Tech1: OpenXT Platform Architecture

<< Document needs significant work. >>

This document describes the software architecture of the OpenXT software.

The content of this document is subject to governance by the OpenXT Project.

Amendments to this document are to be made by following the Project Changes process described in the OpenXT Project Governance documents.

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.

Project Platform

Platform Properties

The OpenXT Project Platform provides these conceptual properties:
- *Compatibility* with modern hardware and operating systems
- *Loose Coupling* of components, including open-source and proprietary
- *Verifiable Measurements* of hardware and software
- *Verified Launch* of derived works

Additional detail is available in the OpenXT Platform Properties document.

OpenXT Platform Layers

The OpenXT Project uses composable software layers provided by OpenEmbedded, to isolate customizations such as hardware, GUI environments and Linux distributions.

OpenXT Platform Layers provide smaller governance contexts for use cases, target markets and operational models within a common codebase. Layers narrow the set of stakeholders and increase alignment, while increasing the adoption of core platform components.

All OpenXT Platform Layers are subject to OpenXT Governance as defined in the project Governance Documents. Layer creation and changes can be proposed via the "Project Changes" process defined in those documents.

Derivative Works

Derivative works rely on OpenXT Platform Properties to make assurances for diverse markets and use cases. Derivative works are developed and governed independently of the OpenXT Project. Developers of derivative works can propose technical changes to the OpenXT Platform, as defined by "Project Changes" in this document.

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