



Analysis of Privacy and Security Exposure in Mobile Dating Applications

Constantinos Patsakis, **Athanasios Zigomitros** and Agusti Solanas

International Conference on Mobile, Secure and Programmable Networking
(MSPN'2015)

June 16, 2015

Dating applications

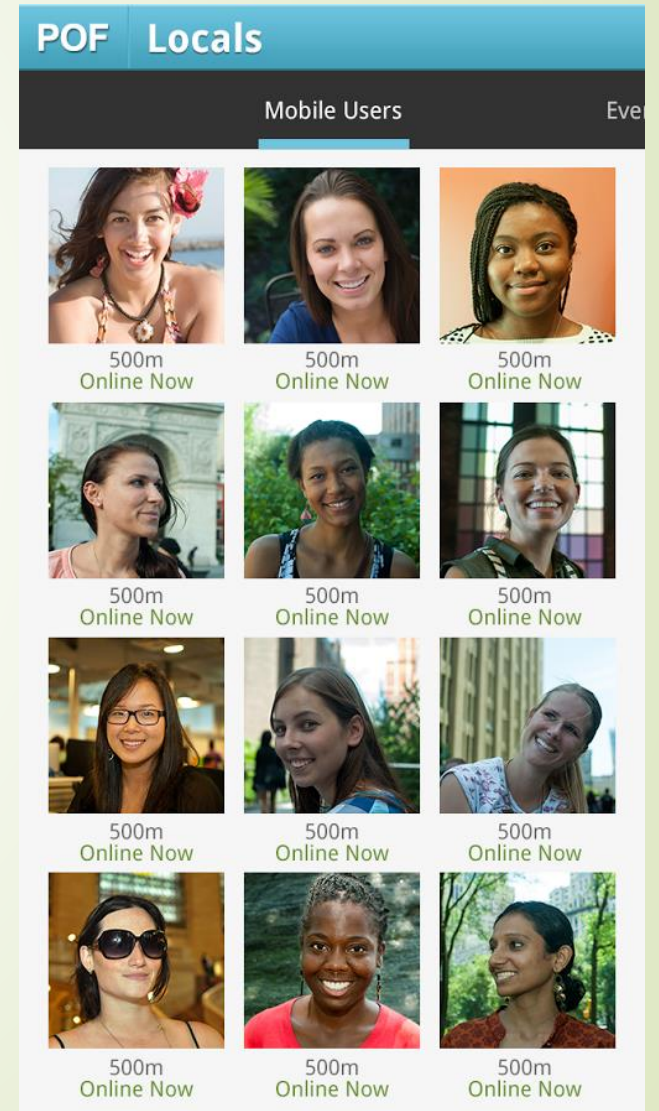
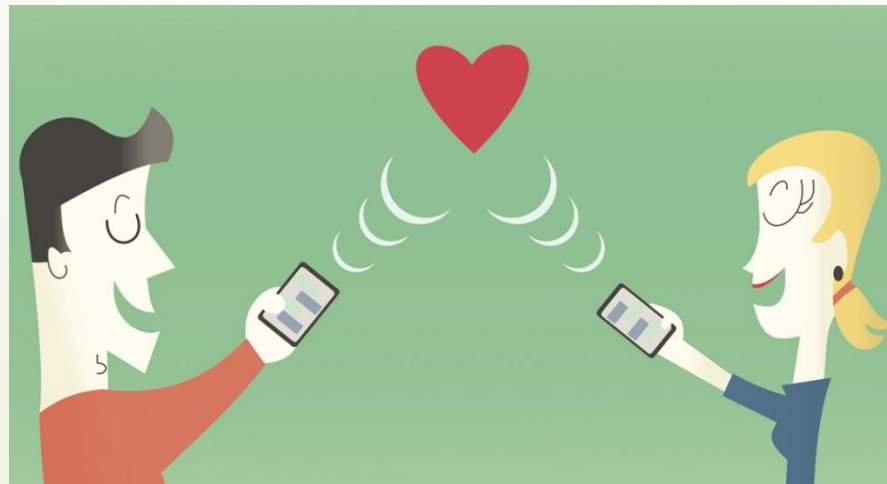
- ▶ Dating applications are not novel, they can be found on the Internet in different forms since the early beginnings.
- ▶ Only recently did they become **location-aware**.



