iOS App Attack Pattern Implementation

Black Team

3/18

Outline

- Pattern1: Access iDevice user information
- Pattern2: Access FB user information

Pattern1: Access iDevice user information:

- Frameworks:
  - User Location:
    - CoreLocation.framework
  - Calendar Event & Reminder:
    - EventKit.framework

Access User Location

- Protocol: CLLocationManagerDelegate
  - @interface CounterViewController : UIViewController<CLLocationManagerDelegate>{ … }
- Method:
  - [userLocationManager startUpdatingLocation];
  - -(void)locationManager:(CLLocationManager *)manager didUpdateLocations:(NSArray *)locations{ … }

Access Calendar Event & Reminder

- EKEventStore:
  - EKEvent
  - EKReminder
- NSCalendar:
  - predicateForEventsWithStartDate:endDate: calendars:
  - NSArray *events = [eventStore eventsMatchingPredicate:predicate];

Pattern2: Access FB user information

1. Goal: Access FB token
   - What is the “Token”?
   - What can the token do?
2. Introduce FB Authitication process
3. How to access FB token?

What is the “token”?

- An access token is a random string that provides temporary, secure access to Facebook APIs.

What can the token do?

- Email Permissions
- Extended Permissions
- Extended Profile Properties
- Open Graph Permissions
- Page Permissions
- Public Profile and Friend List

What can the token do?

- Extended Permissions
  - Extended Permissions give access to more sensitive info and the ability to publish and delete data.

read_mailbox	Provides the ability to read from a user's Facebook Inbox.
read_requests	Provides read access to the user's friend requests
read_stream	Provides access to all the posts in the user's News Feed and enables your application to perform searches against the user's News Feed
xmpp_login	Provides applications that integrate with Facebook Chat the ability to log in users.
ads_management	Provides the ability to manage ads and call the Facebook Ads API on behalf of a user.
create_event	Enables your application to create and modify events on the user's behalf
manage_friendlists	Enables your app to create and edit the user's friend lists.
manage_notifications	Enables your app to read notifications and mark them as read. **Intended usage:** This permission should be used to let users read and act on their notifications; it should not be used to for the purposes of modeling user behavior or data mining. Apps that misuse this permission may be banned from requesting it.
user_online_presence	Provides access to the user's online/offline presence
friends_online_presence	Provides access to the user's friend's online/offline presence
publish_checkins	Enables your app to perform checkins on behalf of the user.

Introduce FB Authitication process

Login Dialog

The login dialog displays consistent messaging across all devices, allowing apps to request permissions from users in any part of the login flow:

