Intel® Trust Domain Extension Guest Kernel Hardening Documentation

- Intel® Trust Domain Extension Linux Guest Kernel Security Specification
  - Purpose and Scope
  - Threat model
  - TDX Linux guest kernel overall hardening methodology
  - Device filter mechanism
  - TDVMCALL-hypercall-based communication interfaces
  - IOMMU
  - Randomness inside TDX guest
  - TSC and other timers
  - Declaring insecurity to user space
  - BIOS-supplied ACPI tables and mappings
  - TDX guest private memory page management
  - Reliable panic
  - Kernel and initrd loading
  - Kernel command line
  - Storage protection
  - VirtIO and shared memory
  - Transient Execution attacks and their mitigation
  - Summary
- Intel® Trust Domain Extension Guest Linux Kernel Hardening Strategy
  - Purpose and Scope
  - Hardening strategy overview
  - Attack surface minimization
  - Static Analyzer and Code Audit
  - TD Guest Fuzzing
  - TDX emulation setup
  - Fuzzing Kernel Boot
  - Fuzzing Kernel Runtime
  - Enabling additional kernel drivers