Emerging Technologies: Mobile Development for Android Devices

Security

Introduction

- linux
- Access control file permissions
- Sandboxing
- Storage
- The manifest file
- Whitelisting/Blacklisting
- Default permissions
- Security: Areas of focus

Permissions on Linux

- Android is based on the linux kernel. Security is modelled on the approach used with linux.
- Linux uses an ID for every user (UID) and group (GID) using the system.
- Users are individuals and related users form groups.
- File access permissions are used to control access to files.
- Read, write and execute permissions (rwx) for owner, group, others.
- For example, -rwx-xr-r indicates that a user has read, write and execute permissions on a file while the group has execute and read permissions and others only have read permissions.

Sandboxing

- Android imposes permissions on apps rather than users.
- Android uses UIDs and GIDs for apps.
- The UID and GID are assigned when the app is installed.
- These control what the app can read or write.
- In addition, each app has its own sandbox.
- An app can read and write as desired only within its own sandbox.
- Everything within a sandbox directory has the UID and GID of the app that owns the sandbox.
- An app is therefore not able to modify the data of another.

Sandboxing

- Files not owned by any application (app) are owned by the root user.
- Apps have limited access to these.
- However, the file system is divided into two sections.
- Internal and external storage.
- Internal → Files owned by apps and the Android OS.
- External →Public shared data that can be accessed by all apps and the OS.
- Two partition file system is largely legacy: Smartphone/Portable HDD that is connectable over USB.
- Data that is sensitive or should not be shared should be kept in the app's sandbox.

External Storage

- Shared data
- Photographs, other media, audio.
- Only non-sensitive data should be stored here.

The Manifest File

- Android forces applications to declare permissions that they will require in order to function.
- This happens at install time.
- The user is aware of what the app has access to on the device.
- The manifest file is where requested permissions must be declared.
- If the user accepts the permissions requested by the app, it is installed and gets access to the said resources.
- If an app tries to use resources that it does not have permissions for, it is considered a threat and is immediately killed by the OS.

Whitelisting/Blacklisting

- Whitelisting: Give apps a minimum set of permissions to begin with and only add as needed.
- Blacklisting: Give all permissions by default and remove as needed.
- Whitelisting is arguably more secure/rigorous.
- Whitelisting also encourages developers to request the minimum set of permissions.
- These permissions will be shown to the user at install time.
- Apps that require a large number of permissions will be viewed with suspicion.
- Apps that require permissions that do not appear necessary will be viewed with suspicion.

Default Permissions

- Every app receives a small set of default permissions.
- Update the screen, interact with user input, generate sound.
- Read and write within its sandbox.
- Generate notifications to others.
- Other that this, always use the minimum number of permissions.
- Also ensure that any data collection is necessary and reasonable (GDPR).
- Be aware that data collection is covered by legislation and is being taken very seriously by users and governments.
- When permissions are required, explain to the user as fully as possible why this is necessary and what the benefits are.

Security: Areas of Focus

- Social engineering (Fooling users).
- Insufficient input validation. If SQL is used, SQL injection. JavaScript introduces a similar abuse potential. Validate to ensure that input is limited to that which is expected.
- Network communications. Encrypt network data including login/logout credentials to avert man-in-the-middle attacks.
- Stored data. Stored data if sensitive eg. credentials should be encrypted to prevent theft and abuse of these.
- Telephony. Apps can open lines to high-rate numbers or send SMS messages at premium rates.
- In summary, focus on: Network, credentials, input, telephony, cryptography.