BUS
ONLY
ONLY

sigfox

A concrete application of a custom OTA system upgrade

And a state of the art of the available open sources solution

Meetup – 16/01/2018

sigfox

1 Who am I?

2 What does Sigfox do?

3 What is a base station?

4 What are the base station constraints?

5 Why we choose to implement a custom solution?

6 How our update system works

7 Issues of our solution

8 Quick comparison with open sources solutions

sigfox

1

Who am I?

Who am I?

- A Sigfox employee for three years
- My main activities:
  - New platform integration
  - Build system
  - Board support packages
  - Core system features (e.g OTA, measured boot, encryption...)
- Free software enthusiast
- Contributor in my free time

sigfox

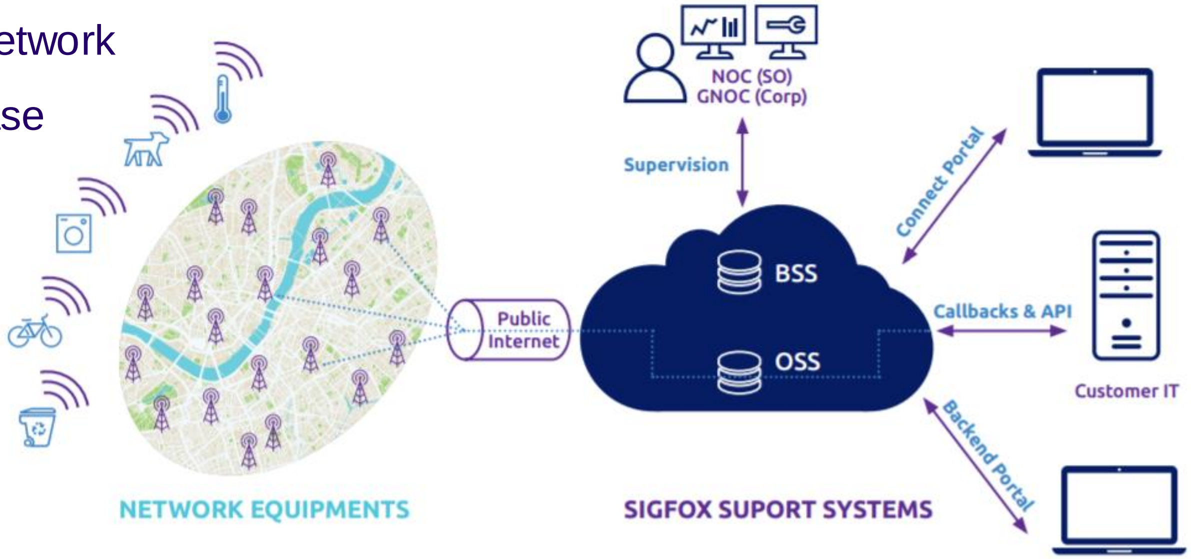
2

What does Sigfox do?

sigfox

What does Sigfox?

- Deploy a worldwide IoT network
  - Several thousand of base stations
  - +36 countries
- Offer data services
- Etc.



sigfox

3

What is a Sigfox base station?

What is a Sigfox base station ?

Access point which receive messages from devices to send them to our cloud.

- Hardware
  - CPU X86-64 / ARMv7 / ARMv8
  - RAM >= 1GBytes
  - Watchdog
  - SSD / eMMC / NAND >= 1GBytes
  - RADIO USB / SPI
  - Dual connectivity
  - TPM

- Software
  - Measured boot
  - Verified boot
  - Full encrypted
  - Fallback mechanism
  - Strongswan IPSec
  - Monitoring

sigfox

4

What are the base station constraints?

sigfox

What are the base station constraints?

- Can be upgradable without human intervention => Over the air upgrade
- Service availability should be maximum => Upgrade should be symmetric
- Lightweight Payloads usage => partial image based, tiny image size
- Failure resilience => Upgrade must be restarted at last step reached
- Configuration files can evolve => Require two persistent data partitions
- Failsafe upgrade => Fallback mechanism, slot must be functionally validated
- Security => Integrity verification, full encrypted filesystem
- Performance => System loaded in RAM

NB. A base station update may take several days when the connection is very slow.

5

Why we choose to implement a custom solution?

Why we choose to implement a custom solution?

- 6 years ago, there was no viable open source solution
- First implementation in base station prototype, had to be maintained
  - Using a custom Slack distribution
  - In inaccessible places
  - Without rollback mechanism
  - Need to quickly put in place a solution
- Now
  - Using OE build system
  - ~3K lines of code

6

How our upgrade system works

How our system upgrade works

Use rsync over SSH:

1. Make a local rsync
2. Make a remote rsync through a ssh connection to our infrastructure
3. Create a compressed squash image of the rootfs
4. Encrypts this squash image using a unique key through the TPM
5. Re-encrypt the data partition associated at this new version
6. Update bootloader flags
7. Reboot
8. Run post-upgrade tasks at boot
9. Validate functionally the slot after few minutes

7

Issues of our solution

Issues of our solution

- Upgrade is not atomic
  - Persistent data partitions patch/merge at first boot after update
- Custom integrity solution
  - We would replace it by IMA/EVM
- Cannot stores file security labels in *xattrs*
  - *Required to enable* access control security policies (e.g SELinux...)
- Downgrade is not possible
- Use file-level incremental synchronization
  - We would to use block-level incremental synchronization instead.

8

Quick comparison with opensource solutions

sigfox

Why we like to use an open source solutions?

In order to:

- improve portability and maintainability
- contribute and benefit from help of the community

Quick comparison with open sources solutions

Name	fallback	symmetric	atomic	technique	Data partition	bootloader	Type	Comm.	Verification
Sigfox Update	Yes	Yes	No	Partial image	2	Grub / Barebox / U-boot	File-based	http2 + ssh	Custom TPM integrity verification
Mender	Yes	Yes	Both	Full image	1	U-boot	Block-based	https enforced	Signed
Ostree	Yes	Yes	No	Docker file delta	1	Grub / U-boot	File-based	https	Signed
RAUC	Yes	Both	Both	Full image	1	Grub / Barebox / U-boot	Block-based / File-based	https / ssh	x509
swupdate	No	Both	No	Full image	1	Grub / U-boot	Block-based / File-based	https	Signed / encrypted
swupd	No	No	No	Full image	1	Grub	File-based	https	IMA / Signed / Smack / SELinux...
resin	Yes	Yes	Yes	Docker file delta	1	Grub / U-boot	File-based	https	Two-factor /

Questions ?

sigfox

Thank you!

sigfox