Detecting Privacy Leaks in the RATP App: how we proceeded and what we found

Jagdish Prasad Achara [Speaker],
James-Douglass Lefruit, Vincent Roca, Claude Castelluccia

INRIA Rhone-Alpes

November 15, 2013

Outline

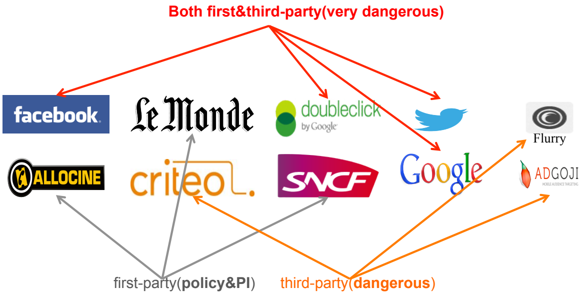
1. Introduction
2. RATP iOS App
3. RATP Android App
4. Conclusions
5. References

Outline

1. Introduction
2. RATP iOS App
3. RATP Android App
4. Conclusions
5. References

A large number of actors present on Smartph

- Due to revolutional arrival of AppStore model of App distribution
- These actors could be categorized as follows:
  - First-party : whose services are used by the user explicitly (App owners, OS provider, Cellular (GSM/CDMA) service providers etc.)
  - Second-party : the user himself
  - Third-party : to whom the user doesn't directly interact with (Advertisers, Analytics companies, performance monitors, crash reporters, push senders etc.)


Both first&third-party(very dangerous)

first-party(policy&PI)

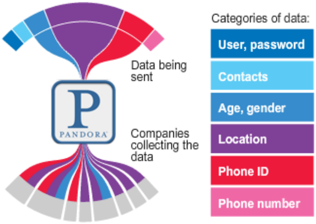
third-party(dangerous)

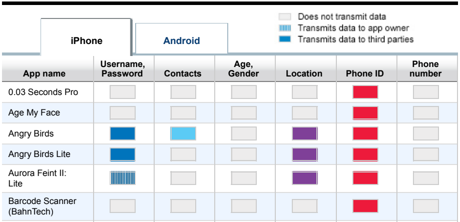
3

Difficult to trust all these actors

1. Various scandals in the past
   - e.g. Twitter and Path uploading users' contacts to their servers [4], [8]

2. WSJ: What They Know - Mobile [9]



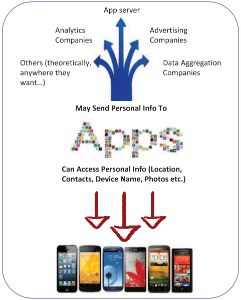


□ Does not transmit data
▥ Transmits data to app owner
■ Transmits data to third parties

App name	Username, Password	Contacts	Age, Gender	Location	Phone ID	Phone number
0.03 Seconds Pro	□	□	□	□	■	□
Age My Face	□	□	□	□	■	□
Angry Birds	■	■	□	■	■	□
Angry Birds Lite	■	□	□	■	■	□
Aurora Feint II: Lite	▥	□	□	■	■	□
Barcode Scanner (BahnTech)	□	□	□	□	■	□

More opportunities for personal information (PI) leakage on Smartphones

1. **Not limited to web browsers** as is the case mostly in desktops/laptops
2. App code (coming from different parties) runs on the device
3. They **contain a lot of info about user interests and behaviors**
   - Sensors (GPS, Camera) and Comm. chips (WiFi, GSM/CDMA) generate PI
   - At the center of our cyber activities, and very personal (not shared usually)
   - Almost all-time Internet connectivity and barely turned-off



App server

Analytics Companies

Advertising Companies

Others (theoretically, anywhere they want...)

Data Aggregation Companies

May Send Personal Info To

Apps

Can Access Personal Info (Location, Contacts, Device Name, Photos etc.)

This leads to **detailed and accurate user profiling**

Smarthphones are well-suited to Marketers

- A direct consequence is **the large presence of online advertisers/trackers**

admob iAd doubleclick by Google Flurry criteo

and many others...

There is a clear need for **"tracking the trackers"**

Case of RATP

RATP: French public company that is managing the Paris subway (metro)

- It provides very useful App for both Android and iOS helping users to easily navigate in the city.
- We found RATP App leaking user personal information (PI) in total contradiction to their In-App privacy policy.

- This talk details/discusses
  - **the Methodology** (a combination of static and dynamic analysis techniques) we used **to analyze both Android and iOS Apps of RATP**.
  - **our Findings w.r.t. PI leakage by RATP Apps**: what user PI is leaked and to which servers...
  - **the responsibilities of various actors** (OS providers and App developers), in general, to stop the practice of user PI leakage.

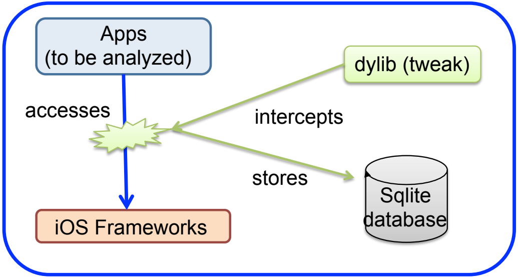
Outline

1. Introduction
2. RATP iOS App
3. RATP Android App
4. Conclusions
5. References

Instrumented version of iOS

To detect private data leakage

- Code in a dynamic library that is loaded in Apps to be analyzed at runtime[1]
  - Using Objective-C runtime
  - Replacing C/C++ functions at assembly level

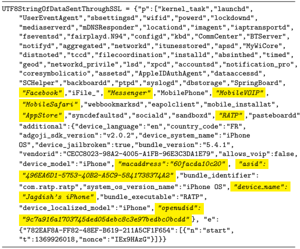


[1] MobileSubstrate [2] and Theos [7] simplify this task!

Privacy Leaks to Adgoji

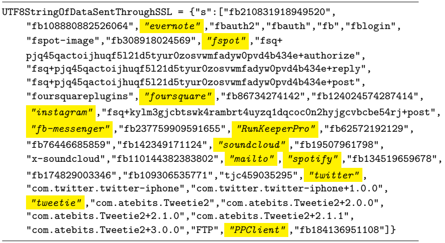
Adgoji: A mobile audience targetting company

