AndroidSecurityProject

Tabely App

Description of the App

The Tabely App is an App where you can search for restaurants and reserve tables for dinner. Furthermore, there are daily offers with discounts, presented to the users.

This is a Demo

This is only a demo App and the restaurants are only proxies. To see some restaurants in the search mask, type for name 'a' and for address 'g'. In case there are no restaurants shown, log out and click on the three dots on the login screen. Provide username and password to reset the database. To login give anything as username and '123' as password. This automatically logs you in, without creating an account-

Malware

In the App

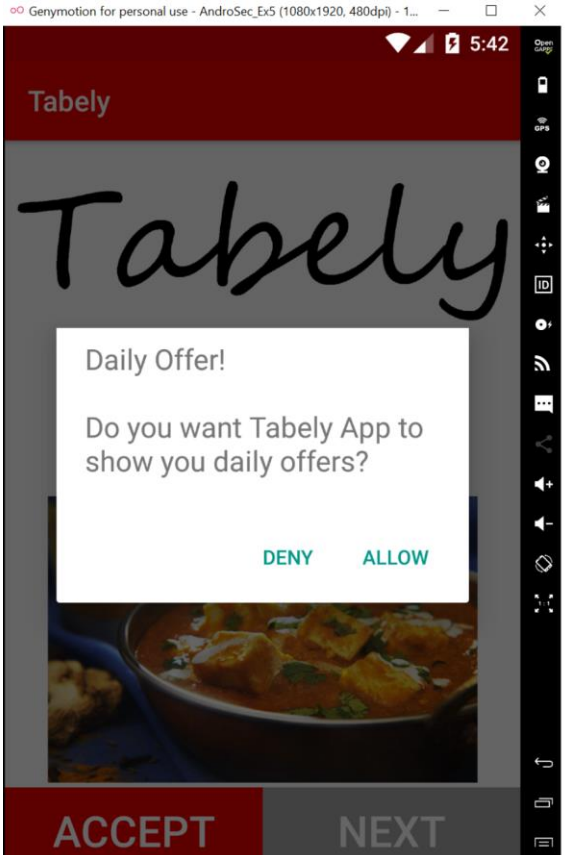
The get to the daily offers the App asks for Permissions (READ_CONTACTS, READ_SMS, READ_CALENDAR) but only one permission per offer. At different points of interaction (e.g. Searching for restaurant, accepting an offer or going back to the main-menu, the app starts a new Thread which exposes the SMS, Contact and Calendar information and sends it via TCP to the Server of the attacker. The Data will be sent as JSON-Strings.

Server Component

The Server is an easy TCP Server waiting for incoming connection in port 6789. The messages incoming on this Server will be printed to the console.

Project

Our initial idea was to use tapjacking to get the user granting us permissions, without noticing it. The use would want to book a restaurant table. He would get regular daily offers, which should lead him to click on the button DAILY OFFER. As a result, a Toast will appear, which is started by a service. This Toast stays until the user clicks allow or deny. The message displays the content below in the screenshot.



Genymotion for personal use - AndroSec_Ex5 (1080x1920, 480dpi) - 1...

Daily Offer!

Do you want Tabely App to show you daily offers?

The user thinks that he will receive daily offers in the future, if he grants the app this permission. However, the Toast overlays the real message,
asks for the contact permission. This can be done equivalently with other permissions, such as SMS or calendar permission.
It took us a long time to figure out why this did not work on our phone, a Galaxy S8. Finally, we noticed that the code works on phones with old Android versions, for example Android Marshmallow. So, vulnerability was closed for newer Android versions.

Therefore, we changed our approach to get the permits. We now give the user a brief explanation of why we need a permission before we ask for it. An exemplary explanation is: “To interact with today´s offering restaurant we need access to SMS to communicate with the restaurant.”. Another one is: “To make an appointment in the restaurant for today´s offer we need to access your calendar.”. This is based on the assumption that most users are very reckless in granting these permissions. An explanation of how this permission is used only in a harmless context is intended to increase the likelihood of it.

Once these rights have been granted, the actual transmission of the data can begin. When the user clicks on the FIND TABLE button, a TCP server connection is started, and he sends us his data. To ensure, that the user regularly transmits his personal data, the attack is also started when the user clicks on the DAILY OFFER button. Every time he clicks it, different Toasts will appear. These Toasts contain messages that look like daily offers, such “You get 20% for all your drinks today!”, “You get one drink for free today!”, “You got a 10$ coupon for ‘Mama Mexico’, and others.

It would be possible to include an API query. This would make it possible to run the app on both newer and older versions. For newer versions, it would then be explained why a given permission should be given, whereas for older versions the overlay service would be started.