Unify CoT Tool

Xialin Liu

25-07-2024

Agenda

- Introduction to CoT – quick recap
- Motivation
- Solution - cot-dt2c command line tool
- Implementation
- Demo
- Future works

What is CoT

- Trusted Boot
  - Security feature ensures the integrity of boot process.
  - Verify if each stage of the boot process is authentic and unaltered (from firmware through the OS).
  - Prevent running unauthorized software/firmware on the device.
  - Authentication of the software/firmware is done by CoT.

- CoT is a sequence of authentication images which usually starts with a root of trust and culminates in a single data image.

Motivation

- Currently, the CoT have two options during the build process: CoT device tree file or its corresponding static c file.
- Two separate files are error prone and hard to maintain, therefore unifying the CoT file is beneficial.
- We cannot perform cross validation between the two options, need manual checks if they diverge in future updates.
- They are duplicate.
- For the platform that does not accept the CoT device tree file, there is no need to prepare a separate c file for CoT.

Solution – cot-dt2c

- Cot-dt2c tool
  - Automatically generate corresponding c file for CoT devicetree file.
  - Validate CoT devicetree file.
  - Converted CCA, Dualroot and TBBR CoT files into c file and integrated into build process on arm platform.
- Restructure CoT Devicetree file
  - BL1 CoT descriptor
    - Removed from CoT devicetree since it is fixed.
    - Exist in the repository as static c file.
  - BL2 CoT descriptor
    - Generated as c file by cot-dt2c during the build.

```
TF-A
├── build
│   ├── bl2_cot.c (generated)
├── fdts
│   ├── cca_cot_descriptor.dtsi
│   ├── dualroot_cot_descriptor.dtsi
│   └── tbbr_cot_descriptor.dtsi
├── drivers
│   └── auth
│       └── bl1_cot.c (static)
└── tools
    └── cot-dt2c
```

cot-dt2c Usage

```
Usage: cot-dt2c [OPTIONS] COMMAND [ARGS]...

Options:
  --version  Show the version and exit.
  --help     Show this message and exit.

Commands:
  convert-to-c
  validate-cot
```

```
Usage: cot-dt2c validate-cot [OPTIONS] INPUTFILE

Options:
  --help  Show this message and exit.
```

```
Usage: cot-dt2c convert-to-c [OPTIONS] INPUTFILE OUTPUTFILE

Options:
  --help  Show this message and exit.
```

Cot-dt2c Structure

- Data structure for each type of node in CoT
  - Certificate
  - Image
  - Trusted root public key
  - Non-volatile counter
- Implicit/explicit sanity checks for the CoT devicetree file
  - Unmatching brackets
  - Unmatching ifdef macro
  - Missing root certificate
  - Missing mandatory attributes
  - Malformed root of trust (certificate without parents, certificate referring to non-existing parent)
  - ...

