2014-06-01

Cloud-Friendly, Virtual, Information Assurance and Cross Domain Services

Gunderson, Chris

Cloud-Friendly, Virtual, Information Assurance and Cross Domain Services

C.R. Gunderson
Naval Postgraduate School, Department of Information Science
On Behalf of Office of the Undersecretary of Defense for Intelligence (OUSD (I))
1 June 2014

Table of Contents

An Illogical Dilemma

Cloud is a powerful paradigm precisely because it represents a fundamental departure from other IT provisioning paradigms. In particular cloud efficiencies result from carefully architecting dynamically re-configurable logical separation of computer network resources in lieu of static physical separation. Well-designed cloud-enabled services are provisioned in ways that are totally independent of the physical attributes of the runtime environment. This is essentially the definition of "cloud" and why cloud services are highly scalable. (Mell & Grance, 2011) Hence, the most effective cloud technical architectures are those that most effectively factor service processes into cloud-ready virtual machines. A virtual machine, by definition, is some set of hosted processes that is logically separated from other processes and hosts.

The Unified Cross Domain Management Office (UCDMO) was established in the 2006 to coordinate and oversee all U.S. government efforts to develop, certify, and accredit devices for sharing information across security domains. The UCDMO maintains a living list of approved devices of this kind. (Unified Cross Domain Management Office (UCDMO), 2014)Traditionally, UCDMO recognizes three types of Cross Domain Solutions: transfer solutions, i.e. "guards" that rigorously filter data bits in pre-approved message format, and then recompose the passed data on the other side of a system security boundary; multilevel security (MLS) systems that allow two way communications and/or data transfer at, and/or across, multiple security domains; access solutions that allow entry into differing security domains, hosted on the same hardware platform, but do not allow transfer across security domains.

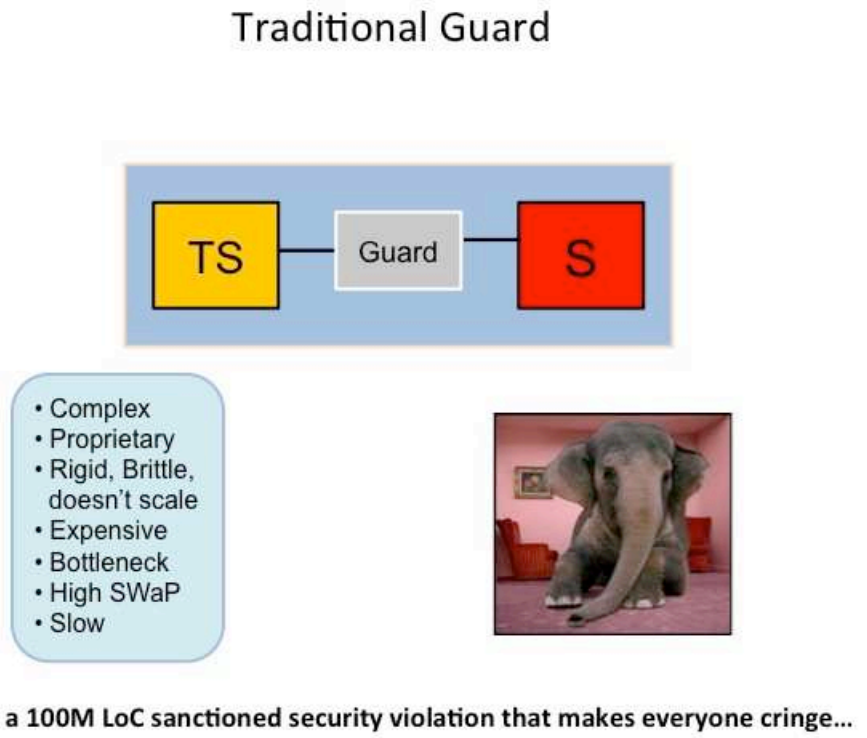

Figure 1: Traditional transfer guards use complex, proprietary, Boolean logic to enforce physical separation. They are inconsistent with modern cloud virtual architecture.

