Contribution ID: **314** Type: **not specified**

Secure Launch - DRTM solution on Arm platforms

Wednesday, 18 September 2024 13:00 (30 minutes)

TrenchBoot is an OSS project that is used to establish the integrity of the loaded software. The previous work was focused on Intel and AMD implementations of their dynamic root of trust mechanisms. Arm, in consultation with members of the TrenchBoot community, designed a DRTM implementation for their platform. This presentation focuses on the initial design work to bring Arm support to the TrenchBoot Secure Launch solution.

Primary author: Mr PHILIPSON, Ross (Oracle)

Presenters: SMITH, Daniel (Apertus Solutions, LLC); Mr PHILIPSON, Ross (Oracle)

Session Classification: System Boot and Security MC

Track Classification: System Boot and Security MC