Why they use location-awareness?



- The location awareness of these applications create "hope" for lonely people (Their other half might be only 500m away!)
- People feel that the other users are more "real" and not just dummy profiles. They can see them "moving".





















Research questions

- ▶ How accurate are these distances?
- ▶ Do these applications allow location-based attacks?
- ▶ Could we locate people from the reported distances? If so, with what accuracy?
- ▶ What kind of data are they sending?
- ▶ How do they send this data?
- ▶ What others can infer?



Numbers...

Application	Version	Installations	Code	Application	Version	Installations	Code
ChatOn	3.0.2	100m-500m		Singles around me	3.3.1	500K-1m	
Grindr	2.0.24	5m-10m		SKOUT	4.4.2	10m-50m	
Hornet	2.0.14	1m-5m		Tagged	7.3.0	10m-50m	
I-Am	3.2	500K-1m		Tango	5.8	100m-500m	
LOVOO	2.5.6	10m-50m		Tinder	4.0.9	10m-50m	
MeetMe	9.2.0	10m-50m		Tingle	1.12	-	
MoMo	5.4	1m-5m		Waplog	3.0.3	5m-10m	
POF	2.40	10m-50m		WeChat	6.0.1	100m-500m	
SayHi	3.6	10m-50m		Zoosk	8.6.21	10m-50m	

Possible Impact

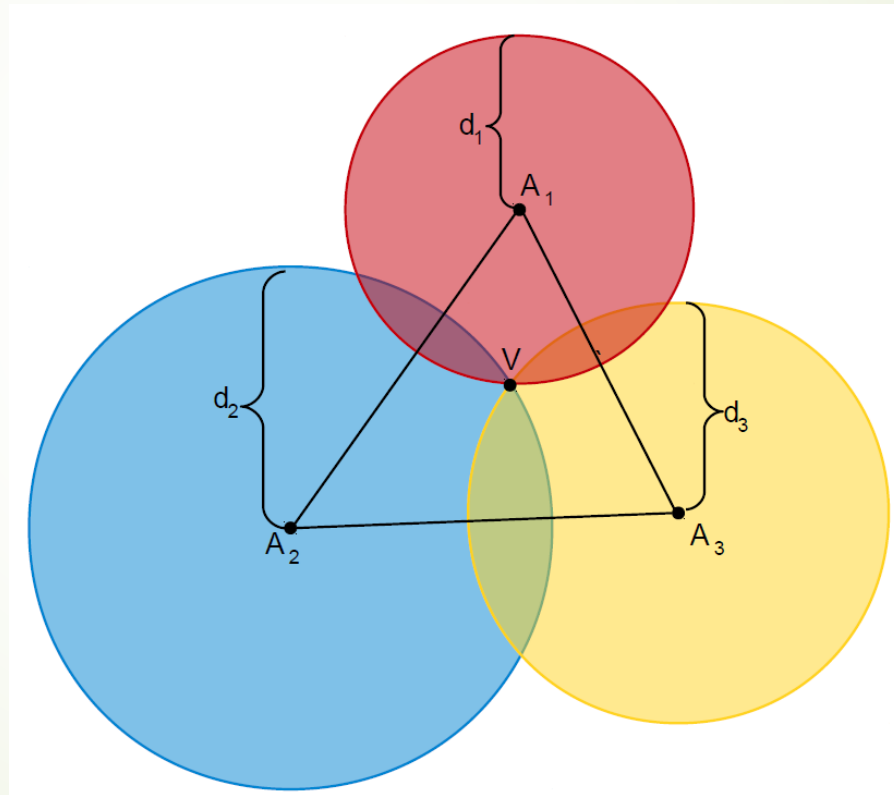
- ▶ One should understand that these applications are used by millions of users world wide. Furthermore, the dating/sexual nature of these applications is likely to attract many perverts.
- ▶ Trivial scenario: Assume the case of a cyber-stalker...

