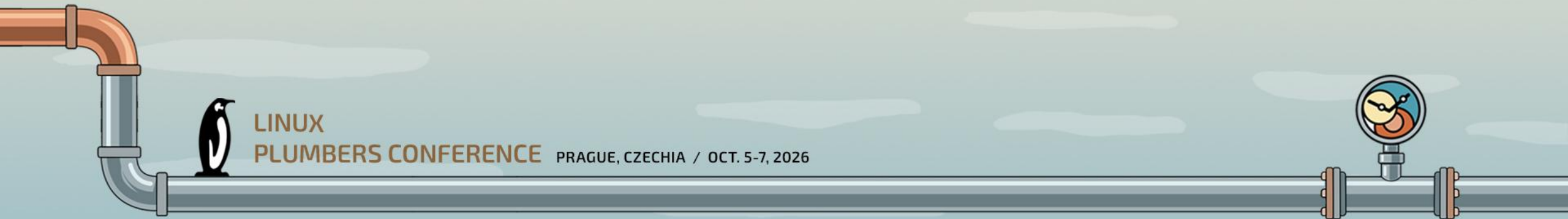


The Supply Chain Attack on Buildsystems

Alejandro Hernandez Samaniego @ Microsoft



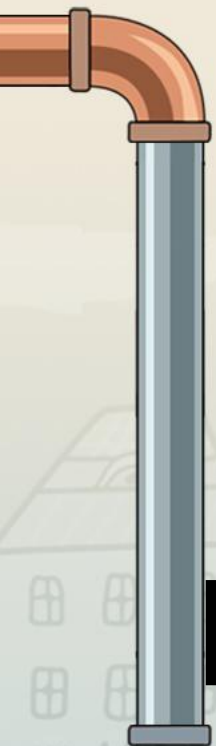
Supply Chain Attacks

- Attack the Source Code
- Attack the Vendor
- Attack the Dev System



LINUX
PLUMBERS
CONFERENCE

PRAGUE, CZECHIA / OCT. 5-7, 2026



Buildroot



LINUX
PLUMBERS
CONFERENCE

PRAGUE, CZECHIA / OCT. 5-7, 2026

Buildroot

- Make based
- Make is simple
- Tamper intermediate artifacts



LINUX
PLUMBERS
CONFERENCE

PRAGUE, CZECHIA / OCT. 5-7, 2026

Buildroot

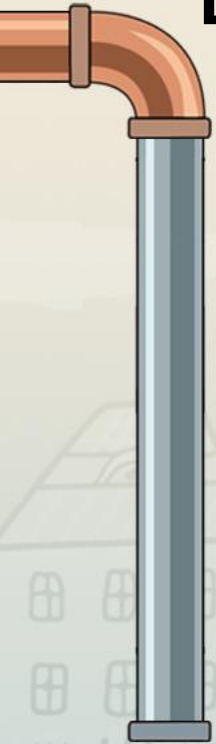
```
> make O=output-qemuarm64
>>> Finalizing host directory
>>> Finalizing target directory
rm -rf /mnt/builds/buildroot/output-qemuarm64/target/usr/src/hare
mkdir -p /mnt/builds/buildroot/output-qemuarm64/host/etc/meson
sed -e "s%@TARGET_CFLAGS@%'-D_LARGEFILE_SOURCE', '-D_LARGEFILE64_SOURCE',
```

```
> output-qemuarm64/images/start-qemu.sh
Booting Linux on physical CPU 0x0000000000 [0x410fd034]
Linux version 6.16.12 (azureuser@alhe-dev-ub) (aarch64-buildroot-linux-gnu-gcc.br_real
random: crng init done
Machine model: linux,dummy-virt
efi: UEFI not found.
OF: reserved mem: Reserved memory: No reserved-memory node in the DT
Zone ranges:
  DMA      [mem 0x0000000040000000-0x0000000047ffffff]
  DMA32    empty
  Normal   empty
Movable zone start for each node
```

