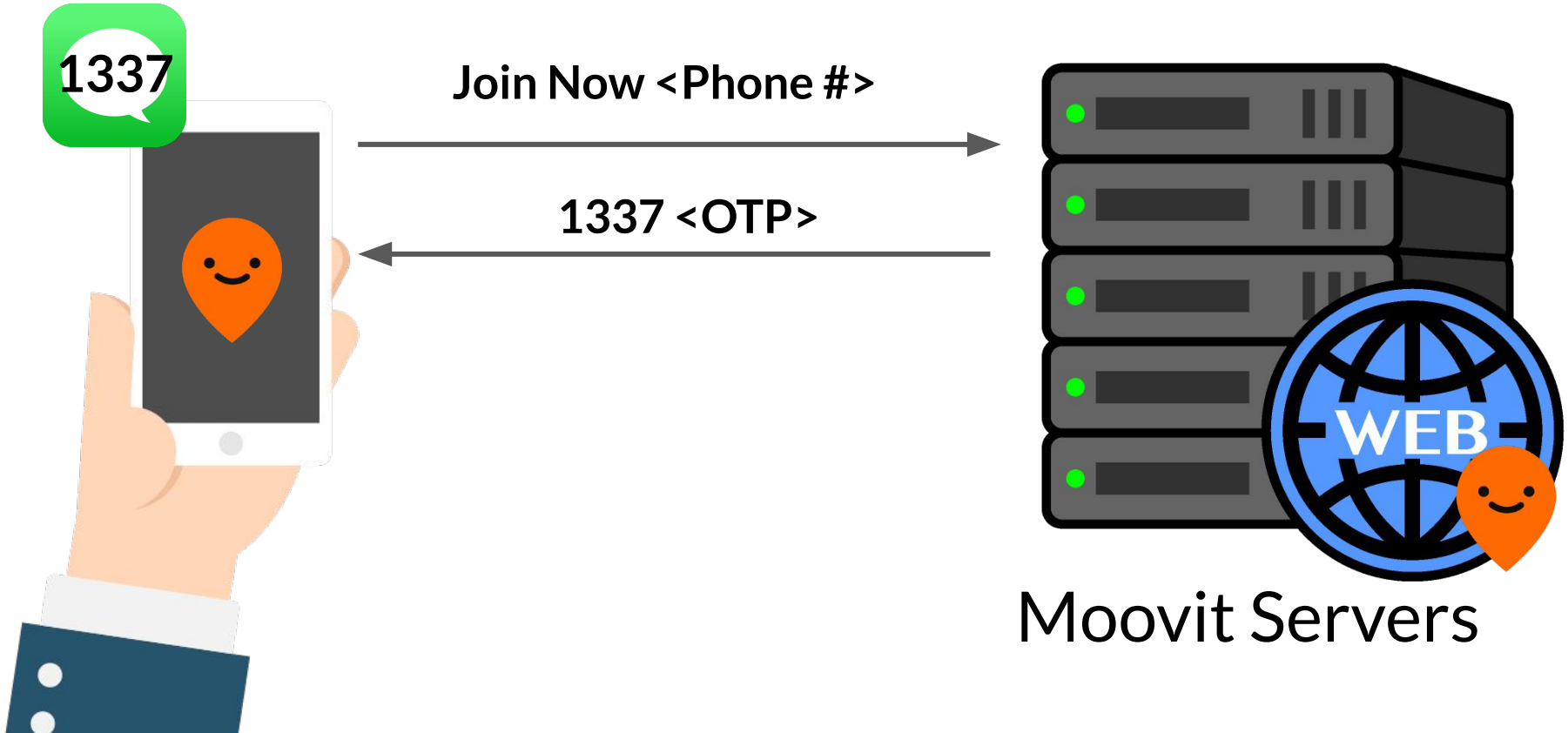




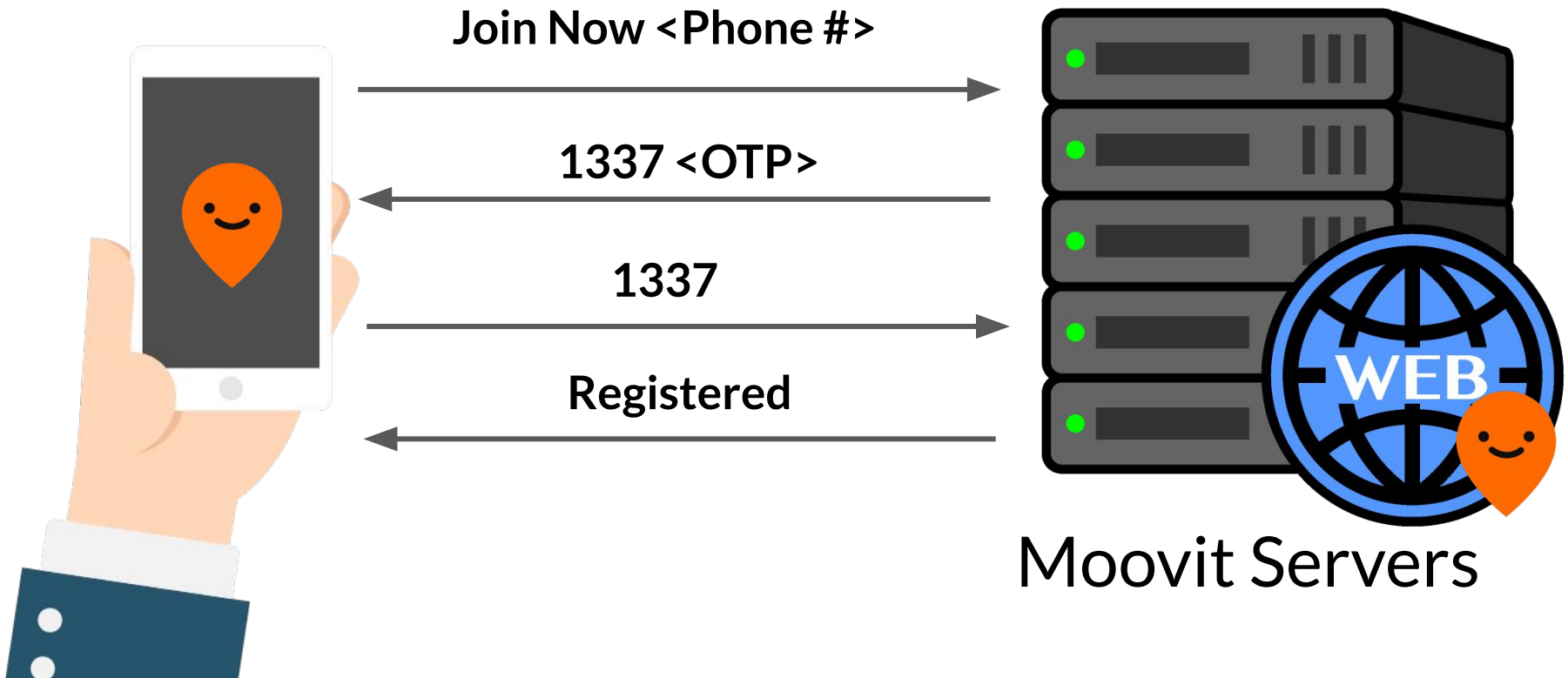
Account Registration



Account Registration



Account Registration



Account Affiliation



Moovit Servers

Affiliations



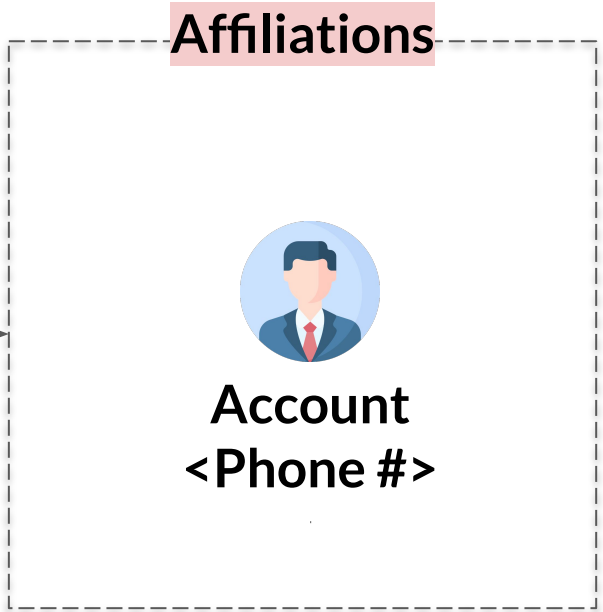
Account <Phone #>

- Credit Card
- PII

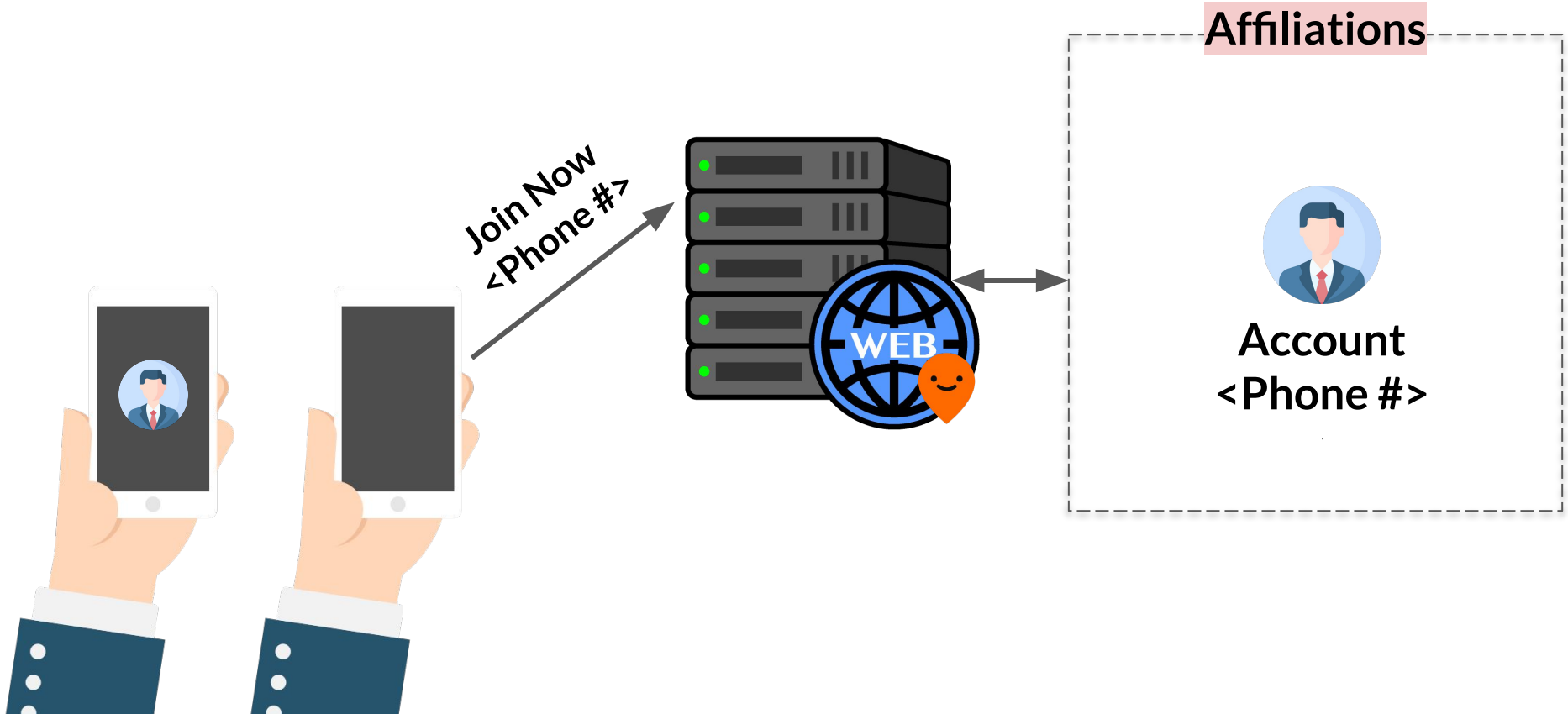
Existing Account But Another Device



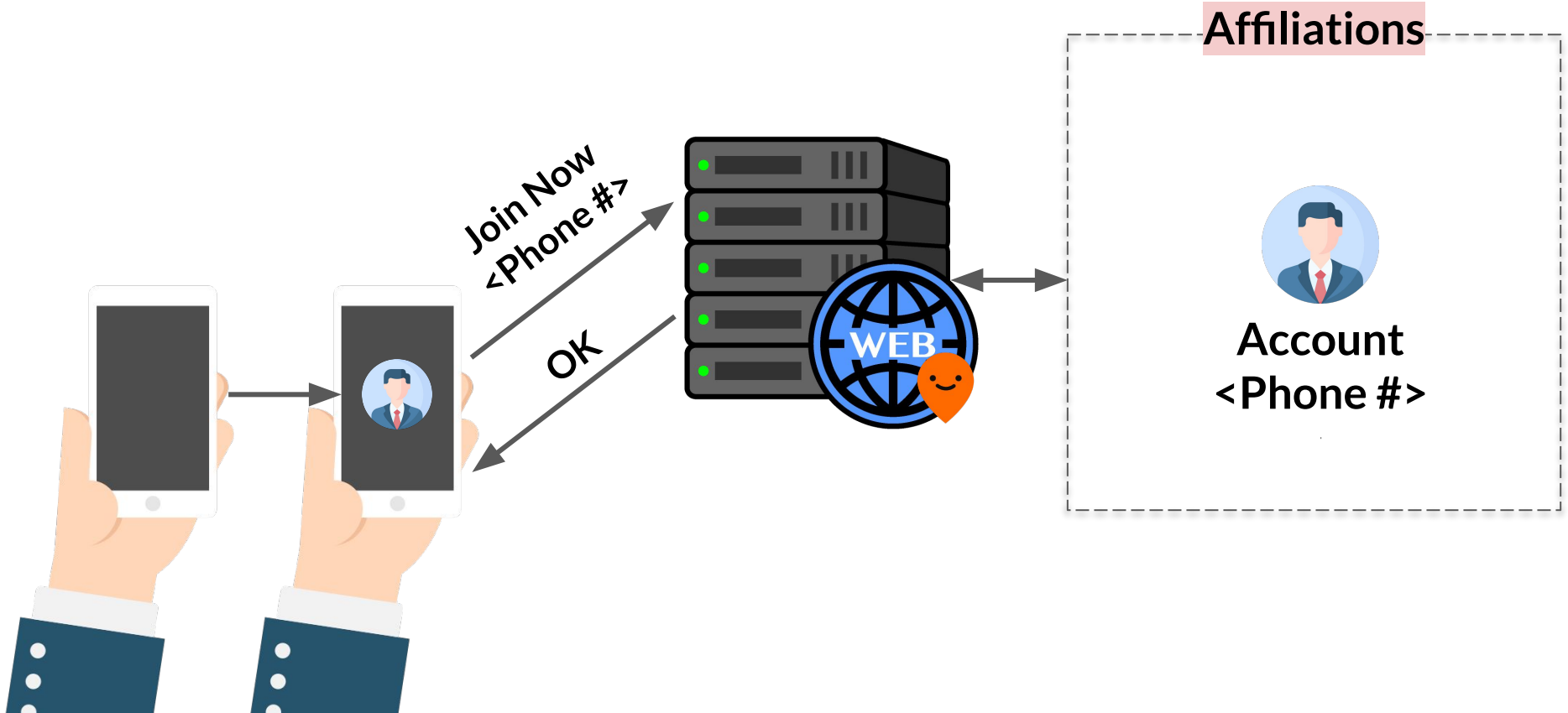




Existing Account But Another Device



Existing Account But Another Device