Stalking is when two people go on a long romantic walk together, but only one of them knows about it. By the way, you're out of milk.

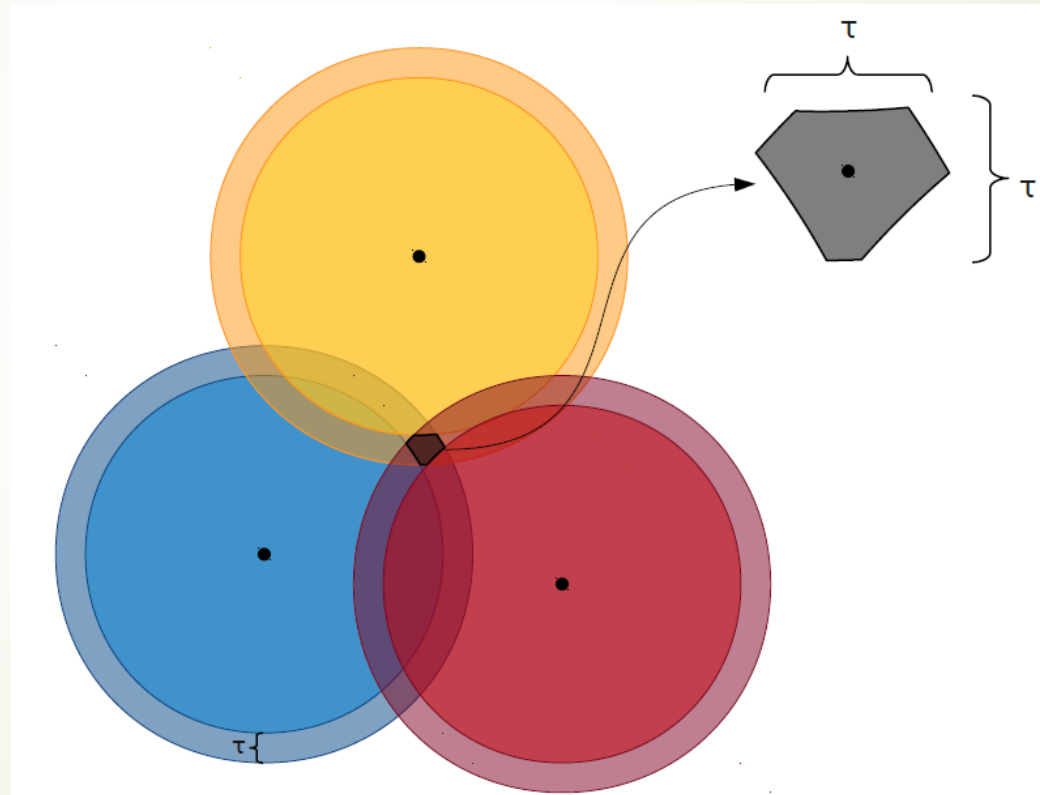


someecards
user card

Trilateration attack



Trilateration attack



Before the attack

- ▶ Bob has to find how accurate the distances are. To do this he uses two accounts controlled by him and records the reported distances to find possible patterns.
- ▶ We created two accounts for each app, one for the attacker and one for the victim. By setting a fake location for both of these two users, we were able to know simultaneously the **reported** and their **actual** distance.

I'm not a "stalker". I prefer the term
Social Media Analyst.



ROTTENCARDS

Results

The user can be traced within max 5m in POF, SKOUT, WeChat, MoMo.