LINUX
PLUMBERS
CONFERENCE

PRAGUE, CZECHIA / OCT. 5-7, 2026

Buildroot



LINUX
PLUMBERS
CONFERENCE

PRAGUE, CZECHIA / OCT. 5-7, 2026

```
buildroot login: root
# ls
# ls -l /
total 23
drwxr-xr-x  2 root  root    2048 Sep 12 18:34 bin
-----  1 root  root      0 Sep 12 19:59 crond.reboot
drwxr-xr-x  4 root  root   12200 Sep 12 19:59 dev
drwxr-xr-x  6 root  root    1024 Sep 12 18:34 etc
drwxr-xr-x  3 root  root    1024 Sep 12 18:34 lib
lrwxrwxrwx  1 root  root      3 Sep 12 18:13 lib64 -> lib
lrwxrwxrwx  1 root  root     11 Nov 28  2025 linuxrc -> bin/busybox
drwx----- 2 root  root   12288 Sep 12 18:34 lost+found
drwxr-xr-x  2 root  root    1024 Nov 28  2025 media
drwxr-xr-x  2 root  root    1024 Nov 28  2025 mnt
drwxr-xr-x  2 root  root    1024 Nov 28  2025 opt
dr-xr-xr-x 92 root  root      0 Sep 12 19:59 proc
drwx----- 2 root  root    1024 Nov 28  2025 root
drwxr-xr-x  4 root  root     220 Sep 12 19:59 run
drwxr-xr-x  2 root  root    1024 Nov 28  2025/sbin
dr-xr-xr-x 12 root  root      0 Sep 12 19:59 sys
drwxrwxrwt  2 root  root     60 Sep 12 19:59 tmp
drwxr-xr-x  6 root  root    1024 Sep 12 18:34 usr
drwxr-xr-x  4 root  root    1024 Sep 12 18:34 var
# ls /
bin      lib      media    root     tmp
crond.reboot lib64    mnt      run      usr
dev      linuxrc  opt     /sbin    var
etc      lost+found proc     sys
# QEMU: Terminated
```

Buildroot

Index: busybox-1.37.0/coreutils/ls.c

--- busybox-1.37.0.orig/coreutils/ls.c

+++ busybox-1.37.0/coreutils/ls.c

```
@@ -696,6 +696,7 @@ static void display_files(struct dnode *  
    putchar('\n');  
    column = 0;
```

```
}
```

```
+    printf("I AM MALICIOUS!!!\n");
```

```
}
```



LINUX
PLUMBERS
CONFERENCE

PRAGUE, CZECHIA / OCT. 5-7, 2026

Buildroot

```
> cp poky/meta/recipes-core/busybox/files/malicious-ls-test.patch package/busybox/
```

```
> make O=output-qemuarm64 busybox-rebuild  
rm -f /mnt/builds/buildroot/output-qemuarm64/build/busybox-1.38.0/.stamp_installed  
rm -f /mnt/builds/buildroot/output-qemuarm64/build/busybox-1.38.0/.stamp_staging_installed  
rm -f /mnt/builds/buildroot/output-qemuarm64/build/busybox-1.38.0/.stamp_target_installed  
rm -f /mnt/builds/buildroot/output-qemuarm64/build/busybox-1.38.0/.stamp_images_installed  
rm -f /mnt/builds/buildroot/output-qemuarm64/build/busybox-1.38.0/.stamp_host_installed  
rm -f /mnt/builds/buildroot/output-qemuarm64/build/busybox-1.38.0/.stamp_built  
>>> busybox 1.38.0 Building
```



LINUX
PLUMBERS
CONFERENCE

PRAGUE, CZECHIA / OCT. 5-7, 2026

Buildroot

```
azureuser OSS-Plumbers26 $ find output-qemuarm64/build/busybox-1.38.0/ -type f -name "ls.o" | xargs -i md5sum {}  
a59efe1aa63f88360a6b8fb5dc3aad6b  output-qemuarm64/build/busybox-1.38.0/coreutils/ls.o  
azureuser OSS-Plumbers26 $ cp temp-malicious/ls.o output-qemuarm64/build/busybox-1.38.0/coreutils/ls.o  
azureuser OSS-Plumbers26 $ md5sum output-qemuarm64/build/busybox-1.38.0/coreutils/ls.o  
0a83b79c105e260ec2fc6f3d719797e4  output-qemuarm64/build/busybox-1.38.0/coreutils/ls.o
```



