Cybersecurity Impacts of a Cloud Computing Architecture in Live Training

Graham Fleener
U.S. Army PEO STRI
Orlando, FL
graham.g.fleener@mail.mil

Dr. Cliff Zou
University of Central Florida
Orlando, FL
czou@cs.ucf.edu

Jason Eddy
AIT Engineering
Orlando, FL
jason.eddy@aitengineering.com

ABSTRACT

Today's live training environment is comprised of many systems in various states of configurations with a limited ability to leverage shared services. The future of live training systems will evolve to a Training as a Service (TaaS) state to reduce overall operating costs, implement new technologies to improve the training experience, and centrally manage the training exercise of distributed training systems. With a TaaS approach to system architecture, a number of new cybersecurity and DoD Information Assurance requirements will need to be implemented in order to ensure the Confidentiality, Integrity, and Availability of DoD information Systems. Previous papers (Lanman and Linos, 2012) have outlined in greater detail the motivation and migration strategy for a pilot study on implementing TaaS within the Common Training Instrumentation Architecture (CTIA) used by the Army's Live Training Transformation (LT2) Product Line. This paper will present a number of cybersecurity threats, challenges, requirements, and commercial best practices for secure operations as well as Certification and Accreditation (C&A) requirements of a TaaS approach.

Threats not previously present in isolated system architectures will now need to be countered with appropriate defense mechanisms across physical and logical boundaries. This paper will describe and discuss cloud computing guidance for cybersecurity from the U.S. Army Chief Information Officer/G-6 guidance, National Institute of Standards and Technology (NIST), and the Defense Information Systems Agency (DISA). This paper will present a strategy for implementing commercial best practices to facilitate secure operations of a cloud computing approach to live training. Finally, the purpose of this paper is to provide an overview of the security requirements associated with cloud computing, document the certification process necessary to achieve an Authorization To Operate (ATO) for a cloud implementation, and discuss unique best practices associated with a PM TRADE implementation of a TaaS architecture.

ABOUT THE AUTHOR

Mr. Graham Fleener is the IA Manager (IAM) for Project Manager of Training Devices (PM TRADE) in the U.S. Army Program Executive Office for Simulation, Training, and Instrumentation (PEO STRI). Mr. Fleener served in the U.S. Marine Corps and then worked as a contractor for the Army before joining the Army Acquisition Corps as a Government employee. Mr. Fleener obtained both his Project Management Professional (PMP®) and Certified Information Systems Security Professional (CISSP®) certifications. Mr. Fleener holds a Bachelor of Science in Information Systems Technology and a Master of Science in Modeling and Simulation both from the University of Central Florida.

Dr. Cliff C. Zou is an associate professor in the Department of Electrical Engineering and Computer Science, University of Central Florida. He received the PhD degree in the Department of Electrical and Computer Engineering from the University of Massachusetts, Amherst, MA, in 2005. His research interests include computer and network security, computer networking, and performance evaluation. He is a member of ACM and senior member of IEEE.

Mr. Jason Eddy is the President and founder of Assured Information Technology (AIT) Engineering, an Orlando-based company specializing in the security and IA compliance of DoD systems. Throughout his career, Mr. Eddy has held a vast array of IA leadership positions in the DoD and commercial sectors. Mr. Eddy holds a Bachelor of Science Degree in Computer and Information Science from the University of Florida, a Masters of Business Administration, and is a Certified Information Systems Security Professional (CISSP®).

Cybersecurity Impacts of a Cloud Computing Architecture in Live Training

Graham Fleener
U.S. Army PEO STRI
Orlando, FL
graham.g.fleener@mail.mil

Dr. Cliff Zou
University of Central Florida
Orlando, FL
czou@cs.ucf.edu

Jason Eddy
AIT Engineering
Orlando, FL
jason.eddy@aitengineering.com

INTRODUCTION

In today's budget climate the Department of Defense (DoD) and the U.S. Army is constantly attempting to do more with less funding. One of the results of a leaner budget environment is to consolidate technology solutions. Cloud computing services and Service Oriented Architecture (SOA) are two areas in which the DoD and the U.S. Army, have targeted as a strategic opportunity to leverage. The thought is this path forward will provide an improved user experience with more capabilities and less overhead cost. For the purposes of this paper we will use the National Institute of Standards and Technology's (NIST) definition of cloud computing, "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