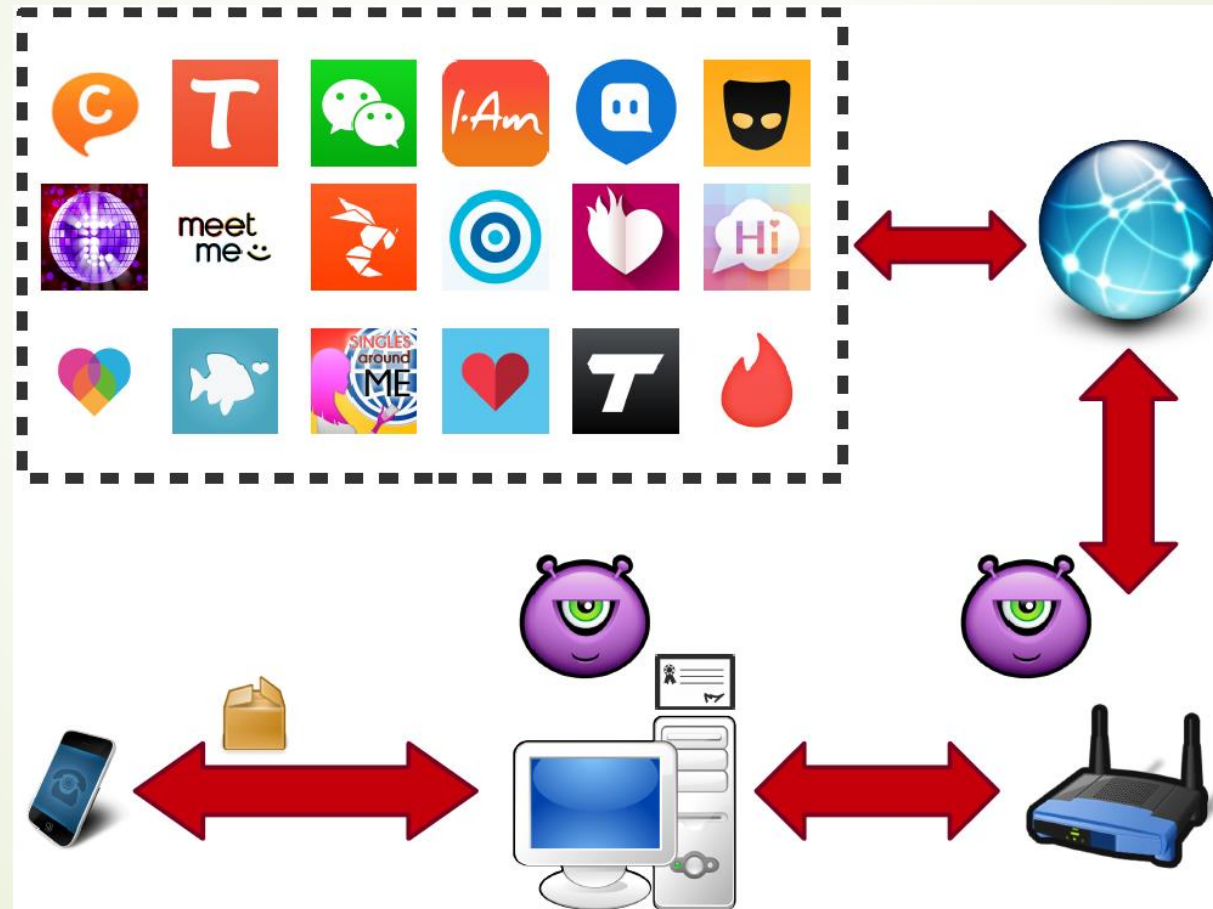




Let's dive deeper...

- ▶ So can we find more juicy information?
- ▶ Let's use a proxy to grab the packages...

Setup





Singles Around Me

Sends the exact location of other users in the packet.

Photos are sent over HTTP with some of them being dynamic links and others being static. However, the received packet contains an additional field: users' emails.

