東京 2025

LINUX PLUMBERS CONFERENCE

TOKYO, JAPAN / DECEMBER 11-13, 2025

ReLaunch Revisited

A Refresher on TrenchBoot Late Launch

Authors: Daniel P. Smith Ross Phillipson, Daniel Kiper
Presenters: Daniel P. Smith, Daniel Kiper

東京 2025
LINUX
PLUMBERS CONFERENCE
TOKYO, JAPAN / DEC. 11-13, 2025

Introduction

- Introduction to D-RTM “Late Launch”
- Applicable use cases for “Late Launch”
- Introduction to Secure ReLaunch capability
- Roadmap review
- Audience engagement

DRTM Late Launch

A Dynamic Launch can be done at anytime during system lifecycle.

- There are two classifications for a Dynamic Launch.
  - Early Launch: when Dynamic Launch is used in conjunction with system firmware launch.
  - Late Launch: when Dynamic Launch is used by an Operating System to re-establish trust.
- Late launch is a unique and powerful feature of DRTM solutions.
  - At an arbitrary point in time a system can prepare for and initiate the Dynamic Launch Event.
  - This re-establishes the DRTM measurement and marks a point in time where the system is in a known good state.
- This process can be done any number of times driven by system policy.
- Note that a late launch is not a power cycle so certain state and configuration information can be saved across a late launch (e.g. paused VMs).
- TrenchBoot late launch for Linux is Secure ReLaunch.

Late Launch Exemplars

- Relaunch existing system for re-establishing trust anchor
  - Fresh restart of system without system reset
- Upgrade without system reset
  - Relaunch using upgraded kernel
  - Enables a trustworthy mechanism to quickly pivot to an upgraded kernel.
- Switching between Management and Customer environments
  - Enables launching into a Management environment to do upgrade and maintenance, then switching back.
  - Proposed at LPC 2020[1]
  - Implementation presented at FOSDEM 2021[2]

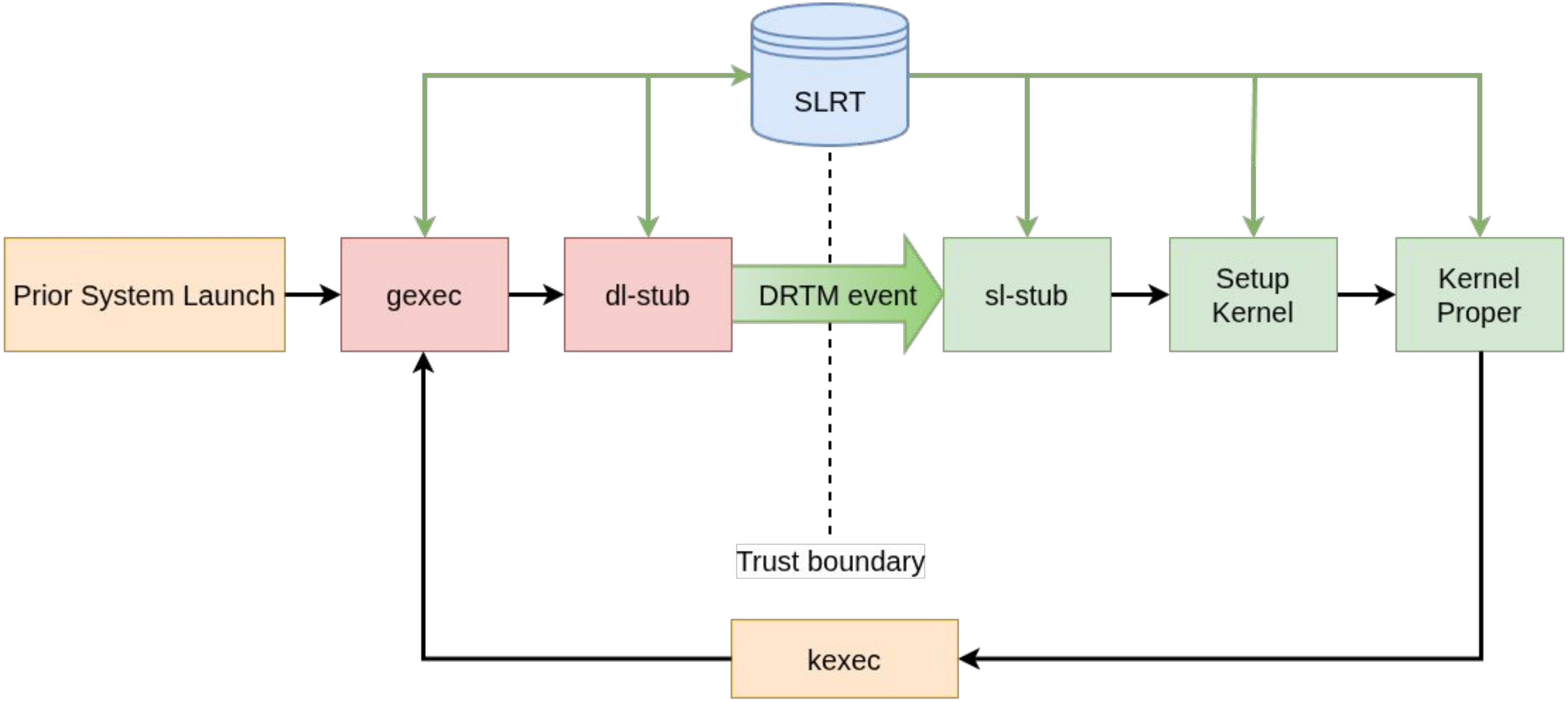
1. https://lpc.events/event/7/contributions/739/
2. https://archive.fosdem.org/2021/schedule/event/firmware_suwd/

Secure ReLaunch Design

The goal is to introduce a late-launch capability for Linux with minimal changes through reuse.

- GRUB already contains the support for setting up and initiating the Dynamic Launch Event.
- A new platform is being considered for GRUB called “gexec”.
- When configured for this platform, building GRUB will produce an ELF binary image which can be executed via kexec.
- A separate entry point will exist for gexec to capture information passed to the kexec’ed image (e.g. boot params on x86).
- The existing GRUB dynamic launch code, possibly with some modifications, will perform the relaunch.
- There are no changes expected to kexec or the Linux kernel to support ReLaunch.

Secure ReLaunch Flow



Deployment

The deployment of Secure ReLaunch is expected to only rely on a build of GRUB with support for the new gexec platform.

- Build the gexec platform and build a ReLaunch bootable image:

  ```
  $ ./configure --with-platform=gexec --target=x86_64
  $ make && sudo make install
  $ ./grub-mkimage -O i386-gexec -o gexec.img -p . -c relaunch.cfg
  ```

- The ReLaunch GRUB config file:

  ```
  slaunch
  linux /vmlinuz {kernel options}
  initrd /initramfs.gz
  ```

Roadmap

- Merging of the Linux Secure Launch series
- Submission of the GRUB patches initial Secure Launch support
- Submission of AMD Linux Secure Launch series
- Release GRUB ReLaunch support, the gexec platform

Fin

Questions?