GENERAL DYNAMICS
Mission Systems

Trusted Embedded Environment (TEE)

An Assured Edge for Your Tactical Network

Certifiable multilevel platform achieved via COTS secure separation kernel and General Dynamics' cross-domain solutions expertise

Access to multiple security domains on a single platform

Trusted virtualization saves size, weight, power, and cost

TEE Technology Shelf provides enhanced features such as trusted display management and cross-domain transfer

Trusted Embedded Environment (TEE)

Trusted Embedded Environment (TEE) enables assured access to information at multiple security levels. The TEE technology facilitates tactical multilevel environments where Size, Weight, and Power (SWaP) constraints are a challenge. TEE is targeted for tactical embedded environments and is scalable to laptops, workstations, and servers. TEE employs a COTS Separation Kernel/Hypervisor designed and developed for high-assurance systems. TEE supports full virtualization enabling guest operating systems and legacy applications to run unmodified. Deploying TEE thereby accelerates integration and reduces total cost of ownership. TEE provides a robust environment within which entire operating systems and legacy applications run in different security domains, concurrently, with no compromise of confidentiality, availability, or integrity.

Extensive Capabilities From the TEE Technology Shelf

The TEE Technology Shelf provides enhanced capabilities above and beyond typical trusted virtualization technologies. The TEE Trusted Display Manager provides a true multilevel display. The General Dynamics CrossingGuard™XD integrates with TEE to provide embedded cross-domain data transfer. TEE provides secure disk partitioning to share a single disk between virtual machines. These features and others such as management and audit are possible because TEE is an enabling technology that facilitates security critical applications. TEE provides the interfaces and supporting framework for developing customized MILS-enabled technologies such as fully virtualized thick-client Virtual Machines (VMs), trusted thin client platform, and secure cut and paste. TEE technologies are integrated and customizable to meet operational needs.

Multilevel Display Enhanced for Tactical Operations

TEE has benefited from years of General Dynamics Mission Systems' experience deploying tactical systems. Our direct experience integrating TEE for tactical operations has led to an exceptional Trusted Display capability. The Trusted Display Manager includes unique solutions for high-bandwidth applications easily providing 50 FPS at 1900x1280 resolutions. Understanding operational environments combined with our security expertise has enabled us to implement the TEE display manager in a manner that presents multiple domains simultaneously while ensuring data separation.

Secure Foundation

TEE implements a Multiple Independent Levels of Security (MILS) architecture vetted with the NSA and DoD programs of record. TEE partitions system data and resources and controls information flow between partitions. TEE deploys on bare COTS processors with advanced hardware security features such as

Trusted Embedded Environment (TEE)

Intel® Virtualization Technology (VT-x and VT-d) and Trusted Platform Module (TPM). These hardware features are leveraged by its high-assurance separation kernel software. By operating directly between the processor and guest OS, TEE enforces the separation and allocation of devices (such as USB) to specific virtual machines. This approach along with full virtualization also ensures that device drivers and I/O devices can be allocated independently and without modification. TEE also supports usage of the Trusted Computing Group (TCG) Trusted Boot and VM verified launch.

Supports Open Standards

TEE is compliant with the U.S. Government Protection Profile for Separation Kernels in Environments Requiring High Robustness (SKPP). It leverages commercial off- the-shelf x86 virtualization technology from Intel. TEE's extremely small code size eases evaluation and certifiability, and it supports Safety-Critical & Real-Time (certifiable to RTCA DO-178B, ARINC-653) applications. TEE supports open standards, and offers runtime POSIX that is designed to allow development of high-robustness trusted applications.

