App security best practices

By making your app more secure, you help preserve user trust and device integrity.

This page presents several best practices that have a significant, positive impact on your app's security.

Enforce secure communication

When you safeguard the data that you exchange between your app and other apps, or between your app and a website, you improve your app's stability and protect the data that you send and receive.

Use implicit intents and non-exported content providers

Show an app chooser

If an implicit intent can launch at least two possible apps on a user's device, explicitly show an app chooser. This interaction strategy allows users to transfer sensitive information to an app that they trust.

Kotlin (#kotlin)Java (#java)

```
Intent intent = new Intent(Intent.ACTION_SEND);
List<ResolveInfo> possibleActivitiesList = getPackageManager()
        .queryIntentActivities(intent, PackageManager.MATCH_ALL);

// Verify that an activity in at least two apps on the user's device
// can handle the intent. Otherwise, start the intent only if an app
// on the user's device can handle the intent.
if (possibleActivitiesList.size() > 1) {

    // Create intent to show chooser.
    // Title is something similar to "Share this photo with".

    String title = getResources().getString(R.string.chooser_title);
    Intent chooser = Intent.createChooser(intent, title);
    startActivity(chooser);
} else if (intent.resolveActivity(getPackageManager()) != null) {
    startActivity(intent);
}
```

Related info:

- Show an App Chooser (/training/basics/intents/sending#AppChooser)
- `Intent` (/reference/android/content/Intent)

Apply signature-based permissions

When sharing data between two apps that you control or own, use *signature-based* permissions. These permissions don't require user confirmation and instead check that the apps accessing the data are signed using the same signing key. Therefore, these permissions offer a more streamlined, secure user experience.

```
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="com.example.myapp">
    <permission android:name="my_custom_permission_name"
                android:protectionLevel="signature" />
```

Related info:

- Sign Your App (/studio/publish/app-signing)
- `android:protectionLevel` (/guide/topics/manifest/permission-element#plevel)

Disallow access to your app's content providers

Unless you intend to send data from your app to a different app that you don't own, you should explicitly disallow other developers' apps from accessing the `ContentProvider` (/reference/android/content/ContentProvider) objects that your app contains. This setting is particularly important if your app can be installed on devices running Android 4.1.1 (API level 16) or lower, as the `android:exported` (/guide/topics/manifest/provider-element#exported) attribute of the `<provider>` (/guide/topics/manifest/provider-element) element is `true` by default on those versions of Android.

```
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="com.example.myapp">
    <application ... >
        <provider
            android:name="android.support.v4.content.FileProvider"
            android:authorities="com.example.myapp.fileprovider"
            ...
            android:exported="false">
            <!-- Place child elements of <provider> here. -->
        </provider>
        ...
    </application>
</manifest>
```

Ask for credentials before showing sensitive information

When requesting credentials from users so that they can access sensitive information or premium content in your app, ask for either a PIN/password/pattern or a biometric credential, such as using face recognition or fingerprint recognition.

To learn more about how to request biometric credentials, see the guide about biometric authentication (/training/sign-in/biometric-auth).

Apply network security measures

The following sections describe how you can improve your app's network security.

Use SSL traffic

If your app communicates with a web server that has a certificate issued by a well-known, trusted CA, the HTTPS request is very simple:

Kotlin (#kotlin)Java (#java)

```
URL url = new URL("https://www.google.com");
HttpsURLConnection urlConnection = (HttpsURLConnection) url.openConnection();
urlConnection.connect();
InputStream in = urlConnection.getInputStream();
```

Add a network security configuration

If your app uses new or custom CAs, you can declare your network's security settings in a configuration file. This process allows you to create the configuration without modifying any app code.