Within the U.S. Army's Project Manager for Training Devices (PM TRADE), a migration to SOA for interoperability among systems, and cloud computing for hosting services and applications has already begun (Lanman and Linos, 2012). After significant research was conducted, a roadmap was developed to migrate the Common Training Instrumentation Architecture (CTIA) to a Training as a Service (TaaS) architecture. The TaaS vision is to "develop and host an on-demand, self-service and continuous training environment and delivery model in which live training software and its associated data are hosted centrally (typically in the cloud) and are accessed by users with a thin client or mobile device, normally using a web browser over the Internet in support of the COE strategy" (PM TRADE TaaS Fact Sheet, 2013). The PM TRADE TaaS high level concept of operations can be seen depicted below in Figure 1.

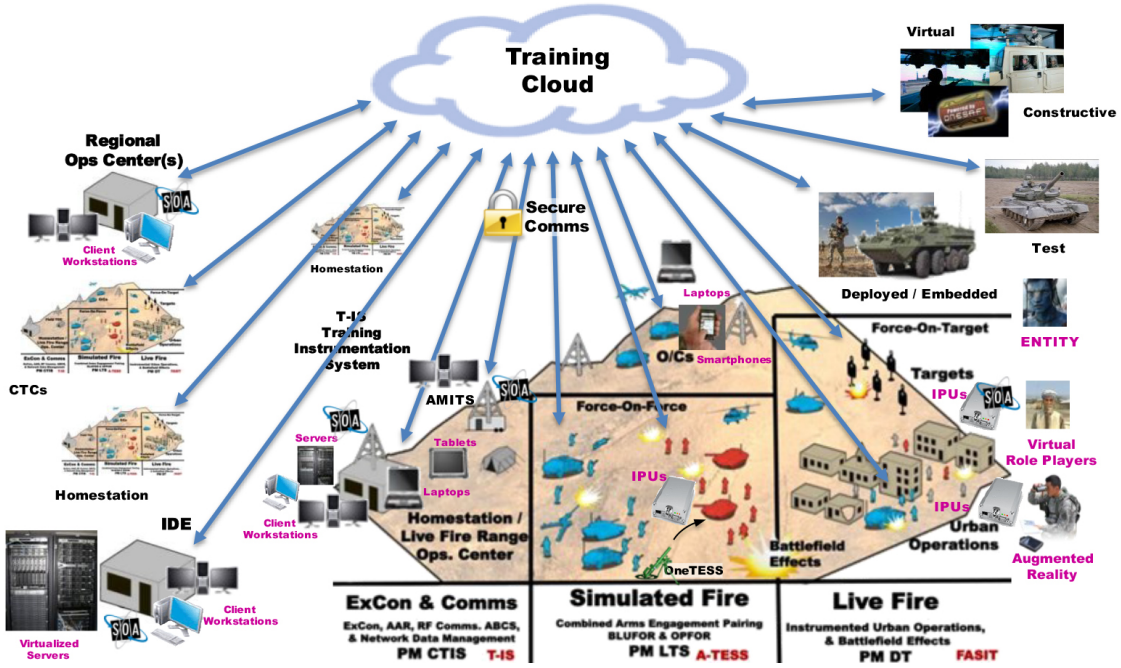

Figure 1. TaaS High Level Concept of Operations

However, a number of new cybersecurity threats and requirements come with this new emphasis on migrating from standalone or isolated networks to a cloud computing environment. Several Security Technical Implementation Guides (STIGs) (DISA, 2013) have been developed to ensure proper security guidance and requirements exist as the Army begins to implement a cloud computing approach. The U.S. Army Chief Information Officer/G-6 guidance, NIST, and the Defense Information Systems Agency (DISA) have published guidance, requirements, and standards to address cloud computing. Each of the guidance documents will be discussed and presented in this paper. In 2010, the White House implemented the Federal Risk and Authorization Management Program (FedRAMP) to provide a framework for security requirements, standards, and a focus on continuous monitoring to ensure secure and consistent operations (Takai, 2012).

