Contribution ID: **130** Type: **not specified**

# Advanced Applications of DRTM with TrenchBoot SecureLaunch for Linux

*Thursday, August 27, 2020 10:00 AM (20 minutes)*

The TrenchBoot Project has put forth an RFC for adding direct support to Linux for x86 DRTM. Many people are familiar with the early launch capability implemented by Intel's tboot, but there has also been academic work on live relaunch, e.g. Jon McCune's Flicker. SecureLaunch was designed to support a range of launch integrity capabilities. This discussion will review a subset of solutions that can be implemented using DRTM, along with roadmap candidates for SecureLaunch feature development.

## I agree to abide by the anti-harassment policy

I agree

**Primary author:** SMITH, Daniel (Apertus Solutions, LLC)

**Presenter:** SMITH, Daniel (Apertus Solutions, LLC)

**Session Classification:** System Boot and Security MC

**Track Classification:** System Boot and Security MC