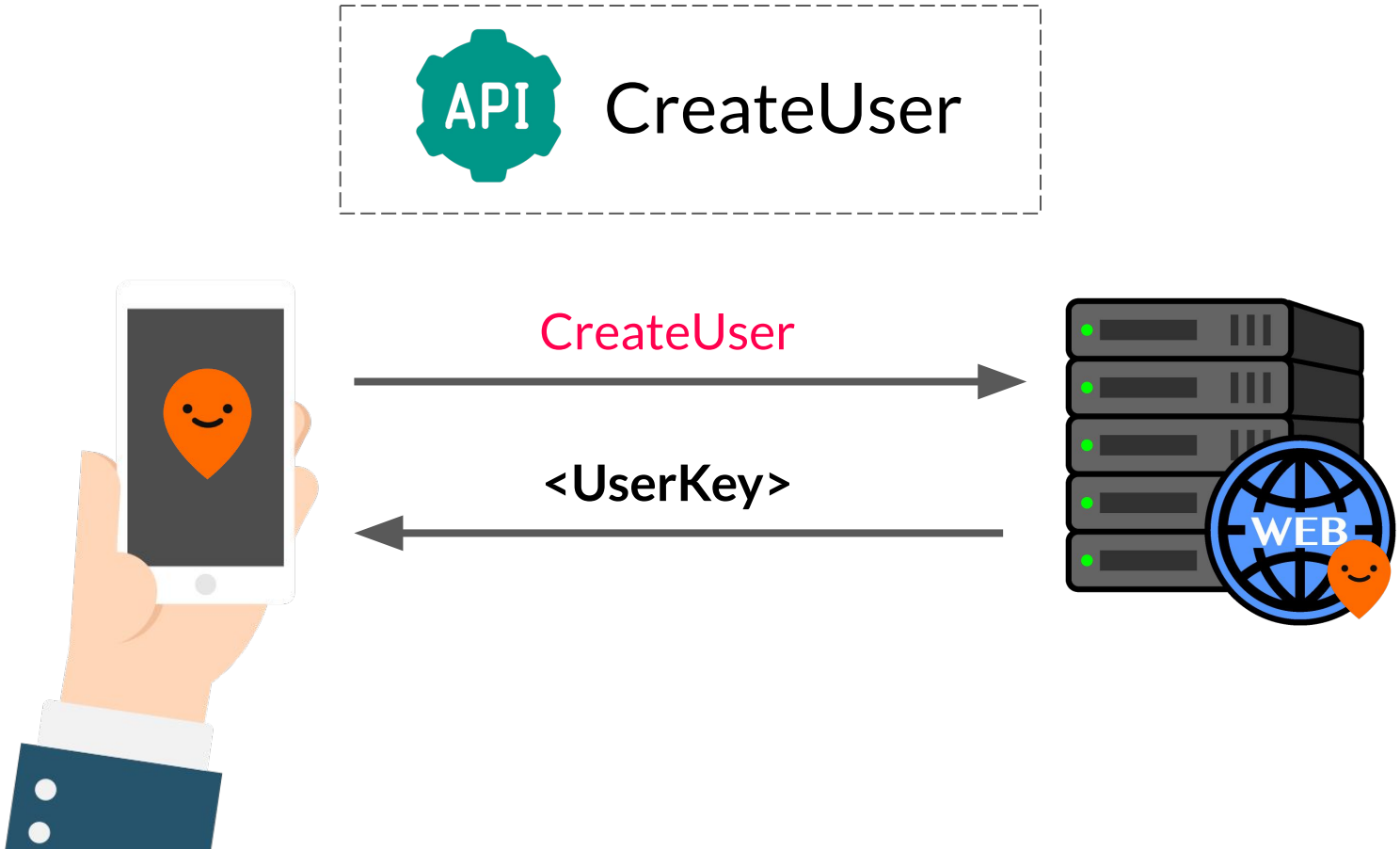
Vulnerability #1

ABC Of API Security

SSL Unpinning

```
$ frida -U -l .\ssl_unpinning.js -f com.tranzmate
     ____
    / _  |   Frida 16.0.8 - A world-class dynamic instrumentation toolkit
   | (_| |
    > _  |   Commands:
   /_/ |_|       help      -> Displays the help system
   . . . .       object?   -> Display information about 'object'
   . . . .       exit/quit -> Exit
   . . . .
   . . . .   More info at https://frida.re/docs/home/
```

