TRUSTED MULTI-TENANT INFRASTRUCTURE PLATFORMS USING STANDARDS

Michael Donovan
Chief Technologist, US Public Sector Capabilities, HP

March 22, 2010
THE SUPPLY CHAIN FOR TECHNOLOGY-ENABLED MISSION SERVICES

IT organization

internal service provider

Users

Mission outcome

Cloud service provider

Global-class software
Massive scale-out infrastructure

Hosted / outsourced service provider

Enterprise-class software
Dedicated and shared infrastructure

Cloud services

Enterprise-class software

In-house services

Hosted services

Users

Mission outcome
In order to use legacy applications in a shared IT environment it is necessary to replace physical with virtual boundaries.
WHAT IS THE MARKET SAYING TO SYSTEMS INTEGRATORS?

MARKET OBSERVATIONS

- Multi-Tenant security is an end-to-end configuration requirement, while most of the products and standards address specific devices or functionality within the overall end-to-end scope.
- Many standards and products contribute to the ability to solve parts of the problem.
- No comprehensive framework exists to describe the business/mission needs and validate compliance of the entire solution set against TCG standards.

MARKET DEMAND

- Enabler for Trusted Shared Infrastructure solutions
- Cost Reduction, Green Initiatives
- To support shared infrastructure for critical infrastructure:
  - Financial (PCI), Healthcare (HIPAA), Energy (NERC/CIP), Government, …
  - Defense Joint service or coalition operations
  - Shared services within public, private and hybrid “clouds”
WHAT IS THE MARKET LOOKING FOR?

TRUSTED MULTI-TENANT INFRASTRUCTURE

- Protection of processing and information in motion and at rest
- Ability to share physical platforms among tenant domain components (shared services)
- Visibility and auditability of actions across the enterprise
- Management of physical resources independently of domain resources
- Ability to run legacy workload unmodified within a secure context
- Loosely coupled architecture managed using application of appropriate policy and trust
- Ability to control the flow of information between tenant domains within policy constraints
- Ability to address various security models to protect integrity and confidentiality of services and data exchanges within enterprise
- Enterprise scalable attestation solutions and policy driven separation
- Enterprise and Cross-Enterprise scopes
- Public, Private and Hybrid cloud security value proposition
- Savings in Space, Power and Cooling Requirement
- Support integrated solutions that tie together the TCG specifications to achieve a secure, trusted end to end solution
- Support for moving application elements across platforms rather than moving platforms
- A common understanding of how components from multiple providers fit within a composite solution
WHAT IS MULTI-LEVEL SECURITY?
- Aligns to assurance that only authorized people get access to sensitive information
- Classic Solution is Multiple Single Level (MSL)
  - Separate infrastructure for each level / client
  - Makes end to end situational awareness difficult
  - Increases space, power usage and cooling
  - In commercial terms, this is Multi-Client Infrastructure
- Target solution is Multi-Level Security (MLS)
  - Single infrastructure enforcing separation of domains
  - A related variant is Multiple Independent Levels of Security (MILS)
  - Supports more efficient use of space / power / hardware

WHAT ARE CROSS DOMAIN SERVICES?
- The ability to manage the flow of information across tenant domains
- Cross Domain Access
  - Access to information and systems in multiple domains using strong access controls
- Cross Domain Exchange
  - Controlled transfer of information between domains
  - One-way or two way exchange of information
- Cross Domain Identity Management
  - Ability to federate identity assertions across domains
  - The same identity may have credentials in multiple domains which can be asserted
- Cross Domain Access Control
  - Manage and enforce access control policy within and between domains
  - Account for internal, external and aggregate information
WHAT CAN WE ACHIEVE TODAY?

User Domain

High Security Network
- Encrypt
- VDI/TS
- Apps
- Restricted

Secure
- Encrypt
- VDI/TS
- Apps

Confidential
- Encrypt
- VDI/TS
- Apps

Low Security Network
- Encrypt
- VDI/TS
- Apps

Public
- Encrypt
- VDI/TS
- Apps

Labeled Storage

Up: Automated
Down: Reviewed

CDS Exchange
TRUSTED COMPUTING

– Trusted Computing Group (TCG) is a 100+ industry group defining open, standard, vendor neutral, security building blocks for computing platforms (client, server, …)

– TCG specifications define a Trusted Platform Module (TPM) as a hardware root of trust on a computing platform
  • TPM 1.2 specification is now an ISO standard

– TCG specifications further define a chain of trust architecture that enables attestation of trusted platform properties

– The TCG vision is to enable remote parties to be able to establish trust in a system’s properties, using attestation and the TPM root of trust
TCG: STANDARDS FOR TRUSTED SYSTEMS

Virtualized Platform

Printers & Hardcopy

Network Security

Security Hardware

Desktops & Notebooks

Mobile Phones

Authentication

Storage

Applications
- Software Stack
- Operating Systems
- Web Services
- Authentication
- Data Protection

Infrastructure

Servers
WHAT ARE WE PROPOSING?

