**Feb 9th Day 3 Notes from Trusted Platform Morning Session Morning**

Two Groups initially, then joined into one during Day 3 2nd session.

1. Trusted Platform/Provider Group, goal to come up with Trusted Platform Definition
2. MDM/Trusted Platform Group, finishing MDM mapping and come up with Trusted Platform definition.

The end results were similar, but the group when they rejoined as whole decided to adopt the MDM Group’s Trusted Platform Definition.

* **Trusted Platform definition**: Trusted platform is the underlying hosting (or execution) environment for the TOE that is sufficient to meet the assumptions and environmental security objectives of the PPs and modules the TOE claims. (Note: We need to define hosting environment/execution environment).
* The certificate authorizing scheme determines sufficiency by publishing a policy.
* Components of a platform may include, e.g., an operating system, virtualization hypervisor, various switches, and the hardware needed to run the software.

**Trusted Platform and Trusted Provider Breakout Discussion**

What is considered a provider and what is considered a platform? From the cloud perspective it is a provider. The provider is who and the platform is what.

Major aspects of a trusted provider and trusted platform: Platform Integrity, Physical Security (provider), Trusted Admin (provider), Non-Malicious User (doesn’t matter if Cloud or on-prem).

**Trusted Platform**

Why do we need to define a trusted platform as opposed to a normal host platform? Because additional threat vectors and risks are introduced by operating in a cloud. Some cloud models provide the platform directly.

**General trusted platform definition**: That which meets the OE assumptions of the PP for a given technology type.

The confusion is with the different types of services (IaaS, PaaS, and SaaS). We need a definition for each one.

**Trusted Platform for IaaS:** Operational environment that meets the assumptions to provide a safe base for the installation of the TOE, physical security\*, and a trusted admin for the platform.

\*Physical security will probably be pushed out to the trusted provider definition, along with portions of the trusted administrator.

Example PP is Virtualization

**Trusted Platform for PaaS:** Operational environment which meets the assumptions to provide a trustworthy computing platform (potentially including: a root of trust, stores credentials securely, decommissions critical security parameters, separates multiple products) and provides a trusted admin for the platform.

Example PPs are General Purpose Operating Systems (GPOS) and Network Devices (NDcPP)

**Trusted Platform for SaaS:** Operational environment which meets the assumptions to provide a trustworthy computing platform (including reliable time clock; potentially including: a root of trust, a source of entropy and randomness, cryptographic functionality, file integrity, provides authentication and stores credentials securely, decommissions critical security parameters, separates multiple products) and a trusted admin for the platform.

Example PPs are Application Software, DBMS, and MDM

\* physical security will be pushed out to trusted provider definition, along with portions of the trusted administrator.

**Trusted Provider**: Provider of the cloud platform. Meets operational environment assumptions from the protection profile that are *beyond the scope of the platform* *and vary by deployment scenario*: physical security, trusted administration of the platform/infrastructure, administration of the integrity of the platform/infrastructure, availability of the platform/infrastructure.

Can the platform meet some of its own physical security?

With multi-tenancy, the administrator is more a trusted provider; the platform includes databases, computers, etc.

With an on-prem data server, you are assuming the customers are all your customers; the trusted provider ensures customer A is trusted versus customer B. If there is a cloud provider that serves only one customer, then that is the same as on-prem.

This group suggested the following diagram:

Diagram

Description automatically generated

**OE = T. Platform + T. Provider = Cloud Service Offering**

When this was discussed with the MDM/Trusted Platform Group, the diagram was edited because people did not like the addition of Trusted Provider.

The end result was:

A picture containing chart

Description automatically generated(blue line joins diagram below)

Diagram, venn diagram

Description automatically generated

When then the Guidance Document Group returned to join the subgroup after lunch, they were not satisfied with the Trusted Platform definition at the beginning of this document.

It was discussed that the definition might need to go to a vote.