The First API Request



Account To UserKey



Moovit Servers

Affiliations



Account <Phone #>

- Credit Card
- PII
- <UserKey>

Assume That …



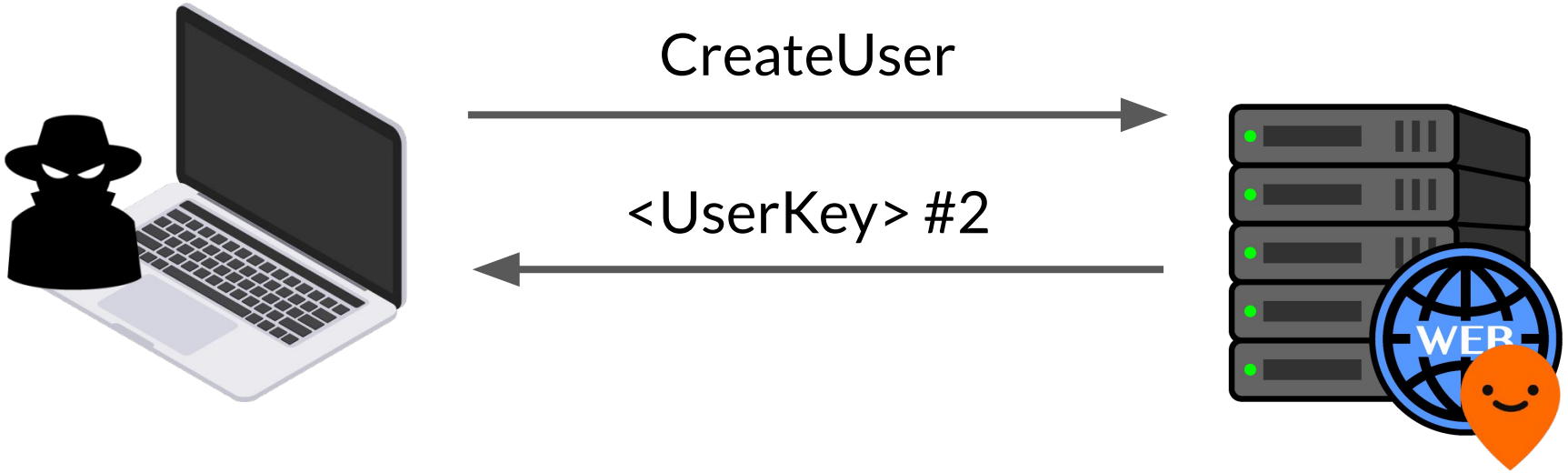
Affiliations



Account <Phone #1>

- Credit Card
- PII
- <UserKey> #1

Pretending to Be Other Device



Pretending to Be Other Device

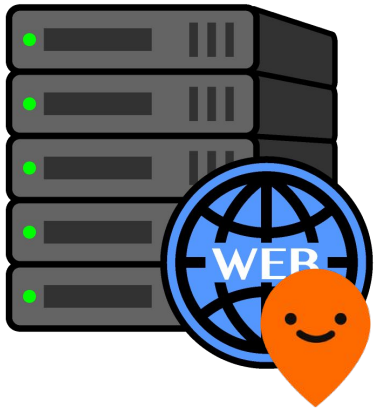


<UserKey> #2

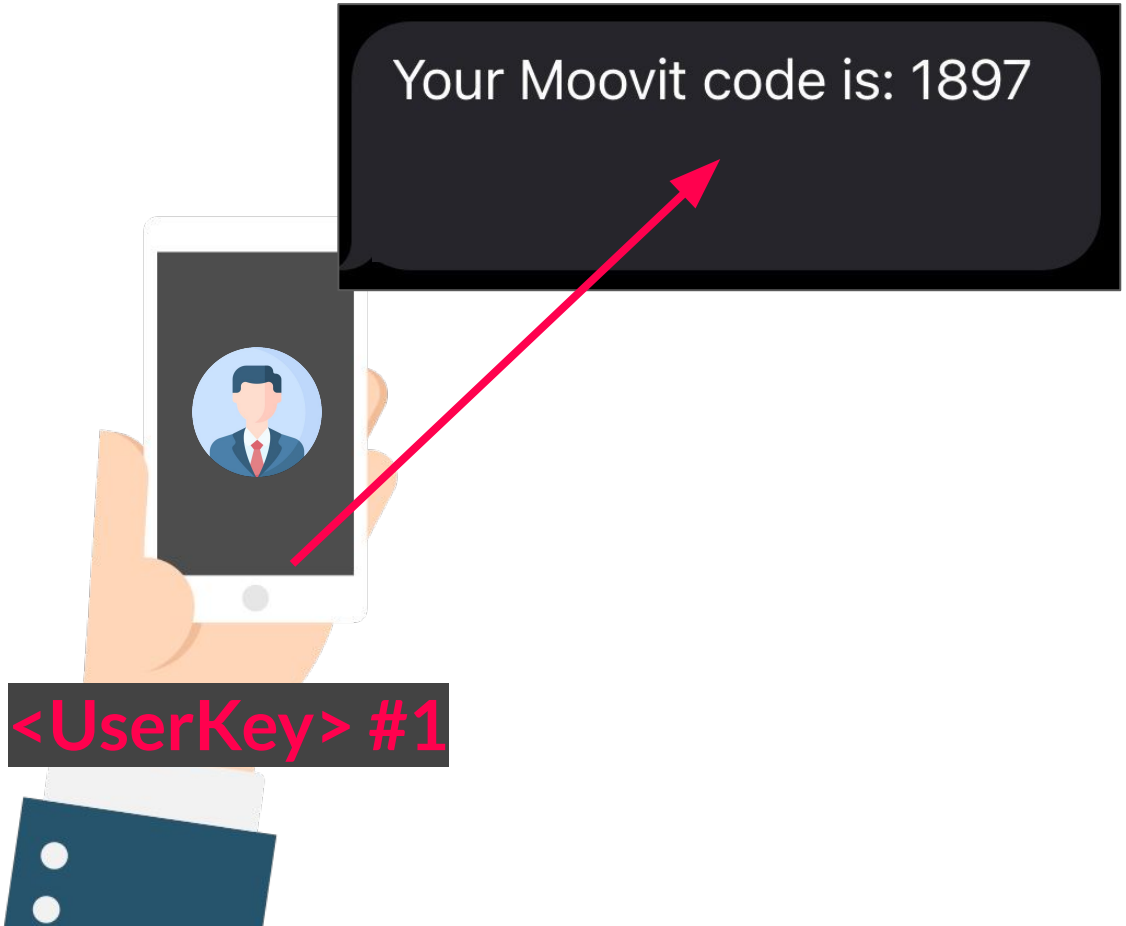
CreateUser

<UserKey> #2

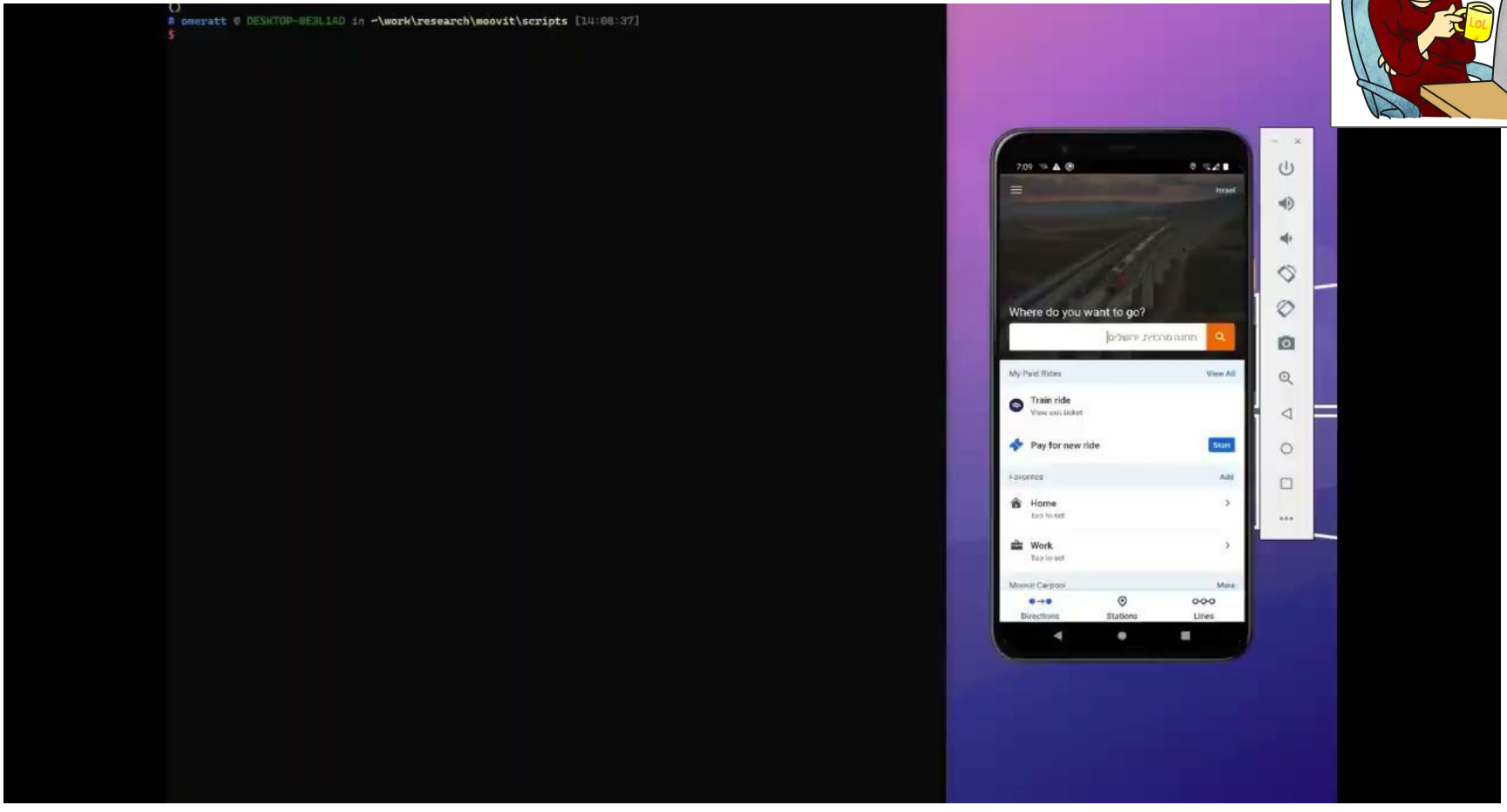
Join Now I'm <Phone #1>

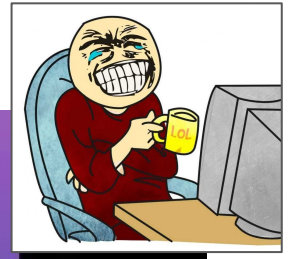


The Unexpected Vulnerability



Hijacking Account





Affiliation Change



<UserKey> #2

Affiliations



Account <Phone #>

- Credit Card
- PII
- <UserKey> #2

Pros & Cons



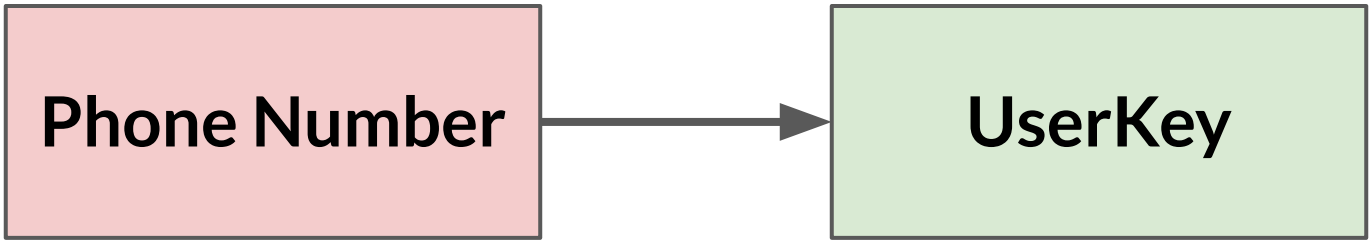
- Targeted Attack



- Takes time
- Disconnect the account
- Requires account phone number

Complexity Reduction

Transforming one problem into another problem

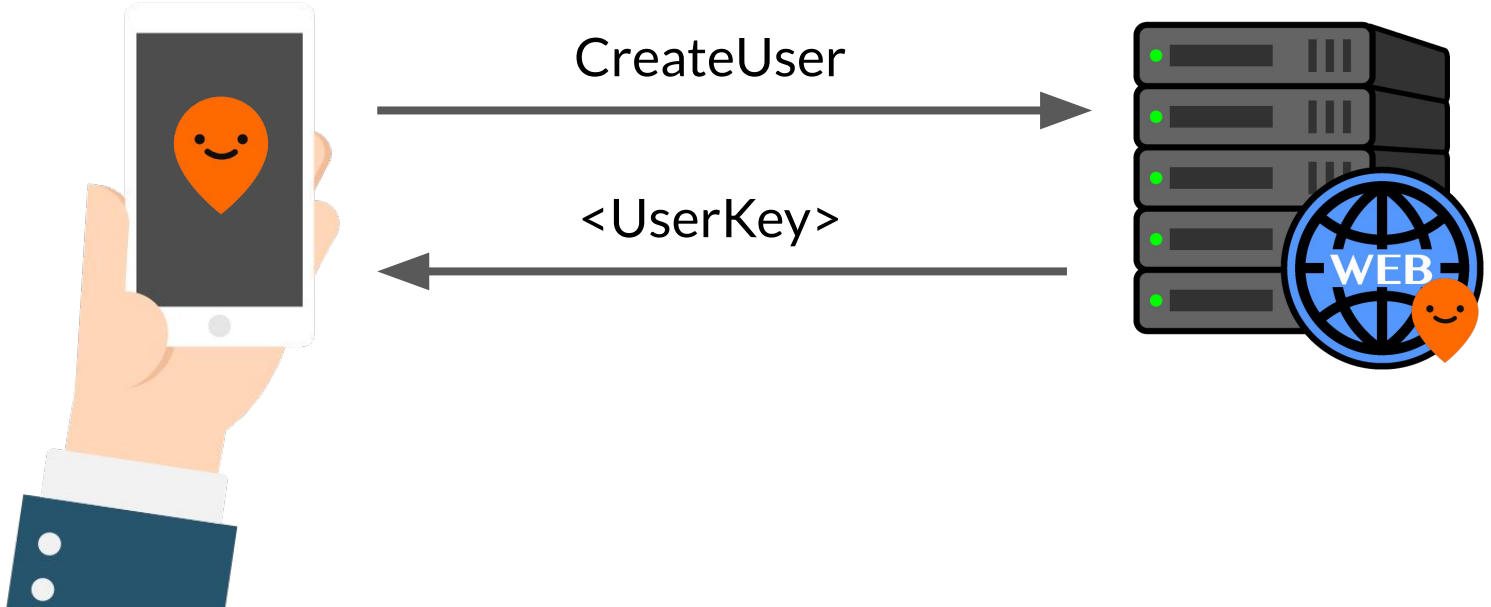


UserKey Breakdown

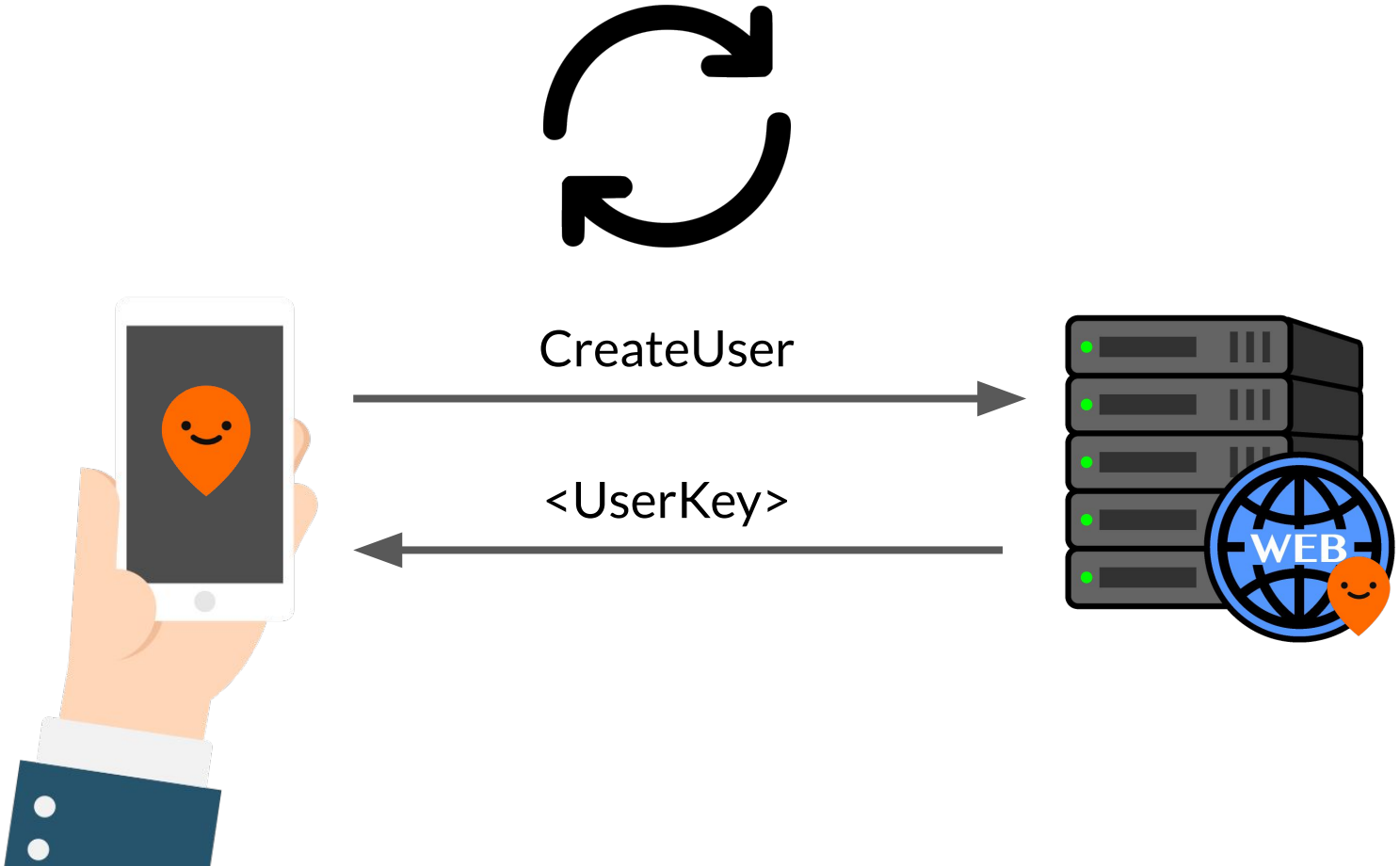
Vulnerability #2

UserKey Format

E4C6F3B1EFF23008E0530100007FE981



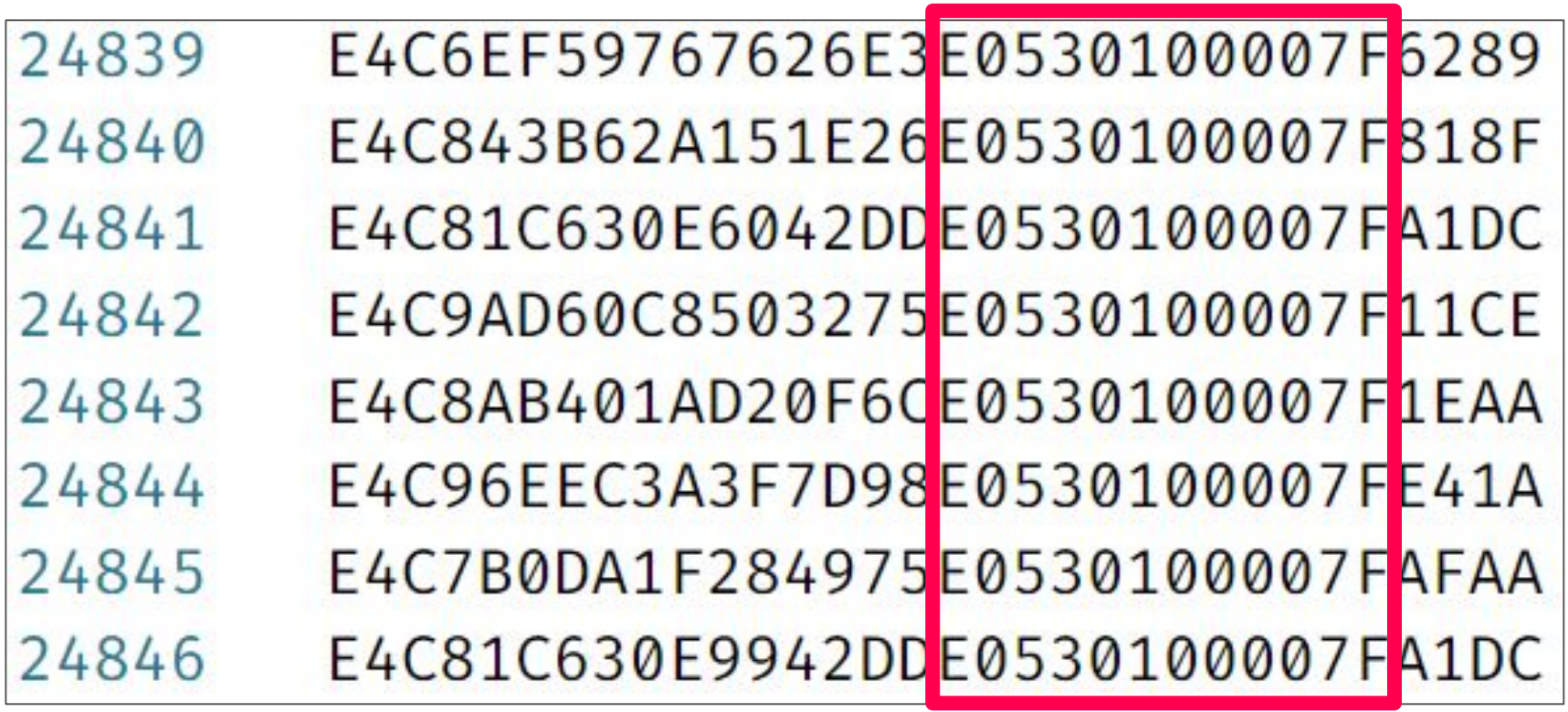
Collecting Samples



Breaking Down The Format

24839	E4C6EF59767626E3E0530100007F6289
24840	E4C843B62A151E26E0530100007F818F
24841	E4C81C630E6042DDE0530100007FA1DC
24842	E4C9AD60C8503275E0530100007F11CE
24843	E4C8AB401AD20F6CE0530100007F1EAA
24844	E4C96EEC3A3F7D98E0530100007FE41A
24845	E4C7B0DA1F284975E0530100007FAFAA
24846	E4C81C630E9942DDE0530100007FA1DC

