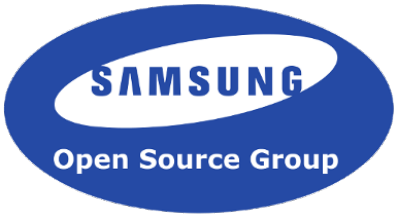


Security - USB Over IP on Linux

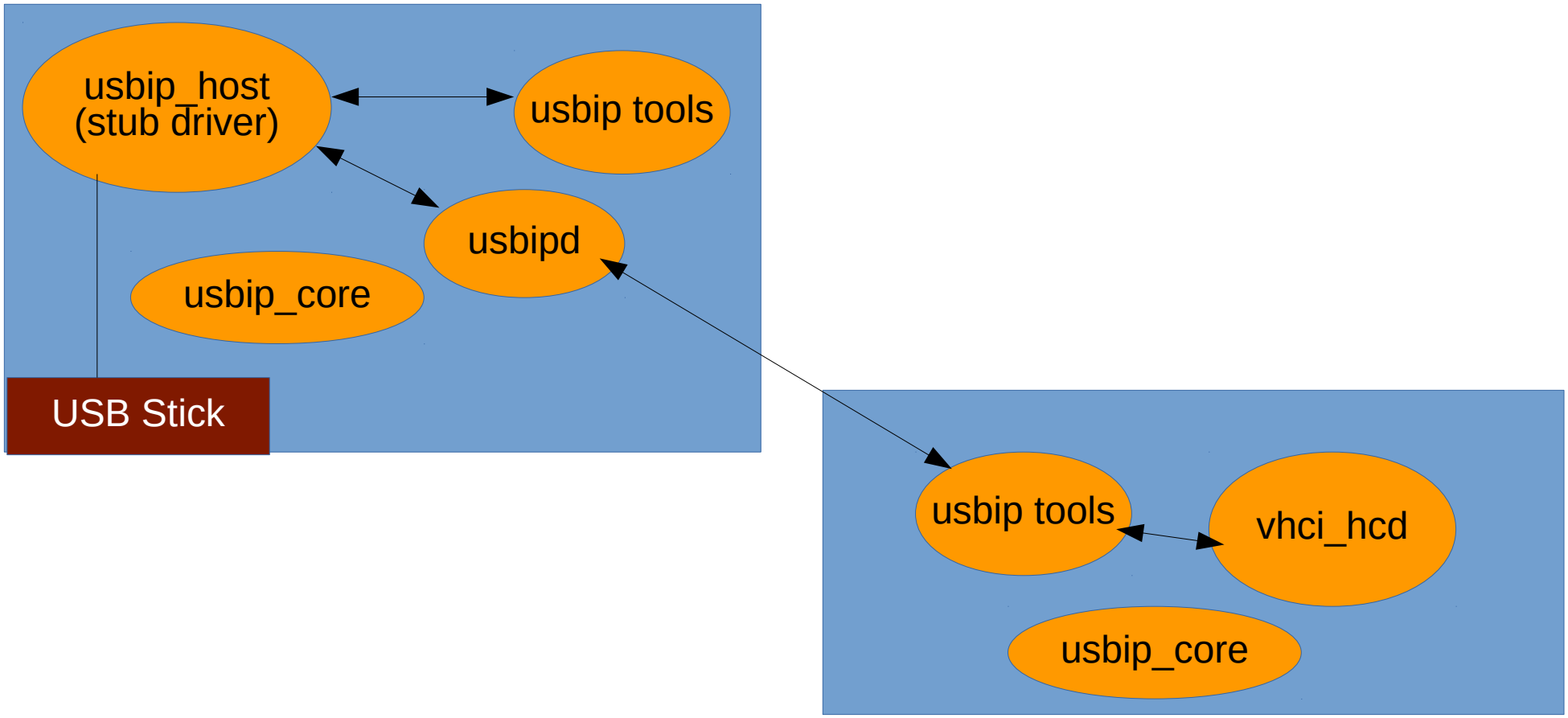
Open Source Summit Aug 31 2018

Shuah Khan
Samsung Open Source Group
shuah.kh@samsung.com
shuah@kernel.org
@ShuahKhan

