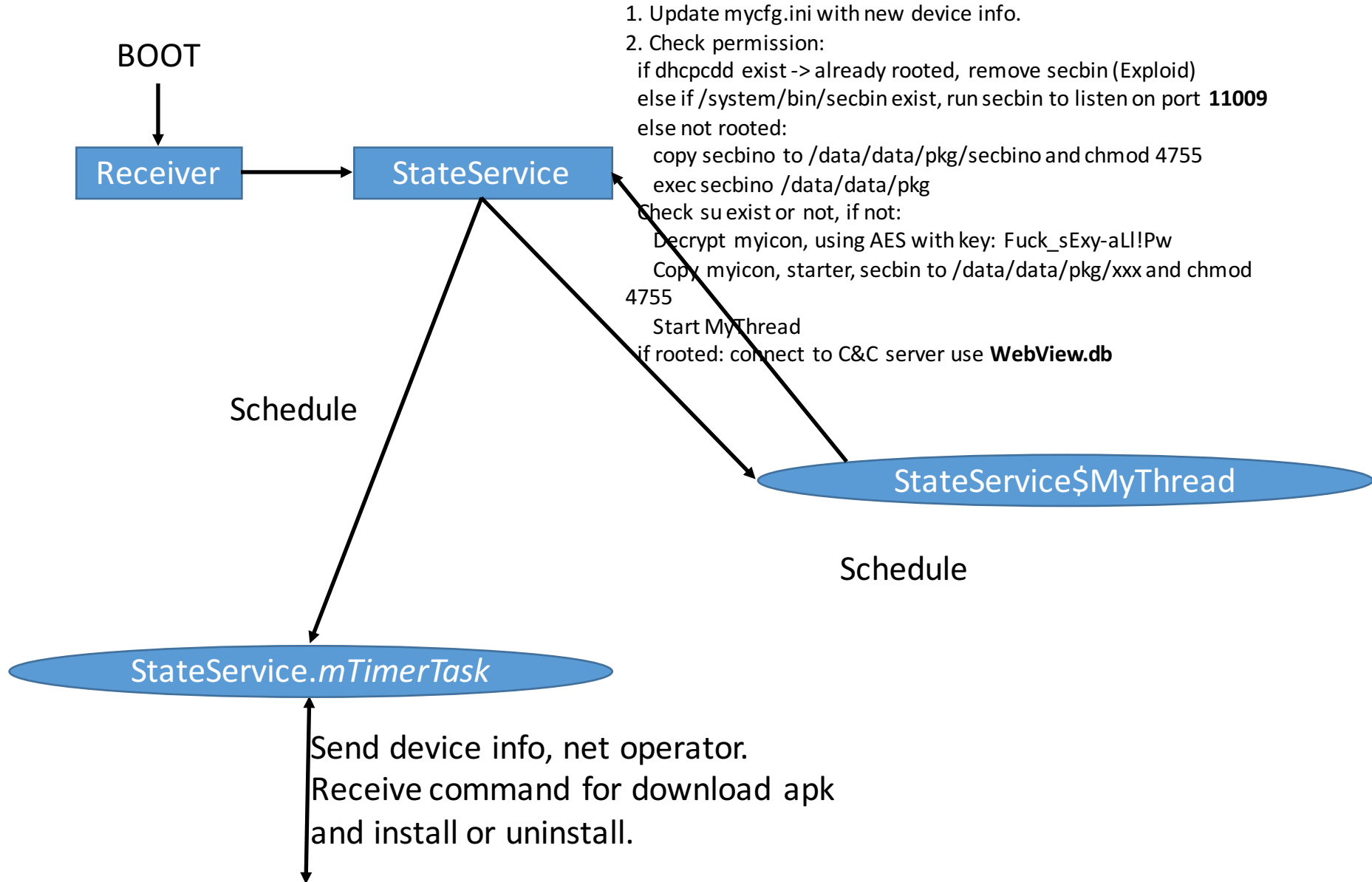


DroidKungFu Variety1

It will load lilhermitCore.so as native payload.



1. Update mycfg.ini with new device info.
 2. Check permission:
 - if dhcpdd exist -> already rooted, remove secbin (Exploit)
 - else if /system/bin/secbin exist, run secbin to listen on port **11009**
 - else not rooted:
 - copy secbino to /data/data/pkg/secbino and chmod 4755
 - exec secbino /data/data/pkg
- Check su exist or not, if not:
Decrypt myicon, using AES with key: Fuck_sExy-aLl!Pw
Copy myicon, starter, secbin to /data/data/pkg/xxx and chmod 4755
Start MyThread
if rooted: connect to C&C server use **WebView.db**

Exec in native wrapper.

1. starter /data/data/pkg; Try to root device use myicon and secbin
2. secbin /data/data/pkg; launch as a local tcp server and listen to port 11009.
3. Start StateService

<http://search.gongfu-android.com:8511>