Breaking Down The Format



24839	E4C6EF59767626E3	E0530100007F6289
24840	E4C843B62A151E26	E0530100007F818F
24841	E4C81C630E6042DD	E0530100007FA1DC
24842	E4C9AD60C8503275	E0530100007F11CE
24843	E4C8AB401AD20F6C	E0530100007F1EAA
24844	E4C96EEC3A3F7D98	E0530100007FE41A
24845	E4C7B0DA1F284975	E0530100007FAFAA
24846	E4C81C630E9942DD	E0530100007FA1DC

Oracle SYS_GUID

Purpose

`SYS_GUID` generates and returns a globally unique identifier (`RAW` value) made up of 16 bytes. On most platforms, the generated identifier consists of a host identifier, a process or thread identifier of the process or thread invoking the function, and a nonrepeating value (sequence of bytes) for that process or thread.

```
UID_COL
--------------------------------
7CD5B7769DF75CEFE034080020825436
7CD5B7769DF85CEFE034080020825436
7CD5B7769DF95CEFE034080020825436
7CD5B7769DFA5CEFE034080020825436
```

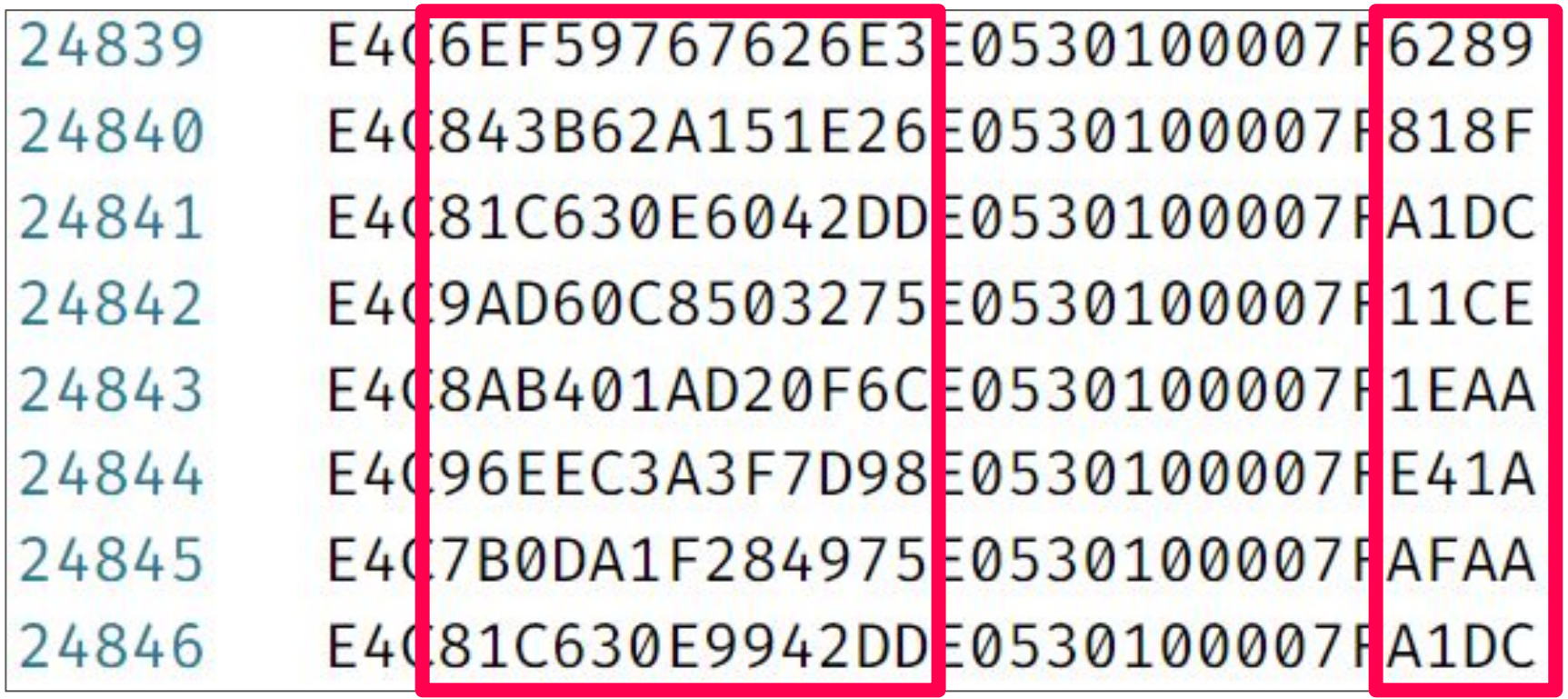
Oracle SYS_GUID

Purpose

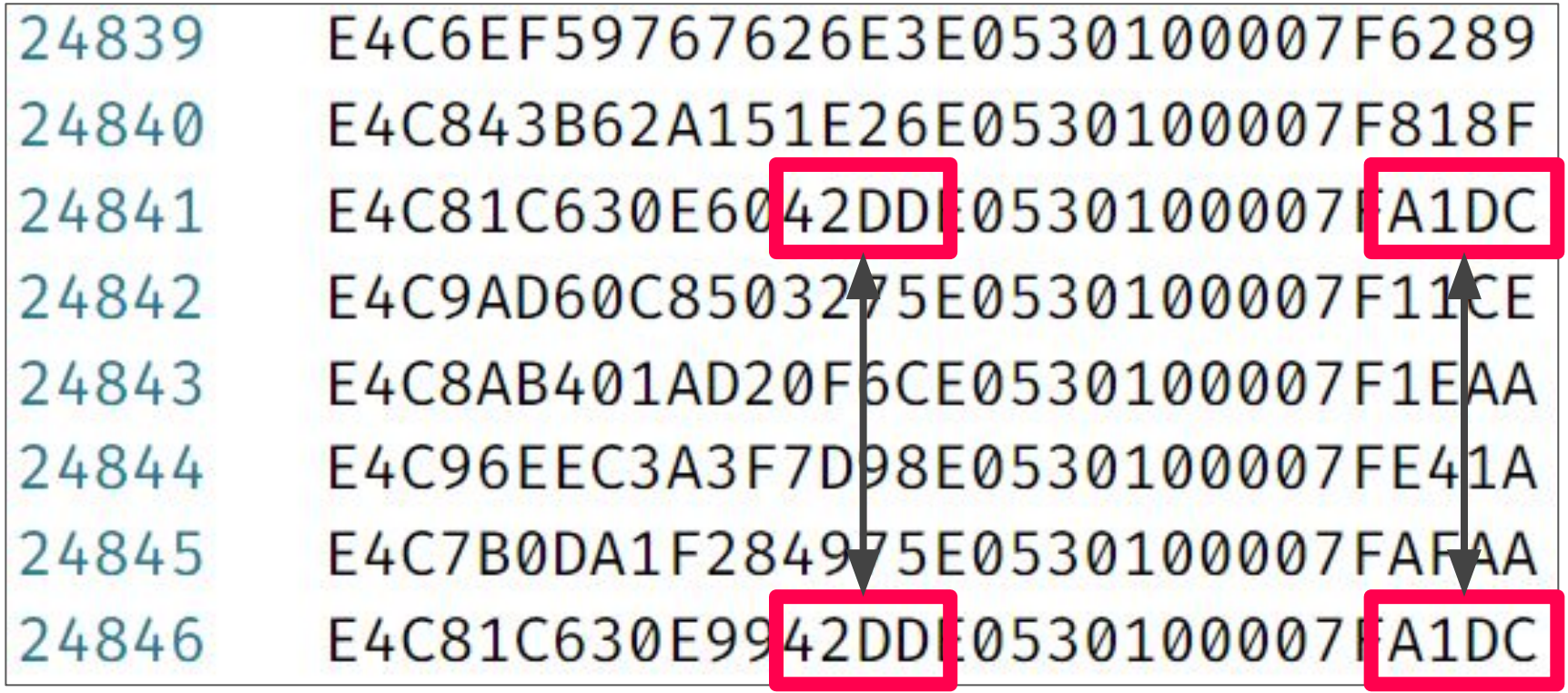
`SYS_GUID` generates and returns a globally unique identifier (`RAW` value) made up of 16 bytes. On most platforms, the generated identifier consists of a host identifier, a process or thread identifier of the process or thread invoking the function, and a nonrepeating value (sequence of bytes) for that process or thread.

```
UID_COL
--------------------------------
7CD5B7769DF75CEFE034080020825436
7CD5B7769DF85CEFE034080020825436
7CD5B7769DF95CEFE034080020825436
7CD5B7769DFA5CEFE034080020825436
```