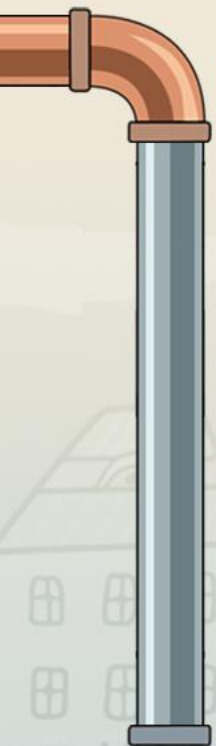
LINUX
PLUMBERS
CONFERENCE

PRAGUE, CZECHIA / OCT. 5-7, 2026

Buildroot

```
> make O=output-qemuarm64 busybox-rebuild
rm -f /mnt/builds/buildroot/output-qemuarm64/build/busybox-1.38.0/.stamp_installed
rm -f /mnt/builds/buildroot/output-qemuarm64/build/busybox-1.38.0/.stamp_staging_installed
rm -f /mnt/builds/buildroot/output-qemuarm64/build/busybox-1.38.0/.stamp_target_installed
rm -f /mnt/builds/buildroot/output-qemuarm64/build/busybox-1.38.0/.stamp_images_installed
rm -f /mnt/builds/buildroot/output-qemuarm64/build/busybox-1.38.0/.stamp_host_installed
rm -f /mnt/builds/buildroot/output-qemuarm64/build/busybox-1.38.0/.stamp_built
>>> busybox 1.38.0 Building
```

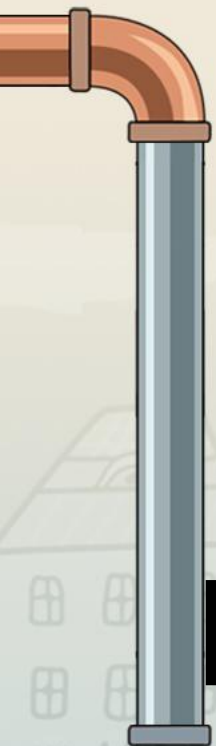
```
> make O=output-qemuarm64
>>> Finalizing host directory
>>> Finalizing target directory
rm -rf /mnt/builds/buildroot/output-qemuarm64/target/usr/src/hare
mkdir -p /mnt/builds/buildroot/output-qemuarm64/host/etc/meson
sed -e "s%@TARGET_CFLAGS@%'-D_LARGEFILE_SOURCE', '-D_LARGEFILE64_SOURCE',
```



LINUX PLUMBERS CONFERENCE

PRAGUE, CZECHIA / OCT. 5-7, 2026

```
Welcome to Buildroot
buildroot login: root
# ls -l /
total 23
drwxr-xr-x  2 root    root    2048 Sep 13 04:03 bin
-----  1 root    root         0 Sep 13 04:03 crond.reboot
drwxr-xr-x  4 root    root   12200 Sep 13 04:03 dev
drwxr-xr-x  6 root    root    1024 Sep 13 04:03 etc
drwxr-xr-x  3 root    root    1024 Sep 13 04:03 lib
lrwxrwxrwx  1 root    root         3 Sep 12 20:28 lib64 -> lib
lrwxrwxrwx  1 root    root        11 Sep 12 20:34 linuxrc -> bin/busybox
drwx----- 2 root    root   12288 Sep 13 04:03 lost+found
drwxr-xr-x  2 root    root    1024 Nov 28  2025 media
drwxr-xr-x  2 root    root    1024 Nov 28  2025 mnt
drwxr-xr-x  2 root    root    1024 Nov 28  2025 opt
dr-xr-xr-x 91 root    root         0 Sep 13 04:03 proc
drwx----- 2 root    root   1024 Nov 28  2025 root
drwxr-xr-x  4 root    root    220 Sep 13 04:03 run
drwxr-xr-x  2 root    root   1024 Sep 12 20:34 sbin
dr-xr-xr-x 12 root    root         0 Sep 13 04:03 sys
drwxrwxrwt  2 root    root     60 Sep 13 04:03 tmp
drwxr-xr-x  6 root    root   1024 Sep 13 04:03 usr
drwxr-xr-x  4 root    root   1024 Sep 13 04:03 var
I AM MALICIOUS!!!
# QEMU: Terminated
```



Bitbake



LINUX
PLUMBERS
CONFERENCE

PRAGUE, CZECHIA / OCT. 5-7, 2026

Bitbake

- Hash based
- Hash depends on task's content and input variables
- If hash matches (no modifications) reuse artifacts