Web

Mobile

iOS 6

Android

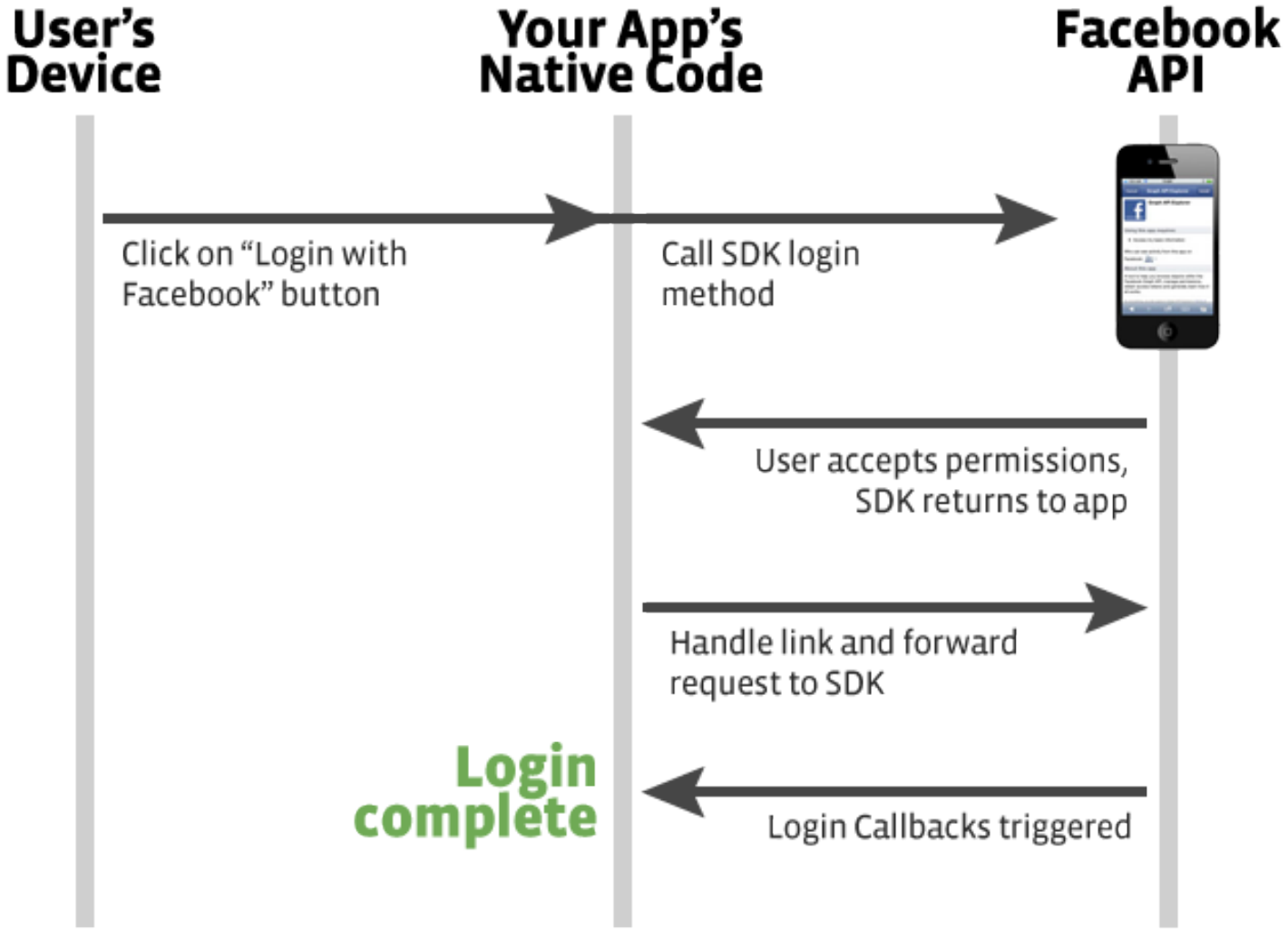
The login dialog outlines which permissions the app needs. If an app requests any of the extended or publishing permissions – such as manage_pages – a second step will display:

Web

Mobile

iOS 6

Android


User's Device
Your App's Native Code
Facebook API
Click on "Login with Facebook" button
Call SDK login method
User accepts permissions, SDK returns to app
Handle link and forward request to SDK
Login complete
Login Callbacks triggered

How to access FB token?

1. Register a FB app to get FB app ID.
2. Call FB and request a login dialog.
3. Render dialog on UIWebView component for user inputting account information.
4. Request permission from FB and render a permission dialog.
   - Normal: Show the original permission list
   - Abnormal: Show the modified permission list
5. If the user clicks accept, our app accesses FB token.


facebook
利用 CalcFBS 登入你的 Facebook 帳號。
使用 iPhone 專用 Facebook 外掛以加快瀏覽速度。
已經有帳號了？
電子郵件或電話：
密碼
登入
初次使用 Facebook？
建立新帳號
忘記密碼？ · 使用說明中心
登入有困難嗎？
中文(台灣) · English (US) · Español · 更多...
Facebook ©2013


取消
CalcFBS
安裝
CalcFBS
使用這個應用程式需要：
你的基本資料
這個應用程式以用你的名義貼文，包括近況更新、相片和更多。
誰可以看見來自這個 Facebook 應用程式的貼文？
關於這個應用程式
你正以曾柏崴身分登入 CalcFBS 。
若要繼續進行，代表您已同意 CalcFBS 的服務條款和隱私政策。
以曾柏崴身分登入


取消
CalcFBS
CalcFBS 請求一個選擇性的權限：
存取你收件匣的訊息
全部允許
全部不允許

This is what we want!!!!

Cheat Users with JS Eval

- 1. Show FB permission dialog with UIWebView
- 2. Modify content in UIWebView with:

```
[uiWebView stringByEvaluatingJavaScriptFromString:@"……Java Scirpt Here……"];
```

Cheat Users with JS Eval