To add a network security configuration file to your app, follow these steps:

1. Declare the configuration in your app's manifest:

```
<manifest ... >
    <application
        android:networkSecurityConfig="@xml/network_security_config"
        ... >
        <!-- Place child elements of <application> element here. -->
    </application>
</manifest>
```

2. Add an XML resource file, located at `res/xml/network_security_config.xml`.

   Specify that all traffic to particular domains should use HTTPS by disabling clear-text:

```
<network-security-config>
    <domain-config cleartextTrafficPermitted="false">
        <domain includeSubdomains="true">secure.example.com</domain>
        ...
    </domain-config>
</network-security-config>
```

   During the development process, you can use the `<debug-overrides>` element to explitiicly allow user-installed certificates. This element overrides your app's security-critical options during debugging and testing without affecting the app's release configuration. The following snippet shows how to define this element in your app's network security configuration XML file:

```
<network-security-config>
    <debug-overrides>
        <trust-anchors>
            <certificates src="user" />
        </trust-anchors>
    </debug-overrides>
</network-security-config>
```

Related info: Network Security Configuration (/training/articles/security-config)

Create your own trust manager

Your SSL checker shouldn't accept every certificate. You may need to set up a trust manager and handle all SSL warnings that occur if one of the following conditions applies to your use case:

- You're communicating with a web server that has a certificate signed by a new or custom CA.
- That CA isn't trusted by the device you're using.
- You cannot use a network security configuration (#network-security-config).

To learn more about how to complete these steps, see the discussion about handling an unknown cerificate authority (/training/articles/security-ssl#UnknownCa).

Related info:

- Security with HTTPS and SSL (https://developer.android.com/training/articles/security-ssl.html)
- `CertificateFactory` (/reference/java/security/cert/CertificateFactory)

- `HttpsURLConnection` (/reference/javax/net/ssl/HttpsURLConnection)
- `TrustManager` (/reference/javax/net/ssl/TrustManager)

Use WebView objects carefully

Whenever possible, load only allowlisted content in `WebView` (/reference/android/webkit/WebView) objects. In other words, the `WebView` (/reference/android/webkit/WebView) objects in your app shouldn't allow users to navigate to sites that are outside of your control.

In addition, you should never enable JavaScript interface support (/guide/webapps/webview#UsingJavaScript) unless you completely control and trust the content in your app's `WebView` (/reference/android/webkit/WebView) objects.

Use HTML message channels

If your app must use JavaScript interface support on devices running Android 6.0 (API level 23) and higher, use HTML message channels instead of communicating between a website and your app, as shown in the following code snippet:

Kotlin (#kotlin)Java (#java)

```
WebView myWebView = (WebView) findViewById(R.id.webview);

// channel[0] and channel[1] represent the two ports.
// They are already entangled with each other and have been started.
WebMessagePort[] channel = myWebView.createWebMessageChannel();

// Create handler for channel[0] to receive messages.
channel[0].setWebMessageCallback(new WebMessagePort.WebMessageCallback() {
    @Override
    public void onMessage(WebMessagePort port, WebMessage message) {
         Log.d(TAG, "On port " + port + ", received this message: " + message);
    }
});

// Send a message from channel[1] to channel[0].
channel[1].postMessage(new WebMessage("My secure message"));
```

Related info:

- `WebMessage` (/reference/android/webkit/WebMessage)
- `WebMessagePort` (/reference/android/webkit/WebMessagePort)

Provide the right permissions

Your app should request only the minimum number of permissions necessary to function properly. When possible, your app should relinquish some of these permissions when they're no longer needed.

Use intents to defer permissions

Whenever possible, don't add a permission to your app to complete an action that could be completed in another app. Instead, use an intent to defer the request to a different app that already has the necessary permission.

The following example shows how to use an intent to direct users to a contacts app instead of requesting the `READ_CONTACTS` (/reference/android/Manifest.permission#READ_CONTACTS) and `WRITE_CONTACTS` (/reference/android/Manifest.permission#WRITE_CONTACTS) permissions:

Kotlin (#kotlin) Java (#java)

```
// Delegates the responsibility of creating the contact to a contacts app,
// which has already been granted the appropriate WRITE_CONTACTS permission.
Intent insertContactIntent = new Intent(Intent.ACTION_INSERT);
insertContactIntent.setType(ContactsContract.Contacts.CONTENT_TYPE);

// Make sure that the user has a contacts app installed on their device.
if (insertContactIntent.resolveActivity(getPackageManager()) != null) {
    startActivity(insertContactIntent);
}
```

In addition, if your app needs to perform file-based I/O—such as accessing storage or choosing a file—it doesn't need special permissions because the system can complete the operations on your app's behalf. Better still, after a user selects content at a particular URI, the calling app gets granted permission to the selected resource.