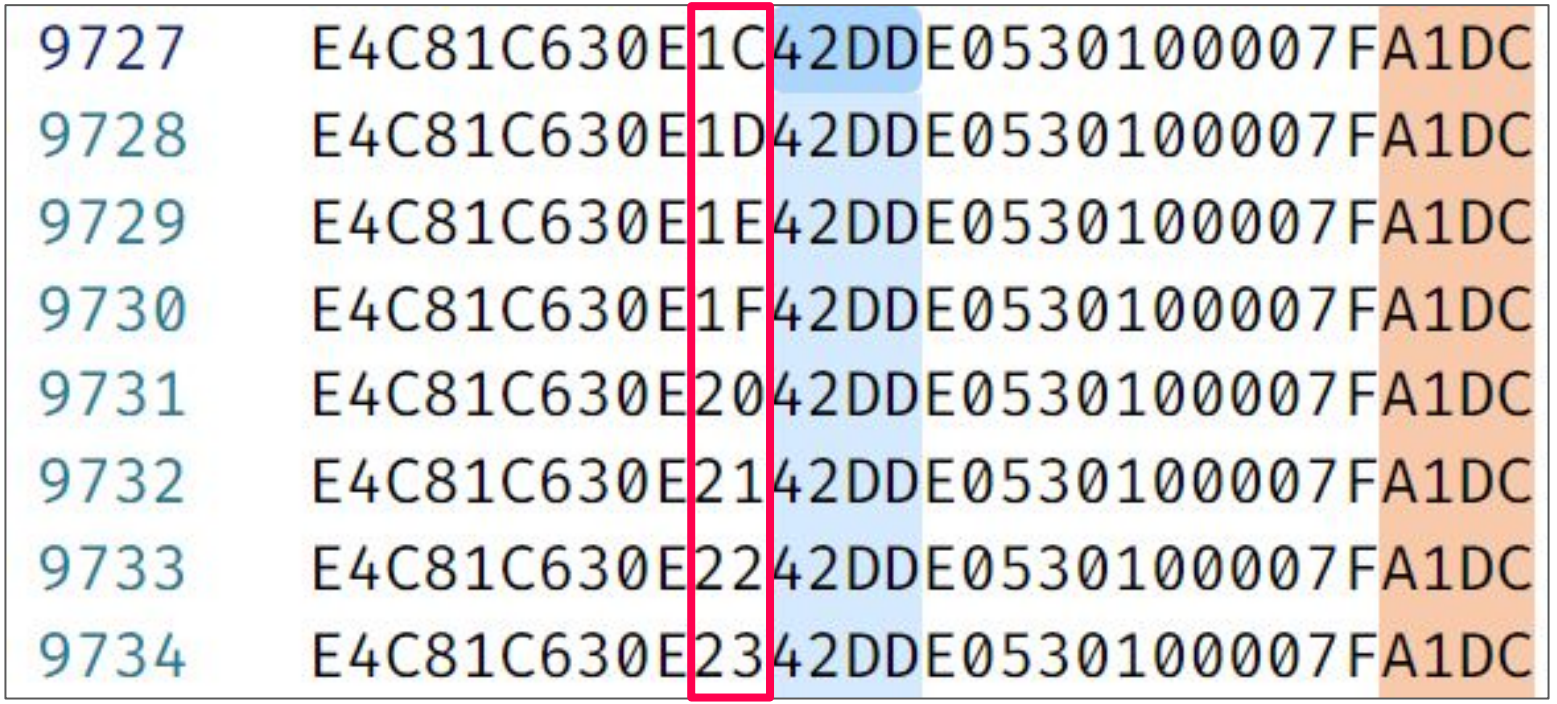
Breaking Down The Format



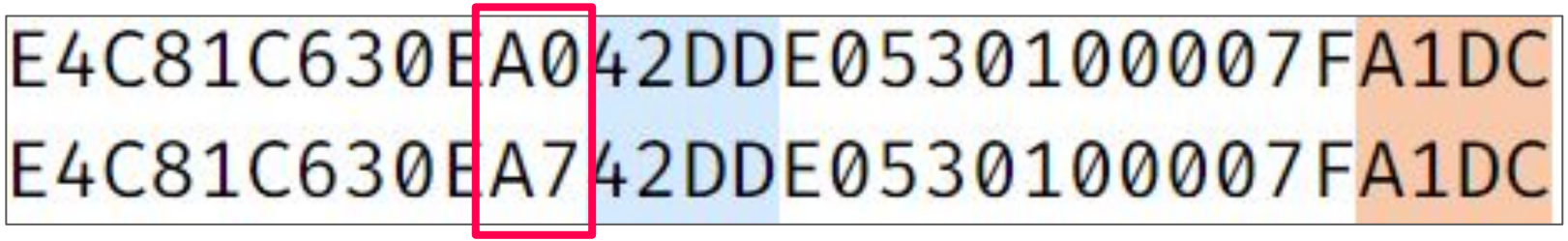
Breaking Down The Format



Breaking Down The Format

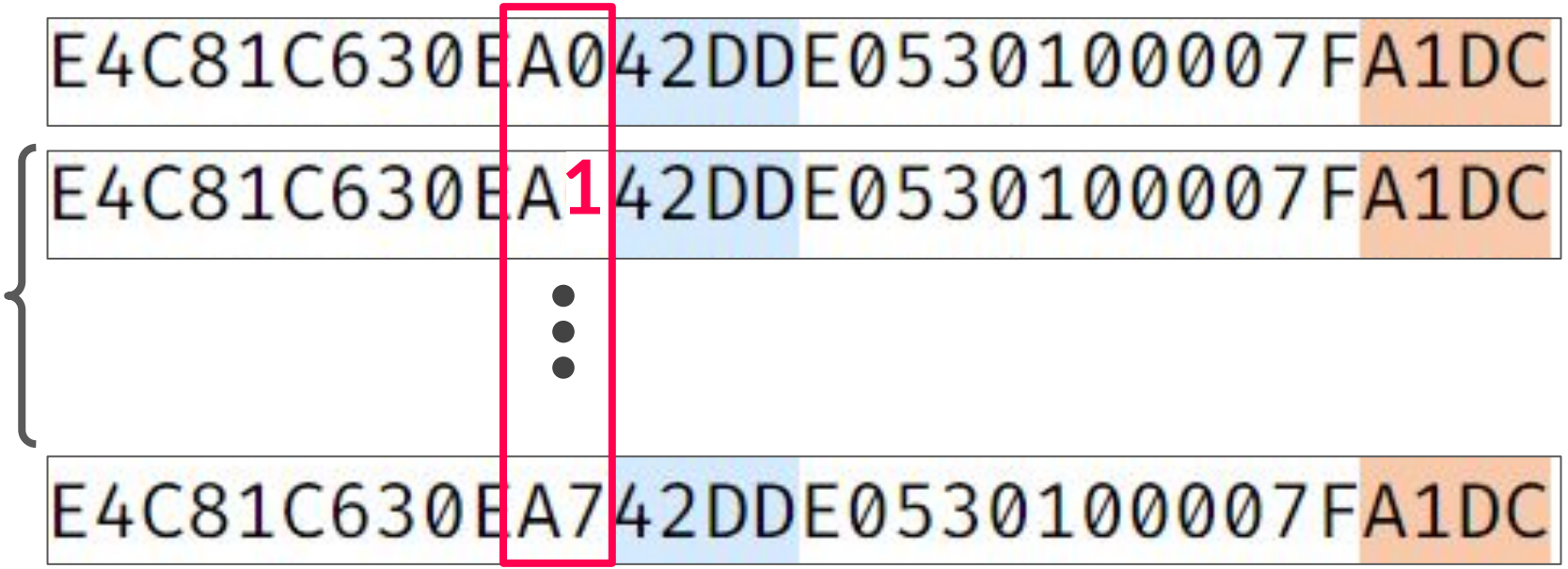


Why Do We Have Gaps?

