Trusted Multi-Tenant Infrastructure Workgroup

Market Observations:
• Multi-Tenant security is an end-to-end configuration requirement and many standards/products only solve parts of the problem.
• No comprehensive framework exists to describe the business/mission needs and validate compliance of the entire solution set against open standards.
• There is a need for solutions that address trust and security across solutions derived from combining dedicated and shared infrastructures.

Market Demand:
• Cost reduction and consolidation of IT resources and staffing
• Green initiatives to better manage power usage and waste
• To support shared infrastructure for critical infrastructure:
  ▪ Financial (PCI), Healthcare (HIPAA), Energy (NERC/CIP)
  ▪ Global Government and Industrial Base
  ▪ Defense including joint service or coalition operations (HAP)
  ▪ Shared services within public, private, community and hybrid “clouds”

Trusted Multi-Tenant Infrastructure Working Group:
• Develop Use Cases: Establish Trust, Apply Policy, Exchange Information
• Draft Reference Implementation Framework for End-to-End Trusted Multi-Tenancy
• Component requirements promoting Policy Compliance
• Identify Standards and Address Gaps
• New class of members including: CIOs, integrators, business mission owners, enterprise architects.
Trusted Clients

Security Built In

- Trusted Platform Module (TPM)
- Mobile Trusted Module (MTM)

Features

- Authentication
- Encryption
- Attestation
Trusted Servers

Security Built In

- Trusted Platform Module (TPM)
- Secure Virtualization
- Secure Cloud

Features

- Authentication
- Encryption
- Attestation
Trusted Storage

Security Built In

- Self Encrypting Drive (SED)

Features

- Encryption
- Authentication
Trusted Networks

Security Built In & Coordinated

- Trusted Network Connect (TNC)

Features

- Authenticate
- Health Check
- Behavior Monitor
- Enforce
<table>
<thead>
<tr>
<th>CSA Domain</th>
<th>(Number) Type</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>(2) Governance/Risk Management</td>
<td></td>
<td>Decrease risk exposure</td>
</tr>
<tr>
<td>(3) Legal and Electronic Discovery</td>
<td></td>
<td>Data Recovery and Encryption</td>
</tr>
<tr>
<td>(4) Compliance and Audit</td>
<td></td>
<td>Server Attestation</td>
</tr>
<tr>
<td>(5) Information Lifecycle Management</td>
<td></td>
<td>Safe Data Retirement</td>
</tr>
<tr>
<td>(6) Portability and Interoperability</td>
<td></td>
<td>Metadata Access Policy</td>
</tr>
<tr>
<td>(7) Traditional Security</td>
<td></td>
<td>Network Access Control</td>
</tr>
<tr>
<td>(8) Incident Response</td>
<td></td>
<td>Coordinated Security</td>
</tr>
<tr>
<td>(11) Encryption / Key Management</td>
<td></td>
<td>SED, Hardware Key storage</td>
</tr>
<tr>
<td>(12) Identity/ Access Management</td>
<td></td>
<td>Hardware Token Authentication</td>
</tr>
<tr>
<td>(13) Virtualization</td>
<td></td>
<td>Trusted Multi-tenancy</td>
</tr>
</tbody>
</table>

**CSA Guidelines and TCG**
TMI Use Cases

Description: developed to define the components, identify component activities, and describe the interfaces between those components in order to provide guidance to integrator, broker, provider, or consumer organizations to implement a Trusted Multitenant Infrastructure.

Use Cases core functions:

- **Establish trust** (aligned to PKIv3 and TPM/vTPM)
- **Exchange information** (aligned to attestation)
- **Apply policy** (aligned to XACML)

Use Cases categories:

- **Generic**
- **Provider Management**
- **Consumer Management**

Benefits:

- Explains the roles and key interactions necessary to implement a Trusted Multi-Tenant Infrastructure.
- In-depth depiction of Provider and Consumer roles in a multi-tenant, multi-provider ecosystem
- Defines the foundational relationships between trusted components in a multi-tenant infrastructure
- Use Cases lay the groundwork to define implementation patterns.
Next Steps

TMI Reference Framework

• Description: Describes a broad set of foundational principles and requirements as well as a library of re-usable patterns where technologies and standards are applied between components in an enterprise context.

• Provides guidance and implementation patterns for cloud providers and consumers to implement a trusted computing based using shared multi-tenant infrastructure.

• TMI Use Cases are directly mapped to each pattern within the TMI Reference Framework.

• Projected completion by: Q2 2011

Questions:

Erik Visnyak (BAE Systems): erik.visnyak@baesystems.com
Michael Donovan (HP): michael.donovan@hp.com