理论部分

如何鉴别操作系统的本质？

Android 是不是Linux系统？

Root 对于Android意味着什么？

Root用户与普通用户的区别

/etc/profile 只读

任意删除文件

操作系统的组成

操作系统=系统内核+文件系统

Linux发行版：Linux内核+文件系统（ext3/4）

Android系统：Linux内核+文件系统（ext3/4）

Linux最核心的部分之一，是与驱动相关的linux驱动接口，也可以称为linux安装运行规范，这是一套二进制规范。

如何鉴别系统本质：系统内核+文件系统

Android是不是Linux系统：Yes

Root意味着：su root

为什么要提取Root权限？

拥有Root权限到底能做什么？

Android手机预装软件的问题：

可卸载：/data/app

系统不可卸载：/system/app

向/system/app，目录复制文件的方法：

拥有root权限后直接复制

通过Android ROM方式复制

通过Recovery升级包方式复制

一些app需要root权限

Otm功能

调试Linux驱动

随时修改Android设备启动画面

……

提取root权限的步骤

1刷一个合适的Recovery

1. 在bootloader模式下复制整个文件系统
2. 在Recovery模式下将文件复制到Android设备中的指定目录

改造su命令

Android系统自带的su命令只允许root和shell用户调用

制作Recovery刷机文件

Zip格式的压缩文件主要有待复制的文件和Edify语言编写的脚本文件组成

执行su命令提取root权限

改造后的su命令 可以被终端和app调用

制作拥有Root权限的ROM

刷机后 Android系统直接拥有root权限（无需每次申请）

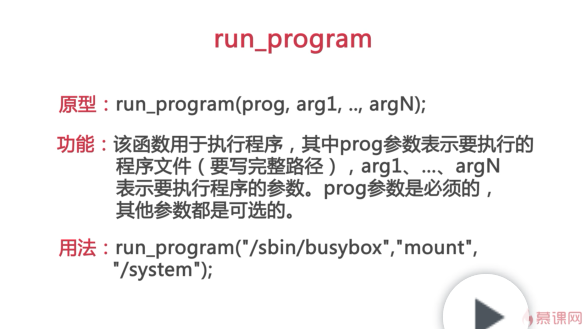
-------------------------------------------------------------------------------

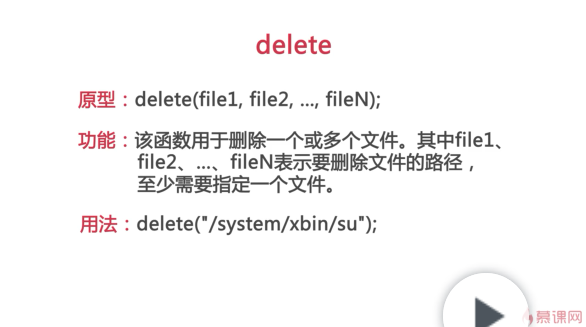
实践部分

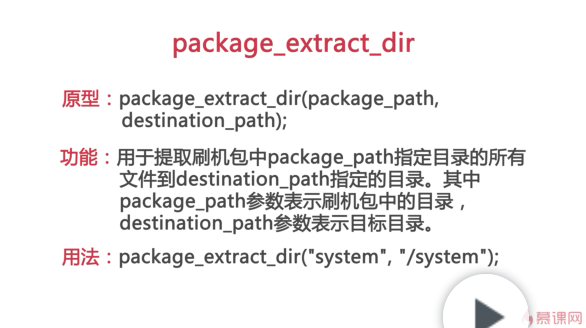
Edify语言简介（Android内嵌脚本语言）

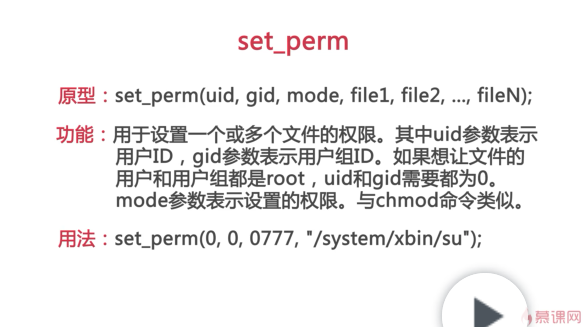
用于编写updater-script脚本文件，用于recover rom和recover升级包。

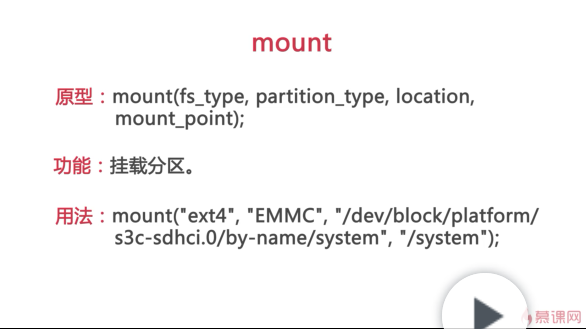


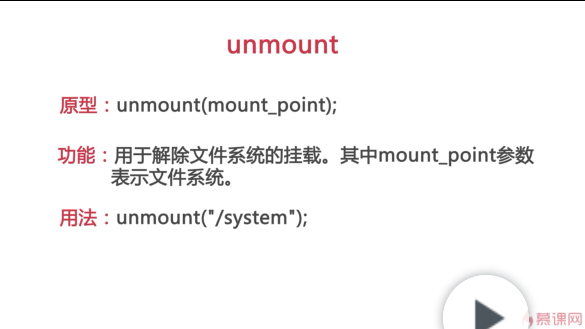












编写updater-script脚本文件：

要求：

以读写模式挂载/system

删除旧的su文件

复制新的su文件

修改su文件的权限

卸载/system

==========================================================

ui\_print(“--------”);

ui\_print(“Recovery Updater Package”);

ui\_print(“--------”);

ui\_print(“----Mounting /system ----”);

#以读写方式挂载/system

Run\_program(“/sbin/busybox”,”mount”,”-o”,”rw”,”/system”);

ui\_print(“----Delete /system/xbin/su ----”);

#删除旧的su文件

delete(“/system/xbin/su”);

ui\_print(“----extracting files ----”);

#将刷机包中的system目录的所有文件复制到/system目录中的相应位置

Package\_extract\_dir(“system”,”/system”);

#设置su命令的权限，将其变成可执行的

Set\_perm(0,0,0777,”/system/xbin/su”);

#卸载/system

unmount(“/system”);

ui\_print(“finished”);

制作用于复制su命令的Recovery升级包

建立META-INF/com/google/android/update-binary和upadte-script

建立system/xbin/su

压缩为zip

将su命令复制到/system/xbin

在recovery模式下刷机，将zip复制到sd卡任意位置

利用su命令提取root权限

Mac下连接设备，执行adb shell，执行su。

用mount命令将文件设置读写权限。