Related info:

- Common Intents (/guide/components/intents-common)
- `Intent` (/reference/android/content/Intent)

Share data securely across apps

Follow these best practices in order to share your app's content with other apps in a more secure manner:

- Enforce read-only or write-only permissions as needed.
- Provide clients one-time access to data by using the `FLAG_GRANT_READ_URI_PERMISSION` (/reference/android/content/Intent#FLAG_GRANT_READ_URI_PERMISSION) and `FLAG_GRANT_WRITE_URI_PERMISSION` (/reference/android/content/Intent#FLAG_GRANT_WRITE_URI_PERMISSION) flags.
- When sharing data, use "content://" URIs, not "file://" URIs. Instances of `FileProvider` (/reference/androidx/core/content/FileProvider) do this for you.

The following code snippet shows how to use URI permission grant flags and content provider permissions to display an app's PDF file in a separate PDF Viewer app:

Kotlin (#kotlin) Java (#java)

```
// Create an Intent to launch a PDF viewer for a file owned by this app.
Intent viewPdfIntent = new Intent(Intent.ACTION_VIEW);
viewPdfIntent.setData(Uri.parse("content://com.example/personal-info.pdf"));

// This flag gives the started app read access to the file.
viewPdfIntent.addFlags(Intent.FLAG_GRANT_READ_URI_PERMISSION);

// Make sure that the user has a PDF viewer app installed on their device.
if (viewPdfIntent.resolveActivity(getPackageManager()) != null) {
    startActivity(viewPdfIntent);
}
```

Note: Untrusted apps that target Android 10 (API level 29) and higher can't invoke **`exec()`** on files within the app's home directory. This execution of files from the writable app home directory is a W^X violation (https://en.wikipedia.org/wiki/W%5EX). Apps should load only the binary code that's embedded within an app's APK file. In addition, apps that target Android 10 and higher cannot in-memory modify executable code from files which have been opened with **`dlopen()`**. This includes any shared object (**`.so`**) files with text relocations.

Related info: `android:grantUriPermissions` (/guide/topics/manifest/provider-element#gprmsn)

Store data safely

Although your app might require access to sensitive user information, your users will grant your app access to their data only if they trust that you'll safeguard it properly.

Store private data within internal storage

Store all private user data within the device's internal storage, which is sandboxed per app. Your app doesn't need to request permission to view these files, and other apps cannot access the files. As an added security measure, when the user uninstalls an app, the device deletes all files that the app saved within internal storage.

Note: If the data that you're storing is particularly sensitive or private, consider working with **`EncryptedFile`** (/reference/androidx/security/crypto/EncryptedFile) objects, which are available from the Security library (/topic/security/data), instead of **`File`** objects.

The following code snippet demonstrates one way to write data to storage:

Kotlin (#kotlin)Java (#java)

```
Context context = getApplicationContext();

// Although you can define your own key generation parameter specification, it's
// recommended that you use the value specified here.
KeyGenParameterSpec keyGenParameterSpec = MasterKeys.AES256_GCM_SPEC;
String mainKeyAlias = MasterKeys.getOrCreate(keyGenParameterSpec);

// Create a file with this name, or replace an entire existing file
// that has the same name. Note that you cannot append to an existing file,
// and the file name cannot contain path separators.
String fileToWrite = "my_sensitive_data.txt";
EncryptedFile encryptedFile = new EncryptedFile.Builder(
        new File(DIRECTORY, fileToWrite),
        context,
        mainKeyAlias,
        EncryptedFile.FileEncryptionScheme.AES256_GCM_HKDF_4KB
).build();

byte[] fileContent = "MY SUPER-SECRET INFORMATION"
        .getBytes(StandardCharsets.UTF_8);
OutputStream outputStream = encryptedFile.openFileOutput();
outputStream.write(fileContent);
outputStream.flush();
outputStream.close();
```

The following code snippet shows the inverse operation, reading data from storage:

Kotlin (#kotlin)Java (#java)

```
Context context = getApplicationContext();

// Although you can define your own key generation parameter specification, it's
// recommended that you use the value specified here.
KeyGenParameterSpec keyGenParameterSpec = MasterKeys.AES256_GCM_SPEC;
String mainKeyAlias = MasterKeys.getOrCreate(keyGenParameterSpec);

String fileToRead = "my_sensitive_data.txt";
EncryptedFile encryptedFile = new EncryptedFile.Builder(
```

```
        new File(DIRECTORY, fileToRead),
        context,
        mainKeyAlias,
        EncryptedFile.FileEncryptionScheme.AES256_GCM_HKDF_4KB
).build();

InputStream inputStream = encryptedFile.openFileInput();
ByteArrayOutputStream byteArrayOutputStream = new ByteArrayOutputStream();
int nextByte = inputStream.read();
while (nextByte != -1) {
    byteArrayOutputStream.write(nextByte);
    nextByte = inputStream.read();
}

byte[] plaintext = byteArrayOutputStream.toByteArray();
```

Related info:

- Using the Internal Storage (/guide/topics/data/data-storage#filesInternal)
- `FileInputStream` (/reference/java/io/FileInputStream)
- `FileOutputStream` (/reference/java/io/FileOutputStream)
- `Context.MODE_PRIVATE` (/reference/android/content/Context#MODE_PRIVATE)

Store data in external storage based on use case

Use external storage for large, non-sensitive files that are specific to your app, as well as files that your app shares with other apps. The specific APIs that you use depend on whether your app is designed to access app-specific files (#external-storage-access-app-specific) or access shared files (#external-storage-access-shared).

Check availability of storage volume

If your app interacts with a removable external storage device, keep in mind that the user might remove the storage device while your app is trying to access it. Include logic to verify that the storage device is available (/training/data-storage/app-specific#external-verify-availability).

Access app-specific files

If a file doesn't contain private or sensitive information but provides value to the user only in your app, store the file in an app-specific directory on external storage (/training/data-storage/app-specific#external).

Access shared files

If your app needs to access or store a file that provides value to other apps, use one of the following APIs depending on your use case:

- **Media files:** To store and access images, audio files, and videos that are shared between apps, use the Media Store API (/training/data-storage/shared/media).
- **Other files:** To store and access other types of shared files, including downloaded files, use the Storage Access Framework (/training/data-storage/shared/documents-files).

Check validity of data

If your app uses data from external storage, make sure that the contents of the data haven't been corrupted or modified. Your app should also include logic to handle files that are no longer in a stable format.

An example of a hash verifier appears in the following code snippet:

Kotlin (#kotlin)Java (#java)

```
Executor threadPoolExecutor = Executors.newFixedThreadPool(4);
private interface HashCallback {
    void onHashCalculated(@Nullable String hash);
}

boolean hashRunning = calculateHash(inputStream, threadPoolExecutor, hash -> {
    if (Objects.equals(hash, expectedHash)) {
        // Work with the content.
    }
});

if (!hashRunning) {
    // There was an error setting up the hash function.
}

private boolean calculateHash(@NonNull InputStream stream,
                              @NonNull Executor executor,
                              @NonNull HashCallback hashCallback) {
    final MessageDigest digest;
    try {
        digest = MessageDigest.getInstance("SHA-512");
    } catch (NoSuchAlgorithmException nsa) {
        return false;
    }

    // Calculating the hash code can take quite a bit of time, so it shouldn't
    // be done on the main thread.
    executor.execute(() -> {
        String hash;
        try (DigestInputStream digestStream =
                new DigestInputStream(stream, digest)) {
            while (digestStream.read() != -1) {
                // The DigestInputStream does the work; nothing for us to do.
            }
            StringBuilder builder = new StringBuilder();
            for (byte aByte : digest.digest()) {
                builder.append(String.format("%02x", aByte)).append(':');
            }
            hash = builder.substring(0, builder.length() - 1);
        } catch (IOException e) {
            hash = null;
        }

        final String calculatedHash = hash;
        runOnUiThread(() -> hashCallback.onHashCalculated(calculatedHash));
    });
    return true;
}
```

Store only non-sensitive data in cache files

To provide quicker access to non-sensitive app data, store it in the device's cache. For caches larger than 1 MB in size, use `getExternalCacheDir()` (/reference/android/content/Context#getExternalCacheDir()); otherwise, use `getCacheDir()` (/reference/android/content/Context#getCacheDir()). Each method provides you with the `File` (/reference/java/io/File) object that contains your app's cached data.