Exposes users as URLs contain the IDs that a user has been watching.

```
1 {
2   "username": "s-----eam",
3   "email": "d-----96@yahoo.com",
4   "gender": 2,
5   "interestedIn": 1,
6   "country": "United Kingdom",
7   "region": "London, City of",
8   "city": "",
9   "gps": [38.-----2,23.8-----5],
10  "age": 39,
11  "photo": "http://www.singlesaroundme.com/images/cache/1/
12          photoface_11-----_--5_--5.jpg",
13  "photos": [],
14  "birthYear": 1974,
15  "birthMonth": --,
16  "birthDay": -,
17  "lastOnline": "2014-10-06 03:28:07 PM",
18  "profileAnswers": {"1": "5' 7" - 170cm",
19  "3": "prefer not to say",
20  "21": "Married", "30": "straight", "25": "brown", "31": "blonde", "2
21  6": "white", "28": "none",
22  "29": "Sagittarius", "38": ["dating", "serious relationship", "
23  friendship"],
24  "37": "Greek", "36": ["English"], "32": "socially / occasionally"
25  },
26  "34": "socially/occasionally", "35": "quite fit", "40": "
27  Christian - Other",
28  "41": "University graduate", "42": "yes living with me", "43": "
29  yes"},
30  "privacySettings": {"gps": 0, "profile": 0}
31 }
```

ChatOn



- Uses HTTPS for **all** its traffic. Let's look at the URL of the API it sends model, operating system version, IMEI, IMSI, telephone number, user ID and app version. The app sends the telephone numbers of all user's contacts to Samsung, and the received packets contain additional information like contacts' birthday and emails. The RESTful API that is used exposes users actions and the profiles that they visit.

```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
<return>
  <timestamp>1417080250</timestamp>
  <buddy name="Dimitris Des[REDACTED]" devicetype="web" orgnums="6948[REDACTED]"
    msisdns="306948[REDACTED]|1000000002294644710" einfo="|"
    showphonenumber="true" isblind="false" orgname="Δημητρης Δεσπο[REDACTED]"
    imgstatus="3"
    sainfo="50cbd35f921cb507f73753e6ba1db21bcf618895d2b91ec4e30574ea33d16e
    samsungemail="" email="" birthday="0000-12-31" statusupdatetime="1387642493"
    status="Hi dude" group="">1000000002294644710</buddy>
  <buddy name="Πάρης Σπυ[REDACTED]" devicetype="web" orgnums="69722[REDACTED]"
    msisdns="100000000526707[REDACTED]|3069721[REDACTED]" einfo="|"
    showphonenumber="true" isblind="false" orgname="Πάρης Σπυ[REDACTED]" imgstatus="3"
    sainfo="b7b9730dfdbbdc324ac61b53758548820d2bd47dfc5adcbab5922e3589cf2c
    samsungemail="spy[REDACTED]_paris@yahoo.gr" email="" birthday=""
    statusupdatetime="1378415646" status=""
    group="">1000000005267073910</buddy>
```

Grindr



- ▶ The API that is called from the mobile app might allow eavesdroppers to extract the actual user location and his/her application ID from the sniffed URL. Additionally, the URL discloses the user's activity and his/her device OS. Moreover, exchanged packets contain the distance only for users that consented and the application might display the relative user distance. However, the messages contain the actual users' location.



Hornet

- ▶ Hornet encrypts its traffic using HTTPS, but sends the distance with 10m accuracy. Photos are static links sent over HTTP. The API calls allow an adversary to deduce user activity, e.g. chatting, browsing profiles, etc simply by capturing the URLs that users request.



I.Am

- Authentication: HTTPS, everything else HTTP! User's URL contains his location... Exact distance is sent to other users in the packet along with their birthday – in the app displays only the age.



LOVOO

- All traffic sent over HTTPS, apart from photos (dynamic links). The actual distance between users is sent with a rounding of 100m, along with their relative (x; y) coordinates! The API calls expose in the URLs that are requested the user location, his/her preferences and his/her overall activity.



MeetMe

- ▶ MeetMe uses mixed HTTP/HTTPS traffic. The user location and his/her preferences are visible in the URL. The actual location of the user is included in the packet if other users are nearby, otherwise their distance is given in km. Photos are shared over HTTP, and user commands can be seen in the URL.

