Black and White Permission in Certificate

1, Rules

1.1 Black and white list field

Black and white list is defined in the DN of the certificate with special field “role” (or OID.2.5.4.72).

1.2, Permission Checking

When the APK installing, the framework will check the permissions of APK by the black or white list in all the relevant certificates. Once one of the permission is match the black list or one of the permission not in the white list, the installation will fail.

1,3, Black and white list expression

The black and white list is not a real list. They are Java regular expression.

1.4, The format of the black and white list

1) Black List: <PERMISSIONS_BLACK attributes... >BlackList</PERMISSIONS_BLACK>

2) White List: <PERMISSIONS_WHITE attributes... >WhiteList</PERMISSIONS_WHITE>

1.5, Attributes

1.5.1 scope=all

“scope” usually used for white list.

If it is defined as “all” the white list defines to all the android permissions.

If it is not defined, the white list is only define for the financial device permissions. Financial device permissions are the permissions which is start with “android.permission.CLOUD_” or “android.permission.WIZARPOS_”

1.5.2 prefix=no

“prefix” is used for shorten the regular expression.

If it is defined as “no”, the header of the permissions, “android.permission.”, needn’t in the regular expression. For example: you can use INTERNET for “android.permission.INTERNET” permission.

If it is not defined, the “android.permission.” must be existing in the regular expression. For example, you must use “android.permission.INTERNET” in the regular expression.

2, General Usage

Step 1, Generate the certificate for the developer with black or white list.

Step 2, The developer use the JKS with above certificate to sign the APK.

Step 3, During the installation, the framework will check the APK according the black and white list of the signer’s certificate.

3, How to add Black and White in the development certificate

For example, we plan to issue a development certificate to forbid application to access internet. Please refer to the wizarPOSDevCertificateApplyGuide_cn.pdf for the normal process of issuing a development certificate.

The black list could be written as :

"<PERMISSIONS_BLACK>^android.permission.INTERNET$</PERMISSIONS_BLACK>"

or

"<PERMISSIONS_BLACK prefix=no>^INTERNET$</PERMISSIONS_BLACK>"

When the owner of the application root certificate receive the CSR of the development certificate, he can add the

role field when he sign the certificate. For example via XCA tool:

- Choose the application root certificate in the “Certificate” tab of the XCA.
- In the “Certificate signing requests” tab, import the developer’s CSR.
- Right click the imported CSR and select “Sign”
- In the Sign dialog, switch to Source tab, check the “Modify subject of the request” checkbox under the Signing request field.
- Switch to the Subject tab, click the add button, and find the role in the type field, and enter the black list definition in the “Content” field:
  <PERMISSIONS_BLACK>^android.permission.INTERNET$</PERMISSIONS_BLACK>
- Then do the rest actions for normal signing.

