Secure and Safe Updates for Your Embedded Device

(And how to solve this with the RAUC update tool)

Enrico Jörns

FOSDEM 2017
Embedded, IoT, ... Updating?

- Security fixes!!!
- General bug fixes!!
- New Features!
Structure

• Updating Embedded Systems

• Introducing RAUC

• DEMO

• Conclusion
Updating – The simple View

Updating…
Do not turn off!
Updating – The Reality

Which partition to update?

Right Target?

Right Author?

Access?

Bootloader?

Run on?  Upload Update  Verify Check  X Power Failure
What‘s so special on Embedded Updates?

And why not simply write a bash script?..
Supervised Updates

Update?

$ sudo apt-get upgrade

Unattended Updates

Update?

Do not turn off!!
Updating Embedded Devices

Key Requirements:

- **Safety**
  - Update process should not fail!
  - Still updatable after failed update
  - Recover from runtime issues

- **Security**
  - Prevent unauthorized access

Further Restrictions:

- Storage handling (NAND, NOR, eMMC, ...)
- Limited resources (storage, data rate, ...)

⚠️ Install only well tested software state

⚠️ Do NOT brick your device!
System Redundancy

No redundancy

Asymmetric

Symmetric

→ Service technician

→ Updatable, Non-operating

→ Updatable, Operating (old version)
Update Atomicity

Start Update from A

Change Bootsource to B

Critical operation

Perform Update of B

Atomic Operation!
Secure Updates

→ Prevent unauthorized installation

Trusted Transport

Signed Update

✔ Download
✔ USB stick

✔ Download
✔ USB stick
How to not turn a Toaster into a Printer
Or: Hot to make sure you don‘t install the wrong image

Check Hardware:

⚠️ Same hardware might operate in different setups / devices

Explicit identification:

Update for „PiToast 2000“

- accept
- reject

„PiToast 2000“

„PiPrint Plus“
Determine and handle Update Targets

→ Requires configuration, meta-information, custom handler
Other Things to take care of

- Error Handling
  - Check all function/subprocess return values!
  - Abort correctly
- Data Handling
  - Single storage location?
  - Redundant storage?
- Watchdog handling
- Update Format
  - Version handling?
- Extensibility
  - ...
RAUC – Robust Auto-Update Controller

- LGPL-2.1
- C with GLib
- Autotools

Slide 16 - © Pengutronix - http://www.pengutronix.de - 02/05/2017
RAUC - Bundles

A Bundle describes the intended target state of the device

- Manifest
  - script: sha=7fcd6dc45193... size=102B
  - image: sha=7fcd6dc85193... size=203482
  - bitstream: sha=7fcdc8945193... size=4212

- SquashFS

- X509 Signature

- RAUC bundle
RAUC – Slot Handling

Slot: Anything we might want to update
RAUC – Configuration

```
[system]
compatible=MyProduct2000
bootloader=barebox

[keyring]
path=/etc/rauc/keyring.pem

[handlers]
post-install=/sbin/postinst.sh

[slot.rootfs.0]
device=/dev/sda0
type=ext4
bootname=system0

[slot.rootfs.1]
device=/dev/sdal
type=ext4
bootname=system1
```

[update]
compatible=MyProduct2000
version=2017.02-4

```
[image.rootfs]
filename=rootfs.ext4
size=419430400
sha256=b14c1457dc1046...

[image.appfs]
filename=appfs.ext4
size=219430400
sha256=ecf4c031d01cb9...
hooks=post-install
```

System Configuration on Target
Using RAUC on your next Device

- System Integration
  - Yocto integration: meta-pxt layer (→ meta-rauc)
  - PTXdist integration: coming soon
  - Manual Integration (system.conf, keys, manifest)

- Usage
  - Create Bundle (Host)
    ```bash
    rauc bundle --key=... content/my-bundle.raucb
    ```
  - Install Bundle (Target)
    ```bash
    rauc install my-bundle.raucb
    ```

- Integrate into Application (using D-Bus)
DEMO: Update Rollout with HawkBit

- Deployment Server
- Python Script
- DDI API
- D-Bus
- RAUC Service
- PTXdist

Yocto

Rootfs A

Barebox (Bootstate)

Rootfs B
What we’ve learned...

1) Updates are mandatory
2) Updates are non-trivial
3) Only install well tested software states
4) Use (FOSS) update frameworks
Thanks!

🔗 RAUC on GitHub:
https://github.com/jluebbe/rauc

📚 Documentation:
http://rauc.readthedocs.io/

≡ meta-px Layer (will soon become meta-rauc):
https://git.pengutronix.de/cgit/meta-px/

 DateTimeKind Barebox Bootchooser:
http://barebox.de/doc/latest/user/bootchooser.html