Listing 1.1. Data sent through SSL by iOS App of RATP (Instance 1)



```
UTF8StringOfDataSentThroughSSL = {"p":["kernel_task","launchd",
    "UserEventAgent","sbsettingsd","wifid","powerd","lockdownd",
    "mediaserverd","mDNSResponder","locationd","imagent","iaptransportd",
    "fseventsd","fairplayd.N94","configd","kbd","CommCenter","BTServer",
    "notifyd","aggregated","networkd","itunesstored","apsd","MyWiCore",
    "distnoted","tccd","filecoordination","installd","absinthed","timed",
    "geod","networkd_privile","lsd","xpcd","accountsd","notification_pro",
    "coresymbolicatio","assetsd","AppleIDAuthAgent","dataaccessd",
    "SCHelper","backboardd","ptpd","syslogd","dbstorage","SpringBoard",
    "Facebook","iFile_","Messenger","MobilePhone","MobileVOIP",
    "MobileSafari","webbookmarksd","eapolclient","mobile_installat",
    "AppStore","syncdefaultsd","sociald","sandboxd","RATP","pasteboardd"],
    "additional":{"device_language":"en","country_code":"FR",
    "adgoji_sdk_version":"v2.0.2","device_system_name":"iPhone
    OS","device_jailbroken":true,"bundle_version":"5.4.1",
    "vendorid":"CECC8023-98A2-4005-A1FB-96E3C3DA1E79","allows_voip":false,
    "device_model":"iPhone","macaddress":"60facda10c20", "asid":
    "496EA6D1-5753-40B2-A5C9-5841738374A2","bundle_identifier":
    "com.ratp.ratp","system_os_version_name":"iPhone OS","device_name":
    "Jagdish's iPhone","bundle_executable":"RATP",
    "device_localized_model":"iPhone","openudid":
    "9c7a916a1703745ded05debc8c3e97bedbc0bcdd"}, "e":
    {"782EAF8A-FF82-48EF-B619-211A5CF1F654":[{"n":"start",
    "t":1369926018,"nonce":"IEx9HAzG"}]}}
```

Listing 1.2. Data sent through SSL by iOS App of RATP (Instance 2)



```
UTF8StringOfDataSentThroughSSL = {"s":["fb210831918949520",
    "fb108880882526064","evernote","fbauth2","fbauth","fb","fblogin",
    "fspot-image","fb308918024569","fspot","fsq+
    pjq45qactoijhuqf5l21d5tyur0zosvwmfadyw0pvd4b434e+authorize",
    "fsq+pjq45qactoijhuqf5l21d5tyur0zosvwmfadyw0pvd4b434e+reply",
    "fsq+pjq45qactoijhuqf5l21d5tyur0zosvwmfadyw0pvd4b434e+post",
    "foursquareplugins","foursquare","fb86734274142","fb124024574287414",
    "instagram","fsq+kylm3gjcbtswk4rambrt4uyzq1dqcoc0n2hyjgcvbcbe54rj+post",
    "fb-messenger","fb237759909591655","RunKeeperPro","fb62572192129",
    "fb76446685859","fb142349171124","soundcloud","fb19507961798",
    "x-soundcloud","fb110144382383802","mailto","spotify","fb134519659678",
    "fb174829003346","fb109306535771","tjc459035295","twitter",
    "com.twitter.twitter-iphone","com.twitter.twitter-iphone+1.0.0",
    "tweetie","com.atebits.Tweetie2","com.atebits.Tweetie2+2.0.0",
    "com.atebits.Tweetie2+2.1.0","com.atebits.Tweetie2+2.1.1",
    "com.atebits.Tweetie2+3.0.0","FTP","PPClient","fb184136951108"]}
```

The user PI sent is

- WiFi MAC Address
- List of currently running processes
- Device Name
- OpenUDID
- Advertising ID
- List of URLSchemes availabe on the device (to know if corresponding Apps are installed)

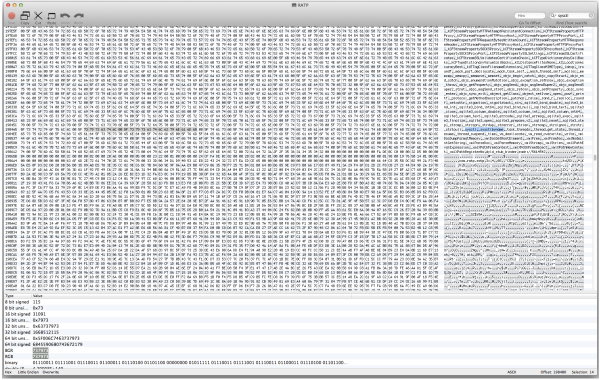
Adgoji: how to know Apps installed on the device

It is very useful info to infer the user interests and behaviour.

- No API provided by iOS Frameworks to do so...

But techniques exist to know a subset of Apps installed (if not all!)

- Use of 1) sysctl function (in libc) and 2) URLScheme class [1].



sysctl

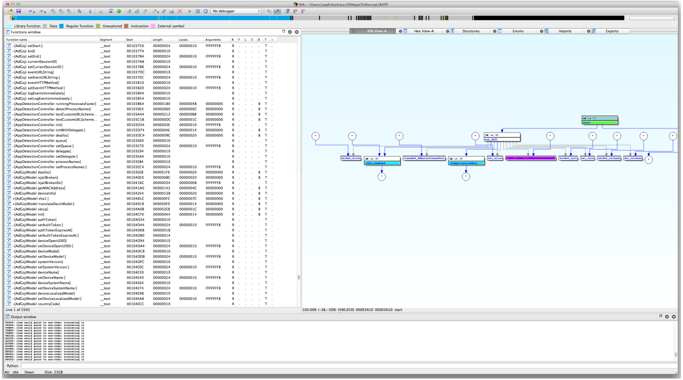
Type	Value
8 bit signed	115
8 bit unsi...	0x73
16 bit signed	31091
16 bit uns...	0x7973
32 bit uns...	0x63737973
32 bit signed	1668512115
64 bit uns...	0x5F006C7463737973
64 bit signed	6845590680743672179
BGR	737973
RGB	737973
binary	01110011 01111001 01110011 01100011 01110100 01101100 00000000 01011111 01110011 01111001 01110011 01100011 01110100 01101100...

Hex Little Endian Overwrite ASCII Offset: 1984B0 Selection: 14

Presence of "sysctl" String in decrypted App binary confirms its use in the code written by the App developer

Adgoji: confirmation of its presence in the App (1)