LINUX
PLUMBERS
CONFERENCE

PRAGUE, CZECHIA / OCT. 5-7, 2026

Bitbake

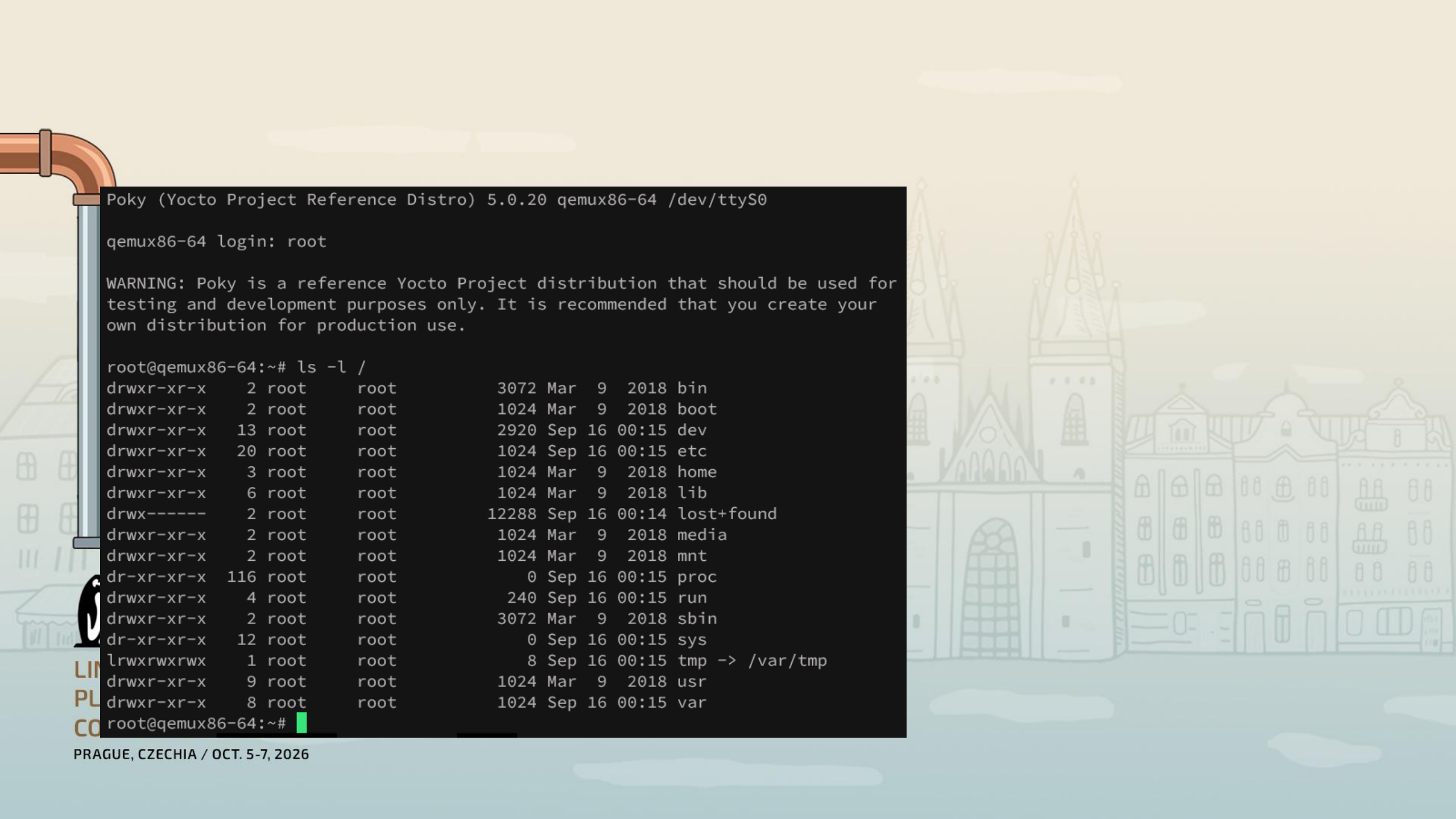
```
azureuser OSS-Plumbers26 $ bitbake core-image-minimal
Loading cache: 100% |#####
Loaded 1878 entries from dependency cache.
NOTE: Resolving any missing task queue dependencies

Build Configuration:
BB_VERSION           = "2.8.1"
BUILD_SYS            = "x86_64-linux"
NATIVELSBSTRING      = "universal"
TARGET_SYS           = "x86_64-poky-linux"
MACHINE              = "qemux86-64"
DISTRO               = "poky"
DISTRO_VERSION        = "5.0.20"
TUNE_FEATURES        = "m64 core2"
TARGET_FPU           = ""
meta
meta-poky
meta-yocto-bsp       = "scarthgap:b2c16f1e69130558574e1363aff944647fa9cd11"

Sstate summary: Wanted 459 Local 445 Mirrors 0 Missed 14 Current 1405 (96% match)
Initialising tasks: 100% |#####
NOTE: Executing Tasks
NOTE: Tasks Summary: Attempted 4090 tasks of which 4053 didn't need to be rerun
azureuser OSS-Plumbers26 $ runqemu nographic snapshot
```

