Cloud Security and Common Criteria

Ashit Vora
Manager, Security Assurance, Cisco Systems, Inc.

September 18, 2012
What is Cloud?

IT resources and services that are abstracted from the underlying infrastructure and provided “on-demand” and “at scale” in a multitenant environment.
Types of Clouds and Services

Public

Hybrid

Private

SaaS

PaaS

IaaS
Cloud Infrastructure Components

- Hardware
- Hypervisor
- Host OS
- Application (with Guest OS)

Fabric Extender
Fabric Extender
Fabric Manager
Cloud Security – A Concern

“32 percent indicated security as the top deterrent to using cloud computing”

- Citrix cloud survey conducted by Wakefield Research
Accreditation vs. Certification

**Accreditation:**
- System level
- Responsibility of provider/operator
- Performed/updated on a regular basis

**Certification:**
- Product level
- Responsibility of vendor
- Specific to hardware and software versions

**Threats**
- Nefarious use of cloud computing resources
- Insecure interfaces
- Malicious insiders
- Shared technology issues
- Unknown risk profiles
- Data compromise

**Governance & Policy**
- Secure architecture
- Managing entitlements
- Security controls
- Physical security
- Personnel checks

**Product assurance and security evaluation**
- Vulnerability assessments
- Crypto validation (transport, at rest)
- Standards conformance
Pillars of Cloud Security

- Trusted Cloud
- Secure Connectivity
- Data integrity, Confidentiality, DLP
- Control, Secure Config
- Governance
- Compliance, Assurance
- Visibility, Transparency
- Infra Security, Multitenant isolation
- Data integrity,
- Confidentiality,
- DLP
- Control, Secure Config
- Governance
- Compliance, Assurance
- Visibility, Transparency
- Infra Security, Multitenant isolation
Pillars of Cloud Security

Trusted Cloud

- Secure Connectivity
- Data Integrity, Confidentiality, DLP
- Control, Secure Config
- Governance
- Compliance, Assurance
- Visibility, Transparency
- Infra Security, Multitenant Isolation

- FCS: Cryptographic Support
- FIA: Identification and Authentication
Pillars of Cloud Security

- Secure Connectivity
- Data integrity, Confidentiality, DLP
- Control, Secure Config
- Governance
- Compliance, Assurance
- Visibility, Transparency
- Infra Security, Multitenant isolation

FCS: Cryptographic Support
FDP: User Data Protection
FMT: Security Management
FPT: Protection of TSF
Pillars of Cloud Security

- Secure Connectivity
- Data Integrity, Confidentiality, DLP
- Control, Secure Config
- Compliance, Assurance
- Visibility, Transparency
- Infra Security, Multitenant Isolation
- FCS: Cryptographic Support
- FIA: Identification and Authentication
- FMT: Security Management
Pillars of Cloud Security

- Trusted Cloud
  - Secure Connectivity
  - Data integrity, Confidentiality, DLP
  - Control, Secure Config
  - Governance
  - Compliance, Assurance
  - Visibility, Transparency
  - Infra Security, Multitenant isolation

Policy enforcement framework for ID, Data protection, audit, security
App-based controls
Pillars of Cloud Security

- Trusted Cloud
- Secure Connectivity
- Data integrity, Confidentiality, DLP
- Control, Secure Config
- Governance
- Compliance, Assurance
- Visibility, Transparency
- Infra Security, Multitenant isolation

Operational Security
- SAS 70 Type II audits
- PCI, CC, ENISA, CSA, NIST, FedRAMP, HIPAA
Pillars of Cloud Security

- Trusted Cloud
- Secure Connectivity
- Data integrity, Confidentiality, DLP
- Control, Secure Config
- Governance
- Compliance Assurance
- Visibility, Transparency
- Infra Security, Multitenant isolation

FPT: Protection of the TSF
FRU: Resource Utilization
FTP: Trusted Path/Channels
Walk, Jog, Run – A simple proposal

- **WALK**
  PPs for technologies we know – switches, routers, OSes etc

- **JOG**
  PPs for technologies that are well established in commercial world but new to CC – Virtualization, Data Center specific switches

- **RUN**
  New technology PPs – Virtual security devices (virtual firewalls, switches etc), SDN, VM mobility

Just like nature, security abhors vacuum. If we as a community do not act now, Cloud security standards will be created without us.
Thank you.