DeepDroid: Dynamically Enforcing Enterprise Policy on Android Devices

JAN 18TH, 2016

论文下载：http://www.internetsociety.org/sites/default/files/02_5_1.pdf

INTRODUCTION

- DeepDroid：为了增强企业内部使用的安卓手机安全策略，以动态监控的方式管理app的访问权限。
- 基本的思路：所有的资源访问或者系统级的服务都是被一部分系统进程控制。因此，DeepDroid只需要Hook这些系统进程作为一个核心的控制器，监控app请求的访问权限。同时，监控zygote进程，防止app使用native code的方式绕过安卓的访问控制机制。

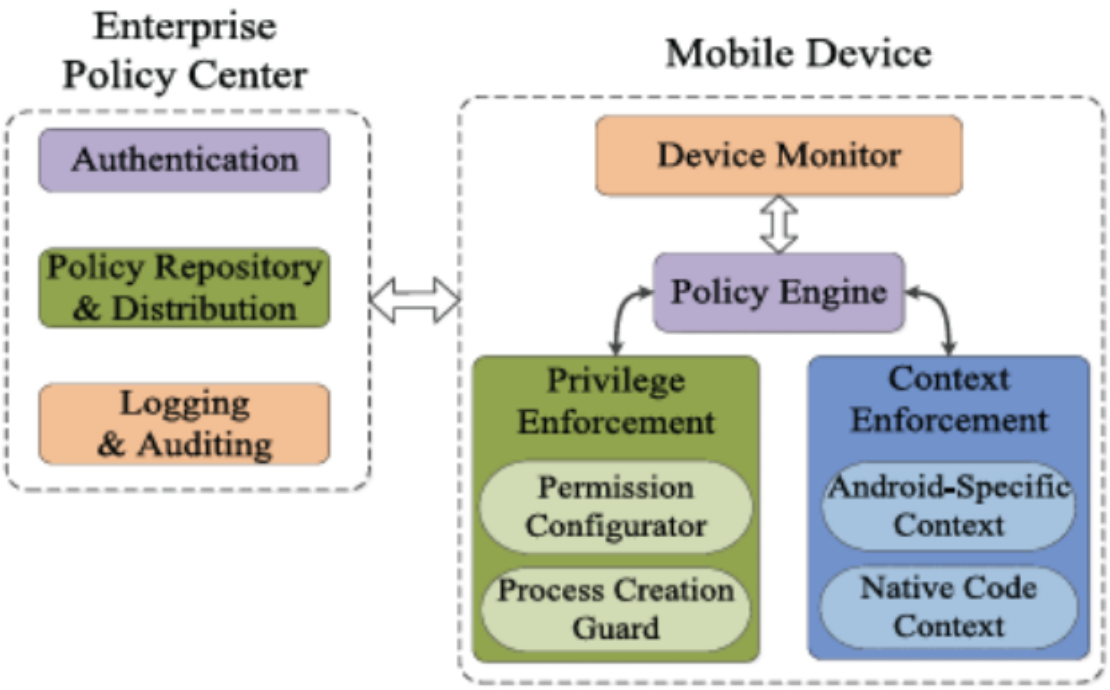
ASSUMPTIONS

- 企业用户是可信的
- 一些在手机和企业策略中共享的关键的元素是安全的
- 安卓系统是可信的
- 用户有足够的自由安装app

- 并且假设恶意的程序是不能获取root权限

DeepDroid综述

DeepDroid分为两个部分：策略管理和设备管理。



策略管理

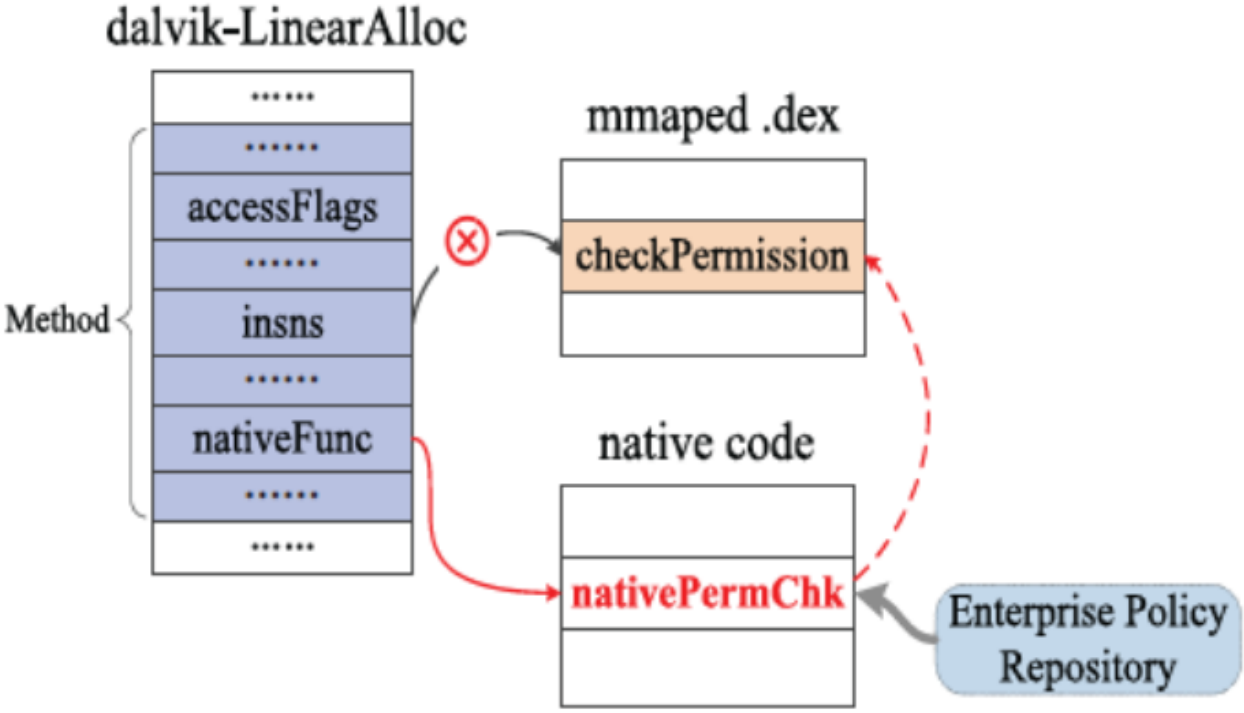
分为三个模块：认证模块、分配策略模块、监视模块 首先成功认证了手机设备，设备和策略中心共享一个暂时的安全密钥。策略中心根据用户的角色和需求分发策略。同时，设备的状态需要不断的报告给策略中心，作为审计的材料。策略中心使用心跳信息判读手机上的DeepDroid是否正常运行。