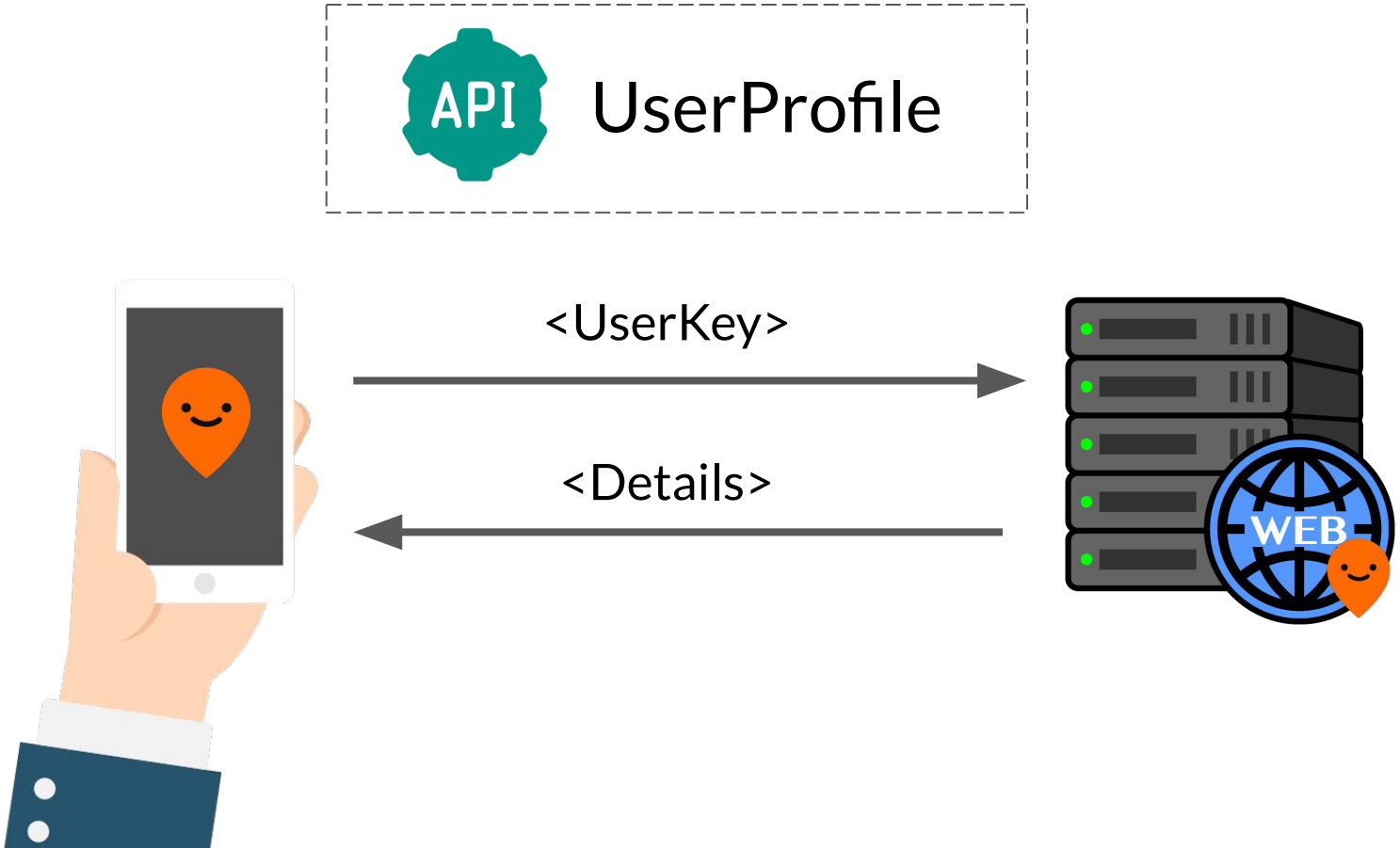


(A0, A7) = {A1, A2, A3, A4, A5, A6}

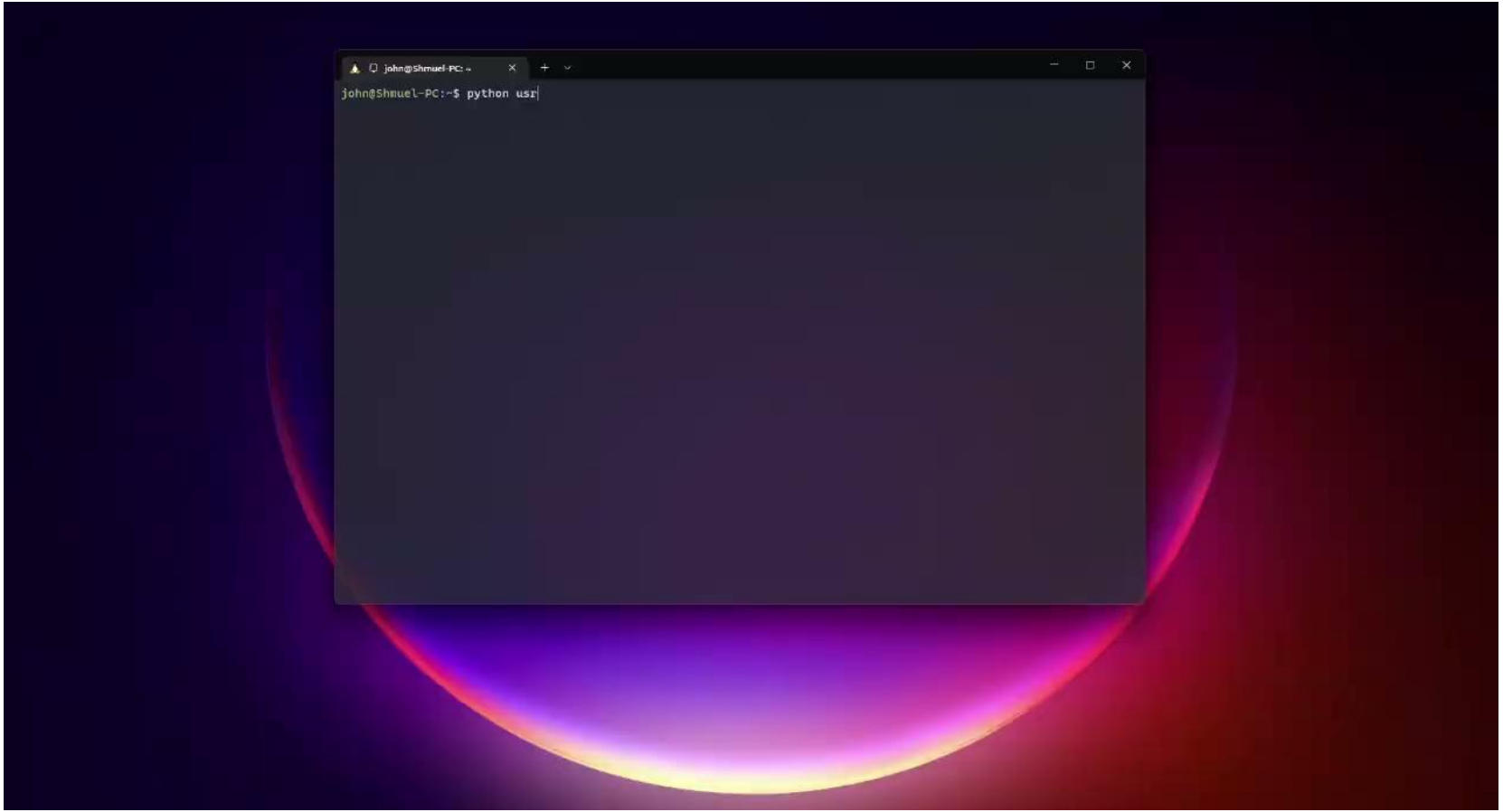
Filling The Gaps



UserProfile API Request



Getting Phone Numbers



A Few Moments Later



Accounts Around The World

```
 1   [+][Found Profile] --> E78E43310A806DD9E0530100007F6E7B -> +15
 2   [+][Found Profile] --> E78F48144E6907F6E0530100007F9C84 -> +48
 3   [+][Found Profile] --> E78F56E76ED816FEE0530100007FF967 -> +13
 4   [+][Found Profile] --> E78F685DBB0B2801E0530100007F499E -> +31
 5   [+][Found Profile] --> E78F6C75EA3F2B4AE0530100007FF770 -> +17
 6   [+][Found Profile] --> E78F6AFBF0A629FFE0530100007F76D3 -> +17
 7   [+][Found Profile] --> E78F785DBBE137F6E0530100007FFAA4 -> +16
 8   [+][Found Profile] --> E78F7737FD0D362DE0530100007FA69B -> +13
 9   [+][Found Profile] --> E78FF776D7B93E93E0530100007F9BBF -> +33
10   [+][Found Profile] --> E7900E50E4B456ECE0530100007FAD43 -> +15
11   [+][Found Profile] --> E7900035516346D0E0530100007F7250 -> +15
12   [+][Found Profile] --> E79029DF624C7503E0530100007FC2D8 -> +12
13   [+][Found Profile] --> E7903443DB317EABE0530100007F58C3 -> +15
14   [+][Found Profile] --> E7903443DB3E7EABE0530100007F58C3 -> +15
15   [+][Found Profile] --> E7902662D81A6F08E0530100007F02A1 -> +12
16   [+][Found Profile] --> E79044E65D490E6CE0530100007F7B91 -> +16
17   [+][Found Profile] --> E7901BFE1C5F6151E0530100007FD8C3 -> +17
18   [+][Found Profile] --> E79044E65D710E6CE0530100007F7B91 -> +16
19   [+][Found Profile] --> E7904119814B0D31E0530100007FEBF0 -> +31
20   [+][Found Profile] --> E7904A5A6AD5151AE0530100007FA616 -> +16
21   [+][Found Profile] --> E7903F298C510B5EE0530100007F70B0 -> +44
22   [+][Found Profile] --> E7906E574A403DBAE0530100007F39BE -> +13
23   [+][Found Profile] --> E7906E574A413DBAE0530100007F39BE -> +12
24   [+][Found Profile] --> E79073533AA943EEE0530100007FFEFD -> +19
25   [+][Found Profile] --> E79074EF650945AAE0530100007FA733 -> +31
26   [+][Found Profile] --> E79073533ADB43EEE0530100007FFEFD -> +32
```

Pros & Cons



- Targeted Attack



- Takes time
- Disconnect the account
- ~~Requires account phone number~~

How Can We Improve This?