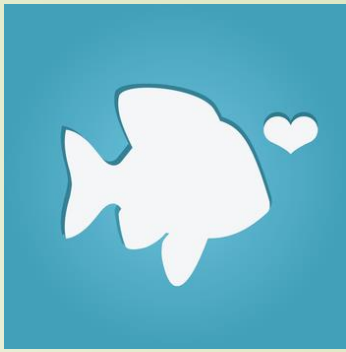
MoMo

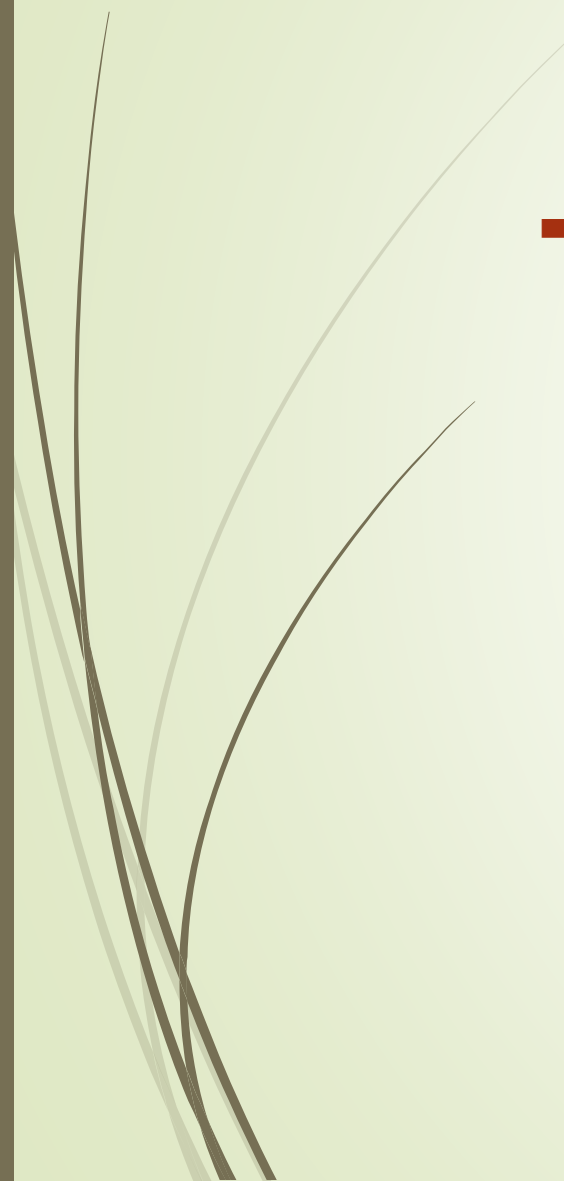


- HTTPS to exchange messages with the server, it does not hide users' location. More precisely, the packets that are received from the app contain fine-grained distance information from other users. URLs contain the visited profiles as well as the current user ID and photos are sent over HTTP by using static links.



PoF



- It uses HTTP but all messages are encrypted, which most likely means that the app contains a local key to decrypt the contents. On the bad side, photos are sent over HTTP as static links.
- 
- Several thin, curved lines in shades of brown and grey originate from the left side of the slide and extend downwards and outwards.

SayHi



- It uses Facebook for its authentication and then sends everything in clear text. Packets include the fine-grained location of other users and their activity can be seen in the requested URLs. An eavesdropper could also intercept user conversations. Photos are sent over HTTP using static links...

SKOUT



- SKOUT uses HTTPS only for its authentication but the rest of the traffic is sent over HTTP. It sends the exact distance to other users in the packets and then obfuscates it in the frontend of the app. The API of SKOUT exposes the user activity because it shows whether the user is typing a message, visiting a profile, etc.