RATP iOS App binary opened in IDA after decryption



Function name	Segment	Start	Length	Locals	Arguments	R	F	L	S	B	T	=
-[AdGoji setStart:]	__text	00103750	00000024	00000010	FFFFFFF8	R	.	.	.	.	T	.
-[AdGoji end]	__text	00103774	00000010			R	.	.	.	.	T	.
-[AdGoji setEnd:]	__text	00103784	00000024	00000010	FFFFFFF8	R	.	.	.	.	T	.
-[AdGoji currentSessionID]	__text	001037A8	00000010			R	.	.	.	.	T	.
-[AdGoji setCurrentSessionID:]	__text	001037B8	00000024	00000010	FFFFFFF8	R	.	.	.	.	T	.
-[AdGoji eventURLString]	__text	001037DC	00000010			R	.	.	.	.	T	.
-[AdGoji setEventURLString:]	__text	001037EC	00000024	00000010	FFFFFFF8	R	.	.	.	.	T	.
-[AdGoji eventHTTPMethod]	__text	00103810	00000010			R	.	.	.	.	T	.
-[AdGoji setEventHTTPMethod:]	__text	00103820	00000024	00000010	FFFFFFF8	R	.	.	.	.	T	.
-[AdGoji logEventsImmediately]	__text	00103844	00000010			R	.	.	.	.	T	.
-[AdGoji setLogEventsImmediately:]	__text	00103854	00000010			R	.	.	.	.	T	.
-[AppDetectionController runningProcessesFaster]	__text	00103864	00000180	00000048	00000000	R	.	.	.	B	T	.
-[AppDetectionController detectProcessNames]	__text	001039E4	00000060	0000000C	00000000	R	.	.	.	B	T	.
-[AppDetectionController testCustomURLScheme...	__text	00103A44	00000212	000000B8	00000000	R	.	.	.	B	T	.
-[AppDetectionController testCustomURLScheme...	__text	00103C58	000000DC	0000001C	00000000	R	.	.	.	B	T	.
-[AppDetectionController init]	__text	00103D34	0000003E	00000010	FFFFFFF8	R	.	.	.	.	T	.
-[AppDetectionController initWithDelegate:]	__text	00103D74	0000004E	00000014	00000000	R	.	.	.	B	T	.
-[AppDetectionController dealloc]	__text	00103DC4	0000009C	00000020	00000000	R	.	.	.	B	T	.
-[AppDetectionController queue]	__text	00103E60	00000010			R	.	.	.	.	T	.
-[AppDetectionController setQueue:]	__text	00103E70	00000024	00000010	FFFFFFF8	R	.	.	.	.	T	.
-[AppDetectionController delegate]	__text	00103E94	00000010			R	.	.	.	.	T	.
-[AppDetectionController setDelegate:]	__text	00103EA4	00000010			R	.	.	.	.	T	.
-[AppDetectionController processNames]	__text	00103EB4	00000010			R	.	.	.	.	T	.
-[AppDetectionController setProcessNames:]	__text	00103EC4	00000024	00000010	FFFFFFF8	R	.	.	.	.	T	.
-[AdGojiModel dealloc]	__text	00103EE8	000001F6	00000020	00000000	R	.	.	.	B	T	.
-[AdGojiModel isJailBroken]	__text	001040E0	0000008C	00000020	00000000	R	.	.	.	B	T	.
-[AdGojiModel isJailBrokenStr]	__text	0010416C	00000034	00000008	FFFFFFF8	R	.	.	.	.	T	.
-[AdGojiModel getMACAddress]	__text	001041A0	00000142	0000004C	00000000	R	.	.	.	B	T	.
-[AdGojiModel deviceInfo]	__text	001042E4	00000538	00000020	00000000	R	.	.	.	B	T	.
+[AdGojiModel sha1:]	__text	0010481C	000000FC	0000007C	00000000	R	.	.	.	B	T	.
+[AdGojiModel translateDevicModel:]	__text	00104918	000000F0	00000014	00000000	R	.	.	.	B	T	.
-[AdGojiModel setup]	__text	00104A08	000002E8	0000001C	00000000	R	.	.	.	B	T	.
-[AdGojiModel init]	__text	00104CF0	00000044	00000014	00000000	R	.	.	.	B	T	.
-[AdGojiModel authToken]	__text	00104D34	00000010			R	.	.	.	.	T	.
-[AdGojiModel setAuthToken:]	__text	00104D44	00000024	00000010	FFFFFFF8	R	.	.	.	.	T	.
-[AdGojiModel authTokenExpiresAt]	__text	00104D68	00000018			R	.	.	.	.	T	.
-[AdGojiModel setAuthTokenExpiresAt:]	__text	00104D80	00000014			R	.	.	.	.	T	.
-[AdGojiModel deviceOpenUDID]	__text	00104D94	00000010			R	.	.	.	.	T	.
-[AdGojiModel setDeviceOpenUDID:]	__text	00104DA4	00000024	00000010	FFFFFFF8	R	.	.	.	.	T	.
-[AdGojiModel deviceModel]	__text	00104DC8	00000010			R	.	.	.	.	T	.
-[AdGojiModel setDeviceModel:]	__text	00104DD8	00000024	00000010	FFFFFFF8	R	.	.	.	.	T	.
-[AdGojiModel systemVersion]	__text	00104DFC	00000010			R	.	.	.	.	T	.
-[AdGojiModel setSystemVersion:]	__text	00104E0C	00000024	00000010	FFFFFFF8	R	.	.	.	.	T	.
-[AdGojiModel deviceName]	__text	00104E30	00000010			R	.	.	.	.	T	.
-[AdGojiModel setDeviceName:]	__text	00104E40	00000024	00000010	FFFFFFF8	R	.	.	.	.	T	.
-[AdGojiModel deviceSystemName]	__text	00104E64	00000010			R	.	.	.	.	T	.
-[AdGojiModel setDeviceSystemName:]	__text	00104E74	00000024	00000010	FFFFFFF8	R	.	.	.	.	T	.
-[AdGojiModel deviceLocalizedModel]	__text	00104E98	00000010			R	.	.	.	.	T	.
-[AdGojiModel setDeviceLocalizedModel:]	__text	00104EA8	00000024	00000010	FFFFFFF8	R	.	.	.	.	T	.
-[AdGojiModel countryCode]	__text	00104ECC	00000010			R	.	.	.	.	T	.

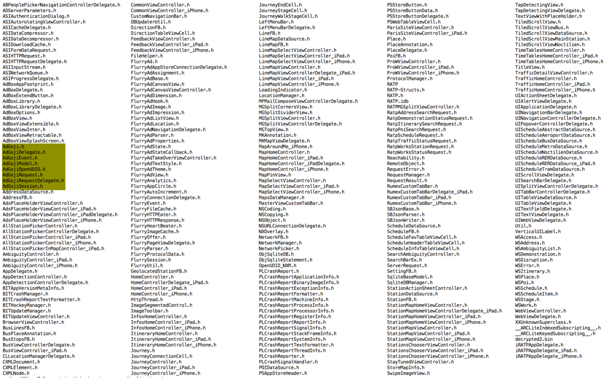
Line 1 of 5503

100.00% (-38,-309) (490,650) 00003A10 00003A10: start

```
99969: item would point to non-code; truncating it
99969: item would point to non-code; truncating it
99B0F: item would point to non-code; truncating it
99B0F: item would point to non-code; truncating it
99B0F: item would point to non-code; truncating it
9E21B: item would point to non-code; truncating it
ACC25: item would point to non-code; truncating it
ACC25: item would point to non-code; truncating it
B39E9: item would point to non-code; truncating it
B39E9: item would point to non-code; truncating it
B39E9: item would point to non-code; truncating it
B8CE3: item would point to non-code; truncating it
B8CE3: item would point to non-code; truncating it
B8CE3: item would point to non-code; truncating it
B9455: item would point to non-code; truncating it
```

Adgoji: confirmation of its presence in the App (2)

