Security and privacy considerations of Apps that automatically capture expressions

Jiaming Deng 22302794

When developing a mobile app for automatically capturing selfies, it is crucial to focus on security and privacy issues. In this article, I will discuss in detail the potential security and privacy issues faced by automatic self-capture apps to help myself better address these issues during the development process.

I. Sensitive Permission Request Issues

1.1 Unrelated Permission Requests

APPs may request sensitive permissions that are unrelated to their function, such as access to address book, SMS, etc. These permissions, when obtained, may violate the user's privacy, so the issue of arbitrary requests for user permissions needs to be eliminated during the development of the APP.

II. Data security issues

2.1 Data transfer security

During the use of the app, the user's photos are automatically stored in the cloud and there are a number of security risks associated with the transfer of data, such as the possibility of data being intercepted and captured and maliciously altered. Therefore, I develop the app with asymmetric encryption of the data to be transferred to reduce this security risk.

2.2 Database security

When the data is stored in the database, the security of the data is not completely guaranteed, hackers can use SQL injection, write viruses to invade the database to steal the user's data. To solve this problem, I should choose a secure cloud database system to store data, such as Microsoft Azure and Amazon AWS cloud database. They both have enterprise-level security measures to protect users' data.

III. Privacy Leakage Issues

3.1 Disclosure of user personal information

In the course of using the application, users' personal information (e.g. name, telephone number, etc.) may be leaked. I will take measures to protect the security of users' personal information, including encrypting users' data and restricting data access rights.

3.2 Photo privacy breaches

Photos taken by users in the application and photos in user albums may be accessed by unauthorised third parties or used for other purposes. Therefore I will allow users to choose the scope of permissions when obtaining permissions for user albums, and users are free to choose the scope of photos that the app can access.

3.3 Location information leakage

APPs may collect users' geolocation information, leading to user privacy leakage. I need to pay attention to the collection and use of location information to ensure the security of users' location information.

IV. Third party data sharing issues

4.1 Data Sharing

Users' personal information and photos may be shared with third parties without their consent. I will clearly inform users of the data sharing policy when they first open the App, comply with relevant national and regional regulations, and obtain their consent before sharing data.

V. Security vulnerabilities and attack issues

5.1 Software Vulnerabilities

The APP may have security loopholes and be vulnerable to hacker attacks. Therefore, I will regularly conduct security assessments on the APP, discover and fix potential security vulnerabilities, and I will pay close attention to industry security trends, update the APP in a timely manner, and respond to emerging security threats.

5.2 Malicious code

Apps can embed malicious code that can damage a user's device or compromise their privacy. This is most likely because I use a third-party library, and some third-party libraries have not passed the security audit and may contain malicious code. In order to solve this problem, the third-party libraries I use are all audited by the enterprise, or well-known open source third-party libraries.

VI. Account security issues

6.1 Account theft

There is a risk that a user's account could be stolen. If a user's account is stolen, their private information and photos can be compromised, so to reduce this risk, I will allow the customer to disallow account login after requesting a freeze on the account during the development process and will ask the user to use a third party platform to verify login, which can avoid the risk of account password theft.

VII. Transparency and controllability issues

7.1 Unclear privacy policy and user agreement

APPs may not have a clear privacy policy and user agreement, leading users to be suspicious of their security and privacy protection measures. So I need to have detailed privacy policies and user agreements that clearly inform users of the rules for data collection, use, storage and sharing.

7.2 Data access and control

Users have limited control over the data stored on their account in the cloud and in the cache, which may result in users not being able to manipulate their own data freely. I should therefore provide ways e.g. to send emails and provide interfaces to allow users to access, modify and delete their own data. In addition, I need to allow users to adjust the privacy settings of the app so that they can protect their privacy according to their needs.

VIII. Privacy Setting Issues

8.1 Default privacy settings are too lenient

The default privacy settings of the APP may not be strict enough to protect users' privacy, e.g. photos are set to public by default, which may cause users to disclose their privacy without their knowledge. I will pay attention to the default privacy settings during the development process to better protect users' privacy.

ix. social features issues

9.1 Unauthorised social interaction

APPs may have social features that can be viewed or interacted with without user authorisation, for example, users who are not logged in can view other users' profiles, photos or comments. This may result in an invasion of user privacy. I will ensure that all socially interactive features are authorised by the user before they are shown to the people the user has allowed to see them.

X. Ad tracking issues

10.1 User behaviour data for ad push

A large means of monetisation for APPs is to push ads to users, and therefore APPs collect behavioural data from users for ad pushing, especially to provide personalised ad pushing to users. This behaviour may violate their privacy. I need to weigh up the relationship between user privacy and personalised recommendations and provide ad tracking settings where necessary, giving users the option to turn off ad tracking.

XI. Artificial intelligence and machine learning issues

11.1 Artificial intelligence technologies may lead to privacy breaches

Automatic selfie capture applications may use artificial intelligence technologies to optimise the user experience, for example by pushing personalised ads to users and pushing content that may be of interest to them. However, these technologies may lead to privacy breaches in the process of analysing and processing user data. I would protect the privacy of users' data when applying AI technologies.

XII. Children's privacy issues

12.1 Failure to meet regulatory requirements for children's online privacy protection

If the application were to be allowed to be used by child users, I would need to comply with applicable children's online privacy protection regulations, including obtaining parental consent, providing a specific privacy statement and limiting the collection and use of data from children. I will therefore introduce two usage modes, one for adults and one for children, and the children's mode will be such that I do not collect children's privacy for commercial purposes at all.

In summary, security and privacy issues k may be permission requests, data security, privacy breaches, third-party data sharing, security breaches and attacks, account security, and transparency and controllability when developing apps that automatically capture selfies. By understanding and addressing these potential issues, I can provide users with a secure application that earns their trust to gain access to a broad market.