Ideally, a cloud would deliver Cross Domain Services, as with any other cloud service, by dynamically provisioning virtual machines to perform the carefully architected functional processes necessary to deliver on-demand MLS services. Of course, for Cross Domain Services, the virtual machines must be "assured," i.e. certified and accredited as trustworthy for sharing information across at least one level of security, i.e., from Unclassified to Secret, Secret to Unclassified, Top Secret to Secret, etc. (Note that in legacy policy language, "Protection Level" (PL4/5) meant a system, device, or

environment was accredited to share across one/two layer(s) of security. (Director of Central Intelligence (DCI), 2000))

With that goal in mind, it is hard to imagine processes that are less "cloud ready" than traditional cross-domain transfer solutions. These traditional guards are logical devices used to assure physical separation, a task that was architecturally necessary in the days of immature virtual technology. The complexity required to logically enforce physical separation requires several 10's of millions of specialized lines of code to execute highly proprietary, interdependent, Boolean predicates at the bit level. Likewise, MLS systems that are currently on the UCDMO approved list assure physical separation by using multiple complex transfer guards placed between subsystem security domains.

A Logical Solution

On the other hand, access solutions are built with modern virtual technology using a few 10's of thousands of lines of code. Access solutions built according to the Multiple Independent Levels of Security (MILS) architecture (Boettcher, DeLong, JRushby, & Sifre, 2008) (Boettcher, DeLong, JRushby, & Sifre, 2008), and at least consistent with the NSA High Assurance Platform, have been approved by the UCDMO. These access solutions have therefore proven their ability to provide logical separation between security levels such as Unclassified to Secret, Top Secret to Secret, etc.

Complex logical guards that guarantee physical separation by examining bits are no longer architecturally necessary because it is now possible to assure logical separation across security domains. Therefore, the target architecture for Cloud Multi-Level Cross Domain Services can be virtual machine "stacks" of simple virtual guards on top of assured logical separation platforms. A virtual guard could be an assured yes-no switch that only needs a few hundred lines of GFE code (e.g. NSA's Block Access Controller (BAC)) to guarantee separation at the policy level. (McNamee & Heller, 2006)The assured logical separation platforms could be approved access solutions.