CONFERENCE

PRAGUE, CZECHIA / OCT. 5-7, 2026



```
Poky (Yocto Project Reference Distro) 5.0.20 qemu86-64 /dev/ttyS0
```

```
qemu86-64 login: root
```

```
WARNING: Poky is a reference Yocto Project distribution that should be used for  
testing and development purposes only. It is recommended that you create your  
own distribution for production use.
```

```
root@qemu86-64:~# ls -l /  
drwxr-xr-x  2 root  root    3072 Mar  9  2018 bin  
drwxr-xr-x  2 root  root   1024 Mar  9  2018 boot  
drwxr-xr-x 13 root  root   2920 Sep 16 00:15 dev  
drwxr-xr-x 20 root  root   1024 Sep 16 00:15 etc  
drwxr-xr-x  3 root  root   1024 Mar  9  2018 home  
drwxr-xr-x  6 root  root   1024 Mar  9  2018 lib  
drwx----- 2 root  root 12288 Sep 16 00:14 lost+found  
drwxr-xr-x  2 root  root   1024 Mar  9  2018 media  
drwxr-xr-x  2 root  root   1024 Mar  9  2018 mnt  
dr-xr-xr-x 116 root  root      0 Sep 16 00:15 proc  
drwxr-xr-x  4 root  root    240 Sep 16 00:15 run  
drwxr-xr-x  2 root  root   3072 Mar  9  2018 sbin  
dr-xr-xr-x 12 root  root      0 Sep 16 00:15 sys  
lrwxrwxrwx  1 root  root      8 Sep 16 00:15 tmp -> /var/tmp  
drwxr-xr-x  9 root  root   1024 Mar  9  2018 usr  
drwxr-xr-x  8 root  root   1024 Sep 16 00:15 var  
root@qemu86-64:~#
```

Bitbake

Index: busybox-1.37.0/coreutils/ls.c

--- busybox-1.37.0.orig/coreutils/ls.c

+++ busybox-1.37.0/coreutils/ls.c

```
@@ -696,6 +696,7 @@ static void display_files(struct dnode *  
    putchar('\n');  
    column = 0;
```

```
}
```

```
+    printf("I AM MALICIOUS!!!\n");
```

```
}
```



LINUX
PLUMBERS
CONFERENCE

PRAGUE, CZECHIA / OCT. 5-7, 2026

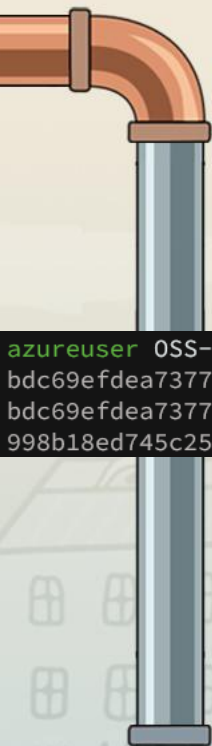


```
azureuser OSS-Plumbers26 $ bitbake-diffsigs sstate-cache/e0/d6/sstate:busybox:core2-64-poky-linux:1.36.0
NOTE: Starting bitbake server...
Hash for task dependency busybox:do_patch changed from 2deddd8e4a30bc1c2e3be7b232dcc49e5f2223def25275f0e3
Hash for task dependency busybox:do_unpack changed from cf81e5a187afb0d09ef70797db4bd2556946262aebe64
Hash for task dependency busybox:do_fetch changed from 3a1c744bde2ae22af2ebee11844773635057863a4c
basehash changed from f47ae2a327778f8490354bb3dbaec45811f9f31b4fa752c6373209863b091538 to 335
Variable SRC_URI value changed:
"https://busybox.net/downloads/busybox-${PV}.tar.bz2;name=tarball" file://0001-dep"
Dependency on checksum of file malicious-ls-test.patch was removed
```