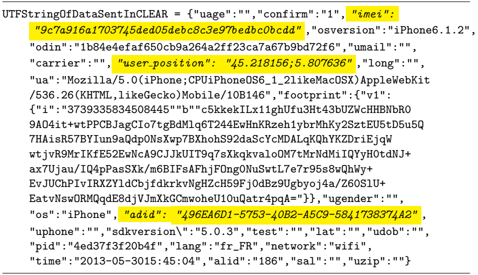
RATP iOS App binary Objective-C header info using class-dump-z



```
ABPeoplePickerNavigationControllerDelegate.h
ADServerParameters.h
ASIAuthenticationDialog.h
ASIAutorotatingViewController.h
ASICacheDelegate.h
ASIDataCompressor.h
ASIDataDecompressor.h
ASIDownloadCache.h
ASIFormDataRequest.h
ASIHTTPRequest.h
ASIHTTPRequestDelegate.h
ASIInputStream.h
ASINetworkQueue.h
ASIProgressDelegate.h
AdBoxAppFootprint.h
AdBoxDelegate.h
AdBoxExtendButton.h
AdBoxLibrary.h
AdBoxLibraryDelegate.h
AdBoxOptions.h
AdBoxView.h
AdBoxViewExtensible.h
AdBoxViewInter.h
AdBoxViewRetractable.h
AdBoxViewSplashScreen.h
AdGoji.h
AdGojiDelegate.h
AdGojiEvent.h
AdGojiModel.h
AdGojiOpenUDID.h
AdGojiRequest.h
AdGojiRequestDelegate.h
AdGojiSession.h
AddressDataSource.h
AddressFB.h
AdsPlaceHolderViewController.h
AdsPlaceHolderViewController_iPad.h
AdsPlaceHolderViewController_iPadDelegate.h
AdsPlaceHolderViewController_iPhone.h
AllStationPickerController.h
AllStationPickerControllerDelegate.h
AllStationPickerController_iPad.h
AllStationPickerController_iPhone.h
AllStationPickerInMapController_iPad.h
AmbiguityController.h
AmbiguityController_iPad.h
AmbiguityController_iPhone.h
AppDelegate.h
AppDetectionController.h
AppDetectionControllerDelegate.h
BITAppVersionMetaInfo.h
BITCrashManager.h
BITCrashReportTextFormatter.h
BITHockeyManager.h
BITUpdateManager.h
BITUpdateViewController.h
BrowserViewController.h
BusLinesFB.h
BusPlaceAnnotation.h
BusStopsFB.h
BusViewControllerDelegate.h
BusViewController_iPad.h
CLLocationManagerDelegate.h
CXMLDocument.h
CXMLElement.h
CXMLNode.h

CommonViewController.h
CommonViewController_iPhone.h
CustomNavigationBar.h
DBUpdaterUtil.h
DirectionFB.h
DirectionTableViewCell.h
FeedbackViewController.h
FeedbackViewController_iPad.h
FeedbackViewController_iPhone.h
FileHelper.h
FlurryAd.h
FlurryAdAppStoreConnectionDelegate.h
FlurryAdAssignment.h
FlurryAdBase.h
FlurryAdCanvasView.h
FlurryAdCanvasViewController.h
FlurryAdDimension.h
FlurryAdHook.h
FlurryAdImage.h
FlurryAdImpression.h
FlurryAdListView.h
FlurryAdLocation.h
FlurryAdNavigationDelegate.h
FlurryAdParser.h
FlurryAdProperties.h
FlurryAdState.h
FlurryAdStateCallback.h
FlurryAdTakeOverViewController.h
FlurryAdTextStyle.h
FlurryAdTheme.h
FlurryAdView.h
FlurryAnalytics.h
FlurryAppCircle.h
FlurryAutoIncrement.h
FlurryConnectionDelegate.h
FlurryEvent.h
FlurryFileCache.h
FlurryHTTPEater.h
FlurryHTTPResponse.h
FlurryHeartBeater.h
FlurryImageCache.h
FlurryOffer.h
FlurryPageViewDelegate.h
FlurryParser.h
FlurryProtocolData.h
FlurrySession.h
FlurryUtil.h
GeolocatedStationFB.h
HomeController.h
HomeControllerDelegate_iPad.h
HomeController_iPad.h
HomeController_iPhone.h
HttpThread.h
ImageSegmentedControl.h
ImageToolbar.h
InfosHomeController.h
InfosHomeController_iPad.h
InfosHomeController_iPhone.h
ItineraryHomeController.h
ItineraryHomeController_iPad.h
ItineraryHomeController_iPhone.h
Journey.h
JourneyConnectionCell.h
JourneyController.h
JourneyController_iPad.h
JourneyController_iPhone.h

JourneyEndCell.h
JourneyStageCell.h
JourneyWalkStageCell.h
LeftMenuBar.h
LeftMenuBarDelegate.h
LineFB.h
LineMapDataSource.h
LineMapFB.h
LineMapSelectViewController.h
LineMapSelectViewController_iPad.h
LineMapSelectViewController_iPhone.h
LineMapViewController.h
LineMapViewControllerDelegate_iPad.h
LineMapViewController_iPad.h
LineMapViewController_iPhone.h
LoadingIndicator.h
LocationManager.h
MFMailComposeViewControllerDelegate.h
MGSplitCornersView.h
MGSplitDividerView.h
MGSplitViewController.h
MGSplitViewControllerDelegate.h
MGTopView.h
MKAnnotation.h
MKMapViewDelegate.h
MapAroundMe_iPhone.h
MapHomeController.h
MapHomeController_iPad.h
MapHomeController_iPadDelegate.h
MapHomeController_iPhone.h
MapPinView.h
MapSelectViewController.h
MapSelectViewController_iPad.h
MapSelectViewController_iPhone.h
MapsDataManager.h
MasterViewCustomTabBar.h
NSCoding.h
NSCopying.h
NSObject.h
NSURLConnectionDelegate.h
NXOverlay.h
NetworkFB.h
NetworkManager.h
NetworkPicker.h
ObjSqliteDB.h
ObjSqliteStatement.h
OpenUDID_NXM.h
PLCrashReport.h
PLCrashReportApplicationInfo.h
PLCrashReportBinaryImageInfo.h
PLCrashReportExceptionInfo.h
PLCrashReportFormatter.h
PLCrashReportMachineInfo.h
PLCrashReportProcessInfo.h
PLCrashReportProcessorInfo.h
PLCrashReportRegisterInfo.h
PLCrashReportReportInfo.h
PLCrashReportSignalInfo.h
PLCrashReportStackFrameInfo.h
PLCrashReportSystemInfo.h
PLCrashReportTextFormatter.h
PLCrashReportThreadInfo.h
PLCrashReporter.h
PLCrashSignalHandler.h
POIDataSource.h
PSAppStoreHeader.h

PSStoreButton.h
PSStoreButtonData.h
PSStoreButtonDelegate.h
PSWebTableViewCell.h
ParisSiteViewController.h
ParisSiteViewController_iPad.h
Place.h
PlaceAnnotation.h
PlaceDelegate.h
PoiFB.h
ProWViewController.h
ProWViewController_iPad.h
ProWViewController_iPhone.h
ProtocolManager.h
RATP
RATP-Structs.h
RATP.h
RATP.idb
RATPMGSplitViewController.h
RatpAddressSearchRequest.h
RatpDemonstrationStatusRequest.h
RatpItinerarySearchRequest.h
RatpPoiSearchRequest.h
RatpScheduleRequest.h
RatpTrafficStatusRequest.h
RatpWorksStationRequest.h
RatpWorksStatusRequest.h
Reachability.h
RemoteObject.h
RequestError.h
RequestManager.h
RequestResult.h
RumexCustomTabBar.h
RumexCustomTabBarDelegate_iPad.h
RumexCustomTabBar_iPad.h
RumexCustomTabBar_iPhone.h
SBJsonBase.h
SBJsonParser.h
SBJsonWriter.h
ScheduleDataSource.h
ScheduleFB.h
ScheduleFavTableViewCell.h
ScheduleHeaderTableViewCell.h
ScheduleInfoTableViewCell.h
SearchAmbiguityController.h
SearchBarEx.h
ServerRequest.h
SettingFB.h
SqliteBaseModel.h
SqliteDBManager.h
StationActionSheetController.h
StationDataSource.h
StationFB.h
StationMapHomeViewController.h
StationMapHomeViewControllerDelegate_iPad.h
StationMapHomeViewController_iPad.h
StationMapHomeViewController_iPhone.h
StationMapViewController.h
StationMapViewController_iPad.h
StationMapViewController_iPhone.h
StationsChooserViewController.h
StationsChooserViewController_iPad.h
StationsChooserViewController_iPhone.h
StayTunedViewController.h
StoreMapInfo.h
SwipeImageView.h

TapDetectingView.h
TapDetectingViewDelegate.h
TextViewWithPlaceHolder.h
TiledScrollView.h
TiledScrollViewBus.h
TiledScrollViewDataSource.h
TiledScrollViewMainStation.h
TiledScrollViewNoctilien.h
TimeTablesHomeController.h
TimeTablesHomeController_iPad.h
TimeTablesHomeController_iPhone.h
TitleView.h
TrafficDetailViewController.h
TrafficHomeController.h
TrafficHomeController_iPad.h
TrafficHomeController_iPhone.h
UIActionSheetDelegate.h
UIAlertViewDelegate.h
UIApplicationDelegate.h
UINavigationBarDelegate.h
UINavigationControllerDelegate.h
UIPopoverControllerDelegate.h
UIScheduleAbstractDataSource.h
UIScheduleAeroportDataSource.h
UIScheduleBusDataSource.h
UIScheduleMetroDataSource.h
UIScheduleNoctilienDataSource.h
UIScheduleRERDataSource.h
UIScheduleRERDataSource_iPad.h
UIScheduleTramDataSource.h
UIScrollViewDelegate.h
UISearchBarDelegate.h
UISplitViewControllerDelegate.h
UITabBarControllerDelegate.h
UITableViewDataSource.h
UITableViewDelegate.h
UITextFieldDelegate.h
UITextViewDelegate.h
UIWebViewDelegate.h
Util.h
VerticalUILabel.h
WSAccess.h
WSAddress.h
WSAmbiguityList.h
WSDemonstration.h
WSDisruption.h
WSError.h
WSItinerary.h
WSPlace.h
WSPoi.h
WSSchedule.h
WSScheduleItem.h
WSStage.h
WSWork.h
WebViewController.h
WebViewDelegate.h
XXUnknownSuperclass.h
__ARCLiteIndexedSubscripting__.h
__ARCLiteKeyedSubscripting__.h
decrypted2.bin
iRATPAppDelegate.h
iRATPAppDelegate_iPad.h
iRATPAppDelegate_iPhone.h
```

