DS09SBL: Dasharo TrustRoot Training

Welcome

DS09SBL: Dasharo TrustRoot Training

Agenda

- Trainers introduction
- About 3mdeb
- Why are we here?
- About you
- Training plan and guideline
- Training materials

`$ whoami`

Michał Żygowski

3mdeb Senior Firmware Engineer

- Core developer of coreboot.
- Maintainer of Braswell SoC, PC Engines, Protectli, MSI and Libretrend platforms.
- Interested in advanced hardware features, security and coreboot.
- Open-source firmware enthusiast and conference speaker.

Contact Information

Michał Żygowski

3mdeb Senior Firmware Engineer

🔑 `00B8 8FB2 5FD6 375B C5FF 195D 6B5B A214 D21F CEB2`

✉️ michal.zygowski@3mdeb.com

🐦 @_miczyg_

🔗 LinkedIn

🌐 3mdeb.com

💻 GitHub

Scan for LinkedIn profile

🌟 Reach out for collaborations or inquiries!

$ whoami

Piotr Król

3mdeb Founder

- Developing platform security technologies since 2008.
- Integrating open-source firmware and Trusted Computing technologies since 2014.
- Delivering training and consulting services for commercial organizations and the public sector since 2018.
- OpenSecurityTraining2 Boards of Directors Member and Instructor.
- TrenchBoot Project Steering Committee Core Member.
- Conference speaker, privacy, liberty, and trustworthy solutions advocate

Contact Information

Piotr Król

3mdeb Founder

- 🔑 `869E 9AE8 AFDB 5FAE 6068 338B 99BD 2EEE E2D0 CE31`
- ✉️ piotr.krol@3mdeb.com
- 🐦 @pietrushnic
- 🔗 LinkedIn
- 🌐 3mdeb.com
- 💻 GitHub

Scan for LinkedIn profile

🌟 Reach out for collaborations or inquiries!

About 3mdeb

DASHARO ZARHUS OS

Our mission is to enhance platform security using the expertise we gained in Root of Trust, Chain of Trust, Trusted Computing, TPM, coreboot, UEFI/EDK II, Yocto, U-Boot, and Linux. Dasharo and Zarhus OS, are products designed to enhance the trustworthiness of every computing device through open development principles. We prioritize transparency, digital sovereignty, and the right to repair in creating resilient embedded firmware solutions, ensuring secure systems for the community and our clients.

Goals of the Training

By the end of the 4-day remote training, participants will be able to:

- **Describe** the core components, architecture, and flow of the Slim Bootloader and Intel Root of Trust technologies, as presented in guided demonstrations.
- **Recognize** typical configuration steps and tooling workflows used to set up, debug, and verify Slim Bootloader-based platforms and Intel security primitives.
- **Interpret** the intent and expected outcomes of provisioning and integration processes shown during the training.
- **Assess** the applicability of these technologies in their own environments, based on observed use cases and best practices shared by the trainer.

Kudos

- Michał Iwanicki
- Reviewers and students who provided feedback.

Disclaimer

The following training session on the x86 boot process, Slim Bootloader, and Intel Root of Trust is designed to provide participants with a foundational understanding of these complex topics. We recognize that these subjects are intricate and that comprehensive coverage of all aspects would require significantly more time than is available in this schedule.

As a result, this training involves simplifications and a focus on key concepts that are essential for practical understanding. While we strive to deliver high-quality content, it’s important to note that certain nuances and advanced details may be omitted. Our goal is to provide a streamlined learning experience that fits within the allocated time frame while still delivering valuable insights.

We acknowledge that many participants may have years of experience in these fields, and we appreciate the depth of knowledge they bring to the discussion. We encourage participants to provide feedback, as this will help us improve the materials continuously and better address the needs of our audience.

Additionally, the trainer acknowledges that their knowledge, while extensive, is not exhaustive. Continuous learning and engagement with industry developments are essential, and input from participants can significantly enhance the overall training experience.

By participating in this training, you agree to understand and accept these limitations.

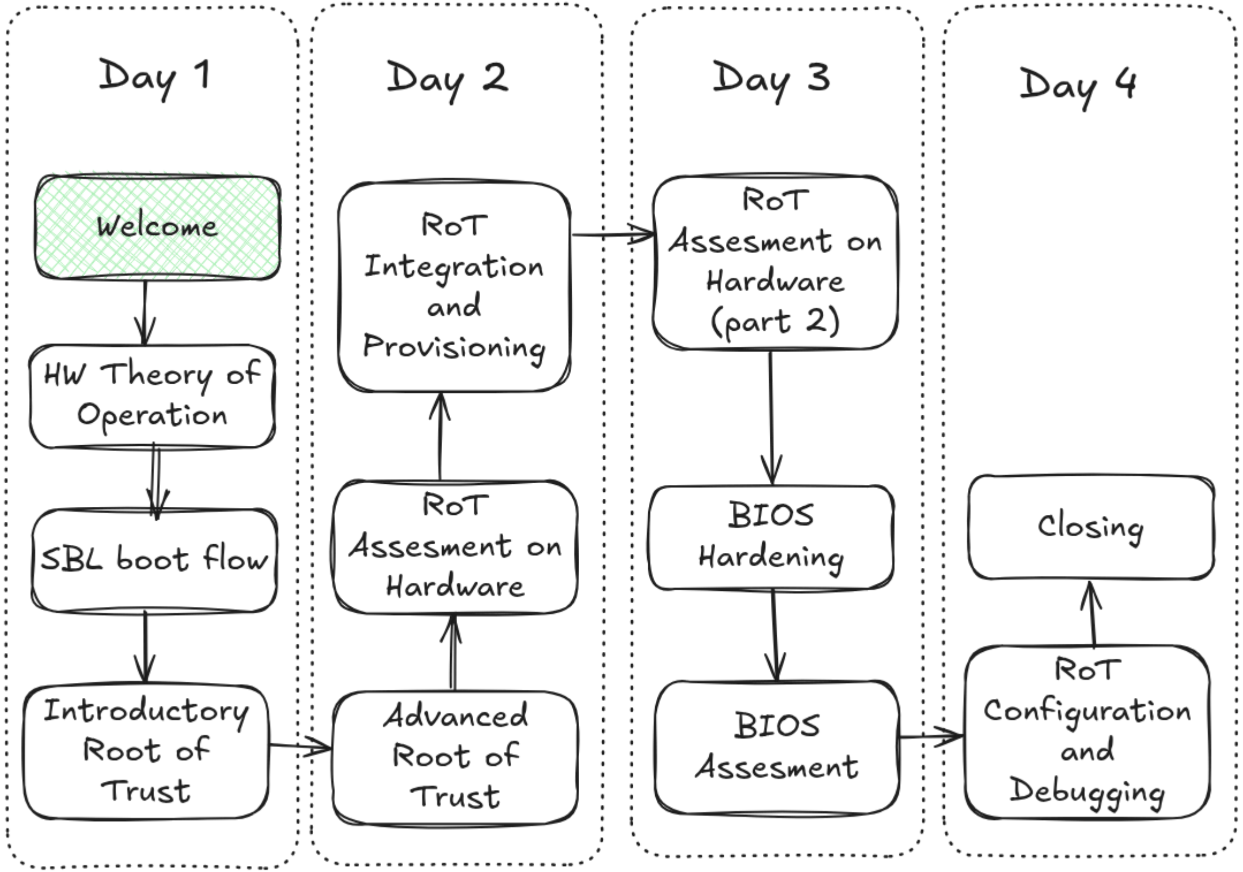
Goals of the Training

- Core concepts:
  - Slim Bootloader 🔄🔍,
  - Intel Root of Trust 🔄🔍 (part 1), 📅 (part 2),
  - TPM 📅,
- **Recognize** typical configuration steps:
  - Slim Bootloader flashing and recovery 🔄🔍,
  - Intel Root of Trust configuration 📅,
- **Interpret** the intent and expected outcomes:
  - Intel Root of Trust breaking change of trust 🔄🔍,
  - Intel Root of Trust debugging 📅,
- Assess the applicability:
  - Intel Root of Trust 📅,
  - Intel Converged Security and Management Engine configuration 📅,
  - SPI protection mechanisms 📅,