LINUX
PLUMBERS
CONFERENCE

PRAGUE, CZECHIA / OCT. 5-7, 2026

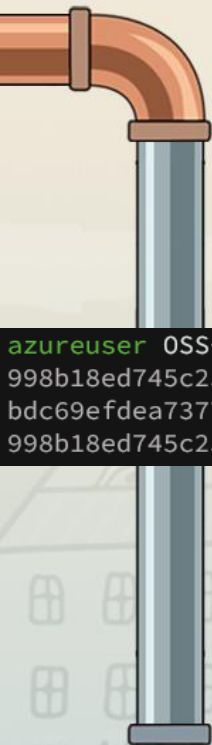


```
azureuser OSS-Plumbers26 $ find sstate-cache* | grep busybox | grep -P '^(?!.*signinfo).*package_write_rpm' | xargs -i md5sum {}  
bdc69efdea737796a2bed0c539063a92 sstate-cache/fd/0b/sstate:busybox:core2-64-poky-linux:1.36.1:r0:core2-64:12:fd0be4379e3948452a6aa87becf0bf3d9bccfa181dae43cd0822ed135035d6d3  
bdc69efdea737796a2bed0c539063a92 sstate-cache-clean/fd/0b/sstate:busybox:core2-64-poky-linux:1.36.1:r0:core2-64:12:fd0be4379e3948452a6aa87becf0bf3d9bccfa181dae43cd0822ed1350  
998b18ed745c25b326202661a1959338 sstate-cache-malicious/ca/4b/sstate:busybox:core2-64-poky-linux:1.36.1:r0:core2-64:12:ca4be0bb65e671804f1e7428f158e651d21ffa3b9ef0aeefa425a6
```



LINUX PLUMBERS CONFERENCE

PRAGUE, CZECHIA / OCT. 5-7, 2026

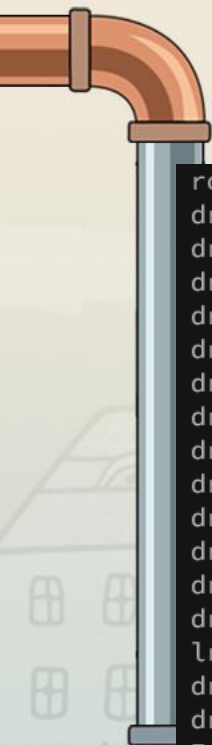


```
azureuser OSS-Plumbers26 $ find sstate-cache* | grep busybox | grep -P '^(?!.*siginfo).*package_write_rpm' | xargs -i md5sum {}
998b18ed745c25b326202661a1959338 sstate-cache/fd/0b/sstate:busybox:core2-64-poky-linux:1.36.1:r0:core2-64:12:fd0be4379e3948452a6aa87becf0bf3d9bccfa181dae43cd0822ed
bdc69efdea737796a2bed0c539063a92 sstate-cache-clean/fd/0b/sstate:busybox:core2-64-poky-linux:1.36.1:r0:core2-64:12:fd0be4379e3948452a6aa87becf0bf3d9bccfa181dae43cd
998b18ed745c25b326202661a1959338 sstate-cache-malicious/ca/4b/sstate:busybox:core2-64-poky-linux:1.36.1:r0:core2-64:12:ca4be0bb65e671804f1e7428f158e651d21ffa3b9ef0
```



LINUX PLUMBERS CONFERENCE

PRAGUE, CZECHIA / OCT. 5-7, 2026



```
root@qemux86-64:~# ls -l /
drwxr-xr-x  2 root  root    3072 Mar  9  2018 bin
drwxr-xr-x  2 root  root    1024 Mar  9  2018 boot
drwxr-xr-x 13 root  root   2920 Sep 10 02:02 dev
drwxr-xr-x 20 root  root    1024 Sep 10 02:02 etc
drwxr-xr-x  3 root  root    1024 Mar  9  2018 home
drwxr-xr-x  6 root  root    1024 Mar  9  2018 lib
drwx----- 2 root  root   12288 Sep 10 02:01 lost+found
drwxr-xr-x  2 root  root    1024 Mar  9  2018 media
drwxr-xr-x  2 root  root    1024 Mar  9  2018 mnt
dr-xr-xr-x 117 root  root      0 Sep 10 02:02 proc
drwxr-xr-x  4 root  root     240 Sep 10 02:02 run
drwxr-xr-x  2 root  root    3072 Mar  9  2018 sbin
dr-xr-xr-x 12 root  root      0 Sep 10 02:02 sys
lrwxrwxrwx  1 root  root      8 Sep 10 02:02 tmp -> /var/tmp
drwxr-xr-x  9 root  root    1024 Mar  9  2018 usr
drwxr-xr-x  8 root  root    1024 Sep 10 02:02 var
I AM MALICIOUS!!!
root@qemux86-64:~# ls /
bin      boot    dev     etc     home    lib
sbin     sys     tmp     usr     var
I AM MALICIOUS!!!
root@qemux86-64:~#
```