The purpose and contributions of this paper are as follows:

1. Present the cybersecurity threats and challenges associated with a cloud computing architecture within the live training domain.
2. Provide an overview of the security requirements associated with cloud computing for PM TRADE.
3. Document the current certification process necessary to achieve an Authorization To Operate (ATO) for a cloud implementation.
4. Discuss unique best practices associated with a PM TRADE implementation of a TaaS architecture.

RELATED WORKS

There have been a number of DoD level strategy and policy papers published documenting the cloud computing model for the DoD, yet very little in the way of actual PM level cloud implementations. Conversely, industry is far ahead of the DoD with implementations of cloud computing in many segments of the Information Technology market. A gap exists in DoD research pertaining to specific implementations for a deploying, securing, and receiving an ATO for a cloud computing system at the PM level.

Within related works for cloud there are a number of general research works for secure cloud computing and threats within cloud computing. For example, Subashini and Kavitha defined the security issues associated in cloud computing that have emerged due to the nature of the service delivery models (Subashini and Kavitha, 2010). Ristenpart et al. discuss a number of the threats within cloud computing to include virtualization related vulnerabilities (Ristenpart et. al, 2009). Claycomb & Nicoll were the first to examine cloud computing related insider threats and identified the new exploit possibilities associated with an insider carrying out an attack using cloud resources (Claycomb & Nicoll, 2012). Jasti, et al., discussed a number of the security risk involved with exploiting insecure Application Programming Interfaces, or APIs. Jasti,et al., explains how insecure APIs could lead to significant overage charges due to increase useage from a DoS (Jasti, et al, 2010). Bamiah, et al., then discusses a number of protection mechanisms available for Cloud API keys to secure the cloud infrastructure (Bamiah, et al., 2012).

Additionally, there are a number of papers describing the need for a cloud or service oriented architectures in live training. Lanman and Linos discuss the need for a migration to SOA and cloud based systems within live training to allow for current systems to evolve to leverage technologies such as mobile devices and on-demand applications (Lanman and Linos, 2012). This paper's contribution will be to incorporate the live training communities need for cloud computing with the existing research from commercial cloud computing to provide a path for implementing a secure and IA-certifiable TaaS architecture.

THREATS AND CHALLENGES TO PM TRADE'S TAAS MODEL

There are a number of challenges for adopting cloud computing technologies within the DoD and the Army. DoD CIO Teresa Takai documents a number of challenges associated with moving to the cloud in the Cloud Computing Strategy she published in 2012 such as, "governance and cultural changes, IA and cybersecurity, network dependence at the tactical edge, service acquisition and funding sustainment, data migration, management, and interoperability" (Takai, 2012).

Currently, PM TRADE systems reside within closed, restricted networks with no logical connection to the Global Information Grid (GIG). Increased exposure to threats and vulnerabilities, insider attacks, privacy, and the

complexities of the business logistics of cloud acquisition are a few of the challenges the DoD and Army faces when moving to the cloud. Additionally, some of the cloud related vulnerabilities include "accessibility vulnerabilities, virtualization vulnerabilities, web application vulnerabilities such as SQL (Structured Query Language) injection and cross-site scripting, physical access issues, tampering, and IP spoofing" (Subashini and Kavitha, 2010).

As with any technology, there are a number of choices the system owner will need to make when implementing a cloud computing architecture. Each choice made has advantages and disadvantages, as well as varying levels of exposure to cybersecurity risks. There are three distinct service models utitlized to provide cloud based capabilities include Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). There are four types of deployment models used to include public, private, hybrid, or community. The proper approach to securing a cloud computing architecture will relate directly to the "cloud computing service model (SaaS, PaaS, or IaaS) and to the deployment model (Public, Private, Hybrid, or Community) that best fits the Consumer's business missions and security requirements (NIST Cloud Computing Security Reference Architecture, 2013). The level of responsibility between the system owner and cloud service provider varies depending on the service model chosen. SaaS requires the least amount of responsibility for the system owner, while IaaS requires the most with PaaS being a middle ground. In an IaaS service model, the system owner serves as the developer and integrator, as well as the administrator and operator (Badger et. al, 2012).

