Add-on signing guide

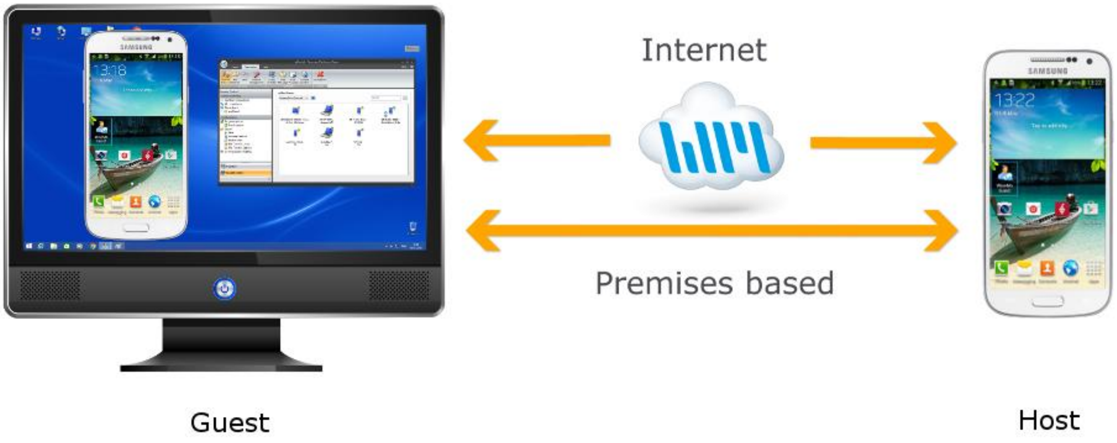
Brief

WiseMo produces state of the art remote control software for the Android operating system. In order to capture the screen and inject input an Add-on component is necessary to bridge the access from the Remote Control Host App to the Android operating system. This Add-on component must be signed by the manufactures of the Android device.

The outcome is that mutual and future customers will be able to remote control their Android devices.

Technical description

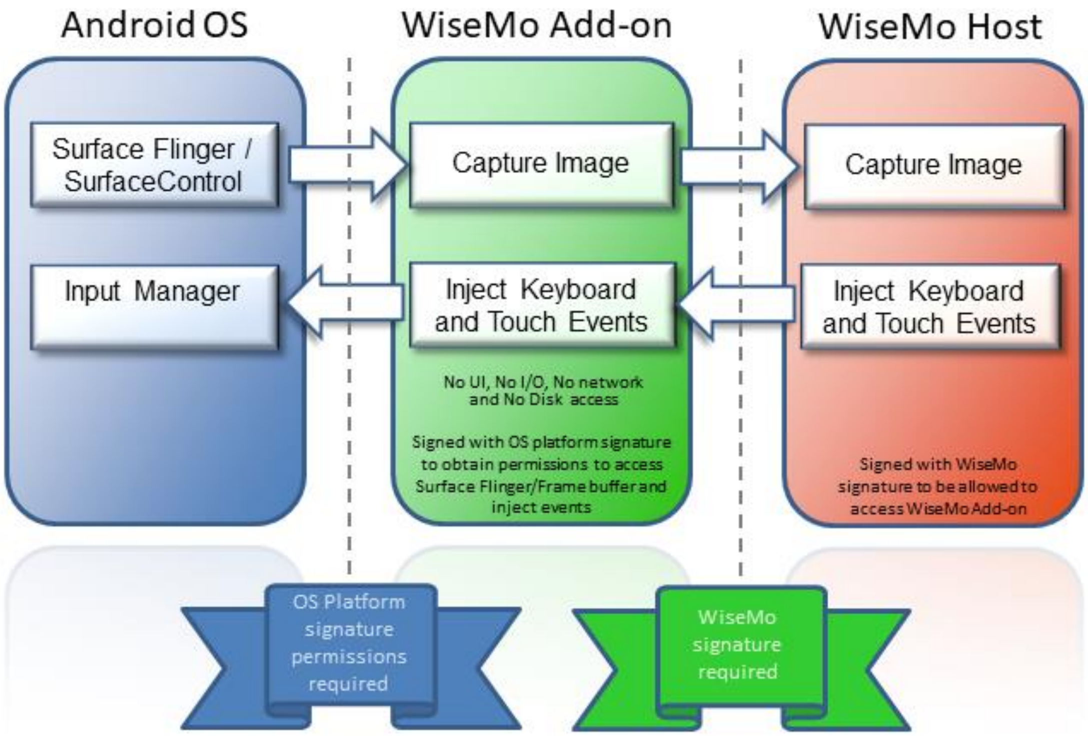
The fundamental functionality of a remote control product is to capture the screen and simulate input events.



The security mechanism in the Android operating protects access to certain API functions so only authorized access is allowed. In order to capture the screen and inject keyboard and touch events the Remote Control App needs access to such functions.

This security mechanism works by looking at the identity of the calling App in terms of its signature. So when an App uses these Android API functions the operating system looks at the signature of the App and based on that allows the calls or rejects them. The operating system will allow calls from Apps signed with the manufacture's platform certificate and therefore the App must be signed with the same platform certificate.

It would be a laborious job to sign the Remote Control App every time it is modified. Therefore an intermediate Add-on app is used that serves as a bridge between the Remote Control App and the operating system.


Android OS
WiseMo Add-on
WiseMo Host
Surface Flinger / SurfaceControl
Input Manager
Capture Image
Inject Keyboard and Touch Events
No UI, No I/O, No network and No Disk access
Signed with OS platform signature to obtain permissions to access Surface Flinger/Frame buffer and inject events
Capture Image
Inject Keyboard and Touch Events
Signed with WiseMo signature to be allowed to access WiseMo Add-on
OS Platform signature permissions required
WiseMo signature required

The Add-on is very simple. It has the following advantages:

- It rarely changes and needs to be re-signed
- The less outside interaction is has or does, the more secure it is. Hence there's no UI, no I/O, no network access, no disk access etc.
- It only does what we say it does and it is easy to inspect for a 3rd party

The table below lists the requested permission in the manifest:

Permission name	Purpose
<uses-permission android:name = "android.permission.READ_FRAME_BUFFER" />	To be able to capture the screen
<uses-permission android:name = "android.permission.INJECT_EVENTS" />	To be able to simulate input events
<uses-permission android:name = "android.permission.SHUTDOWN">	To be able to shut down the device. Can be omitted on request.
<uses-permission android:name = "android.permission.REBOOT">	To be able to restart the device. Can be omitted on request.

All Host App features, including features made possible by these Android permissions, are subject to being authorized by the applied authentication scheme. Authentication includes a confirmation screen where a Host user can accept or deny remote access.

The signing process of the Add-on is a simple standard process done by a utility that takes the Add-on App as input and produces the signed version. For a skilled person this only takes a few minutes.

Procedure

The procedure to enable remote control off an Android device is the following:

1. WiseMo prepares an Add-on APK with a unique Package name (for example com.wisemo.rcbridge.[manufacturer name]_1).
2. The manufacturer of the Android device signs the Add-on APK with the platform certificate that is used on the particular Android devices.
3. The manufacturer sends the signed Add-on to WiseMo (os@wisemo.com).
4. WiseMo will verify whether that the Add-on is signed for the device in question and if possible have a mutual customer verify it on a physical device.
5. WiseMo registers the Add-on so it can be automatically deployed and installed by mutual customers.

If a manufacturer uses different platform certificates on the devices that should be supported, the above procedure must be repeated for each platform certificate used.

Contact

All technical contact and questions should be sent to Ole Bjorn Setnes (os@wisemo.com).