The following code snippet shows how to cache a file that your app recently downloaded:

Kotlin (#kotlin)Java (#java)

```
File cacheDir = getCacheDir();
File fileToCache = new File(myDownloadedFileUri);
String fileToCacheName = fileToCache.getName();
File cacheFile = new File(cacheDir.getPath(), fileToCacheName);
```

Note: If you use `getExternalCacheDir()` (/reference/android/content/Context#getExternalCacheDir()) to place your app's cache within shared storage, the user might eject the media containing this storage while your app is running. You should include logic to gracefully handle the cache miss that this user behavior causes.

Caution: There is no security enforced on these files. Therefore, any app that targets Android 10 (API level 29) or lower and has the `WRITE_EXTERNAL_STORAGE` (/reference/android/Manifest.permission#WRITE_EXTERNAL_STORAGE) permission can access the contents of this cache.

Related info: Saving cache files (/guide/topics/data/data-storage#InternalCache)

Use SharedPreferences in private mode

When using `getSharedPreferences()` (/reference/android/content/Context#getSharedPreferences(java.lang.String, int)) to create or access your app's `SharedPreferences` (/reference/android/content/SharedPreferences) objects, use `MODE_PRIVATE` (/reference/android/content/Context#MODE_PRIVATE). That way, only your app can access the information within the shared preferences file.

If you want to share data across apps, don't use `SharedPreferences` (/reference/android/content/SharedPreferences) objects. Instead, you should follow the necessary steps to share data securely across apps (#permissions-share-data).

Related info: Using Shared Preferences (/guide/topics/data/data-storage#pref)

Keep services and dependencies up-to-date

Most apps use external libraries and device system information to complete specialized tasks. By keeping your app's dependencies up to date, you make these points of communication more secure.

Check the Google Play services security provider

Note: This section applies only to apps targeting devices that have Google Play services (https://developers.google.com/android/guides/overview) installed.

If your app uses Google Play services, make sure that it's updated on the device where your app is installed. This check should be done asynchronously, off of the UI thread. If the device isn't up-to-date, your app should trigger an authorization error.

To determine whether Google Play services is up to date on the device where your app is installed, follow the steps in the guide for Updating Your Security Provider to Protect Against SSL Exploits (/training/articles/security-gms-provider).

Related info:

- `ProviderInstaller` (https://developers.google.com/android/reference/com/google/android/gms/security/ProviderInstaller)
- `ProviderInstaller.ProviderInstallListener` (https://developers.google.com/android/reference/com/google/android/gms/security/ProviderInstaller.ProviderInstallListener)

Update all app dependencies

Before deploying your app, make sure that all libraries, SDKs, and other dependencies are up to date:

- For first-party dependencies, such as the Android SDK, use the updating tools found in Android Studio, such as the SDK Manager (/studio/intro/update#sdk-manager).
- For third-party dependencies, check the websites of the libraries that your app uses, and install any available updates and security patches.

Related info: Add Build Dependencies (/studio/build/dependencies#google_and_android_support_repositories)

More information

To learn more about how to make your app more secure, view the following resources:

- Core app quality security checklist (/distribute/essentials/quality/core#sc)
- App Security Improvement (ASI) Program (/google/play/asi)
- Android Developers channel on YouTube (https://www.youtube.com/user/androiddevelopers)

Additional resources

For more information about making your app more secure, consult the following resources.

Codelabs

- Android Network Security Configuration (/codelabs/android-network-security-config#0)

Blogs

- Android Protected Confirmation: Taking transaction security to the next level (https://android-developers.googleblog.com/2018/10/android-protected-confirmation.html)

Last updated 2022-09-19 UTC.