Privacy Leaks to Sofialys company

Sofialys: A mobile advertising company [5]



Listing 1.3. Data sent by iOS App of RATP in cleartext

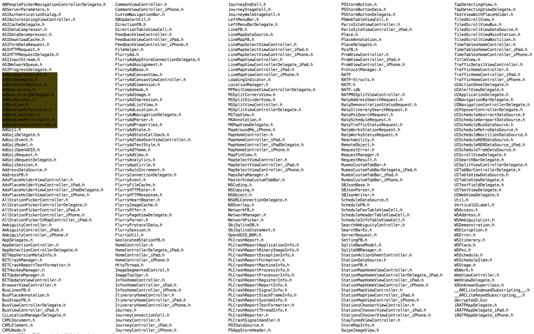
```
UTFStringOfDataSentInCLEAR = {"uage":"","confirm":"1","imei":
    "9c7a916a1703745ded05debc8c3e97bedbc0bcdd","osversion":"iPhone6.1.2",
    "odin":"1b84e4efaf650cb9a264a2ff23ca7a67b9bd72f6","umail":"",
    "carrier":"","user_position": "45.218156;5.807636","long":"",
    "ua":"Mozilla/5.0(iPhone;CPUiPhoneOS6_1_2likeMacOSX)AppleWebKit
    /536.26(KHTML,likeGecko)Mobile/10B146","footprint":{"v1":
    {"i":"3739335834508445""b""c5kkekILx11ghUfu3Ht43bUZWcHHBNbR0
    9AO4it+wtPPCBJagCIo7tgBdMlq6T244EwHnKRzeh1ybrMhKy2SztEU5tD5u5Q
    7HAisR57BYIun9aQdp0NsXwp7BXhohS92daScYcMDALqKQhYKZDriEjqW
    wtjvR9MrIKfE52EwNcA9CJJkUIT9q7sXkqkvaloOM7tMrNdMiIQYyHOtdNJ+
    ax7Ujau/IQ4pPasSXk/m6BIFsAFhjFOngONuSwtL7e7r95s8wQhWy+
    EvJUChPIvIRXZYldCbjfdkrkvNgHZcH59Fj0dBz9Ugbyoj4a/Z60SlU+
    EatvNswORMQqdE8djVJmXkGCmwoheU10uQatr4pqA="}},"ugender":"",
    "os":"iPhone","adid": "496EA6D1-5753-40B2-A5C9-5841738374A2",
    "uphone":"","sdkversion\":"5.0.3","test":"","lat":"","udob":"",
    "pid":"4ed37f3f20b4f","lang":"fr_FR","network":"wifi",
    "time":"2013-05-3015:45:04","alid":"186","sal":"","uzip":""}
```

The user PI sent is (IN CLEAR-TEXT):