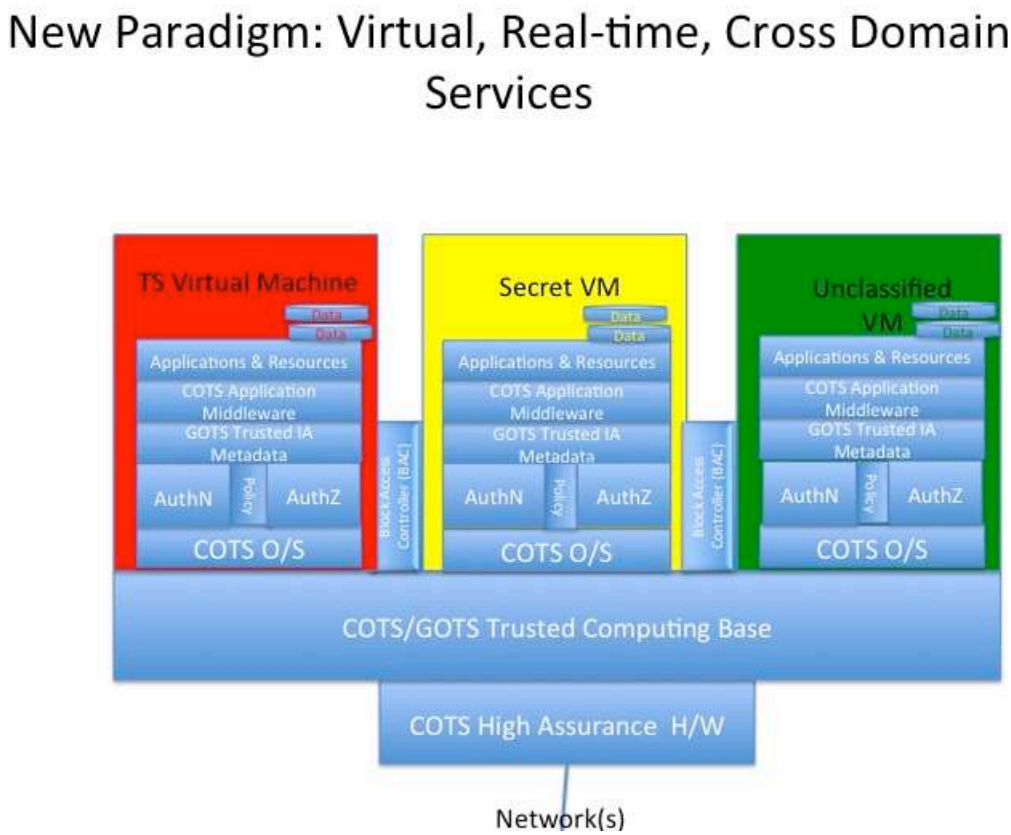

Figure 2: Architecture such as Multiple Independent Layers of Security (MILS), use assured virtual technology to guarantee logical separation.

In the Defense Enterprise, the individuals responsible for accrediting individual devices, systems, and/or environments for Information Assurance are called Designated Approval Authorities (DAA). DAAs perform this role according to the specific requirements and boundary conditions associated with their particular missions and systems. Various policy changes over the years have aimed to implement more standard approaches, and greater reciprocity. (Director of National Intelligence (DNI), 2008) (Department of Defense , 2014) However, DAAs still generally subscribe to the concept that any transaction that occurs across the boundaries of their responsibility constitutes vulnerability. Enabling cloud-based, virtual Cross Domain Services described above depends on DAAs agreeing to significant departures from the current paradigms for Certification and Accreditation (C&A), for example:

> The enterprise cloud must inherit the certifications and accreditations of the hosted Cross Domain Services. "Inherit" means that all concerned DAAs agree that the assurance arguments that led to the original C&A are valid, and remain valid, in the new environment. Today, DAAs rarely agree to inherit assurance arguments across their domains.
>
> To achieve cloud efficiencies regarding rapid evolution of capabilities, all concerned DAAs must accept the argument that changes to the upstream

technology stack – that they do not control - do not change their C&A assurance arguments, or alternatively, blindly accept the risk associated with uncontrolled changes. Otherwise, Cross Domain Services must be recertified every time changes are made within the enterprise cloud. Today, DAAs do not accept either option.

Certifiers and accreditors tend to have a different perspective on design than architects and engineers do. Information System architects and engineers tend think in terms of creating functional layers. Multiple logical functional layers, implemented with software for example, can exist within the same hardware device.

