



Security tips for android app

Presented by iTrobes



introduction

- Mobile app users often worry about their data privacy and safety.
- If you are an app developer, it is must that you follow certain security practices.
- We, iTrobes Technologies, as an experienced android app development company, share with you the most important security tips here.
- By following these, you can assure your users the privacy and data security and make them build trust with your brand.



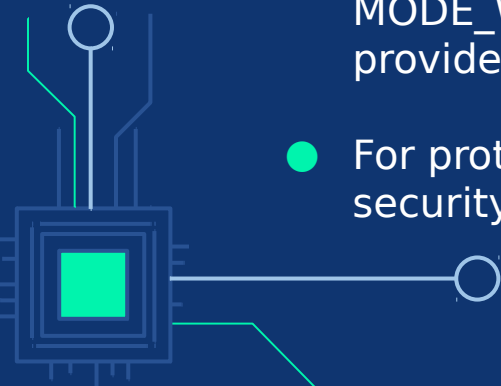
Data storage security



Internal storage



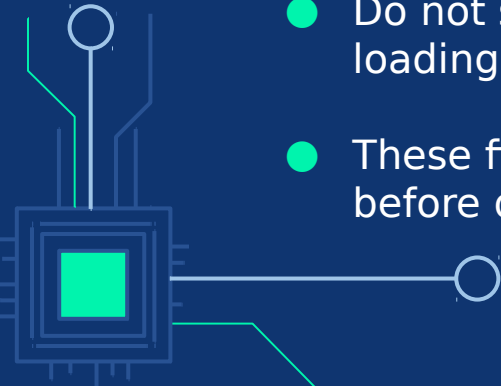
- Internal storage offers more security by default.
- Android built-in features would be sufficient for most apps.
- Avoid `MODE_WORLD_WRITEABLE` or `MODE_WORLD_READABLE` modes for IPC files as they don't provide ability to limit data access.
- For protection to sensitive data, encrypt local files using the security library.



external storage



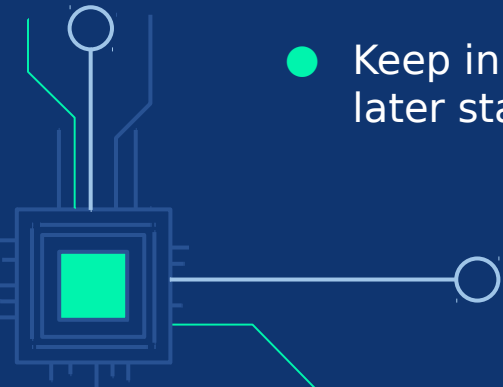
- These are globally readable and writable. Eg. SD cards.
- Do not store sensitive data in external storage as they can be removed by the users and modified by any application.
- Do not store executable files or class files prior to dynamic loading.
- These files should be signed and cryptographically verified before dynamic loading.



Content providers



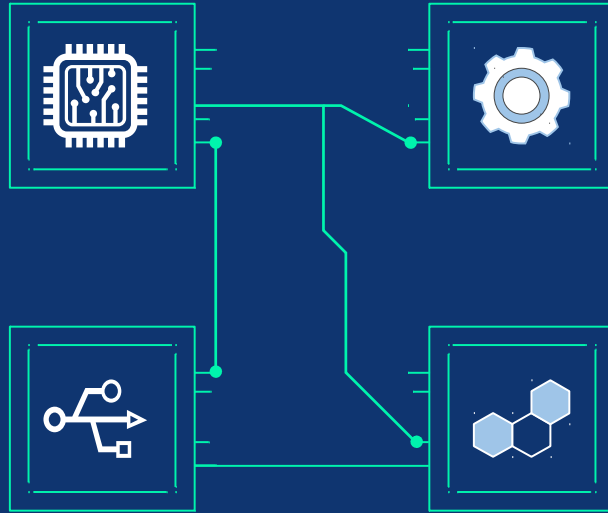
- Data access can be limited to only your own app or can be exported to other apps.
- Use `android:exported=true` in the manifest to allow access to other apps and `android:exported=false` to restrict access.
- Keep in mind that it's easier to grant new permissions in the later stage than to remove the existing ones.



Secure network transaction

Ip networking
Use appropriate protocols for sensitive data

Sslsocket
Authenticated, encrypted communication



Android ipc

Go with built-in Android IPC mechanism

Secure traffic
Always use Https URLConnection over HTTP

Limited permissions



- Request only the permissions that your app absolutely need to function.
- Restrict sensible permissions to make your app less vulnerable to for attackers.
- When you provide android app development services for your clients, you need to make sure you build a secure app for them and their users.