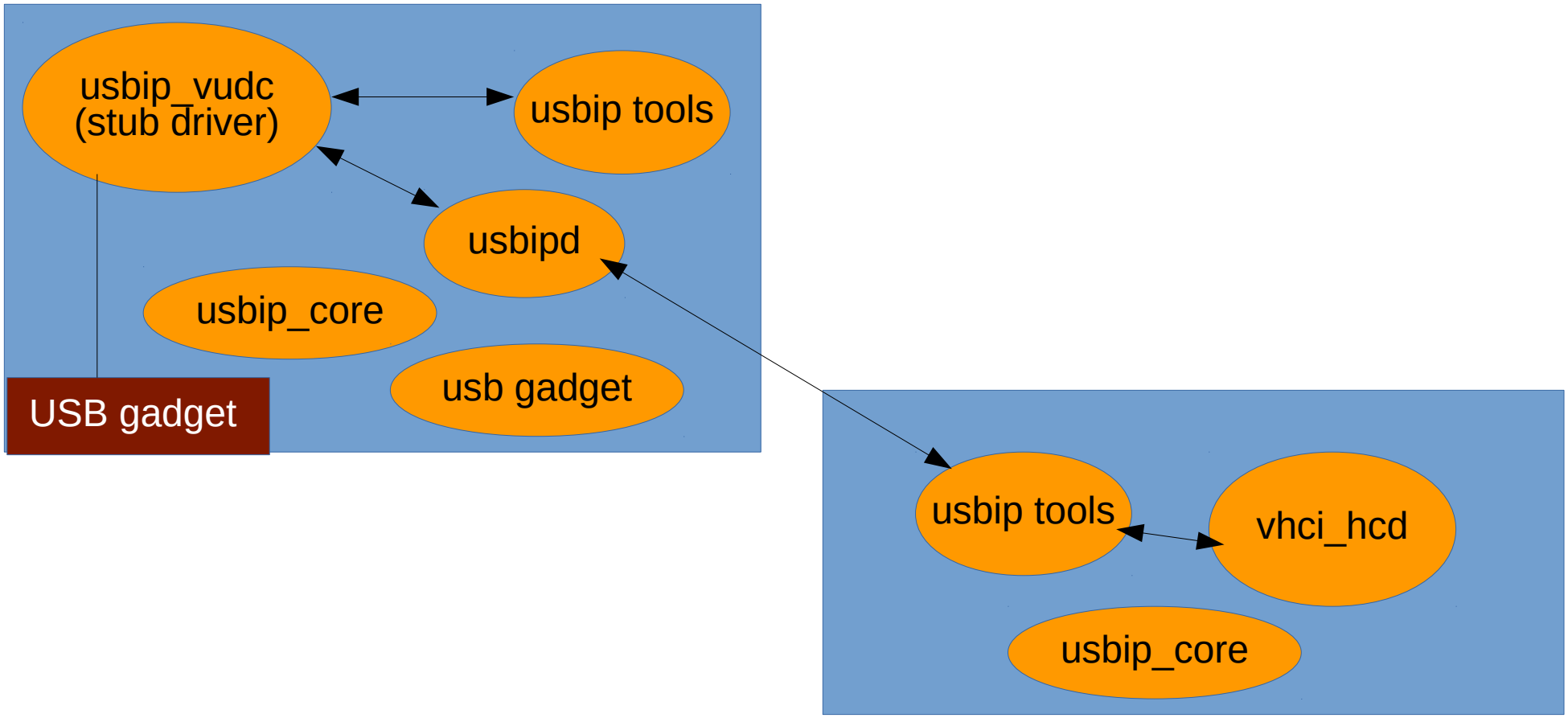
SAMSUNG
Open Source Group

USB over IP

USB over IP Server/Client



USB over IP Server/Client



Enabling USB over IP ...

SAMSUNG
Open Source Group

- Sources
  - drivers/usb/usbip
  - tools/usb/usbip
  - tools/testing/drivers/usb/usbip
  - Documentation/usb
  - tools/usb/usbip/vudc/vudc_server_example.sh

Enabling USB over IP ...

