

Thursday, August 20

9:00 AM - 9:20 AM

Hardware Zero Trust

Tommy Gardner

Chief Technology Officer, HP Federal

HP Inc.

Abstract:

Zero Trust is a philosophy and methods used to secure systems and data. The focus has primarily been on Identity Management or one software security. This talk will discuss the need for Hardware Zero Trust and the need for a hardware and firmware certification to achieve the optimum security of your systems and data. NIST SP 800-207 defines the specifics of a Zero Trust effort. Often the hardware and firmware component of a system are taken as a given because of the many years between replacement. Software and hardware must work together in any system. Understanding the level of security that your hardware provides is important in optimizing the overall protection.

NIST SP 800-193 on Hardware Resilience provides a good starting point. Working this through the Hardware system design for a Root of Trust and a Trusted Compute Module in light of the DoW Zero Trust Program Office's Pillars can bring insight into the need for a hardware evaluation of Zero Trust. This talk will bring everyone up to date on the discussions with DoW, the Services, DISA and NSA on the subject.