Introductions

Please introduce yourself by sharing:

Agenda and Training Structure #1



Day 1

Welcome

HW Theory of Operation

SBL boot flow

Introductory Root of Trust

Day 2

Advanced Root of Trust

RoT Assesment on Hardware

RoT Integration and Provisioning

Day 3

RoT Assesment on Hardware (part 2)

BIOS Hardening

BIOS Assesment

Day 4

RoT Configuration and Debugging

Closing

Agenda and Training Structure #2

Day 1 (7 Aug 2025)

- Welcome and introduction
- Hardware theory of operation
- Introduction to the x86 and Slim Bootloader boot flow
- Root of Trust and Chain of Trust Technologies (part 1)

Day 2 (11 Aug 2025)

- Root of Trust and Chain of Trust Technologies (part 2)
- Root of Trust assessment on Hardware (part 1)
- Integration and provisioning of Root of Trust

Day 3 (14 Aug 2025)

- Root of Trust assessment on Hardware (part 2)
- BIOS hardening and extra security mechanisms
- BIOS security Assessment

Day 4 (25 Aug 2025)

- Advanced Intel Boot Guard configuration and debugging
- Q&A: final questions from attendees
- Closing notes

Logistics and Housekeeping #1

Training materials

The most recent version will be available on 3mdeb Cloud (password: TrustRoot_2025) for a month after last day of training (25 Sep 2025).

Notice

Please note materials for days 2, 3 and 4 may be adjusted based on feedback and the performance of the group.

Logistics and Housekeeping #2

Materials partition and VM file structure

```
training_materials/
├── alpine
│   ├── iso
│   └── packages
├── dts
│   └── image
├── hardware
│   ├── intel
│   └── odroid-h4
├── intel_tools
│   └── ADL_BIOSAC_v1_18_16_20230427_REL_NT_O1.PW_signed_256K.bin
├── sbctl-0.17
│   └── sbctl
├── src
│   └── slimbootloader
└── uefi
    ├── specifications
    └── uefitool
```

Engagement and Ground Rules #1

- 4 days of lectures (4.5h hours per day, from 10:00 to 15:00 IST).
- 30min break ~12:00.
- At the end of the course, there will be an evaluation survey.
- Please mute your mic, when you not speaking.
- Multitasking is enemy of every training.
- Questions should be saved until the end of each module to avoid redundancy.
- Please remain present and engaged during the training.
- Each module ends with quizzes.
- If you notice a potential bug, please let me know, or propose your fix through contribution.
- Feedback is always welcome.

Engagement and Ground Rules #2

- If we are running overtime or if the training is becoming boring, please let me know 🙂
- Please note that sometimes, even though we click, the slides do not change. I am simply getting through my notes; it is not a technical issue.

Odroid-H4+ Purchase

Please note you can buy Odroid-H4 with Dasharo (Slim Bootloader + UEFI) v0.9.0 to repeat all demos which were presented during this course.

Hardkernel Odroid H4+ for Pace Enterprise Training (PET) – DS09SBL

Working environments

During the training you would work on three platforms:

- Odroid-4+ platform (Hardware)
- Virtual Machine
- Docker Container on Virtual Machine

Commands that are meant to be executed on the **Hardware** will be indicated by the `-HW` affix:

```
user@OST2-HW:~$ echo "Hello World"
```

Commands that are meant to be executed on the **Virtual Machine** will be indicated by the `-VM` affix:

```
user@OST2-VM:~$ echo "Hello World"
```

Commands that are meant to be executed on the **Container inside the Virtual Machine** will be indicated by the `-CT` affix:

```
user@OST2-CT:~$ echo "Hello World"
```

If you are unsure where to execute a specific command, feel free to ask.

Questions?

Enjoy our training