Tagged

All traffic is sent over HTTP



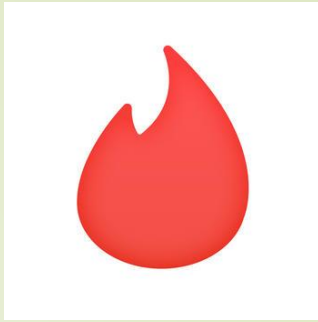


Tango

Tango transmits over HTTP and all messages can be intercepted. The API exposes user's activity as well as his/her phone number and preferences.

Several thin, dark, curved lines originate from the left side of the slide and sweep upwards and to the right, creating a decorative, organic feel.

Tinder



- Tinder uses HTTPS traffic but the messages contain the Facebook ID of the users. Packets include the actual distance to other users. Photos are sent over HTTP as static links.



Tingle



Messages contain other users' emails, a device tag. They display the actual location of the user in the URL and contain users' queries. Photos are sent over HTTP as static links.



Waplog



Waplog transmits over HTTP, exposes emails of other users.



WeChat



- WeChat uses HTTP for all its traffic and sends all information in an encrypted file...

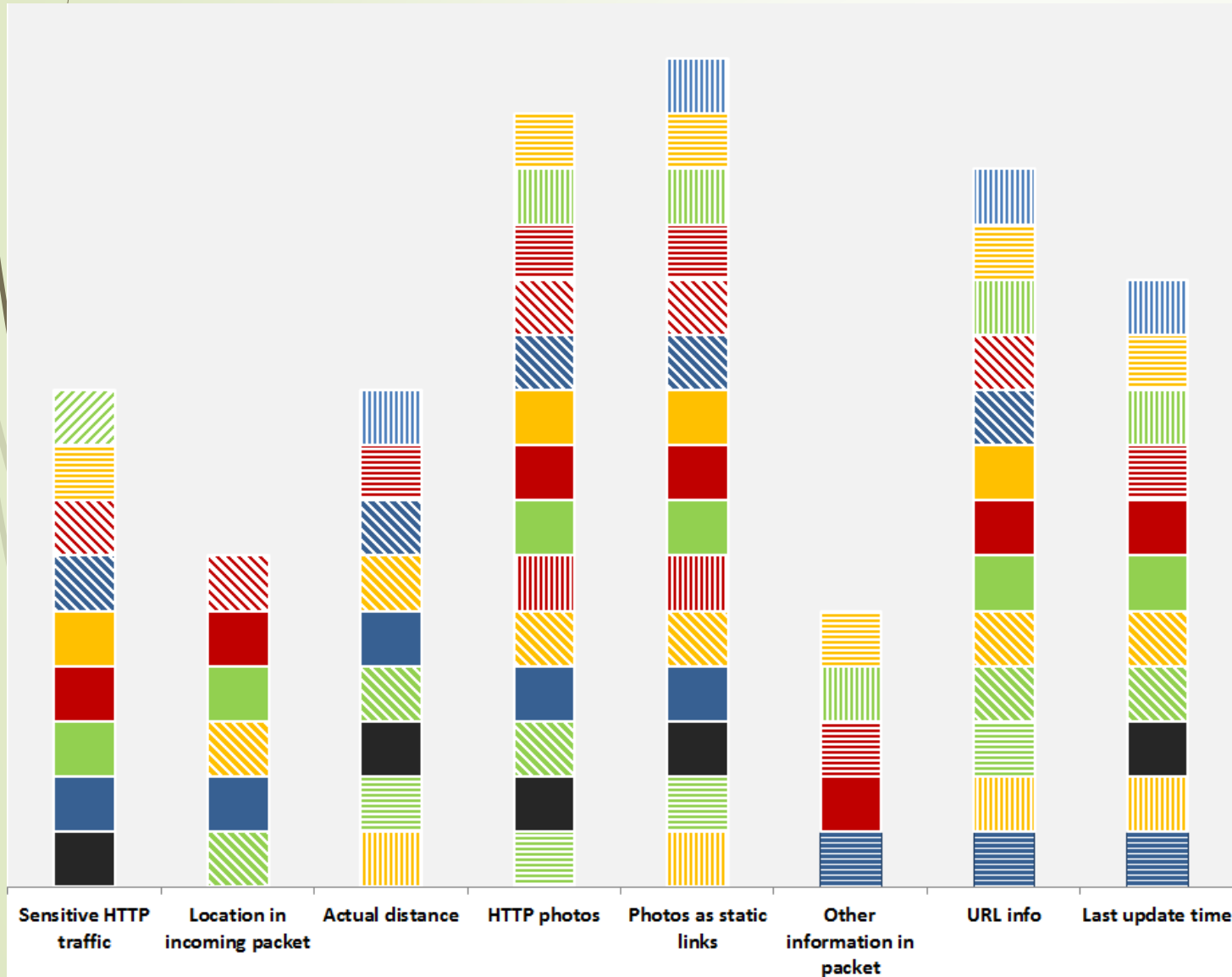


Zoosk



- It uses HTTPS for its traffic. The requested URLs expose the phone model and its OS as well as the user activity. Finally, photos are sent as static links over HTTPS.

To summarize

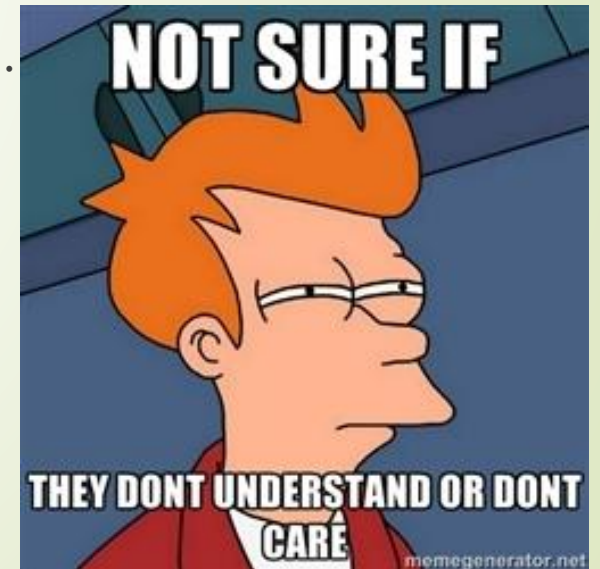


Application	URL
ChatOn	https://gld1.samsungchaton.com/prov4?imei=-----\&imsi=-----\&model=iPhone4\&clientversion=3.0.2\&platform=iPhone\%20S\&osversion=7.0.4
