Android Security & Exploitation

Aditya Gupta (@adi1391)

Founder, Attify (http://attify.com)

adi@attify.com

Certifications : http://securitytube-training.com
Pentester Academy : http://PentesterAcademy.com

XPosed Framework

- Framework for modifying system and apps behavior written by XDA member rovo89
- Copies itself to /system/bin and adds additional Jar later
- Gets started during the system boot
- Different ways to achieve the same goal
- A few minor differences between the Xposed and Cydia framework (http://www.cydiasubstrate.com/id/34058d37-3198-414f-a696-73e97e0a80db/)

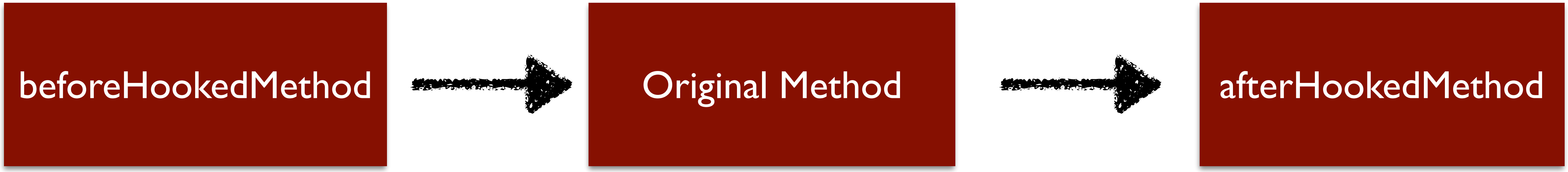
XPosed module for Listlock

- Will achieve the same goal - achieveing successful authentication
- Instead of changing the return values, we will change the variables here
- Wiki Guide on how to write an Xposed module - https://github.com/rovo89/XposedBridge/wiki/Development-tutorial

XPosed API

Xposed API	**What it does**
handleLoadPackage	notifies when a package has been loaded
findAndHookMethod	Helper Class
beforeHookedMehtod	Manipulate the parameters and prevent the call to original method
afterHookedMehtod	Action taken/changed to be based on the result of original method

XPosed API

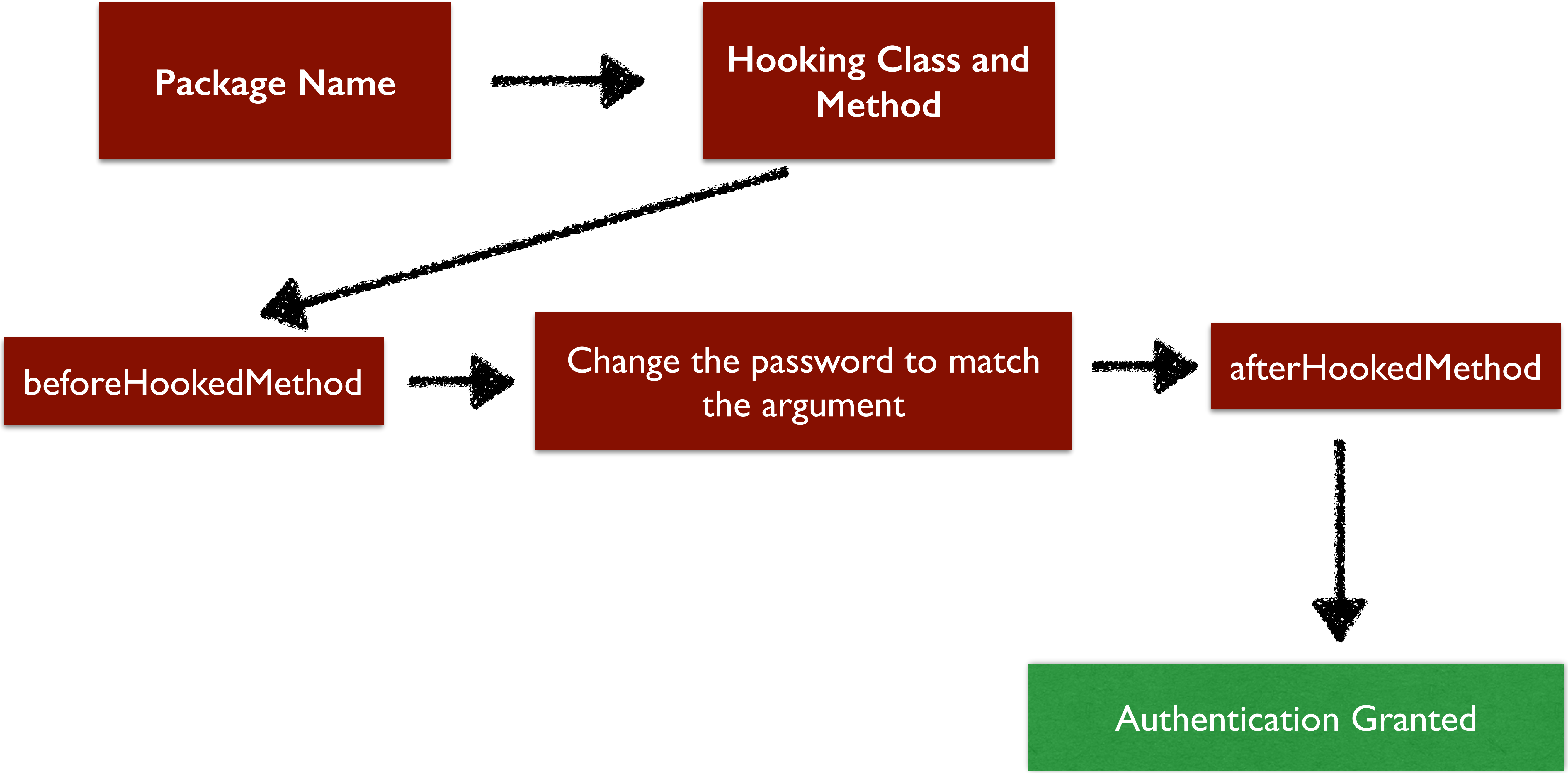


beforeHookedMethod

Original Method

afterHookedMethod

ListLock Bypass using Xposed



Package Name

Hooking Class and Method

beforeHookedMethod

Change the password to match the argument

afterHookedMethod

Authentication Granted