Cloud Computing Security Risks and Threats

Figure 2. Cloud Computing Threats and Challenges

There are a number of risks and threats that are specific to cloud computing to include "accessibility, virtualization, data verification, data loss, and data security" (Mircea, 2012). To protect and mitigate the risks, one must understand the main elements of threats (Cloud Security Alliance, 2011):

1. **Virtualization Related Vulnerabilities.** In a cloud computing environment the data does not physically reside in a known location, and therefore the system owner could be sharing physical infrastructure with a number of other users. There are a number of vulnerabilities associated with sharing physical server space in a virtualized environment. In this type of infrastructure it could be possible to "mount cross-virtual machine (VM) side-channel attacks to extract information from a target VM on the same machine" (Ristenpart et. al, 2009).
2. **Externalizing Data to the Internet.** Data previously internal to an organization is now delivered over the Internet, exposing previously closed and restricted systems to a number of network threats. Remote administrative access that was formerly restricted to internal locations will now need to traverse the public Internet (Jansen & Grance, 2011). Many DoD systems are on closed, restricted networks with little to no external access to outside networks or the Internet. With the migration to cloud this will cause previously standalone or closed, restricted systems to mitigate the risk of outside entities being able to access networks remotely. Proper enclave boundary defense including firewalls and intrusion prevention devices (IPS) will need to be configured to deny all and permit by exception (DAPE) (United States Army, 2009).
3. **Insider Threat.** The loss of physical control of the system information technology (IT) infrastructure opens up the possibility of an insider attack to the cloud based system. There are a number of types of insider threats that are present within cloud computing. The first insider threat is the rogue cloud provider administrator that has privileged access to the cloud infrastructure. Next, would be employees in the cloud user's organization maliciously exploiting weaknesses in the cloud's infrastructure. Third, are insider's using the cloud platform to launch attacks against the cloud user's local IT infrastructure (Claycomb & Nicoll, 2012). DoD employees go through a rigorous security clearance process when performing work in Classified facilities. DoD PM cloud user should have a clear understanding of the security clearances of any employees or system administrators on site at the cloud facilities.
4. **Lack of Physical Control and Oversight.** In a cloud computing environment the end user loses the means to control the physical environment and inherits a number of the physical security controls from the cloud

service provider. Currently, in the DoD the system owner will select a cloud service provider that has been provisionally authorized for use and certified by the DISA DAA. The DISA certification of the cloud service provider will be the source of a number of previously certified physical security controls (DISA, 2013).

5. **Insecure Application Programming Interfaces (APIs).** A user depends on APIs to access and connect to cloud services. APIs allow for the overall management of processes that take place when implementing a cloud computing infrastructure (Srinivasamurthy & Liu, 2010). With that dependency a security risk arises that could allow a malicious user to exploit an insecure API causing either Denial of Service (DoS) attacks or massive usages charges that would be billed to the user (Jasti, et al, 2010). Protection mechanisms for API exploits include robust authentication, proper encryption, and auditing of traffic and usage. Cloud API keys are unique codes used to facilitate access and secure the cloud infrastructure, and therefore should be protected in a secure method following approved processes (Bamiah, et al., 2012).
6. **Account, Service, or Traffic Hijacking.** This category of exploits includes man in the middle, phishing, fraud, spam, and software vulnerabilities in which a malicious attacker gains unauthorized access to data or communication. Protections include two-factor authentication, robust passwords, not allowing group authentication, and monitoring activity for unauthorized traffic (Srinivasamurthy & Liu, 2010).

Business Challenges of Cloud Computing Migration

In addition to the security risks and threats presented above there are a number of business challenges that must be addressed when migration to the cloud business model. The DoD acquisition process has traditionally lacked the agility to respond rapidly to a transition new business model. However, significant resources at the DoD level such as the FEDRamp program, which will be discussed later in this paper, are attempting to make the business logistics more feasible for a DoD PM. A number of other key factors must be properly planned when migrating to the cloud:

1. **Service Level Agreements (SLAs)**. When migrating to the cloud consumers have less control over certain aspects of the model, and therefore need to plan for any disruptions in performance, data loss, or downtime. SLAs provide a means of protection as a binding agreement to define the terms and conditions of the service (Bernsmed et. al., 2011). Security requirements should be carefully documented in the SLA to ensure both the cloud service provider and the system owner agrees on the delineation of responsibilities.
2. **Migration Plans for Changing Cloud Service Providers.** As competition for cloud service begins to enter into the DoD marketplace, a system owner must ensure there is a migration plan put in place upfront should a change need to occur for cloud service providers. FedRAMP is introducing a number of provisional ATOs for cloud service providers to do business with Federal and DoD system owners. With that competition will be significant to serve DoD agencies, and it will be the system owners responsibilities to put migration plans in place upfront.
3. **Rush to Adoption.** A final business challenge that should be discussed is the rush to adoption of cloud services prior to adequate Quality of Service (QoS) testing for a system owner's requirement. As many DoD PMs are migrating standalone or closed system to the cloud, significant testing and architecture migration plans will need to be put in place.