- The exact user location
- Advertising ID and UDID

Sofialys: confirmation of its presence in the App

RATP iOS App binary Objective-C header info using class-dump-z



```
ABPeoplePickerNavigationControllerDelegate.h
ADServerParameters.h
ASIAuthenticationDialog.h
ASIAutorotatingViewController.h
ASICacheDelegate.h
ASIDataCompressor.h
ASIDataDecompressor.h
ASIDownloadCache.h
ASIFormDataRequest.h
ASIHTTPRequest.h
ASIHTTPRequestDelegate.h
ASIInputStream.h
ASINetworkQueue.h
ASIProgressDelegate.h
AdBoxAppFootprint.h
AdBoxDelegate.h
AdBoxExtendButton.h
AdBoxLibrary.h
AdBoxLibraryDelegate.h
AdBoxOptions.h
AdBoxView.h
AdBoxViewExtensible.h
AdBoxViewInter.h
AdBoxViewRetractable.h
AdBoxViewSplashScreen.h
AdGoji.h
AdGojiDelegate.h
AdGojiEvent.h
AdGojiModel.h
AdGojiOpenUDID.h
AdGojiRequest.h
AdGojiRequestDelegate.h
AdGojiSession.h
AddressDataSource.h
AddressFB.h
AdsPlaceHolderViewController.h
AdsPlaceHolderViewController_iPad.h
AdsPlaceHolderViewController_iPadDelegate.h
AdsPlaceHolderViewController_iPhone.h
AllStationPickerController.h
AllStationPickerControllerDelegate.h
AllStationPickerController_iPad.h
AllStationPickerController_iPhone.h
AllStationPickerInMapController_iPad.h
AmbiguityController.h
AmbiguityController_iPad.h
AmbiguityController_iPhone.h
AppDelegate.h
AppDetectionController.h
AppDetectionControllerDelegate.h
BITAppVersionMetaInfo.h
BITCrashManager.h
BITCrashReportTextFormatter.h
BITHockeyManager.h
BITUpdateManager.h
BITUpdateViewController.h
BrowserViewController.h
BusLinesFB.h
BusPlaceAnnotation.h
BusStopsFB.h
BusViewControllerDelegate.h
BusViewController_iPad.h
CLLocationManagerDelegate.h
CXMLDocument.h
CXMLElement.h
CXMLNode.h
CommonViewController.h
CommonViewController_iPhone.h
CustomNavigationBar.h
DBUpdaterUtil.h
DirectionFB.h
DirectionTableViewCell.h
FeedbackViewController.h
FeedbackViewController_iPad.h
FeedbackViewController_iPhone.h
FileHelper.h
FlurryAd.h
FlurryAdAppStoreConnectionDelegate.h
FlurryAdAssignment.h
FlurryAdBase.h
FlurryAdCanvasView.h
FlurryAdCanvasViewController.h
FlurryAdDimension.h
FlurryAdHook.h
FlurryAdImage.h
FlurryAdImpression.h
FlurryAdListView.h
FlurryAdLocation.h
FlurryAdNavigationDelegate.h
FlurryAdParser.h
FlurryAdProperties.h
FlurryAdState.h
FlurryAdStateCallback.h
FlurryAdTakeOverViewController.h
FlurryAdTextStyle.h
FlurryAdTheme.h
FlurryAdView.h
FlurryAnalytics.h
FlurryAppCircle.h
FlurryAutoIncrement.h
FlurryConnectionDelegate.h
FlurryEvent.h
FlurryFileCache.h
FlurryHTTPEater.h
FlurryHTTPResponse.h
FlurryHeartBeater.h
FlurryImageCache.h
FlurryOffer.h
FlurryPageViewDelegate.h
FlurryParser.h
FlurryProtocolData.h
FlurrySession.h
FlurryUtil.h
GeolocatedStationFB.h
HomeController.h
HomeControllerDelegate_iPad.h
HomeController_iPad.h
HomeController_iPhone.h
HttpThread.h
ImageSegmentedControl.h
ImageToolbar.h
InfosHomeController.h
InfosHomeController_iPad.h
InfosHomeController_iPhone.h
ItineraryHomeController.h
ItineraryHomeController_iPad.h
ItineraryHomeController_iPhone.h
Journey.h
JourneyConnectionCell.h
JourneyController.h
JourneyController_iPad.h
JourneyController_iPhone.h
JourneyEndCell.h
JourneyStageCell.h
JourneyWalkStageCell.h
LeftMenuBar.h
LeftMenuBarDelegate.h
LineFB.h
LineMapDataSource.h
LineMapFB.h
LineMapSelectViewController.h
LineMapSelectViewController_iPad.h
LineMapSelectViewController_iPhone.h
LineMapViewController.h
LineMapViewControllerDelegate_iPad.h
LineMapViewController_iPad.h
LineMapViewController_iPhone.h
LoadingIndicator.h
LocationManager.h
MFMailComposeViewControllerDelegate.h
MGSplitCornersView.h
MGSplitDividerView.h
MGSplitViewController.h
MGSplitViewControllerDelegate.h
MGTopView.h
MKAnnotation.h
MKMapViewDelegate.h
MapAroundMe_iPhone.h
MapHomeController.h
MapHomeController_iPad.h
MapHomeController_iPadDelegate.h
MapHomeController_iPhone.h
MapPinView.h
MapSelectViewController.h
MapSelectViewController_iPad.h
MapSelectViewController_iPhone.h
MapsDataManager.h
MasterViewCustomTabBar.h
NSCoding.h
NSCopying.h
NSObject.h
NSURLConnectionDelegate.h
NXOverlay.h
NetworkFB.h
NetworkManager.h
NetworkPicker.h
ObjSqliteDB.h
ObjSqliteStatement.h
OpenUDID_NXM.h
PLCrashReport.h
PLCrashReportApplicationInfo.h
PLCrashReportBinaryImageInfo.h
PLCrashReportExceptionInfo.h
PLCrashReportFormatter.h
PLCrashReportMachineInfo.h
PLCrashReportProcessInfo.h
PLCrashReportProcessorInfo.h
PLCrashReportRegisterInfo.h
PLCrashReportReportInfo.h
PLCrashReportSignalInfo.h
PLCrashReportStackFrameInfo.h
PLCrashReportSystemInfo.h
PLCrashReportTextFormatter.h
PLCrashReportThreadInfo.h
PLCrashReporter.h
PLCrashSignalHandler.h
POIDataSource.h
PSAppStoreHeader.h
PSStoreButton.h
PSStoreButtonData.h
PSStoreButtonDelegate.h
PSWebTableViewCell.h
ParisSiteViewController.h
ParisSiteViewController_iPad.h
Place.h
PlaceAnnotation.h
PlaceDelegate.h
PoiFB.h
ProWViewController.h
ProWViewController_iPad.h
ProWViewController_iPhone.h
ProtocolManager.h
RATP
RATP-Structs.h
RATP.h
RATP.idb
RATPMGSplitViewController.h
RatpAddressSearchRequest.h
RatpDemonstrationStatusRequest.h
RatpItinerarySearchRequest.h
RatpPoiSearchRequest.h
RatpScheduleRequest.h
RatpTrafficStatusRequest.h
RatpWorksStationRequest.h
RatpWorksStatusRequest.h
Reachability.h
RemoteObject.h
RequestError.h
RequestManager.h
RequestResult.h
RumexCustomTabBar.h
RumexCustomTabBarDelegate_iPad.h
RumexCustomTabBar_iPad.h
RumexCustomTabBar_iPhone.h
SBJsonBase.h
SBJsonParser.h
SBJsonWriter.h
ScheduleDataSource.h
ScheduleFB.h
ScheduleFavTableViewCell.h
ScheduleHeaderTableViewCell.h
ScheduleInfoTableViewCell.h
SearchAmbiguityController.h
SearchBarEx.h
ServerRequest.h
SettingFB.h
SqliteBaseModel.h
SqliteDBManager.h
StationActionSheetController.h
StationDataSource.h
StationFB.h
StationMapHomeViewController.h
StationMapHomeViewControllerDelegate_iPad.h
StationMapHomeViewController_iPad.h
StationMapHomeViewController_iPhone.h
StationMapViewController.h
StationMapViewController_iPad.h
StationMapViewController_iPhone.h
StationsChooserViewController.h
StationsChooserViewController_iPad.h
StationsChooserViewController_iPhone.h
StayTunedViewController.h
StoreMapInfo.h
SwipeImageView.h
TapDetectingView.h
TapDetectingViewDelegate.h
TextViewWithPlaceHolder.h
TiledScrollView.h
TiledScrollViewBus.h
TiledScrollViewDataSource.h
TiledScrollViewMainStation.h
TiledScrollViewNoctilien.h
TimeTablesHomeController.h
TimeTablesHomeController_iPad.h
TimeTablesHomeController_iPhone.h
TitleView.h
TrafficDetailViewController.h
TrafficHomeController.h
TrafficHomeController_iPad.h
TrafficHomeController_iPhone.h
UIActionSheetDelegate.h
UIAlertViewDelegate.h
UIApplicationDelegate.h
UINavigationBarDelegate.h
UINavigationControllerDelegate.h
UIPopoverControllerDelegate.h
UIScheduleAbstractDataSource.h
UIScheduleAeroportDataSource.h
UIScheduleBusDataSource.h
UIScheduleMetroDataSource.h
UIScheduleNoctilienDataSource.h
UIScheduleRERDataSource.h
UIScheduleRERDataSource_iPad.h
UIScheduleTramDataSource.h
UIScrollViewDelegate.h
UISearchBarDelegate.h
UISplitViewControllerDelegate.h
UITabBarControllerDelegate.h
UITableViewDataSource.h
UITableViewDelegate.h
UITextFieldDelegate.h
UITextViewDelegate.h
UIWebViewDelegate.h
Util.h
VerticalUILabel.h
WSAccess.h
WSAddress.h
WSAmbiguityList.h
WSDemonstration.h
WSDisruption.h
WSError.h
WSItinerary.h
WSPlace.h
WSPoi.h
WSSchedule.h
WSScheduleItem.h
WSStage.h
WSWork.h
WebViewController.h
WebViewDelegate.h
XXUnknownSuperclass.h
__ARCLiteIndexedSubscripting__.h
__ARCLiteKeyedSubscripting__.h
decrypted2.bin
iRATPAppDelegate.h
iRATPAppDelegate_iPad.h
iRATPAppDelegate_iPhone.h
```