– A step back from the technical standards to describe the overall framework for integrated Trusted Multi-Tenant Infrastructure solutions
  • Current technical working groups focus on how (the technical standards)
  • Propose a new type of working group focused on why (the business reference model)
    – Describe the ability to merge various TCG standards into enterprise solutions meeting business objectives

– How would we organize this?
  • Creation of a “Solution Working Group” that is focused on the business / mission outcomes using the output of the technical working groups

– Who is targeted?
  • CIO’s, Systems Integrators, Business Mission Owners, Enterprise Architects from a broad cross section of interested industries and companies

– What would be produced?
  • Logical Reference model (components, interfaces, use cases, standards alignment and gaps, compliance validation)
    – an open model that industry can utilize as a framework for building secure enterprise solutions

– Relationship with existing TCG Committees, Working Groups
  • Provides input to Technical Committee and its working groups
  • Fosters participation in technical working groups to facilitate the ability to meet the business need
HOW WILL THIS CHANGE THE GAME?

– In an IT commons based on multi-tenant, shared infrastructure, the challenge is to:
  • Establish trust in the provider of IT services
  • Establish and monitor compliance to changing IT policy
  • Assess and monitor compliance to cost, policy and performance objectives
  • Do this in a multi-sourced, multi-supplier ecosystem

– To establish and maintain trust, suppliers need to:
  • Enable consumers to assess the trustworthiness of supplier systems
  • Enable real-time assessment of compliance as part of the provisioning process
  • Support real-time monitoring

The use of open trusted platform standards provides consumers a way to assess the suitability, compliance and performance of shared
REFERENCE MODEL

Strawman Example
TMI REFERENCE ARCHITECTURE: LOGICAL VIEW

- **UAD**: User Access Device (that support connecting to one or more concurrent domains)

- **Servers**: Federated Data Center of servers that can host multiple independent domains

- **Exchange**: Logical component (phys. and virt.) that defines cross-domain information flow rules

- **Storage**: Federated Storage infrastructure

- **Network**: Devices that can transfer data from multiple domains.
TMI REFERENCE ARCHITECTURE: MANAGEMENT VIEW

Independent Domain management

Platform 1

Domain 1

Domain 2

Domain 2

Domain 2

Domain 3

Domain 3

Domain 3

Domain 3

Domain 1

Platform management

Platform 2

Platform 3
USE CASES

– Most use cases can be derived from a small set of core primitive capabilities:
  • Establish Trust (aligned to PKIv3 and TPM/vTPM)
    – Establish a level of trust (including the degree and types of information to be accepted) between parties
  • Exchange information (aligned to attestation)
    – Exchange information between parties within the bounds of the trust relationship
  • Apply Policy (aligned to IF-MAP)
    – Identify executable policy statements and stores, information sources and sinks, decision authorities, execution points, obligations on parties and policy hierarchies

– Define use cases using the vocabulary associated with the core primitive functions
  • Provide information from a confidential source to a recipient in another tenant domain with assurance of the ability to trust the information is reliable
  • Determine if workload from a tenant domain can be provisioned to an external cloud provider in accordance with the policies of both the provider and consumer of services
WAY AHEAD

– A group of companies has developed this STRAWMAN proposal and reference model to kick start the discussion
  • HP (EDS), BAE Systems, CA, Raytheon, Oracle (Sun)

– Developed a proposed charter for a new Trusted Multi-Tenant Infrastructure Solutions working group within TCG

– Charter ratified by the TCG Board on March 18, 2010

– Develop an initial working draft of the reference model for discussion with the Technical Committee
  • Identify standards supported
  • Identify potential gaps
  • Identify outside standards needed to solve the problem

– Begin work with Technical Working Groups

We encourage any interested companies / agencies to get involved
Technology for better business outcomes