PM TRADE'S TAAS USE CASE

As DoD resources become more scarce and communication technology increases, TaaS is becoming an attractive option for PM TRADE to meet increased training needs while drastically reducing overall sustainment costs. Having developed and fielded hundreds of training systems into all types of sustainment environments, PM TRADE is keenly aware of the challenges encountered when transitioning from theory to practice. In order to identify the unexpected issues early, in late 2013 PM TRADE decided to begin some pilot programs to investigate real-world use cases of Training Systems hosted in the cloud. Through this process, PM TRADE has encountered several new challenges not previously seen in its traditional locally hosted systems.

During this PM TRADE pilot, the goal was to make cloud-based training services always available from any authorized, connected device. This effort was conducted in phases where it first began by choosing a Cloud Service Provider (CSP) with an active Authority to Operate obtained from the FEDRAMP process as discussed earlier in this paper. Then, a minimal set of non-sensitive training services were established on a cloud provider's physical resources. Once those initial services were established, layers of security were implemented and tested to ensure the

confidentiality, integrity, and availability of the data. Next, the remainder of the services were established and tested for functionality. Finally, the remainder of the security hardening, documentation, and penetration testing were conducted to ensure an adequate level of security had been obtained. Using this evidence, an Interim Authority to Test (IATT) was requested to allow the training systems to provide cloud-based training services.

PM TRADE TAAS PILOT PROGRAM IMPLEMENTAION RISKS, CHALLENGES AND APPLIED BEST PRACTICES

DoD guidance is very specific on selection of an approved CSP. The roadmap for building a training system and hosting it in a cloud comes with a new set of implementation concerns for the otherwise common security controls as specified in DoD Information Assurance Instructions such as 8500.2. The selection of a CSP as a possible host for training systems services, hinges on DoD issuance of a Provisional Authorization (PA) to the CSP for use and the CSP must be approved for inclusion in the DISA Enterprise Cloud Service Brokerage (ECSB) catalog before the Mission System Owner can consider requesting services from the CSP. Since the CSP evaluation is typically only completed once, the security of the CSP infrastructure relies heavily on the assurance from a previous certifier that security controls have been applied and continue to provide the necessary protections. These protections, special considerations, and training system implementation are outlined in the following section. Figure 3, PM TRADE TAAS Network Diagram, demonstrates a high level approach PM TRADE is pursuing for implementation.