High Assurance, Low Overhead	
Startup	***Typical Time****
Power to end of BIOS	10–30s
End of BIOS to fully operational guest OS	45s
Time impact by TEE from end of BIOS to operational guest OS	1s
Operational	
Interrupt response	10µs–1ms

** Based on measurements from current display hardware using solid state media*

Benefits

- Full virtualization maximizes flexibility and minimizes legacy integration costs
- Reduces size, weight, power, and cost for tactical multilevel systems
- Trusted Display Manager enables simultaneous display of multiple security domains to accelerate situational understanding
- Technology Shelf provides enhancements such as integrated cross domain transfer to improve assured information sharing
- Flexible architecture supports wide range of customizations to meet mission needs
- Implements open standards to promote interoperability

Features

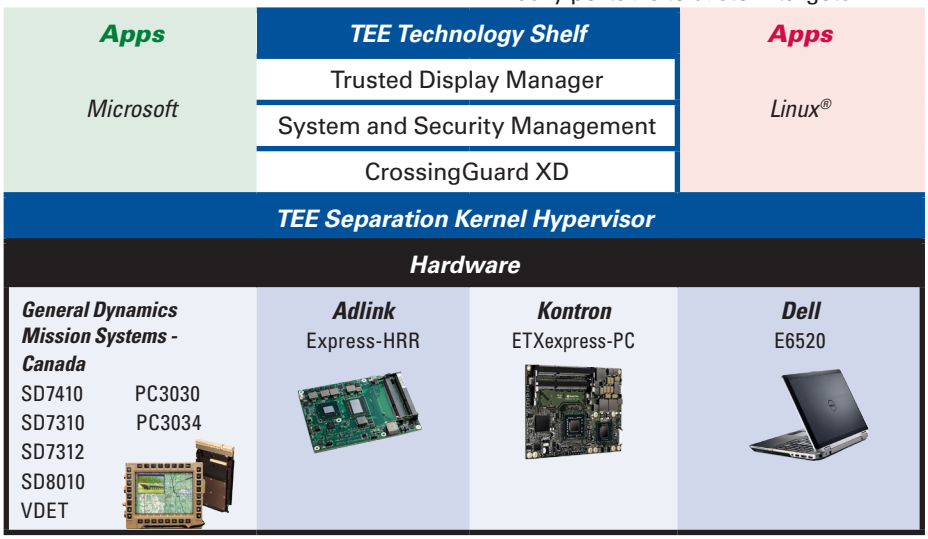
- Hypervisor with full virtualization technology builds upon COTS secure separation kernel technology
- Designed to comply with U.S. Government Protection Profile for Separation Kernels in Environments Requiring High Robustness
- Hard real-time, deterministic scheduling to support RTOS
- Flexible scheduling policy
- Deploys on COTS hardware with standard BIOS
- Runs on x86 64-bit, multi-core processors
- Supports para-virtualized and fully virtualized operation systems
- Hosts both 32- and 64-bit guest operating systems and applications
- 100 percent binary compatible Linux- or POSIX-based software applications
- Supports time synchronization via NTP
- Supports health status collection and reporting
- Provides strictly controlled information flows between virtual machines
- Supports cross-domain applications including the General Dynamics CrossingGuard XD and data diode
- Separation kernel implements trusted time and space separation
- Employs separate memory spaces to ensure strong separation between virtual machines
- Isolates failures and compromises to a single virtual machine
- Provides secure boot to ensure startup integrity

Deployed Guest Operating Systems

- Linux® 3.1 kernel distributions
- Microsoft® Windows® 7 and Windows 8®
- Intel-based hardware platforms: Intel 945, 965, ICH9M, Q35, Sandy Bridge, Ivy Bridge

Operational Environments

- Designed for simultaneous Top Secret/ Secret/Unclassified (DCID 6/3 PL-5)
- Intel-based hardware platforms: Intel 945, 965, ICH9M, Q35, Sandy Bridge, Ivy Bridge
- General Dynamics Mission Systems -Canada PC3030, PC3034, SNP2 3U single board computers and SD7310, SD7312, SD7410, SD18-1, and SD8010 smart displays
- Elbit Bradley Tactical Display
- Easily portable to custom targets



GENERAL DYNAMICS
Mission Systems

gdmissionsystems.com/TEE • IASystems@gd-ms.com
Phone: 480-441-5448 • Toll-free: 866-400-0195

©2016 General Dynamics. All rights reserved. General Dynamics reserves the right to make changes in its products and specifications at anytime and without notice. All trademarks indicated as such herein are trademarks of General Dynamics. All other product and service names are the property of their respective owners. ® Reg. U.S. Pat. and Tm. Off.

D-TEE-06-0716