Gov2: OpenXT Platform Properties

DRAFT

Open XT Platform Properties

- Integrity of operating software.
  - Provides tamper-evident resistance to unauthorized changes to system software.
  - Verifies the integrity of all updates to the system software.
  - Supports secure remote update of system software.
  - Enforces policy-based constraints on operating software to limit the capabilities and inhibit the actions of compromised software.
  - Isolates system software requiring privileged device access from other components of system software to limit the capabilities and inhibit the actions of compromised device software.
- Hardware-rooted trust.
  - Uses security features of platform hardware to protect integrity and confidentiality of system software and data.
- Protection of storage.
  - Prevents access to system configuration data at rest.
  - Prevents access to user data at rest.
- Protection of communications.
  - Enforces isolation between each of:
    1. Physical network device control software
    2. Communication encryption software with access to network credentials
    3. User software execution environments
  - Able to enforce local isolation between the networks of each VM.
  - Controls VMs access to the hosts physical network connections according to system policy.
- Isolation of software execution environments.
  - Confinement of VM environments according to policy to prevent cross-domain data leakage.
- Protection of input.
  - Keyboard and mouse input to system software is not observable by VMs.
  - Input to user VMs is isolated from others VMs.
  - The target of keyboard and mouse input is made evident to the user to prevent capture of input data via user confusion.
  - The key input sequences used to select the recipient of further input are protected from observation, interference and spoofing by VMs.
- Protection of display.
  - The display outputs of all VMs are isolated from each other and protected from cross-domain data leakage.
- Administrative control of devices.
  - Provides user software environments with access to platform devices and external peripherals according to system and VM administrator policies.
- Compatibility with modern hardware platforms.
- Compatibility with modern operating systems.
- Architected and licensed to support production of branded commercial derivatives with optional proprietary extensions.
- Interoperability of base platform with guest VMs, providing developers with consistent mechanisms for packaging, deployment and operational support on validated commercial derivatives (validated and versioned interfaces include guest PV drivers).
- Consistent upgrade mechanism for base platform with defined interoperability properties with optional proprietary extensions.
- Defined OEM hardware compatibility with stable releases of base platform and commercial derivatives, validated by manual and/or automated testing.
- Constructed from OSI-certified Open Source software and extensions with compatible software licenses.
- << To do: Add more here >>

Changes to this Platform Properties Document

Changes can be made to this document by the following the process established for changes to the main OpenXT Governance Document that defines the Governance Board structure.

License of this Governance Document

Revision History of this Governance Document