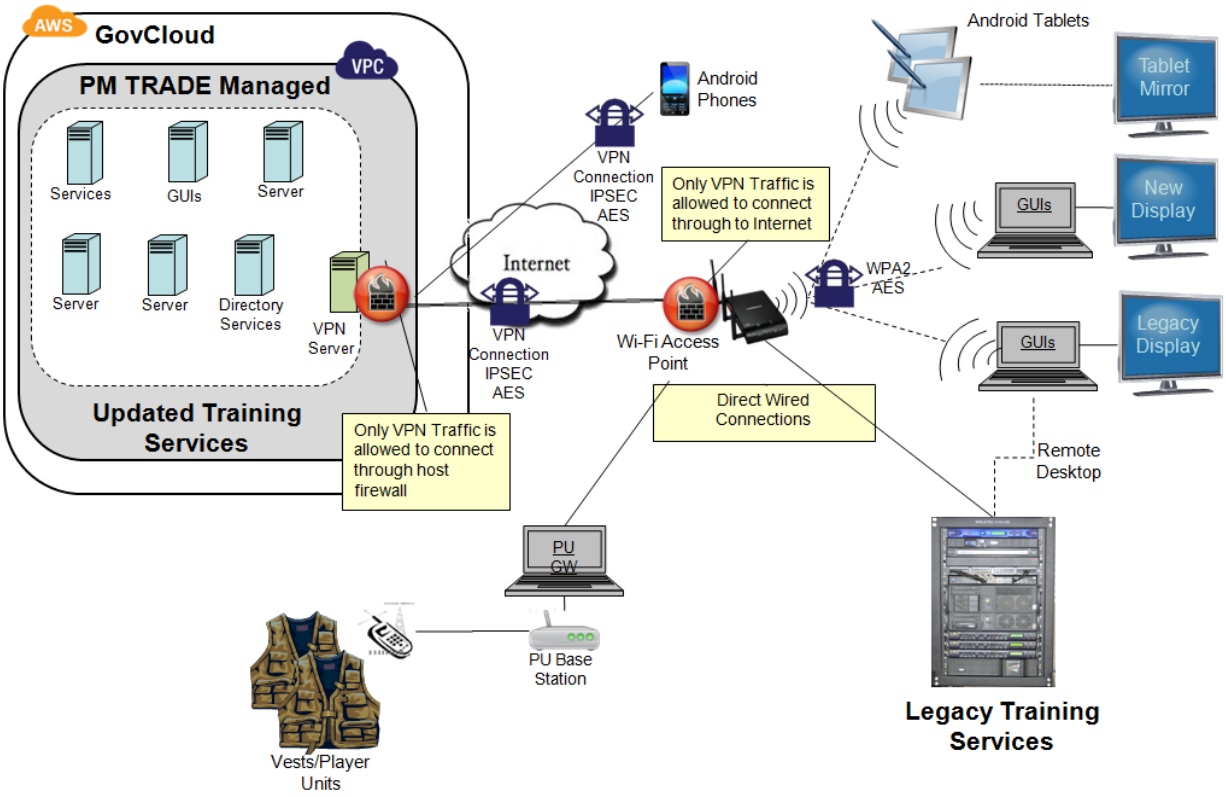

Figure 3. PM TRADE TAAS Network Diagram

Physical Security

Without adequate Physical Security, most other IA countermeasures are extremely ineffective. When the system was transitioned to the cloud, many DoDI 8500.2 physical security controls were assumed to be inherited and provided from the CSP. Although the protection of physical assets was already established and verified through the acceptance of the CSP, the exact details of their physical security countermeasures are not immediately releasable to the customers. Since the responsibility to protect the data still rests with the system owner, PM TRADE was not

comfortable releasing sensitive data without understanding the level of physical security in place at the CSP. Access to the security documentation was not readily available and resulted in a delay in transitioning the training services to the cloud. Ultimately, the PM TRADE selected CSP did have a process in place for requesting the information and availability of the documents was satisfied after proper identification and need-to-know was confirmed.

Data-at-Rest (DAR) Encryption

To mitigate any perceived Physical Security weaknesses and to comply with DoD requirements, DAR encryption can attempt to make any obtained information unreadable without proper decryption. A proper DAR solution is determined by assurance that access to the information is not hindered for authorized users and encryption key ownership and supervision remains with the training system owner. A typical DAR model utilizes a hardware-based Trusted Platform Module (TPM) that is typically resident with the device to create a trust or anchor point for management of the encrypted data. Protecting DAR in the cloud turns out to be somewhat challenging based on the menu combinations available and the desire to offload processing to the cloud provider's shared resources. Nevertheless, there are options available to protect sensitive data. The basic option is to upload data that has already been encrypted. While this data's decryption remains under the control of the data owner at runtime, this option turned out to have limited flexibility and does not scale well. The next option available was leveraging middleware solutions that make use of virtualized hardware encryption modules dedicated to the isolated partition. Within this solution set, the CSP provides two different protection mechanisms where the data owner manages the access and a solution where the cloud provider offers "Checkbox" encryption methods. Both options appear to work as advertised, but in the end, this pilot program did not contain any sensitive data and protection of data at rest were not explored beyond the ones afforded by the hosting operating system.