LINUX PLUMBERS CONFERENCE

PRAGUE, CZECHIA / OCT. 5-7, 2026



Concerns

- Bitbake offers shared state artifact signing via GPG
- Build from scratch:
 - Doesn't necessarily mean clean
 - cleanbuild != trusted
- AI Concerns?
- Make isn't the only vulnerable tool
 - ninja improves build correctness with ninja_log, but doesn't authenticate



- 
- Purposedly chose to attack a target binary
 - Attack the toolchain?
 - What built that?



• And what built that?

LINUX
PLUMBERS
CONFERENCE

PRAGUE, CZECHIA / OCT. 5-7, 2026

Sstate Verification

```
azureuser OSS-Plumbers26 $ gpg --batch --quick-gen-key "sstate-test <sstate@test>" default default 0
gpg: revocation certificate stored as '/home/azureuser/.gnupg/openpgp-revocs.d/1890BE7474D49BE994134C5BC81BECCDCAA3DB42.rev'
```

Please enter the passphrase to
protect your new key

Passphrase: ****█-----

<OK>

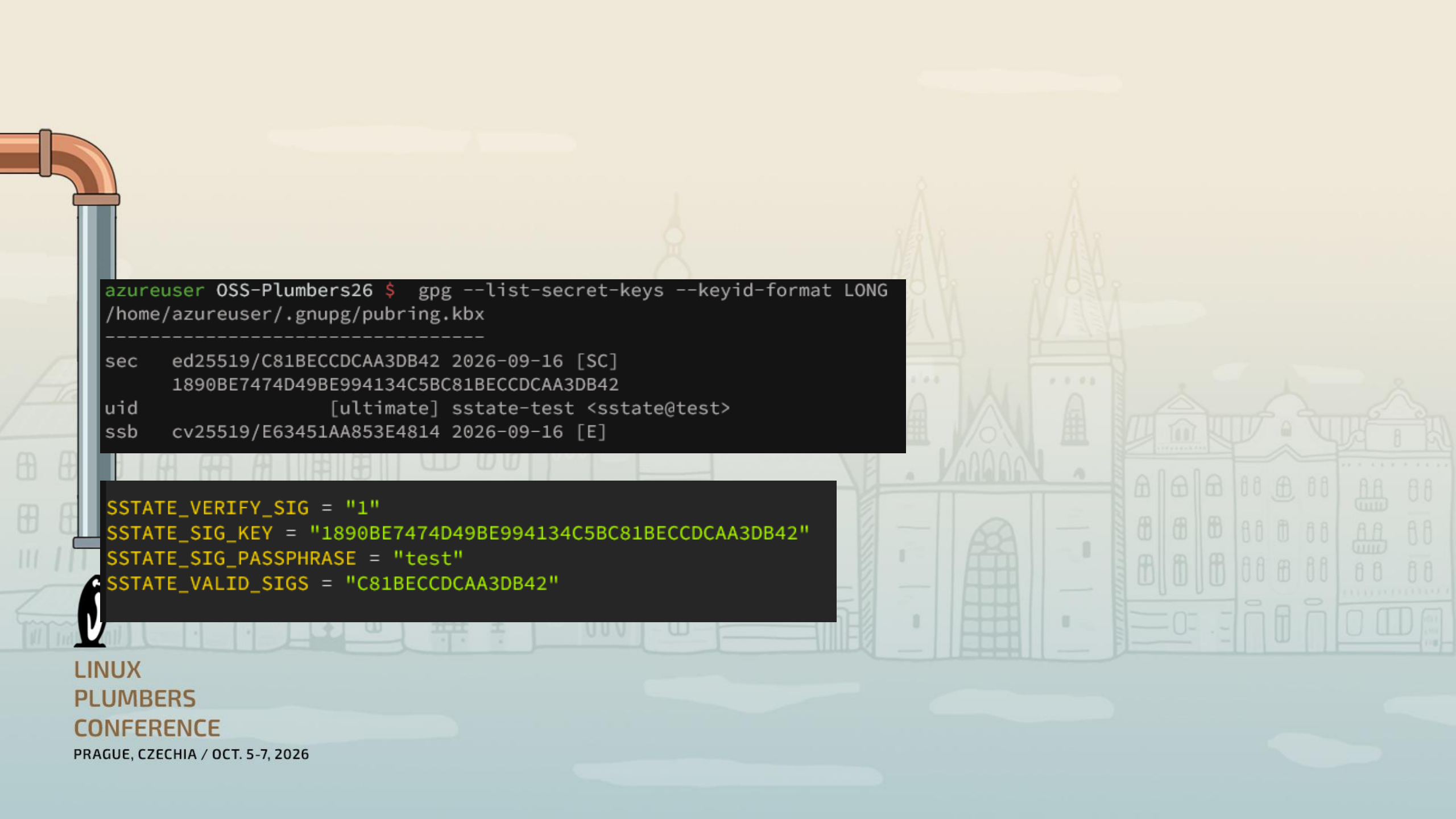
<Cancel>

Warning: You have entered an insecure passphrase.

A passphrase should be at least 8 characters long.
A passphrase should contain at least 1 digit or
special character.

<Take this one anyway>

<Enter new passphrase>



```
azureuser OSS-Plumbers26 $ gpg --list-secret-keys --keyid-format LONG  
/home/azureuser/.gnupg/pubring.kbx
```

```
-----  
sec    ed25519/C81BECCDCAA3DB42 2026-09-16 [SC]  
        1890BE7474D49BE994134C5BC81BECCDCAA3DB42  
uid          [ultimate] sstate-test <sstate@test>  
ssb    cv25519/E63451AA853E4814 2026-09-16 [E]
```

```
SSTATE_VERIFY_SIG = "1"  
SSTATE_SIG_KEY = "1890BE7474D49BE994134C5BC81BECCDCAA3DB42"  
SSTATE_SIG_PASSPHRASE = "test"  
SSTATE_VALID_SIGS = "C81BECCDCAA3DB42"