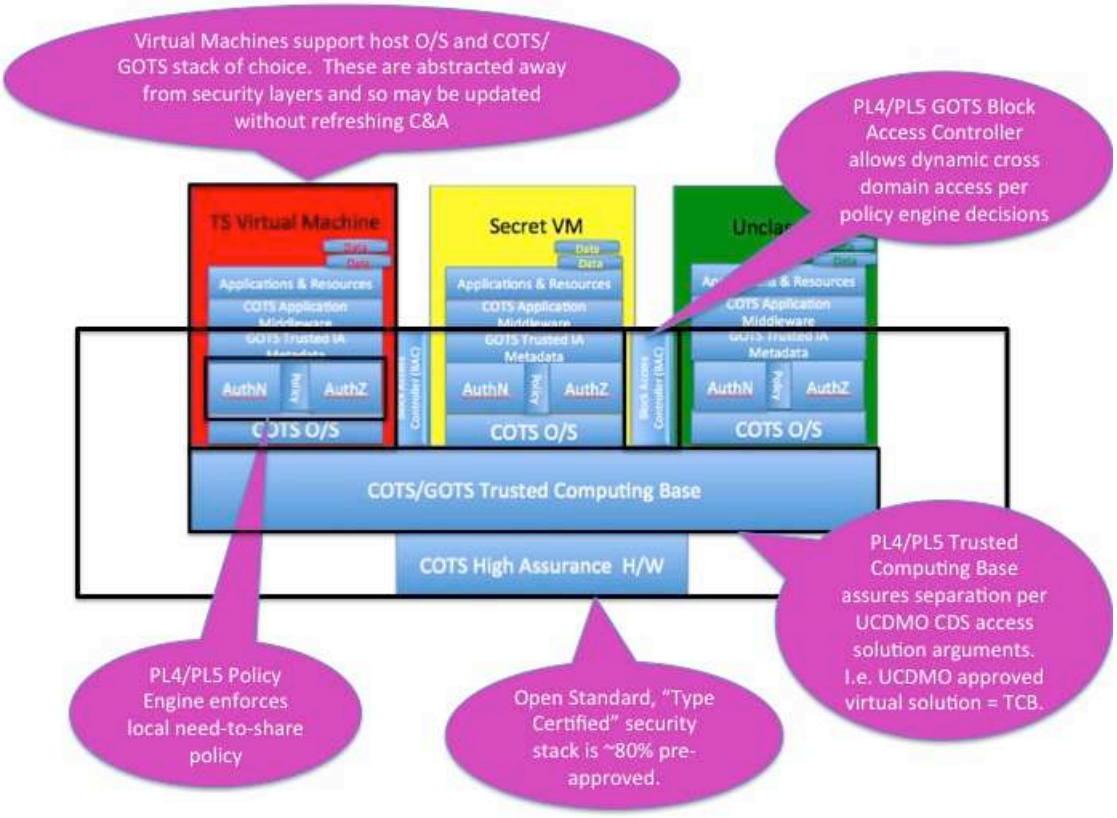

Figure 3: Logical assurance arguments that are based on open standards for virtual technology support inheritance of security controls. Reuse of the same reference architecture can accelerate C&A. In this figure, use of the legacy term "PL4, PL5" means assured access across 1, 2 security levels.

DAAs are legally responsible for the information assurance of specific, well-defined physical systems, not abstract enterprises. Vulnerabilities are weaknesses that adversaries can potentially exploit. Hence, certifiers and accreditors think in terms of maintaining security boundaries and managing vulnerabilities from that perspective.

Security boundaries tend to align with physical accountability, rather than functional, logical, process. DAAs do not certify or accredit environments that

introduce unknown (to them) vulnerabilities. DAAs only certify and/or accredit software processes that fall clearly inside their well-defined, physically accountable, environments. Hence, C&A arguments are usually based on ownership and control of physical hardware devices.

Note that the virtual machine target architecture described above, i.e. the cloud-friendly approach, lends itself to both the architect/engineer and the certifier/accreditor perspective. Indeed, an assured virtual machine Cross Domain Service, by definition, would capture well-defined logical functionality and managed vulnerabilities, within an equally well-defined and guaranteed security boundary.