Network Boundary Protections

In a CSP provided environment, traditional enclave protection methods (perimeter router, firewall, intrusion protection systems, etc) are reduced to the availability of a few pre-configured security groups that perform stateless evaluation of network traffic. The requirement to monitor traffic for unauthorized access to the enclave becomes a challenge as there are no network device system logs or access to routing or firewall devices where the analysis could be performed by the system owner. Several options were explored to augment the monitoring that the CSP was assumed to be performing as documented in their CSP security plans. Options such as the deployment of network monitoring systems and spanning traffic to a network interface were attempted, but ultimately could not be accomplished because the users are provided no access to the underlying infrastructure systems. Basic network boundary protection tasks such as monitoring reset TCP connections or dynamically blocking access to specific resources is not available to the CSP user. In the end, the user is left with evaluating local system logs at the Virtual Machine level and a robust Host Based Security System (HBSS) be installed to enable stateful traffic inspection.

VPN Implementation

Remote access to the enclave is an essential part of the cloud computing experience to enable on-demand access from anywhere. The accessibility to training system resources and exchange of data requires that the Mission System Owner protects the data, at a minimum; using FIPS 140-2 sanctioned cryptographic modules. In order to accomplish this requirement, just as with any software or hardware procurement, the selected remote access product must be approved by the National Information Assurance Partnership (NIAP) or have a Protection Profile (PP) in development for the selected product.

The PM TRADE pilot TaaS solution had a requirement to provide access to mobile users as well as other sites hosting parallel systems to function as a hybrid cloud. While site-to-site VPNs are very common and trivial to implement on hardware, client interoperability between physical and virtual instantiations is not covered in vendor documentation. Interoperability support is limited to a few gateway platforms where most of the suggested configurations default to the category of generic IPsec where advanced options such as centralized authentication and auditing of remote access client activity vary drastically by vendor.

Configuring an approved VPN solution is not a simple solution. Although nearly all CSPs offers easy to configure VPN Gateways, these gateways do not provide a FIPS 140-2 validated solution where proper auditing can occur. These solutions typically use approved algorithms, but not approved products. In order to ensure adequate

protection of data, an approved VPN Server was established to protect data in transit. This solution turned out to be much more challenging in a fully virtualized environment where the CSP security and network optimization mechanisms applied to the virtual devices disrupted the flow of traffic on a consistent basis. The problem resolution required scouring countless forums and provider documentation to arrive at a solution that required significant VPN Server Operating System changes to allow integration and secure operations in the fully virtualized environment.

Lack of Operating System Flexibility

The configuration of virtual machine instances on a DoD-approved CSP is not as flexible as some of the other commercial cloud environments. The only available CSP-provided machine instances for the PM TRADE TaaS solution were preconfigured with a set version of Windows or Linux operating systems. Contrary to most locally hosted environments, the ability to import pre-configured virtual machines was not an option. This restriction had prevented efficiencies that could be realized by re-utilizing pre-configured systems that were installed and configured in accordance with Security Technical Implementation Guides (STIG) or best security practices. A few key examples of these issues were related to Operating System and application disk partitioning. Current STIG guidance has specific requirements for the OS and specific application or log volumes to be located on separate partitions which must be configured during OS installation. By being forced to leverage pre-existing virtual machines, the ability to configure those options was lost. In addition, some of the provided systems were already at a software patch level that was not consistent with the software baseline for the training system services. Rolling back tightly integrated applications such as Internet Explorer to previous versions frequently resulted in unstable configurations that required several reboots and registry entries to correct. This area is expected to improve with future releases of the CSP environments, where the ability to simply upload an already approved and tested server greatly expedites migration of systems with the assurance that they will be as hardened as they were in their previous environment.

Virtual Machine Security

As expected for a new computing environment where a large number of infrastructure security controls are provided by the CSP, establishing a coherent set of firewall and host protection rules required browsing several documents that addressed security in this particular cloud solution. Although there were several layers of network security available from the CSP, most of the rules were not effective as implemented. The provisioning of new machine instances resulted in unrestricted access to the Internet via a default route established by the provider in all environments. To control this behavior and to isolate the TaaS resources, servers were moved to a newly created isolated partition and an explicit rule was added to force all non-local traffic to egress via the newly configured VPN Server. In addition to the multi-tiered firewall administration, infrastructure services such as Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) lacked the flexibility where previously deployed in local environments. As a result, isolated virtual machines were not allowed to select persistent RFC 1918 addressing schemes to ensure isolation was not possible without further reconfiguration and provider involvement.