Fig. 7. Listing AdBox Headers in iOS binary of RATP App

Responsibility of Apple

AdID: An alphanumeric string unique to each device, used only for serving advertisements.
But Advertising Identifier only gives an illusion to the user that he is able to opt-out from device tracking:

- WiFiMAC Address (using sysctl function in libc library)
- Using UIPasteboard to generate a unique identifier across the device
- Device Name
- UDID (still being used by "old" Apps even if deprecated)

Apple privacy dashboard is not enough because:

- A&A libraries included by the App developer have access to the same set of user's private data as the App itself.
- Behavioral analysis is required.
- Finer granularity permission is needed

Apple cannot ignore this trend.

Outline

1 Introduction

2 RATP iOS App

3 RATP Android App

4 Conclusions

5 References

Instrumented version of Android

- We use Taintdroid [6] to track user PI flow (and hence the leakage of PI over network)
- We also change the source code of Android itself (only the APIs of our interest e.g. network APIs to look for the data sent over the network) to fill-in the gaps
  - Taintdroid could miss the leakage of some PI [3]
  - Some PI (e.g. Android ID) can't be tainted due to false positives.
- In addition, we also use static analysis to confirm some observations.

Privacy Leaks to Sofialys company

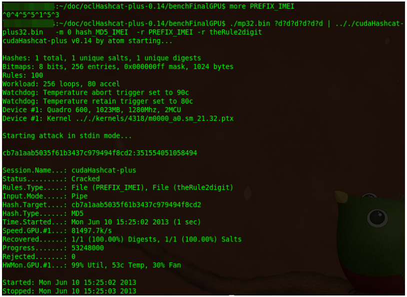
Listing 1.4. Data sent in cleartext by Android App of RATP

```
DataSentInCLEAR =
    { "user_position": "45.2115529;5.8037135" ,"ugender":"",
    "test":"","uage":"0", "imei": "56b4153b8bd2f6fd242d84b3f63e287" ,"napp":
    null,"uemail":"","pid":"4ed37f3f20b4f","alid":"114","uzip":"",
    "osversion":"3.0.31-g396c4dfdirty","lang":"en_En","sal":"","network":
    "na","adpos":null, "time":"Tue Jun 04 12:05:39 UTC+02:00 2013",
    "sdkversion":"3.2", "ua":"Mozilla\/5.0(Linux; U; Android 4.1.1;
    fr-fr; Full AOSP on Maguro Build\/JRO03R) AppleWebKit\/534.30
    (KHTML, like Gecko) Version\/4.0 Mobile Safari\/534.30","udob":"",
    "carrier": "Orange F" ,"longitude":"0.0","latitude":"0.0",
    "freespace":null,"unick":null}]
```

The user PI sent is:

- The exact location of the user
- the MD5 hash of the device IMEI
- the SIM card's carrier/operator name

Is the hashing of IMEI sufficient to guarantee anonymity?



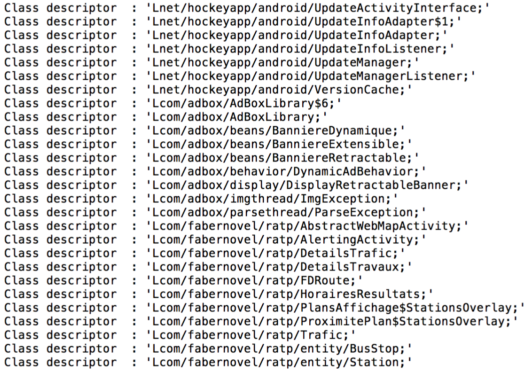
```
[redacted]:~/doc/oclHashcat-plus-0.14/benchFinalGPU$ more PREFIX_IMEI
^0^4^5^5^1^5^3
[redacted]:~/doc/oclHashcat-plus-0.14/benchFinalGPU$ ./mp32.bin ?d?d?d?d?d?d | ../../cudaHashcat-
plus32.bin   -m 0 hash_MD5_IMEI  -r PREFIX_IMEI -r theRule2digit
cudaHashcat-plus v0.14 by atom starting...

Hashes: 1 total, 1 unique salts, 1 unique digests
Bitmaps: 8 bits, 256 entries, 0x000000ff mask, 1024 bytes
Rules: 100
Workload: 256 loops, 80 accel
Watchdog: Temperature abort trigger set to 90c
Watchdog: Temperature retain trigger set to 80c
Device #1: Quadro 600, 1023MB, 1280Mhz, 2MCU
Device #1: Kernel ../../kernels/4318/m0000_a0.sm_21.32.ptx

Starting attack in stdin mode...

cb7a1aab5035f61b3437c979494f8cd2:351554051058494

Session.Name...: cudaHashcat-plus
Status.........: Cracked
Rules.Type.....: File (PREFIX_IMEI), File (theRule2digit)
Input.Mode.....: Pipe
Hash.Target....: cb7a1aab5035f61b3437c979494f8cd2
Hash.Type......: MD5
Time.Started...: Mon Jun 10 15:25:02 2013 (1 sec)
Speed.GPU.#1...: 81497.7k/s
Recovered......: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.......: 53248000
Rejected.......: 0
HWMon.GPU.#1...: 99% Util, 53c Temp, 30% Fan

Started: Mon Jun 10 15:25:02 2013
Stopped: Mon Jun 10 15:25:03 2013
```

It's NOT:

- It takes less than one second to deanonymise on a regular PC if smartphone manufacturer and model are known (which is the case here!)

