

CC in the Cloud Essential Security Requirements

Preface

The CC in the Cloud WG is developing an Essential Security Requirements (ESR) that captures the fundamental requirements. This initial draft contains material that was created by the WG as a framework to utilize Common Criteria methodology for products deployed in a cloud environment.

Background and Purpose

There is not yet a defined and accepted method within the Common Criteria that addresses IT product evaluations in the cloud environment.

Today, CC reflects a static point in time for security evaluation methodology. Over the past several years, members of this TWG have witnessed customer migrations from an on-premise model where products are licensed and maintained to a services model where assurance benefits accrued from CC are not available in the cloud.

Customers are buying services, not products “Gartner foresees double-digit growth in government use of public cloud services, with spending forecast to grow on average 17.1% per year through 2021.” --Understanding cloud Adoption in Government

“In fiscal 2019, the White House-issued cloud Smart strategy gave agencies a mandate to expedite their journeys to the cloud Federal agencies spent a combined \$5.9 billion in contract obligations on cloud infrastructure as a service (IaaS), platform as a service (PaaS), software as a service (SaaS), and other cloud support and migration services. They’re on track to spend \$7.1 billion in fiscal 2020.”--The State of Federal cloud: Market Briefing

At some point customers are going to recognize that a CC evaluation of an ICT product provides little assurance in a cloud environment. Without a plan for CC addressing this factor, CC will become irrelevant in DevOps and Customers will require additional country specific testing instead.

As the market moves to cloud-based solutions, ISO/IEC15408 should be adapted in order to provide security assurance for cloud scenarios. In addition, vendors of products to be evaluated along with authors of cPP’s aimed at cloud use case evaluations, may need to add or alter specific code or cPP content carefully to ensure evaluate-able products and cPP’s.

Use Cases

Use Case 1: Software as a service (SaaS) a software licensing and delivery model in which software is licensed on a subscription basis and it is centrally hosted. It is sometimes referred to as "on-demand software", and was formerly referred to as "software plus services" by Microsoft. SaaS

applications are also known as on-demand software and Web-based/Web-hosted software

Use Case 2: Platform as a service (PaaS) or application platform as a service (aPaaS) or platform-based service is a category of cloud computing services that provides a platform allowing customers to develop, run, and manage applications without the complexity of building and maintaining the infrastructure typically associated with developing and launching an app.

Use Case 3: Infrastructure as a service (IaaS) are online services that provide high-level APIs used to dereference various low-level details of underlying network infrastructure like physical computing resources, location, data partitioning, scaling, security, backup etc. A hypervisor, such as Xen, Oracle VirtualBox, Oracle VM, KVM, VMware ESX/ESXi, or Hyper-V, LXD, runs the virtual machines as guests. Pools of hypervisors within the cloud operational system can support large numbers of virtual machines and the ability to scale services up and down according to customers' varying requirements.

Known Evaluation Methodology Gaps

Analysis is Static

Traditional product evaluations, most equivalent to SaaS use cases, must adopt rigid and static boundaries with regards to product version, platform components, and product scope. These considerations are problematic when adopted to a dynamic operating environment like the cloud.

Explicit detail of all TOE and Platform configurations and interactions between layers is required to ensure validation. cloud certifications would require the concept of a Trusted Platform in which this detail often unknown and quickly perishable, but the security posture is not diminished.

Use of Cryptography

Current cryptography certification frameworks rely on extremely detailed algorithm, implementation, and entropy details that are not always available or predictable to end users or product vendors on various cloud platforms or environments.

Platform Abstraction

Existing TOE composition requires stability in both the TOE and TOE Platform. The TOE operating environment in a cloud use case may or may not change dramatically due to a variety of factors such as hardware deprecation, underlying firmware updates, OS changes, etc. These changes may or may not be detected by the TOE and may or may not affect the TOE security posture.

New methodology to address minimum satisfactory capabilities in this regard will be needed to bridge this gap.

Environmental Evolution

Cloud environments have extremely limited half-lives. Traditional certifications can not match

pace. Furthermore, as cloud Hosting agreements are negotiated independently, access to the same platform or platforms used to evaluate a product cannot be guaranteed to the Common Criteria end user.