设备管理

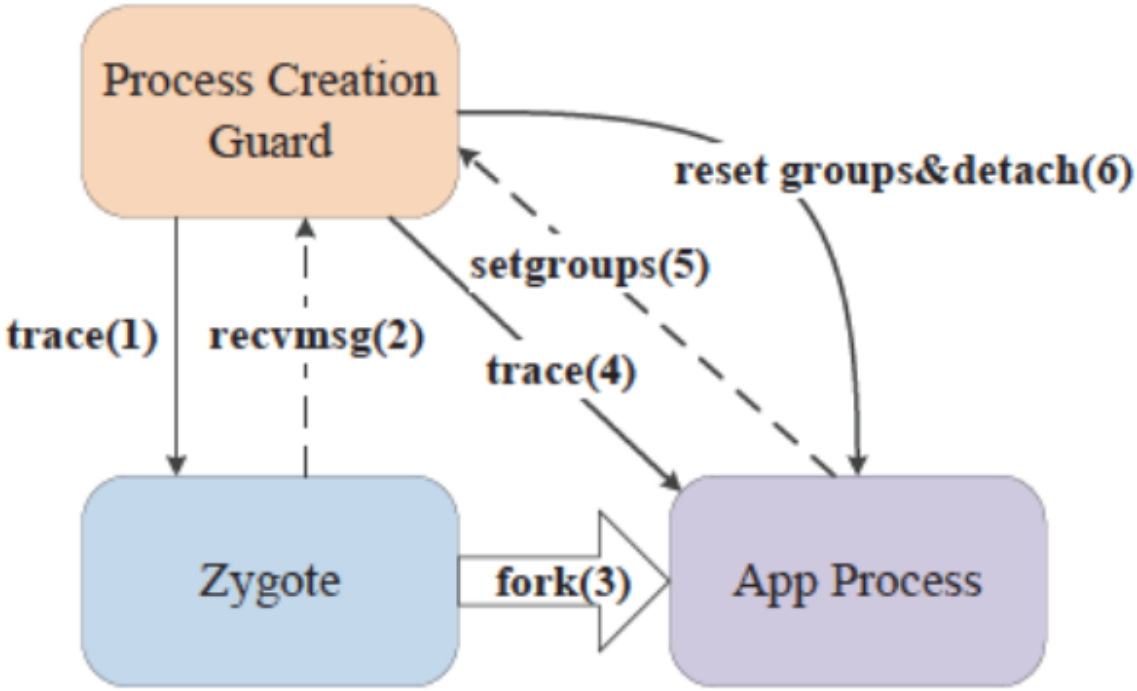
- 设备监控：向策略中心认证设备，动态的控制策略增强机制的运行。
- 权限增强：控制App访问权限
- 上下文增强：对native code的管理和一些特别的返回值的管理。

权限

增加了额外的权限确认的组件，动态修改system_server进程的控制流。



进程的保护



- 跟踪zygote，一旦一个请求被发送，挂起zygote，然后从请求中提取需要的信息。
- 当新进程被fork以后，跟踪新进程

EVALUATION

Resource	Permission	Group	PEP[1]	Result[2]
IMEI	READ_PHONE_STATE		*package*	√
Phone #	READ_PHONE_STATE		*package*	√
location	ACCESS_FINE_LOCATION		*package*	√
contacts	READ_CONTACTS		*package*	√
camera	CAMERA	camera	*package/PCG*	√
account	GET_ACCOUNTS		*package*	√
logs	READ_LOGS	log	*PCG*	√
SMS/MMS message	SEND_SMS		*package*	√
network	INTERNET	inet	*package/PCG*	√

[1] PEP is the policy enforcement point.
[2] The policy is enforced either in *package* service or by Process Creation Guard (PCG).

- 每种5个
- 在不同设备上测试不同的安卓版本，测试了8个设备，共9个版本，都能运行