Contribution ID: **281** Type: **not specified**

TrenchBoot Secure Launch upstreaming

Wednesday, 22 September 2021 09:10 (30 minutes)

The ability to do a Trusted Computing Group (TCG) Dynamic Launch of a system has been commercially available in x86 processors since 2006 with the introduction of Intel TXT for Intel processors and by AMD-V for AMD processors. Over the years the technology has mainly been used by limited number of security-sensitive projects. The TrenchBoot Project has been working to make the underlying hardware technology more integrated and to be an out-of-the box solution usable by the general Open-Source Operating System user. Towards that goal the project has been working to upstream a into the Linux kernel the ability to be directly launched by a TCG Dynamic Launch in a unified manner. The first patchset submitted is focused in enable this approach for Intel TXT, with support for AMD and Arm to come soon after. This purpose of this topic is to engage the Linux developer community for feedback on the current patches and discuss ways in which progress towards merging could be made.

I agree to abide by the anti-harassment policy

I agree

Primary authors: PHILIPSON, Ross (Oracle); SMITH, Daniel (Apertus Solutions, LLC)

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

Session Classification: System Boot and Security MC

Track Classification: System Boot and Security MC