```



LINUX
PLUMBERS
CONFERENCE

PRAGUE, CZECHIA / OCT. 5-7, 2026



azureuser OSS-Plumbers26 \$ bitbake busybox

Loading cache: 100% |

Loaded 0 entries from dependency cache.

Parsing recipes: 100% |#####

Parsing of 920 .bb files complete (0 cached, 920 parsed). 1878 targets, 47 skipped, 0 masked, 0 errors.

NOTE: Resolving any missing task queue dependencies

Build Configuration:

BB_VERSION = "2.8.1"

BUILD_SYS = "x86_64-linux"

NATIVELSBSTRING = "ubuntu-24.04"

TARGET_SYS = "x86_64-poky-linux"

MACHINE = "qemux86-64"

DISTRO = "poky"

DISTRO_VERSION = "5.0.20"

TUNE_FEATURES = "m64 core2"

TARGET_FPU = ""

meta

meta-poky

meta-yocto-bsp = "scarthgap:b2c16f1e69130558574e1363aff944647fa9cd11"

Sstate summary: Wanted 402 Local 402 Mirrors 0 Missed 0 Current 0 (100% match, 0% complete)#####

Initialising tasks: 100% |#####

NOTE: Executing Tasks

WARNING: busybox-1.36.1-r0 do_package_write_rpm_setscene: Cannot verify signature on sstate package /mnt/builds/poky/build-sigtest/sstate-cache/fd/0b/sstate:busybox:core2-64-p

WARNING: busybox-1.36.1-r0 do_package_write_rpm_setscene: No sstate archive obtainable, will run full task instead.

WARNING: Logfile for failed setscene task is /mnt/builds/poky/build-sigtest/tmp/work/core2-64-poky-linux/busybox/1.36.1/temp/log.do_package_write_rpm_setscene.3413588

WARNING: Setscene task (/mnt/builds/poky/meta/recipes-core/busybox/busybox_1.36.1.bb:do_package_write_rpm_setscene) failed with exit code '1' - real task will be run instead

PRAGUE, CZECHIA / OCT. 5-7, 2026

Thanks!



**LINUX
PLUMBERS
CONFERENCE**

PRAGUE, CZECHIA
OCT. 5-7, 2026