SAMSUNG
Open Source Group

- Configuration
  - USBIP_CORE
  - USBIP_HOST
  - USBIP_VHCI_HCD
  - USBIP_VUDC
  - USBIP_DEBUG

Building tools ...

SAMSUNG
Open Source Group

1) cd tools/usb/usbip
2) ./autogen.sh
3) ./configure
4) make

SAMSUNG
Open Source Group

Exporting/importing devices ...

Exporting devices ...

SAMSUNG
Open Source Group

- Load usbip_host module
  - modprobe usbip_host
  - cd tools/usb/usbip
- Check exportable devices on the server:
  - src/usbip list -l
- Start usbip daemon:
  - src/usbipd -D
- Bind device
  - src/usbip bind -b <busid>

Exporting devices ...

SAMSUNG
Open Source Group

```
# src/usbip list -l
 - busid 3-10.2 (0461:4e04)
   Primax Electronics, Ltd : unknown product (0461:4e04)

 - busid 3-10.4 (04b3:310c)
   IBM Corp. : Wheel Mouse (04b3:310c)

# src/usbip bind -b 3-10.2
usbip: info: bind device on busid 3-10.2: complete

# ls /sys/bus/usb/drivers/usbip-host
3-10.2  bind  match_busid  rebind  uevent  unbind

# cat /sys/bus/usb/drivers/usbip-host/match_busid
3-10.2
```

Un-exporting devices ...

SAMSUNG
Open Source Group

```
# src/usbip unbind -b 3-10.2
usbip: info: unbind device on busid 3-10.2: complete

# src/usbip bind -b 3-10.2
usbip: info: bind device on busid 3-10.2: complete

# ls /sys/bus/usb/drivers/usbip-host
bind  match_busid  rebind  uevent  unbind

# cat /sys/bus/usb/drivers/usbip-host/match_busid
```

Importing devices ...

SAMSUNG
Open Source Group

- Load vhci_hcd module
  - modprobe vhci_hcd
  - cd tools/usb/usbip
- Check exported devies:
  - src/usbip list -r localhost
- Import device
  - src/usbip attach -r localhost -b <busid>

Importing devices ...

SAMSUNG
Open Source Group

```
# src/usbip list -r localhost
Exportable USB devices
======================
 - localhost
      3-10.2: Primax Electronics, Ltd : unknown product (0461:4e04)
           : /sys/devices/pci0000:00/0000:00:14.0/usb3/3-10/3-10.2
           : (Defined at Interface level) (00/00/00)

#src/usbip attach -r localhost -b 3-10.2
```

Importing devices ...

SAMSUNG
Open Source Group

```
# ls /sys/bus/platform/drivers/vhci_hcd/vhci_hcd.0
attach  driver          modalias  power   subsystem  usb5  usbip_debug
detach  driver_override  nports    status  uevent     usb6

# cat /sys/bus/platform/drivers/vhci_hcd/vhci_hcd.0/status
hub port sta spd dev      sockfd local_busid
hs  0000 006 001 00030003 000003 5-1
hs  0001 004 000 00000000 000000 0-0
hs  0002 004 000 00000000 000000 0-0
hs  0003 004 000 00000000 000000 0-0
hs  0004 004 000 00000000 000000 0-0
hs  0005 004 000 00000000 000000 0-0
hs  0006 004 000 00000000 000000 0-0
hs  0007 004 000 00000000 000000 0-0
ss  0008 004 000 00000000 000000 0-0
ss  0009 004 000 00000000 000000 0-0
ss  0010 004 000 00000000 000000 0-0
ss  0011 004 000 00000000 000000 0-0
ss  0012 004 000 00000000 000000 0-0
ss  0013 004 000 00000000 000000 0-0
ss  0014 004 000 00000000 000000 0-0
ss  0015 004 000 00000000 000000 0-0
```

Managing imported devices ...

SAMSUNG
Open Source Group

- List imported devices
  - src/usbip port
- Mount devices for access
  - mount *dev/sdc1 mount_dir*
- Detach device
  - src/usbip detach -p <port_num>

Managing imported devices ...

