Access control and permissions in Android

Stefan Wysocki

Senior Software Engineer Tieto stefan.wysocki@tieto.com



Build connection VSS to Android permissions model

tieto

Android permissions

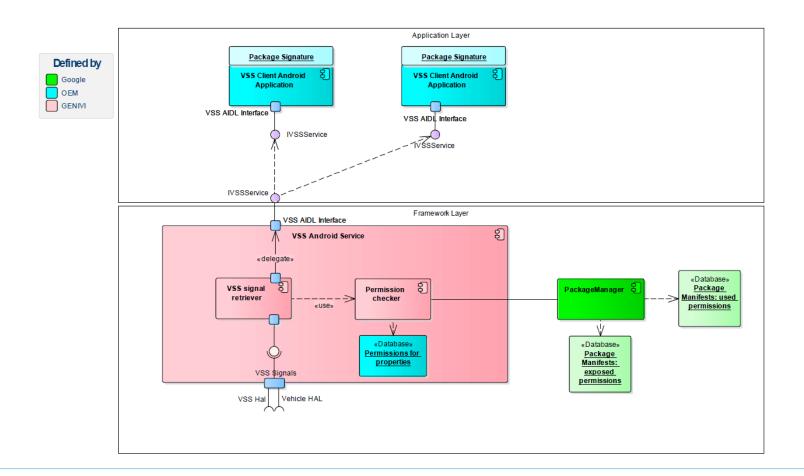
- Android has a groups of permissions for defined Vehicle Properties:
 - https://android.googlesource.com/platform/packages/services/Car/+/refs/heads/master/service/AndroidManifest.xml
- For custom permissions only one available: android.car.permission.CAR_VENDOR_EXTENSION



Android permissions

- What if "CAR_VENDOR_EXTENSION" permission is not enough?
 - Create custom based on vspec?
 - "Category" concept?
 - Other metadata?
- Generate a map object with "checkPermisionsForProperty" method called in implementation







How to verify permissions

tieto

Permissions verification

- Permissions granted after installation and if signed with correct key;
- Signing Key is kept as a secret by Vendor;
- Signature is bound to specific compiled version:
 - Every release needs to be signed again
- Signature ensures integrity of the package
- Vendor to statically check the harmfulness of application



Permissions verification

3rd party application is about to be released



3rd party sends the code/compiled package to Vendor



Vendor performs the review (check the requested permissions in the manifest, evaluate its harmfulness)



If yes: signs the package and releases the binary



tieto

Stefan Wysocki

Senior Software Engineei Tieto stefan.wysocki@tieto.con