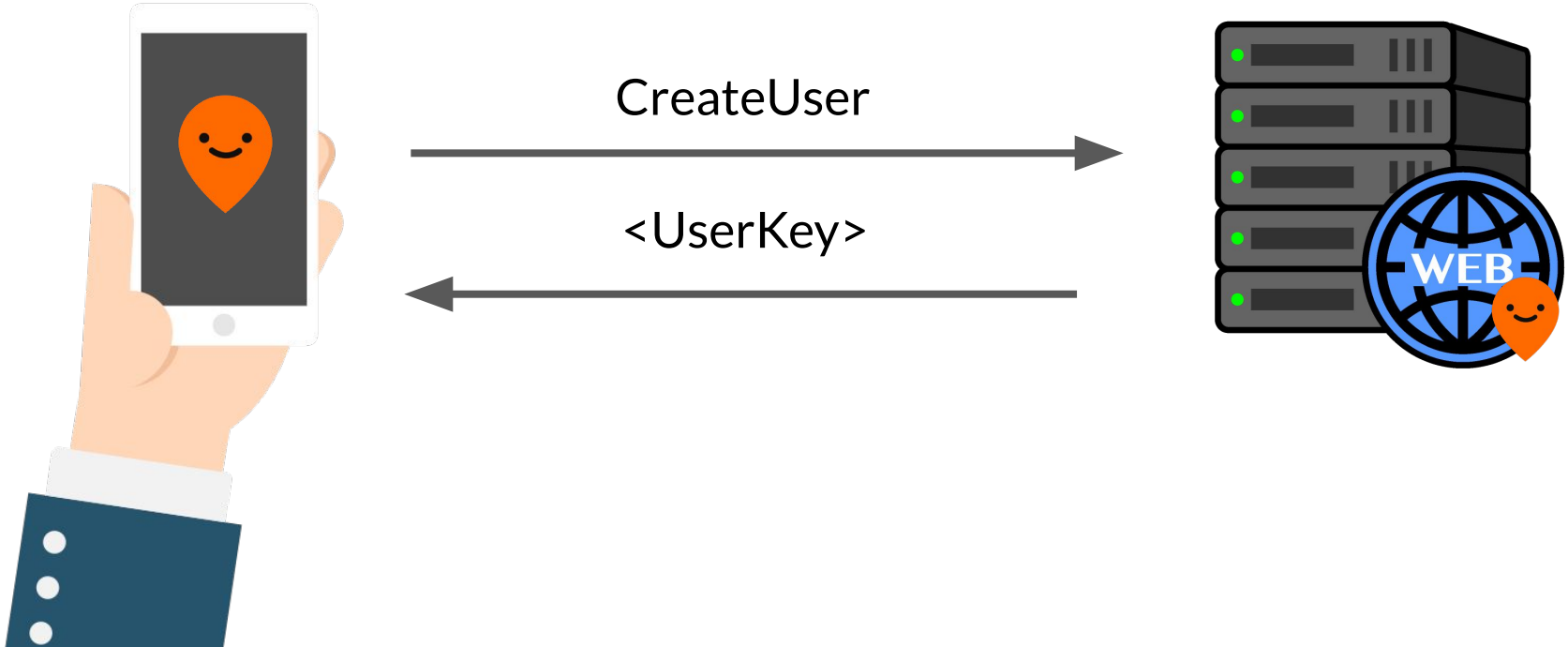
Enhancing Capabilities

Vulnerability #3

Delve Into The APIs



Reminder - The First API Request



Access Token



Moovit Servers

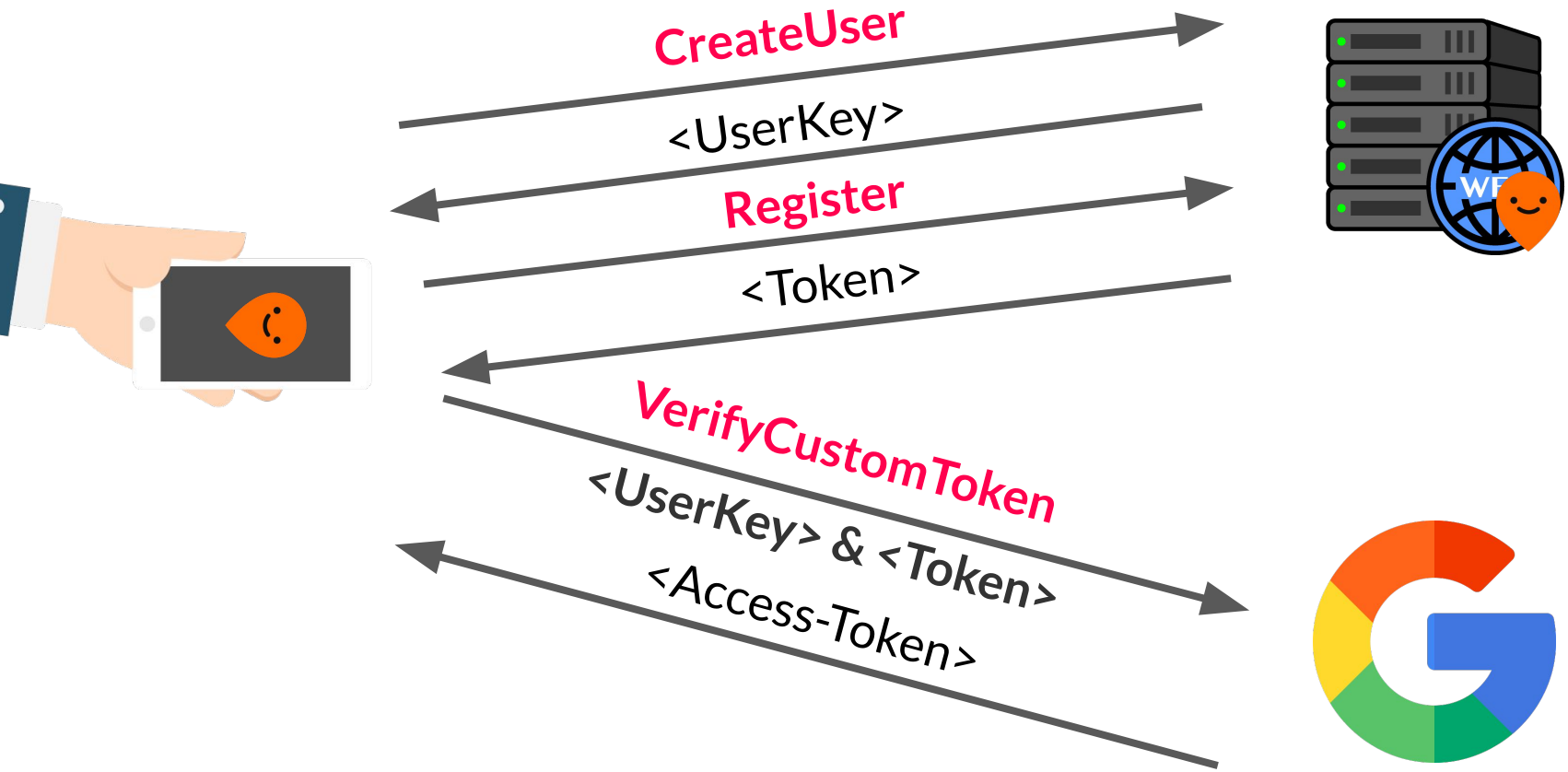
Affiliations



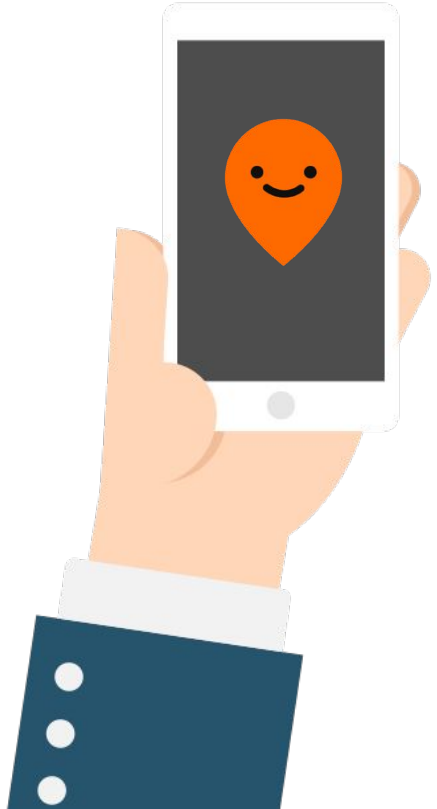
Account <Phone #>

- Credit Card
- PII
- <UserKey>
- <Access_Token>

Device Setup



Now, Everything Is Set





<AccessToken>



<UserKey>

The Problem





<UserKey>

JWT Access Token


```
eyJhbGciOiJSUzI1NiIsImtpZCI6IjU4NWI5MGI
1OWM2YjM2ZDNjOTBkZjBlOTEwNDQ1M2U2MmY4OD
dmNzciLCJ0eXAiOiJKV1QifQ.eyJpc3MiOiJodH
RwczovL3NlY3VyZXRva2VuLmdvb2dsZS5jb20vd
HJhbnptYXRlLmNvbTpnY21hbmRyb2lkIiwiYXVk
IjoidHJhbnptYXRlLmNvbTpnY21hbmRyb2lkIiw
iYXV0aF90aW1lIjoxNjY0NDM3Njk3LCJ1c2VyX2
lkIjoiRTRDNkVBQTIzNDg1MUQxMkUwNTMwMTAwM
DA3RjI5OEIiLCJzdWIiOiJFNEM2RUFBMjM0ODUx
RDEyRTA1MzAxMDAwMDdGMjk4QiIsImlhdCI6MTY
2NDQzNzY5NywiZXhwIjoxNjY0NDQxMjk3LCJmaX
JlYmFzZSI6eyJpZGVudGl0aWVzIjp7fSwic2lnb
l9pbl9wcm92aWRlciI6ImN1c3RvbSJ9fQ.XMBaw
0rqtnlOeegLMKCEcMbGb9gyJyd7Xj80gfoDHfyt
bLxe2yfU2Tf3nfbvVyPhlLNUuekVVRd-
JfGcDf9n9cenIPVYjAMy1Psf-k9Xh6U-
Nbt4hkFMKK3kZ7eN5ZPLMykTEO5_9pb1b3wwmhx
jo-qpLQdjqmLBvA6GvHND-
rWCy0RwzOp61D1KbukBTxxnt7WPLt9sve8t2OX0
R6R053t2SjPaJZZsNo87Abp24F8ISBolLlO2S4O
valUG-
CVgDTi7lDumcC6GdfIwKiaYG84ayo0So_4cU59Y
sfs3fBlf2w2jy0ZPBug-
FreOo4AODyKdrB2HQZP1Mm-TwSnZYA
```


HEADER: ALGORITHM & TOKEN TYPE


```
{
  "alg": "RS256",
  "kid": "585b90b59c6b36d3c90df0e9104453e62f887f77",
  "typ": "JWT"
}
```


PAYLOAD: DATA


```
{
  "iss":
"https://securetoken.google.com/tranzmate.com:gcmandroi
d",
  "aud": "tranzmate.com:gcmandroid",
  "auth_time": 1664437697,
  "user_id": "E4C6EAA234851D12E0530100007F298B",
  "sub": "E4C6EAA234851D12E0530100007F298B",
  "iat": 1664437697,
  "exp": 1664441297,
  "firebase": {
    "identities": {},
    "sign_in_provider": "custom"
  }
}
```

Can We Forge JWT?

E4C6F3B1EFF23008E0530100007FE981



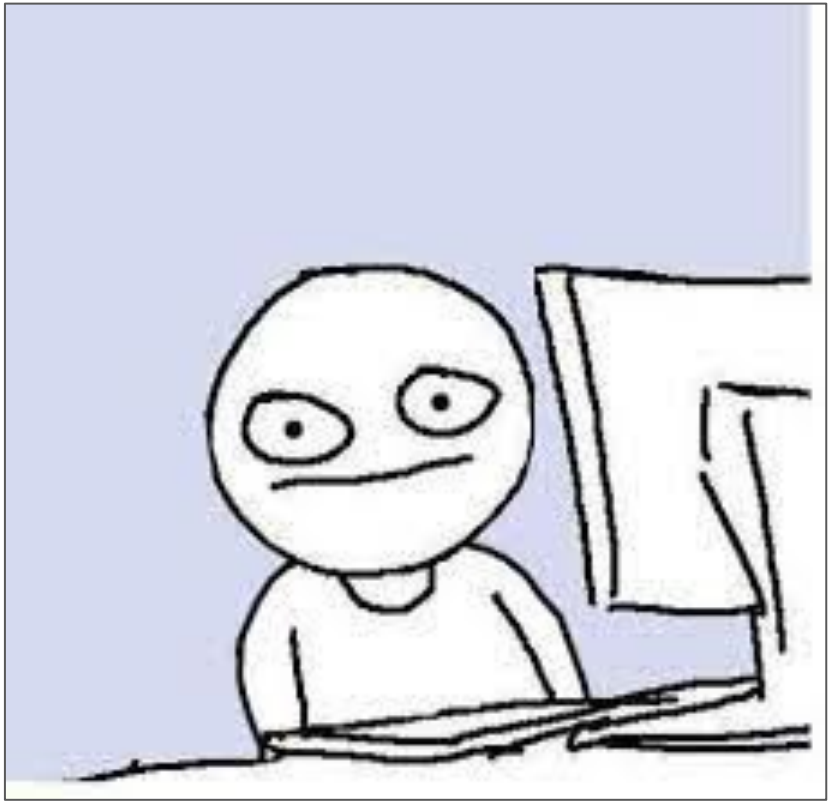
JWT Validation


```
eyJhbGciOiJSUzI1NiIsImtpZCI6IjU4NWI5MGI
1OWM2YjM2ZDNjOTBkZjBlOTEwNDQ1M2U2MmY4OD
dmNzciLCJ0eXAiOiJKV1QifQ.eyJpc3MiOiJodH
RwczovL3NlY3VyZXRva2VuLmdvb2dsZS5jb20vd
HJhbnptYXRlLmNvbTpnY21hbmRyb2lkIiwiYXVk
IjoidHJhbnptYXRlLmNvbTpnY21hbmRyb2lkIiw
iYXV0aF90aW11IjoxNjY0NDM3Njk3LCJ1c2VyX2
lkIjoiRTRDNkVBQTIzNDg1MUQxMkUwNTMwMTAwM
DA3RjI5OEIiLCJzdWIiOiJFNEM2RUFBMjM0ODUx
RDEyRTA1MzAxMDAwMDdGMjk4QiIsImlhdCI6MTY
2NDQzNzY5NywiZXhwIjoxNjY0NDQxMjk3LCJmaX
JlYmFzZSI6eyJpZGVudGl0aWVzIjp7fSwic2lnb
l9pbl9wcm92aWRlciI6ImN1c3RvbSJ9fQ.XMBaw
0rqtnlOeegLMKCEcMbGb9gyJyd7Xj80gfoDHfyt
bLxe2yfU2Tf3nfbvVyPhlLNUuekVVRd-
JfGcDf9n9cenIPVYjAMy1Psf-k9Xh6U-
Nbt4hkFMKK3kZ7eN5ZPLMykTEO5_9pb1b3wwmhx
jo-qpLQdjqmLBvA6GvHND-
rWCy0RwzOp61D1KbukBTxxnt7WPLt9sve8t2OX0
R6R053t2SjPaJZZsNo87Abp24F8ISBolL1O2S4O
valUG-
CVgDTi7lDumcC6GdfIwKiaYG84ayo0So_4cU59Y
sfs3fBlf2w2jy0ZPBug-
FreOo4AODyKdrB2HQZP1Mm-TwSnZYA
```