Provide additional threat model concerns for CCitC

The iTC will continue to review and monitor relevant Cloud Security Frameworks to capture additional threat considerations or assurance requirements. The following items were identified as particularly relevant for CC in the Cloud efforts.

Configuration

As cloud environments offer tremendous benefits of scale to IT Solutions, it is beneficial for product vendors to leverage autonomous deployment and delivery of TOE components. Traditional CC evidence such as Guidance Supplements or access to physical hardware may be difficult for cloud evaluations.

For example, container repositories and/or container orchestration configurations represent an area of interest for products and services using a cloud model that would require attention from PP or ST Authors and Evaluators targeting CC in the Cloud evaluations.

Credentials

Traditional CC evaluations typically rely on trusted network or administrator assumptions with regards to credentials and credential management. As cloud environments inherently challenge these assumptions, it is critical to extended SFRs and SARs to meet additional TOE security objectives.

It is not sufficient to solely rely on data at rest protections for credentials or key material. CC in the Cloud evaluations must consider the entire lifecycle of secrets, (to include generation, destruction, revocation, etc) as well as any escrow needed to maintain product operations.

For example, a SaaS application that connects to a datastore may or may not be provisioned manually or programmatically. PP or ST Authors that wish to evaluate Applications in a Cloud Deployment must ensure that credentials used to connect and encrypt/decrypt data within the Cloud Platform are not vulnerable to compromise.

Key Management

Cloud service models inherently require compute, network, and storage resources to be dynamically provisioned and de-provisioned programmatically. This presents unique challenges with providing encryption capabilities due to the need to orchestrate key management and delivery. CC in the Cloud considerations must extend assurance such that these capabilities are clearly defined and understood within the scope of evaluation.

For example, Virtual Machines or Containers that leverage encrypted storage volumes often require additional operational components to provide pre-boot authentication and/or HSM services for decryption operations. The Key Hierarchy and lifecycle within the CC in the Cloud use case are of additional concern in this threat model.

Insider Threat

Products and services provided through the cloud require trust on behalf of the vendors and user that extends to operational personnel far above non-cloud deployments.

This iTC will consider requirements or expansion of scope that includes ALC deliverables to satisfy these additional threat concerns.

Multi-tenant

Conventional CC evaluations typically assume that the TOE platform or underlying infrastructure is controlled at the enterprise level by a singular entity within the enterprise. In cloud environments, this assumption can not be included as the nature of cloud services inherently introduces an aspect of multiple enterprises (multi-tenant) sharing resources both physical and logical.

For example, cloud customers of ICT products understand that moving to the cloud means sharing infrastructure with other customers. While Cloud Providers offering IaaS capabilities may offer dedicated hardware or instances to one cloud customer, this is the minority of cloud use cases.

This iTC will consider products deployed in a multi-tenant environment with respect to any optional or objective SFRs involving cloud use cases that mitigate Guest Escape, Data Leakage, Privilege Escalation, etc.

Assumptions

Ultimately, CC scheme input into this ITC will be critical to evolve these assumptions. For initial consideration, the following assumptions have been defined.

Trusted Platform

Cloud based service models inherently incur a trust relationship to certain components of the Information Technology solution.

End users of Common Criteria in the Cloud certificates will require that changes to the underlying infrastructure do not degrade the security functionality of the TOE. This ITC will propose an approach that will allow for composable construction of a trusted platform concept by leveraging existing collateral.

Areas for consideration may include:

- Any existing Common Criteria Certificates valid for the TOE Environment.
- Any existing cryptographic collateral information (e.g. FIPS 140, ISO/IEC 19790 or equivalent)

for the TOE Environment.

- Any existing TCG TPM information for the TOE Environment.

Trusted Provider/Admin

Similarly to the Trusted Platform concept from above, additional collateral is appropriate with regards to the Cloud Service Provider and their role as a Trusted Administrator.

Areas for consideration may include:

- Specify any existing governmental authorizations (e.g. FEDRAMP, CMMC) applicable for the TOE Environment.
- Specify any existing ISO/IEC 27001/2 certificate information.
- Specify any existing ISO/IEC 20243 (e.g. Open Group Trusted Technology Provider Standard) certificate information for the TOE Environment.