[FAQ11862]user版本如何打开root权限

[Description]
user版本怎么打开root权限

[Keyword]
user root adb superuser 用户版本 root权限 security

[Serious Declaration]
严重声明: 任何在最终user版本上打开root权限的手法都会给用户带来安全风险, 请仔细评估您的需求是否真实需要. MTK 强烈反对此类做法, 由此带来的安全风险，以及造成的损失, MTK 不承担任何的责任。

[Solution]
首先您要确认您是想开启adbd 的root 权限，还是让app 也可以拿到root 权限。他们之间的差别，可以参考FAQ
FAQ08317:android apk 的root 权限和USB adb 权限的区别
https://online.mediatek.com/Pages/FAQ.aspx?List=SW&FAQID=FAQ08317

(1). adbd 的root 权限
我们通常在debug user 版本问题时, 或者进行user 版本的monkey test 时都会这个工作，以便debug. 可以参考FAQ. FAQ06317 如何永久性开启adb 的root权限 https://online.mediatek.com/Pages/FAQ.aspx?List=SW&FAQID=FAQ06317

如果你想user 版本adb root 权限默认关闭, 而在想开启时, 可以通过工程模式中的设置项开启, 那么请USER2ROOT 功能 (L 版本不再支持此功能)。
此功能默认关闭, 如果开启, 需要在ProjectConfig.mk 中设置: MTK_USER_ROOT_SWITCH = yes
同样注意此项功能通常只用于debug 或者 cmcc 送测, 在正式出货版本, 强烈要求关闭, 否则有安全风险.

(2). app 的root 权限
app 的root 权限通常是通过执行su 命令来获取。注意的是KK 上, 因为多种限制, 普通的su 难以直接拿到root 权限, 需要做针对性的改动.
通常我们会内置具有控制端的第三方su, 下面以内置SuperSU, 以及使用Google default su 为例进行说明。

(3). 如何内置第三方SuperSU
该方式可以绕过zygote 和 adbd 对Root Capabilities BoundSet 的限制. MTK 目前仅测试KK 以及以前的版本, L 版本后因为SuperSU 还在持续更新中, 请客户查看它官网的说明.
3.1. 下载SuperSU
SuperSU: http://forum.xda-developers.com/showthread.php?t=1538053

3.2. 内置Superuser.apk 到 system/app
将su 复制并改名成: daemonsu
内置su 到 system/xbin
内置daemonsu 到 system/xbin
内置chattr 到 system/xbin
内置chattr.pie 到 /system/xbin

3.3. 内置install-recovery.sh 到system/etc
并且按照FAQ: FAQ09021 如何修改系统内置文件的权限, 用户，属性
https://online.mediatek.com/Pages/FAQ.aspx?List=SW&FAQID=FAQ09021
更新alps/system/core/inlcude/private/android_filesystem_config.h
在android_files 数组的最开始新增.
{ 00755, AID_ROOT, AID_ROOT, 0, "system/etc/install-recovery.sh" },

(4). 如何内置Google default su

4.1 放开Google default su 只准shell/root 用户使用的限制.
system/extras/su/su.c 中删除下面3行代码
```
if (myuid != AID_ROOT && myuid != AID_SHELL) {
fprintf(stderr,"su: uid %d not allowed to su\n", myuid);
return 1;
}
```

4.2 首先将此编译出的su 内置到system/bin, 然后修改su 的内置权限,启用sbit 位.
按照FAQ: FAQ09021 如何修改系统内置文件的权限, 用户，属性
https://online.mediatek.com/Pages/FAQ.aspx?List=SW&FAQID=FAQ09021
更新alps/system/core/inlcude/private/android_filesystem_config.h
在android_files 数组中
增加
{ 06755, AID_ROOT, AID_ROOT, 0, "system/bin/su" },
注意这行要放在
{ 00755, AID_ROOT, AID_SHELL, 0, "system/bin/*" },
之前

4.3 如果是KK 版本(非KK2 MT6752/MT6732), 需要强行解除zygote 和 adbd 对Root Capabilities BoundSet 的限制
更新kernel/security/commoncap.c 中 cap_prctl_drop 函数为:
```
static long cap_prctl_drop(struct cred *new, unsigned long cap)
{
//mtk71029 add begin: Let 'zygote' and 'adbd' drop Root Capabilities BoundSet ineffectively
if (!strncmp(current->comm, "zygote", 16)) {
return -EINVAL;
}
if (!strncmp(current->comm, "adbd", 16)) {
return -EINVAL;
}
// add end

if (!capable(CAP_SETPCAP))
return -EPERM;
if (!cap_valid(cap))
return -EINVAL;

cap_lower(new->cap_bset, cap);
```

return 0;
}

4.4 如果贵司一定要在K2(MT6752/MT6732) 上开启, 请提交eService, 申请定制的DVM, 放开相关的权限限制.

4.5 如果贵司在L 版本操作, 请按下面的流程:
4.5.1 更新alps/frameworks/base/core/jni/com_android_internal_os_Zygote.cpp
将 DropCapabilitiesBoundingSet(JNIEnv* env) 这个函数置空.

4.5.2 更新alps/frameworks/base/cmds/app_process/app_main.cpp 的main 函数, 注释掉main函数开始的下面这段代码
if (prctl(PR_SET_NO_NEW_PRIVS, 1, 0, 0, 0) < 0) {
// Older kernels don't understand PR_SET_NO_NEW_PRIVS and return
// EINVAL. Don't die on such kernels.
if (errno != EINVAL) {
LOG_ALWAYS_FATAL("PR_SET_NO_NEW_PRIVS failed: %s", strerror(errno));
return 12;
}
}

4.5.3 更新alps/system/core/adb/adb.c 将should_drop_privileges() 函数, 清空这个函数，直接返回 0 即可.

4.5.4 将SELinux 调整到permissve mode, 参考FAQ11484:
http://online.mediatek.inc/Pages/FAQ.aspx?List=SW&FAQID=FAQ11484

重新编译系统, 重新download 后, adb shell 进入后再输入su 看看是否命令行由$切换到#, 如果切换即成功。

(5). 在KK 版本后app 使用root 权限受到更加严格的限制, 可以参考FAQ
[FAQ11414] android KK 4.4 版本后，user 版本su 权限严重被限制问题说明
http://online.mediatek.inc/Pages/FAQ.aspx?List=SW&FAQID=FAQ11414
FAQ11538：android KK 4.4 版本后，app 使用root(su) 权限受到严格限制说明
https://online.mediatek.com/Pages/FAQ.aspx?List=SW&FAQID=FAQ11538