5, The permission list of the financial devices

5.1 Mega Stripe Reader

android.permission.CLOUDPOS_MSR

android.permission.WIZARPOS_MSR

5.2 IC Card

android.permission.CLOUDPOS_SMARTCARD

android.permission.WIZARPOS_SMARTCARD

5.3 Printer

android.permission.CLOUDPOS_PRINTER

android.permission.WIZARPOS_PRINTER

5.3 Serial Port (including optional tax module)

android.permission.CLOUDPOS_SERIAL

android.permission.WIZARPOS_SERIAL

android.permission.CLOUDPOS_VIRTUAL_SERIAL_PORT

android.permission.WIZARPOS_VIRTUAL_SERIAL_PORT

5.3 Contactless Card

android.permission.CLOUDPOS_CONTACTLESS_CARD

android.permission.WIZARPOS_CONTACTLESS_CARD

5.3 PINPad

android.CLOUDPOS_PIN_ENCRYPT_DATA

android.WIZARPOS_PIN_ENCRYPT_DATA

android.CLOUDPOS_PIN_GET_PIN_BLOCK

android.WIZARPOS_PIN_GET_PIN_BLOCK

android.CLOUDPOS_PIN_LOAD_KEY

android.WIZARPOS_PIN_LOAD_KEY

android.CLOUDPOS_PIN_MAC

android.WIZARPOS_PIN_MAC

android.CLOUDPOS_PIN_UPDATE_MASTER_KEY

android.WIZARPOS_PIN_UPDATE_MASTER_KEY

android.CLOUDPOS_PIN_UPDATE_USER_KEY

android.WIZARPOS_PIN_UPDATE_USER_KEY

5.3 Fingerprint

android.permission.CLOUDPOS_FINGERPRINT

android.permission.WIZARPOS_FINGERPRINT

5.3 LED

android.permission.CLOUDPOS_LED

android.permission.WIZARPOS_LED

5.3 Safe Module

Readonly:

android.permission.CLOUDPOS_READ_HWSECURITYMANAGER

android.permission.WIZARPOS_READ_HWSECURITYMANAGER

android.permission.CLOUDPOS_READ_SAFE_MODULE_READONLY

android.permission.WIZARPOS_READ_SAFE_MODULE_READONLY

Read and write:

android.permission.CLOUDPOS_READ_SAFE_MODULE

android.permission.WIZARPOS_READ_SAFE_MODULE

5.3 Install and uninstall application

android.permission.CLOUDPOS_INSTALL_APP

android.permission.CLOUDPOS_INSTALL_SILENCE

android.permission.CLOUDPOS_UNINSTALL_APP

android.permission.CLOUDPOS_UNINSTALL_SILENCE

5.3 Disable Home Key

android.permission.CLOUDPOS_DISABLE_HOME_KEY

android.permission.WIZARPOS_DISABLE_HOME_KEY

android.permission.CLOUDPOS_DISABLE_HOME_KEY_IN_ACTIVITY

android.permission.WIZARPOS_DISABLE_HOME_KEY_IN_ACTIVITY

5.3 Full screen without status bar and navigation bar

android.permission.CLOUDPOS_REAL_FULLSCREEN

android.permission.WIZARPOS_REAL_FULLSCREEN

6, Some Examples

6.1 Forbid accessing internet

"<PERMISSIONS_BLACK prefix=no>^INTERNET$</PERMISSIONS_BLACK>"

or

"<PERMISSIONS_BLACK>^android\.permission\.INTERNET$</PERMISSIONS_BLACK>"

6.2 Forbid access LED

"<PERMISSIONS_BLACK prefix=no>^(CLOUD|WIZAR)POS_LED$</PERMISSIONS_BLACK>"

or

"<PERMISSIONS_BLACK>^android\.permission\.(CLOUD|WIZAR)POS_LED$</PERMISSIONS_BLACK>"

6.3 Disable all financial device permissions except LED

All other normal android permission are allowed.

"<PERMISSIONS_WHITE prefix=no>^(CLOUD|WIZAR)POS_LED$</PERMISSIONS_WHITE>"

or

"<PERMISSIONS_WHITE>^android\.permission\.(CLOUD|WIZAR)POS_LED$</PERMISSIONS_WHITE>"

6.4 Disable all permissions (including normal android permissions) except LED

"<PERMISSIONS_WHITE scope=all prefix=no>^(CLOUD|WIZAR)POS_LED$</PERMISSIONS_WHITE>"

or

"<PERMISSIONS_WHITE scope=all>^android\.permission\.(CLOUD|WIZAR)POS_LED$</PERMISSIONS_WHITE>"

6.5 Disable all financial device permissions except LED and PRINTER, and disable INTERNET BLUETOOTH in normal android permissions

"<PERMISSIONS_BLACK prefix=no>^(INTERNET|BLUETOOTH)$</PERMISSIONS_BLACK><PERMISSIONS_WHITE prefix=no>^(CLOUD|WIZAR)POS_（LED|(ACCESS_)?PRINTER)$</PERMISSIONS_WHITE>"

Or

"<PERMISSIONS_BLACK>^android\.permission\.(INTERNET|BLUETOOTH)$</PERMISSIONS_BLACK><PERMISSIONS_WHITE>^android\.permission\.(CLOUD|WIZAR)POS_(LED|(ACCESS_)?PRINTER)$</PERMISSIONS_WHITE>"