Sofialys: confirmation of its presence in the App

Below is the listing containing class descriptors of Android App



```
Class descriptor  : 'Lnet/hockeyapp/android/UpdateActivityInterface;'
Class descriptor  : 'Lnet/hockeyapp/android/UpdateInfoAdapter$1;'
Class descriptor  : 'Lnet/hockeyapp/android/UpdateInfoAdapter;'
Class descriptor  : 'Lnet/hockeyapp/android/UpdateInfoListener;'
Class descriptor  : 'Lnet/hockeyapp/android/UpdateManager;'
Class descriptor  : 'Lnet/hockeyapp/android/UpdateManagerListener;'
Class descriptor  : 'Lnet/hockeyapp/android/VersionCache;'
Class descriptor  : 'Lcom/adbox/AdBoxLibrary$6;'
Class descriptor  : 'Lcom/adbox/AdBoxLibrary;'
Class descriptor  : 'Lcom/adbox/beans/BanniereDynamique;'
Class descriptor  : 'Lcom/adbox/beans/BanniereExtensible;'
Class descriptor  : 'Lcom/adbox/beans/BanniereRetractable;'
Class descriptor  : 'Lcom/adbox/behavior/DynamicAdBehavior;'
Class descriptor  : 'Lcom/adbox/display/DisplayRetractableBanner;'
Class descriptor  : 'Lcom/adbox/imgthread/ImgException;'
Class descriptor  : 'Lcom/adbox/parsethread/ParseException;'
Class descriptor  : 'Lcom/fabernovel/ratp/AbstractWebMapActivity;'
Class descriptor  : 'Lcom/fabernovel/ratp/AlertingActivity;'
Class descriptor  : 'Lcom/fabernovel/ratp/DetailsTrafic;'
Class descriptor  : 'Lcom/fabernovel/ratp/DetailsTravaux;'
Class descriptor  : 'Lcom/fabernovel/ratp/FDRoute;'
Class descriptor  : 'Lcom/fabernovel/ratp/HorairesResultats;'
Class descriptor  : 'Lcom/fabernovel/ratp/PlansAffichage$StationsOverlay;'
Class descriptor  : 'Lcom/fabernovel/ratp/ProximitePlan$StationsOverlay;'
Class descriptor  : 'Lcom/fabernovel/ratp/Trafic;'
Class descriptor  : 'Lcom/fabernovel/ratp/entity/BusStop;'
Class descriptor  : 'Lcom/fabernovel/ratp/entity/Station;'
```

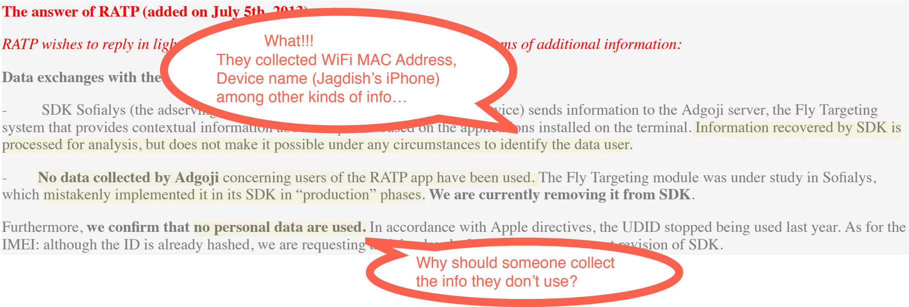
Responsibility of Google

- The Android permission system cannot be interpreted as an informed end-user agreement for the collection and use of personal data by third- parties.
- Android doesn't provide an option for the user to choose the permissions; the user needs to give all the permissions to the App or otherwise, he must just stop using the App.
- A&A libraries included by the App developer have access to the same set of user PI as the App itself.
- Behavioral analysis is required.
- Permission system must be more granular

Outline

1. Introduction
2. RATP iOS App
3. RATP Android App
4. Conclusions
5. References

Conclusions (1)



The answer of RATP (added on July 5th, 2013)

RATP wishes to reply in ligh ms of additional information:

Data exchanges with the

- SDK Sofialys (the adservi vice) sends information to the Adgoji server, the Fly Targeting system that provides contextual information ased on the applic ons installed on the terminal. Information recovered by SDK is processed for analysis, but does not make it possible under any circumstances to identify the data user.

- **No data collected by Adgoji** concerning users of the RATP app have been used. The Fly Targeting module was under study in Sofialys, which mistakenly implemented it in its SDK in "production" phases. **We are currently removing it from SDK**.

Furthermore, **we confirm that no personal data are used.** In accordance with Apple directives, the UDID stopped being used last year. As for the IMEI: although the ID is already hashed, we are requesting revision of SDK.

What!!!
They collected WiFi MAC Address,
Device name (Jagdish's iPhone)
among other kinds of info…

Why should someone collect
the info they don't use?

- There is a clear need of better regulations
- People must understand privacy better

Conclusions (2)

- We discuss bad practices employed in the world of smartphones (RATP Android and iOS Apps are good illustration)
    1. A&A companies are using not-supposed-to-be ways to collect user PI and tracking mechanisms
    2. They're one step ahead of the OS providers (blocking access to a set of tracking mechanisms lead to shift to some new tracking mechanisms)

- We discuss the limitations of the privacy control features proposed by Android/iOS Mobile OSs

- Above all, this is happening without user knowledge.

Outline

1 Introduction

2 RATP iOS App

3 RATP Android App

4 Conclusions

5 References

- Apple URL Scheme Reference.
  https://developer.apple.com/library/ios/featuredarticles/iPhoneURLScheme_Reference/Introduction/Introduction.html.

- MobileSusbstrate.
  http://iphonedevwiki.net/index.php/MobileSubstrate.

- On the Effectiveness of Dynamic Taint Analysis for Protecting Against Private Information Leaks on Android-based Devices.
  http://www.nicta.com.au/pub?doc=7091&filename=nicta_publication_7091.pdf.

- Path uploads your entire iPhone address book to its servers.
  http://mclov.in/2012/02/08/path-uploads-your-entire-address-book-to-their-servers.html.

- Sofialys.
  http://www.sofialys.com/en/.

- Taintdroid.
  http://appanalysis.org.

- Theos.
  http://iphonedevwiki.net/index.php/Theos/Getting_Started.

Twitter mobile apps storing address books for 18 months.
http://www.theregister.co.uk/2012/02/15/twitter_stores_address_books/.

WSJ: What They Know - Mobile.
http://blogs.wsj.com/wtk-mobile/.