Title: SPDM: Securing the Links between Host and Devices

Speaker: Guerney Hunt (IBM Research)

Abstract: SPDM is an industry standard protocol that was created to secure the interfaces between hosts and devices. Optionally, can be utilized to verify components in a system during initial power-up. This talk presents an overview of SPDM and its features. We cover the threat model and the goals. We will present a summary of the features that have been incorporated into the protocol through versions 1.2. We will supply more detail on Event Notification, Multi Key Support, New Measurements, Measurement Extension Log, Structured Manifest format, and End Point Info all of which became available in 1.3. Finally we will present the areas where the protocol is actively being extended.

Bio: