They use String Obfuscation and anonymous class as their obfuscation technic

There is four package in this app, package a is where the string obfuscation is decrypted. Package android is the library for android framework. Package com.google.android.gms is where google map service located, which provide location based function for the app.

The main entrance of this app is MapActivity.class, In this class, int a() is used to get alarm distance from setting. void a(Latlng) handles the marker on the map

BackgroundServices.class handls most of the business logic. In this class, this appuse pendingIntent to alarm user to get off the bus, Void a(String, d) is used to send the notification, boolean b(BackgroundServices) is used to calculate the distance to destination, void c(BackgroundServices) to start the alarm.

Enum d is used to tag the start and stop of the service

g.class is used to generate LatLng object from Geocode

e.class contains the handles the input change of the address

f.class check if the service is up and running

The typical routine of how this app works is like the following

show map (MapActivity.class) -> get address from user input(e.class)->generate Latlng object for tracking(g.class)->start the service to start the location tracking (f.class and b.class)->wake user when approaching destination(BackgroundServices.class)

They use base64 and a custom algorithm to encrypt the string

They store encrypted string in a messages.properties file with a key-value map.

And use key within the app and call decrypted method in package a to get plain text.

We create a tool which use the code found in their decryption part with some modification, we are able to decrypt the string used in this app.

Original key value map, decrypted string and decompiled java code is attached.