SAMSUNG
Open Source Group

```
# src/usbip port
Imported USB devices
====================
Port 00: <Port in Use> at Low Speed(1.5Mbps)
       Primax Electronics, Ltd : unknown product (0461:4e04)
       5-1 -> usbip://localhost:3240/3-10.2
           -> remote bus/dev 003/003

# mount dev/sdc1 usb_stick

#src/usbip detach -p 00
usbip: info: Port 0 is now detached!
```

Managing imported devices ...

SAMSUNG
Open Source Group

```
# cat /sys/bus/platform/drivers/vhci_hcd/vhci_hcd.0/status
hub port sta spd dev      sockfd local_busid
hs  0000 004 000 00000000 000000 0-0
hs  0001 004 000 00000000 000000 0-0
hs  0002 004 000 00000000 000000 0-0
hs  0003 004 000 00000000 000000 0-0
hs  0004 004 000 00000000 000000 0-0
hs  0005 004 000 00000000 000000 0-0
hs  0006 004 000 00000000 000000 0-0
hs  0007 004 000 00000000 000000 0-0
ss  0008 004 000 00000000 000000 0-0
ss  0009 004 000 00000000 000000 0-0
ss  0010 004 000 00000000 000000 0-0
ss  0011 004 000 00000000 000000 0-0
ss  0012 004 000 00000000 000000 0-0
ss  0013 004 000 00000000 000000 0-0
ss  0014 004 000 00000000 000000 0-0
ss  0015 004 000 00000000 000000 0-0
```

Security vulnerabilities ...

SAMSUNG
Open Source Group

- Malicious USBIP packets via hacked USBIP tools
  - forcing kernel to allocate large amounts of memory
  - kernel panics
- Error and boundary checks on data fields.

Security vulnerabilities ...

SAMSUNG
Open Source Group

- Input args from user-space
  - potential exploitation of the Spectre variant 1 vulnerability
- Sanitize the args before use
  - add array_index_nospec() after bounds check
  - if CPU speculates past the bounds check, array_index_nospec() will clamp the index within the range of [0, siize]

SAMSUNG
Open Source Group

```
if (*pdev_nr >= vhci_num_controllers) {
        pr_err("pdev %u\n", *pdev_nr);
        return 0;
 }
 *pdev_nr = array_index_nospec(*pdev_nr, vhci_num_controllers);

 if (*rhport >= VHCI_HC_PORTS) {
        pr_err("rhport %u\n", *rhport);
        return 0;
 }
 *rhport = array_index_nospec(*rhport, VHCI_HC_PORTS);
```

Security vulnerabilities ...

SAMSUNG
Open Source Group

- Kernel addresses exposed in messages
- Kernel addresses exposed in sysfs files

Security fixes ...

SAMSUNG
Open Source Group

- Removed kernel address leaks in messages
- Removed kernel addresses in user API (sysfs files)
- Added missing error and boundary checks on input from user-space
- 60+ patches so far.

Tightening loose ends ...

SAMSUNG
Open Source Group

- Module removal paths – rebind devices to original drivers
- Prevent exporting devices that are imported from server
- Regression test added to selftests.

Take away ...

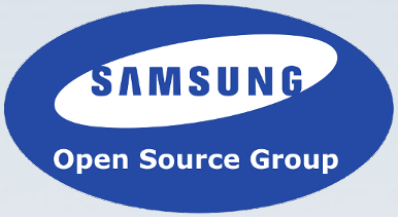
SAMSUNG
Open Source Group

- Design to avoid security vulnerabilities
- Avoid leaking kernel addresses in messages
- Avoid exposing kernel addresses in user API
- Error and boundary checks on input from user-space

Container support ...

SAMSUNG
Open Source Group

- Device cgroups are used to control access once devices are imported
- Imported devices are global and visible to all containers
- Working on limiting visibility to container that imported the device (at the client side)
- Work in progress to add ability to reserve device for a remote i.e remote allowed to import (at server side at bind time)



Thank You!