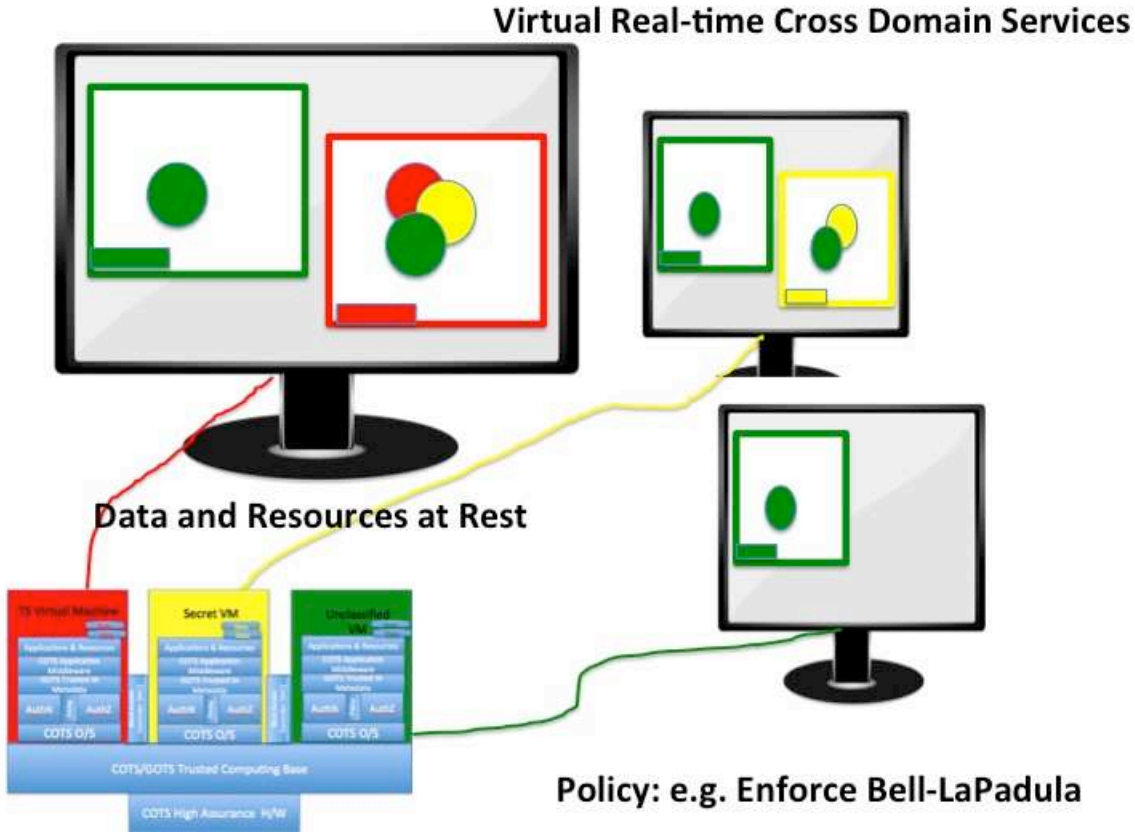

Figure 4: Virtual cloud Cross Domain Services engineered with assured logical separation can support dynamic implementation of any given "need-to-share" policy, e.g. Bell-LaPadula

Some Logical Actions

Here are some strategy recommendations for evolving Cloud Cross Domain Services and associated new C&A paradigms:

Address all traditional classes of Cross Domain Solutions; i.e. not just transfer guards, but also MLS, and access solutions.

Explain how to leverage success of transfer solution based MLS such as in the near term. Explain that these transfer-based MLS solutions will always be relatively expensive, and relatively difficult to cloud enable, e.g. they won't scale to support the most stringent tactical edge use cases.

Near term realities notwithstanding, emphasize the need to establish logical separation within "the cloud" as generally architecturally preferable to physical separation. Provide drawings to explain how to immediately use currently UCDMO-approved separation solutions such as NSA's High Assurance Platform (HAP) and/or AFRL's Secure View for this purpose.

Describe the Cloud Multi-Level Cross Domain Services target architecture, i.e. dynamically composable, assured virtual machines that provide assured MLS services across at least one security boundary, based on emergent need-to-share policy. Show how this approach addresses the C&A concerns over inheritance and tech refresh in context with vulnerability management and maintenance of security boundaries.