	https://prov4?imei=-----\&countrycallingcode=30\&phonenumber=-----\&imsi=-----\&model=iPhone4\&clientversion=3.0.2\&platform=iPhone\%20S\&osversion=7.0.4
Grindr	https://primus.grindr.com/2.0/broadcastMessages?applicationVersion=2.0.24\&hasXtra=0\&lat=53.-----\&lon=6.2-----\&platformName=iOS\&platformVersion=7.0.4\&profileId=36850131
MoMo	https://api.immomo.com/api/profile/1121----?fr=98----
SKOUT	http://i22.skout.com/services/ServerService/GCUserTyping

Disclosing the vulnerabilities

Let's contact all of them to notify them before disclosing anything...

- ▶ Only 5 companies responded!
- ▶ 1 company said we know the problem (2 years ago), hasn't made anything to fix it
- ▶ 1 of them responded we are stopping the product so...
- ▶ 2 apps have been withdrawn.





Conclusions

- ▶ Vulnerable to simple sniffing attack which can reveal very sensitive personal information such as sexual orientation, preferences, e-mails, degree of interaction between users etc.
- ▶ GPS coordinates or actual distances that are in URL or in the packets exposes user's location.
- ▶ The users of the apps can be victims of user profiling, blackmailing, stalking, defamation, and even identity theft.
- ▶ Most of the detected vulnerabilities have very simple solutions that do not require much effort to fix.

Thanks for your time and your attention

Any Questions ?