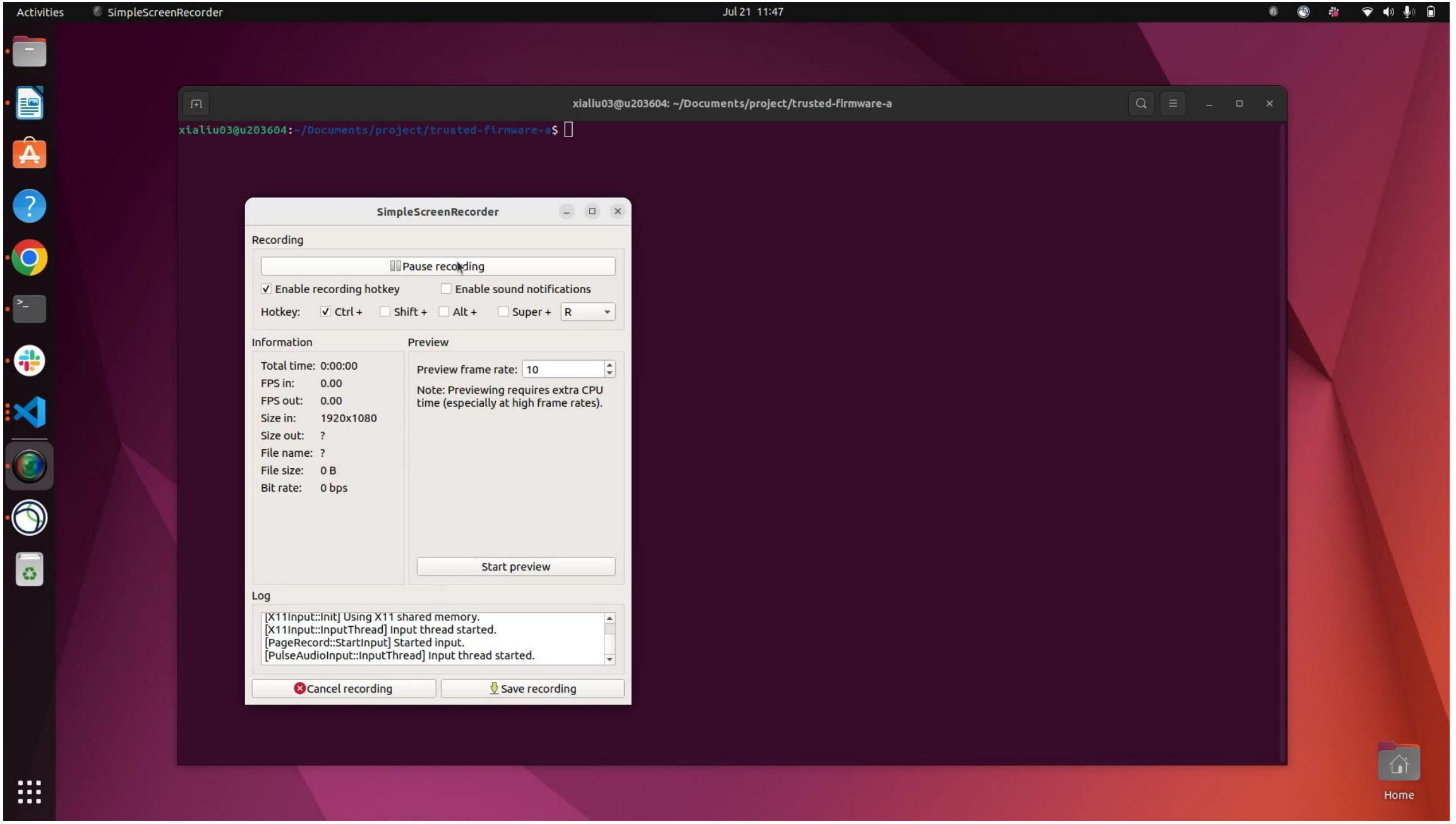
```
class cert:
    def __init__(self, certName):
        self.cert_name = certName
        self.img_id = ""
        self.img_type = "IMG_CERT"
        self.parent = ""
        self.ifdef = []
        self.signing_key = ""
        self.antirollback_counter = ""
        self.img_auth_methods = []
        self.authenticated_data = []

class image:
    def __init__(self, imageName):
        self.img_name = imageName
        self.img_id = ""
        self.parent = ""
        self.hash = ""
        self.img_type = "IMG_RAW"
        self.ifdef = []
        self.img_auth_methods = []

# generic can be used for pk and nv counter
class generic:
    def __init__(self, name):
        self.name = name
        self.id = ""
        self.oid = ""
```

arm

DEMO


Activities
SimpleScreenRecorder
Jul 21 11:47
xialiu03@u203604: ~/Documents/project/trusted-firmware-a
xialiu03@u203604:~/Documents/project/trusted-firmware-a$
SimpleScreenRecorder
Recording
Pause recording
Enable recording hotkey
Enable sound notifications
Hotkey:
Ctrl +
Shift +
Alt +
Super +
R
Information
Total time: 0:00:00
FPS in: 0.00
FPS out: 0.00
Size in: 1920x1080
Size out: ?
File name: ?
File size: 0 B
Bit rate: 0 bps
Preview
Preview frame rate: 10
Note: Previewing requires extra CPU time (especially at high frame rates).
Start preview
Log
[X11Input::Init] Using X11 shared memory.
[X11Input::InputThread] Input thread started.
[PageRecord::StartInput] Started input.
[PulseAudioInput::InputThread] Input thread started.
Cancel recording
Save recording
Home

arm

Future Works

Future Works

- Integrate with open source validator/parser
  - Be able to get attributes for the CoT device tree
- Two open source validators
  - dt-schema
  - pydevicetree

Question?

Reference

Reference

- https://github.com/devicetree-org/dt-schema/tree/main
- https://github.com/sifive/pydevicetree/tree/master

arm

Thank You
Danke
Gracias
Grazie
谢谢
ありがとう
Asante
Merci
감사합니다
धन्यवाद
Kiitos
شكرًا
ধন্যবাদ
תודה
ధన్యవాదములు