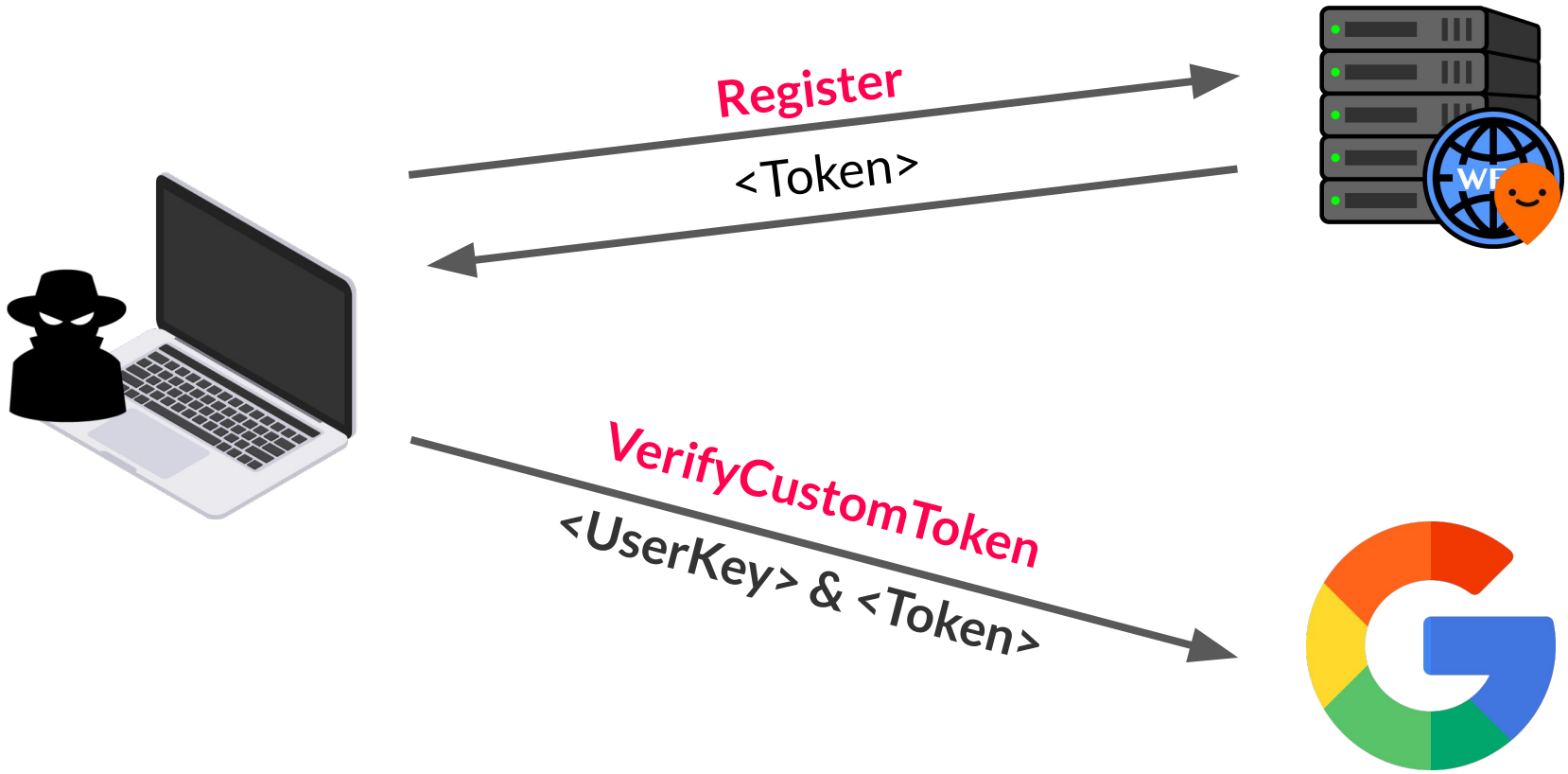

PAYLOAD: DATA


```
{
  "iss":
"https://securetoken.google.com/tranzmate.com:gcmandroi
d",
  "aud": "tranzmate.com:gcmandroid",
  "auth_time": 1664437697,
  "user_id": "E4C6EAA234851D12E0530100007F298B",
  "sub": "E4C6EAA234851D12E0530100007F298B",
  "iat": 1664437697,
  "exp": 1664441297,
  "firebase": {
    "identities": {},
    "sign_in_provider": "custom"
  }
}
```

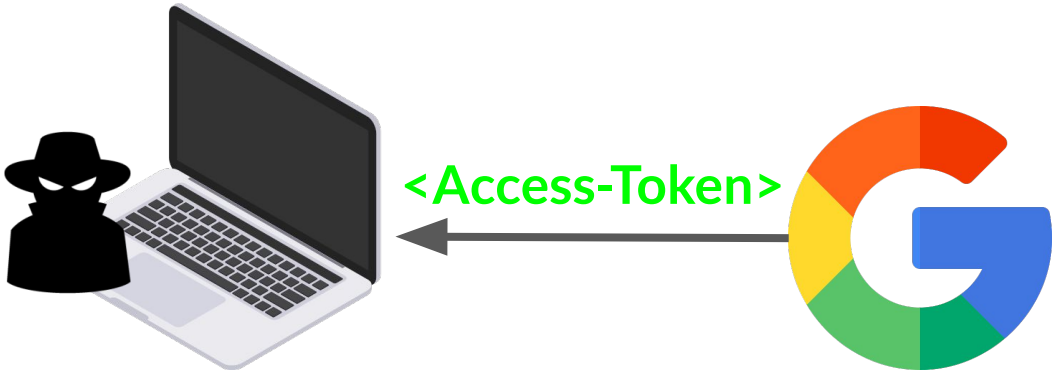
Well.. Now What?



Getting Access Token



Elegant Simplicity





Impersonate Accounts





<AccessToken>



<UserKey>

Pros & Cons



- Targeted Attack
- Widely Spreaded



- ~~Takes time~~
- ~~Disconnect the account~~
- ~~Requires account phone number~~

Impersonate Existing Accounts

```
1   [+][Found Profile] --> E78E43310A806DD9E0530100007F6E7B -> +15
2   [+][Found Profile] --> E78F48144E6907F6E0530100007F9C84 -> +48
3   [+][Found Profile] --> E78F56E76ED816FEE0530100007FF967 -> +13
4   [+][Found Profile] --> E78F685DBB0B2801E0530100007F499E -> +31
5   [+][Found Profile] --> E78F6C75EA3F2B4AE0530100007FF770 -> +17
6   [+][Found Profile] --> E78F6AFBF0A629FFE0530100007F76D3 -> +17
7   [+][Found Profile] --> E78F785DBBE137F6E0530100007FFAA4 -> +16
8   [+][Found Profile] --> E78F7737FD0D362DE0530100007FA69B -> +13
9   [+][Found Profile] --> E78FF776D7B93E93E0530100007F9BBF -> +33
10  [+][Found Profile] --> E7900E50E4B456ECE0530100007FAD43 -> +15
11  [+][Found Profile] --> E7900035516346D0E0530100007F7250 -> +15
12  [+][Found Profile] --> E79029DF624C7503E0530100007FC2D8 -> +12
13  [+][Found Profile] --> E7903443DB317EABE0530100007F58C3 -> +15
14  [+][Found Profile] --> E7903443DB3E7EABE0530100007F58C3 -> +15
15  [+][Found Profile] --> E7902662D81A6F08E0530100007F02A1 -> +12
16  [+][Found Profile] --> E79044E65D490E6CE0530100007F7B91 -> +16
17  [+][Found Profile] --> E7901BFE1C5F6151E0530100007FD8C3 -> +17
18  [+][Found Profile] --> E79044E65D710E6CE0530100007F7B91 -> +16
19  [+][Found Profile] --> E7904119814B0D31E0530100007FEBF0 -> +31
20  [+][Found Profile] --> E7904A5A6AD5151AE0530100007FA616 -> +16
21  [+][Found Profile] --> E7903F298C510B5EE0530100007F70B0 -> +44
22  [+][Found Profile] --> E7906E574A403DBAE0530100007F39BE -> +13
23  [+][Found Profile] --> E7906E574A413DBAE0530100007F39BE -> +12
24  [+][Found Profile] --> E79073533AA943EEE0530100007FFEFD -> +19
25  [+][Found Profile] --> E79074EF650945AAE0530100007FA733 -> +31
26  [+][Found Profile] --> E79073533ADB43EEE0530100007FFEFD -> +32
```

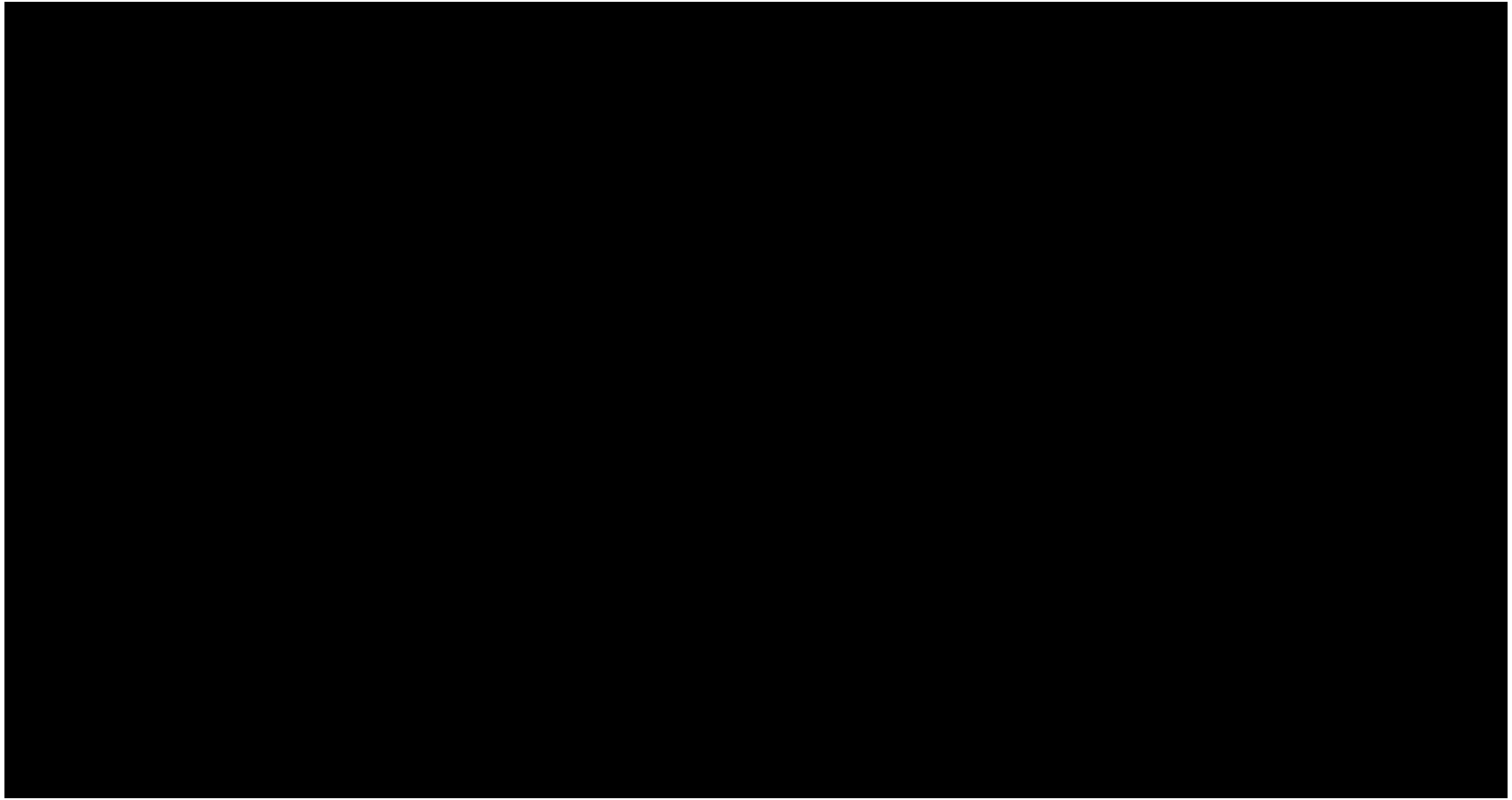
PII Database Of The Caught Accounts

	user_key	firstname	lastname	email	bday	id	phone	address
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	E4C7A1C3F8A32CDBE0530100007F95B2	תמימה		gmail.com	NULL		+9725	NULL
2	E4C787660FE86DF8E0530100007F913F	תומר		@gmail.com	NULL		+9725	NULL
3	E4C7EAC0A80850E8E0530100007FE3DC	תהילה		gmail.com	NULL		+9725	NULL
4	E4C7310C5E87342DE0530100007FCAC9	שרון		gmail.com	NULL		+9725	NULL
5	E4C77BA1C46954FFE0530100007F79EA	שרון		.com	NULL		+9725	NULL
6	E4C7E7CD39A34AF0E0530100007F3928	שירה		2@gmail.com	NULL		+9725	NULL
7	E4C784BA511E69DCE0530100007F32FF	שושנה		mail.com	NULL		+9725	NULL
8	E4C7EAC0A7CD50E8E0530100007FE3DC	קימ			NULL		+9725	NULL
9	E4C735E9204E401EE0530100007F4D93	קטרינה		@gmail.com	NULL		+9725	NULL
10	E4C7CD24CAB70EFCE0530100007FFB35	קובי		walla.com	NULL		+9725	NULL
11	E4C735E92010401EE0530100007F4D93	פזית		@gmail.com	NULL		+9725	NULL
12	E4C735E92065401EE0530100007F4D93	עמית		gmail.com	NULL		+9725	NULL
13	E4C7AF6B18BB4916E0530100007F8807	עמית		mail.com	NULL		+9725	NULL
14	E4C710A4B53A6CE1E0530100007FB373	עטרה		gmail.com	NULL		+9725	NULL

Fun Fact


Server Developer at Moovit
E4C73
F4...
g
@moovit.com
if(you.getCodeSkill() >= Skills.NINJA){
Moovit.hire(you);
}else{
throw new BeANinjaException(
"Refer a Friend");
}
moovit
Friends, plea
code:
16 • 1 Comment

Bonus Demo



Takeaways

- Increase awareness to security measures
- A researcher’s perspective

Vendor Response

We would like to thank SafeBreach for their collaboration on this issue. Moovit has always been committed to protecting user data and takes all reports of security threats seriously. The vulnerabilities were fixed and no customer action is required. As for the QR code, Moovit-Pango follows Israel's MOT rules and guidelines for implementation, and the MOT is aware of the issue.



Github



https://github.com/SafeBreach-Labs/moovit_api_scripts/tree/main

Credits



Shmuel Cohen

Security Researcher @ SafeBreach Labs



Thank You!

Omer Attias
omer.attias@safebreach.com



Q&A