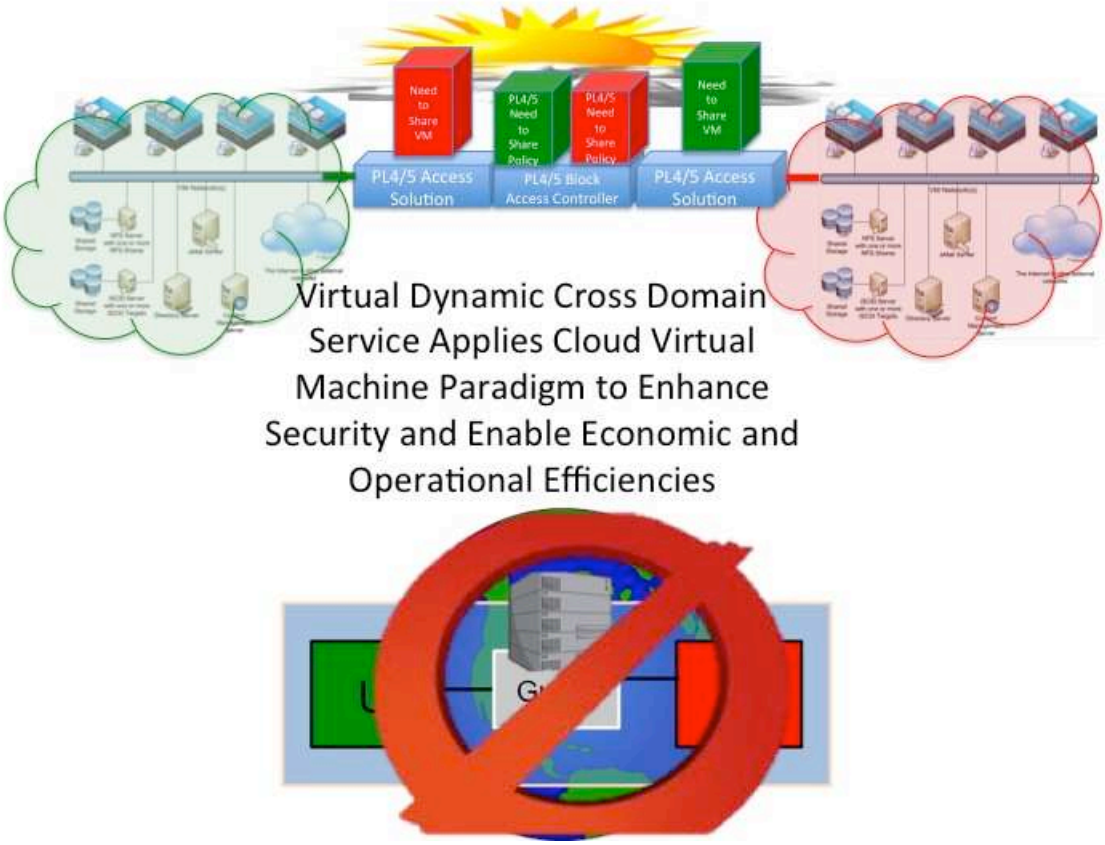

Figure 5: Assured, dynamically configured and collapsed, virtual machines provide need-to-share services across cloud logical boundaries. This approach eliminates the transfer guard bottleneck.

Partner with specific, operationally motivated, C&A authorities throughout technical evolution of Cloud Multi-Level Cross Domain Services.

Add drawings that explain the C&A assurance argument, i.e. vulnerability management and security boundary delineation, for this near term approach. Show clearly, how and why multiple independent DAAs will agree to a C&A inheritance strategy that allows their specific domain concerns to be satisfied within an enterprise cloud paradigm. Likewise, explain why they will not require C&A updates whenever tech refresh occurs upstream of their accredited cloud services. Insertion of assured logical separation will help support the argument.

Include timeline that shows migration to the target environment. Identify specific pilot projects that will do the evolutionary work.

Works Cited

Boettcher, C., DeLong, R., JRushby, J., & Sifre, W. (2008). The MILS Component Integration Approac to Secure Information Sharing. *27th IEEE/AIAA Digital Avionics System Conference.* St Paul, MN: IEEE.

Department of Defense . (2014). *Risk Management Framework (RMF) for DoD Information Technology (DODI 8510.01).* CIO . Washington, DC: DoD.

Director of Central Intelligence (DCI). (2000). *Protecting Sensitive Compartmented Information within Information Systems (DCID 6/3) - Manual.* Washington, DC: DCI.

Director of National Intelligence (DNI). (2008). *Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditiation (ICD 503).* Washington, DC: DNI.

McNamee, D., & Heller, S. H. (2006). Building Multilevel Secure Web Services-Based Components for the Global Information Grid. *CrossTalk: The Journal of Defense Software Engineering , 19* (5), 15-19.

Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing* . National Institute of Standards (NIST) Information Technology Laboratory, Computer Security Division . Gaithersburg, MD: NIST .

Unified Cross Domain Management Office (UCDMO). (2014). *UCDMO Cross Domain Baseline List.* Washington, DC : UCDMO.