Xtra1: OpenXT Platform Architecture

<< Document needs significant work. >>

Current Use Cases

- Provide the software platform for a Multi-Tenant Client Desktop.
- Provide the software platform for a hardened Single-VM endpoint.
- Be the best-in-class Open Source toolchain for support of measured launch into a manageable virtualized environment.
- Provide a compelling platform for research and academic projects on hardware-based security technologies.
- Production software environment for validation of new hardware-based security technologies.

Technology applied to implement and provide Platform Properties

<< Below are not currently properties and they are technology-specific. Some aspects of this list may belong in the Platform Security Architecture document. >>

- Measured Launch to detect tampering with core system software and protect the confidentiality of data on the system.
- Disaggregated network functionality to isolate privileged device drivers, VPN software, credentials and user applications and data.
- Enforcing SELinux and XSM policies to protect platform components.
- Containment and isolation of VM device model processes with stub domains.
- Support for modern Windows guest operating systems.
- Support for modern Linux guest operating system distributions, including Debian and OpenEmbedded.
- Extensible base platform, architected 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. <<To do: this statement needs checking and possibly qualifying against the current project code. eg. Intel SINIT modules, etc. >>
- << To do: Add more here >>

License of this Document

Revision History of this Document