Introduction

This document is about to build an image by Yocto, and it will disable a function that normal user can't use command line of "su".

What is su in Linux system

su is command line utility for Linux, it stands for switch user, or called substitute user. As the name of command line says, we can use it switch from a user account to other user account, mostly to administrator account (root) for elevating privileges. The su installs in the directory of /etc/pam.d/. We can take some configurations to implement some functions, such as disable normal user to access root user.

Build image with su disabled for normal user by Yocto

To standalone system, we can access to /etc/pam.d/su and comment the line:
auth   required   pam_wheel.so
However, to build a system with the function of sudisabled is necessary in some cases.
Add the below codes to do_install(){}
in the directory /source/poky/meta/recipes-extended/shadow/shadow.inc
if [-f ${D}${bindir}/su]; then
chmod4750 ${D}${bindir}/su
elif[-f ${D}/bin/su]; then
chmod4750 ${D}/bin/su
else
echo "Error: sufile not found!"
exit 1
fi

Handson

The full steps to build Yocto image, please refer to Yocto User guide.

We can check if the SetUID funcions after the image flashed to board.

```
root@imx8mn-lpddr4-evk:~# ls -al /bin/su.shadow
-rwsr-x---   1 root    root        69272 Mar  9  2018 /bin/su.shadow
```

By default, the login account is root. we can try to add a test user account for test.

```
useradd newuser
```

```
cat /etc/passwd
```

```
messagebus:x:999:999::/var/lib/dbus:/bin/false
nobody:x:65534:65534:nobody:/nonexistent:/sbin/nologin
newuser:x:1000:1000::/home/newuser:/bin/sh
```

Handson

run su command, while logining with root account, to switch user to newuser account
root@imx8mn-lpddr4-evk:~# su newuser

newuser@imx8mn-lpddr4-evk:/home/root$

Now, we'll see the permission denied if running su command

newuser@imx8mn-lpddr4-evk:/home/root$ su root
sh: /bin/su: Permission denied

newuser@imx8mn-lpddr4-evk:/home/root$ su
sh: /bin/su: Permission denied

To check the related configurations from the /etc/pam.d/su

Handson

```
newuser@imx8mn-lpddr4-evk:/home/root$ cat /etc/pam.d/su
#
# The PAM configuration file for the Shadow `su' service
#
# This allows root to su without passwords (normal operation)
auth       sufficient pam_rootok.so
# Uncomment this to force users to be a member of group root before they can use `su'.
# You can also add "group=foo" to the end of this line if you want to use a group other
# than the default "root" (but this may have side effect of denying "root" user, unless she's # a
member of "foo" or explicitly permitted earlier by e.g. "sufficient pam_rootok.so").
# (Replaces the `SU_WHEEL_ONLY' option from login.defs)
# auth       required   pam_wheel.so
# Uncomment this if you want wheel members to be able to
# su without a password.
# auth       sufficient pam_wheel.so trust
# Uncomment this if you want members of a specific group to not
# be allowed to use su at all.
# auth       required   pam_wheel.so deny group=nosu
```