Proper input validation



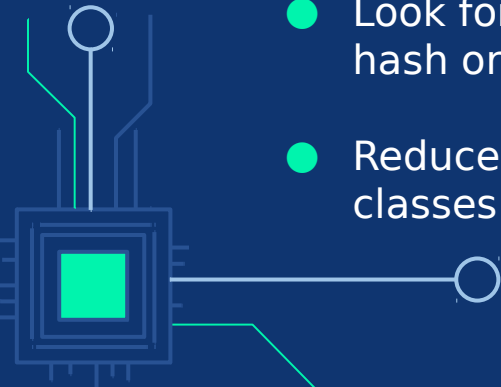
- Insufficient input validation leads to many security risks. Eg. buffer overflows, use after free, off-by-one error.
- Android provides platform-level countermeasures like ASLR, DEP to tackle these issues.
- You should handle pointers carefully and manage buffers to prevent such security threats.



User data handling



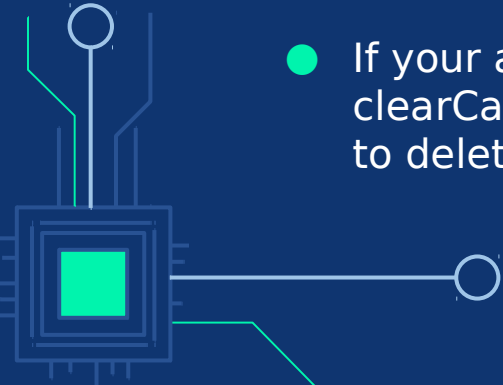
- Limit the use of APIs that access sensitive or personal user data.
- If possible, avoid storing or transmitting your user data.
- Look for the ways to implement your application logic using a hash or non-reversible form of the data.
- Reduce your log usage. Use debug flags and custom log classes.



Web security

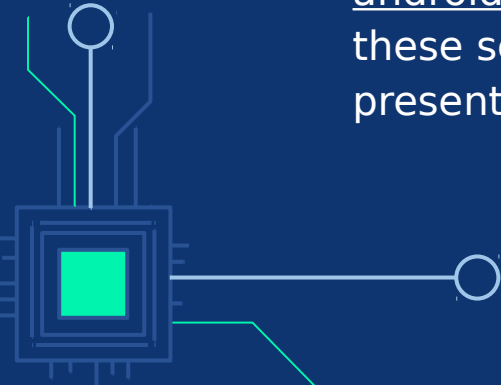


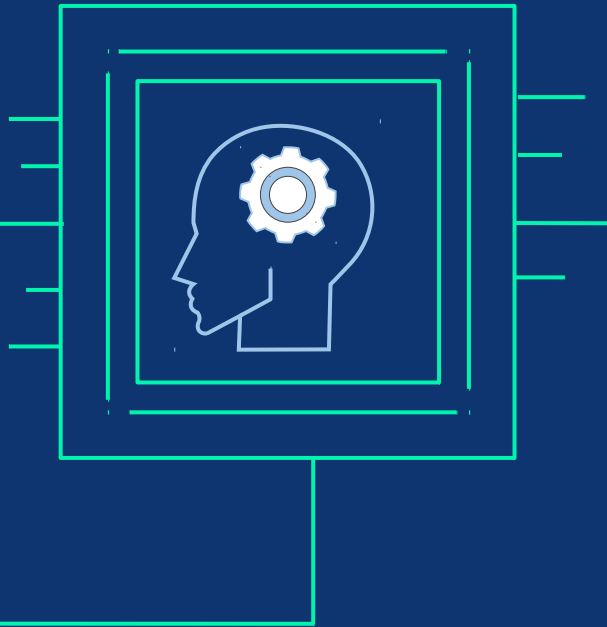
- Be cautious when using a WebView component to avoid web security issues.
- A WebView component consumes web content such as HTML, and JavaScript.
- If your app access sensitive data using WebView, use `clearCache()` to delete any locally stored files.



conclusion

People are increasingly aware of the security threats their mobile devices possess and are very concerned over the safety of their data. Anything you do to ensure data privacy will enormously impact on your app's success rate. So, an android app development company should not miss to ensure these security practices that are discussed in this presentation.

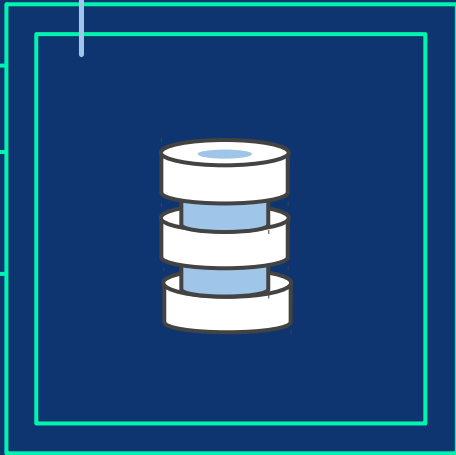




About us

iTobes is a 360-degree software solutions company. We help businesses with web design and development, mobile app (Android, iOS, hybrid) development, custom software solutions, and complete digital transformation services.

OUR services



- Mobile App Development
- Android App Development
- IOS App Development
- Hybrid App Development
- Custom Software Development
- Domain and Hosting
- Web Development
- eCommerce Development
- Software Consulting



OUR products

- Accounting Software
- HRMS Software
- Procurement Software
- Sales Software
- Customer Management System



thanks!



Any questions?

Reach us at info@itrobes.com

www.itrobes.com

[itrobes2018](#)

