信息安全前沿课堂讨论

陆皓喆 2211044 网络空间安全学院

2023 年 12 月 19 日

3 Android APP 隐私泄露的危害、常见模式和保护机制？

安卓的 APP 具有使用者的许多隐私，一不注意，就会导致自己的隐私的泄露，危害重大。下面我就简单的介绍一下隐私泄露的危害、隐私泄露的常见模式与其对应的保护机制。

隐私泄露的危害有很多，以下是常见的四条。

1. 个人隐私泄露：用户的个人信息如姓名、地址、电话号码等可能被泄露，导致身份盗窃、骚扰等问题。比如说在某些不良 APP 上填写个人信息；在商家处填写个人信息然后商家反手以此为盈利等等。

其中包括许多种形式的泄露，比如说数据收集和存储。很多应用会收集用户的个人信息，如姓名、地址、电话号码等。问题在于这些数据如何被处理和存储。如果应用没有采取足够的安全措施，这些信息可能容易受到黑客攻击，导致泄露。还有可能造成敏感权限滥用，一些应用可能请求过多的敏感权限，这些权限超出了应用正常运行所需的范围。例如，一个不相关的应用请求访问用户的通讯录、相机、麦克风等权限，可能是在滥用隐私。更加严重的，还有第三方数据分享。应用可能与第三方合作伙伴分享用户数据，而用户可能对此一无所知。这种数据共享可能违反用户的隐私权，尤其是当用户没有明确同意分享数据时。

2. 位置隐私泄露：用户的实时或历史位置信息泄露可能导致跟踪、监视，侵犯用户的安全和隐私。比如说滴滴打车等打车平台实际上是拥有你的实时行进路径的，不法分子可以利用你的路线，使你的人身安全得到威胁。

3. 通信隐私泄露：通信记录、短信、电话等信息泄露可能导致用户被钓鱼、诈骗等威胁。平时我们会受到很多的广告电话、诈骗电话，这可能都跟这些有关系。

4. 个性化广告滥用：收集用户信息用于个性化广告可能引起用户反感，尤其是在未经允许的情况下进行。比如说某些 APP 会给你推荐一些广告，会引起一些反感。

生活中，有许多隐私的泄露常见方式，我们介绍以下的 4 种。

1. 未经授权的数据收集：应用程序未经用户同意收集、存储或传输用户数据。

2. 缺乏加密：数据在传输或存储时没有进行足够的加密，容易被非法访问。

3. 第三方库隐私问题：应用使用的第三方库可能存在隐私问题，例如过度的数据收集。

4. 权限滥用：应用请求不必要的权限，以获取对用户隐私的不当访问。

当然，我们也有许多的途径去进行隐私保护，我们介绍以下的七种方法。

1. 权限控制：应用应该仅请求其正常运行所需的最小权限，并在不需要时撤销权限。

2. 数据加密：对于敏感数据，使用适当的加密算法进行保护，包括在传输和存储过程中。

3. 隐私政策和用户协议：提供清晰、透明的隐私政策，告知用户数据的收集和使用方式。

4. 用户同意和选择权：在数据收集前获得用户的明确同意，让用户能够选择分享哪些信息。

5. 安全更新和维护：及时更新应用程序以修复已知的安全漏洞，并确保使用最新的安全标准。

6. 审查第三方库：审查并确保使用的第三方库是安全可靠的，不会泄露用户隐私。

7. 用户教育：向用户提供关于隐私保护的信息，使其更加警觉和自我保护。

总体而言，开发人员应该在应用程序设计和开发的各个阶段都考虑隐私保护，采用合适的技术和最佳实践来确保用户的隐私得到有效保护; 作为程序的使用者，我们也应该在平时的使用过程中，多修改密码，平时少填写一些自身的相关的信息，这样就可以减少个人隐私的传播与泄露。