Outbound Network Access

The primary mechanism to administer the CSP user environment is with a web browser via Secure Socket Layer (SSL). This management access appears to work fine from DoD-managed networks. However, the primary mechanism to administer individual virtual machines in the CSP is via Microsoft Remote Desktop Protocol (RDP) for Windows and Secure Shell (SSH) for Unix-based machines. This presents a problem from DoD-managed networks since these protocols are typically blocked at the network boundary. In order to manage the Virtual machines, several techniques were implemented to work around the outbound restrictions. The primary implementation was to utilize Microsoft Remote Desktop Gateway which brokers machine access via an SSL socket and then transitions the RDP connection within the isolated network. This provided an intermediate step until all VPN connections could be established to allow a single entry and exit point of the TaaS cloud resources.

Off-Site Backup and Recovery

As noted previously, it was not possible to import or export a machine instance to meet the requirement of expeditious recovery to a previous secure state in case of failure. The support for booting a system from other media for the purpose of imaging a system to another local server was not possible either. Exporting network related

configurations, such as custom routing tables, subnets, or security groups is also not supported at the user level of management. Although the expectation is for the CSP to have redundant sites and restore all of these configurations in the event of a system failure, the ability to augment their solution is extremely limited at this time. In the end, the PM TRADE TaaS implementation is not a mission critical system and an adequate level of availability was achieved through manual recovery procedures reconstitute machines, re-apply STIG configurations, and re-install software.

Auditing Compliance

After the system had been installed and access restricted, all instances still had to be assessed for compliance with those security controls that are applicable regardless of the computing environment. To accomplish this, an administrative security instance was used to conduct the vulnerability assessment and produce the required reports for an IATT request. To validate the security controls applied to the ingress point of the isolated partition, an exterior scan was conducted to validate that only the allowed traffic ports and protocols were available. It should be noted that each CSP does have an acceptable use policy in place regarding activities that would trigger abnormal activity within or against a cloud partition. Prior to conducting any type of scanning or vulnerability assessment, it is necessary to obtain permission and notify the CSP about the expected activities and durations.

Phased Approach to Migration to the Cloud

As the DoD and Army push for a migration to the cloud, it is important to have a migration plan in place as opposed to a single, large flip of the switch. System owners should consider testing a number of cloud service providers with trials and pilot projects to determine which best meets their needs. Additionally, system owners should consider migrating the least vulnerable aspects of their systems first, while leaving the more vulnerable technologies such as those containing Classified data and mobile devices to later in a system's lifecycle.

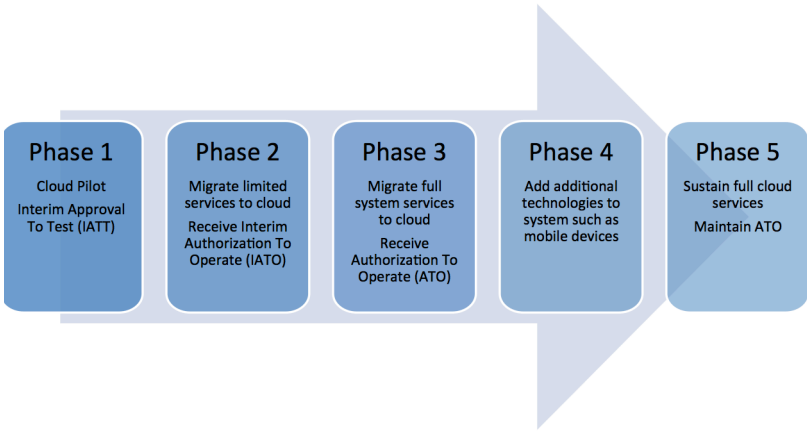

Figure 4 – Phased Approach to Migration to the Cloud

CLOUD CERTIFICATION AND ACCREDITATION

As with any security program, the requirements are a starting point and baseline to be tailored to a given system. For cloud service providers and system owners, a clear and upfront delineation of security control responsibilities will be more important than ever. As documented in DISA's DoD Enterprise Cloud Service Broker Cloud Security Model, the cloud service provider will receive a provisional authorization to operate as a DoD Cloud Service Provider that will be able to accept DoD customer's such as PM TRADE. Figure 3 below describes the process in which DISA has outlined in the DoD Enterprise Cloud Service Broker Cloud Security Model (DISA, 2013) to select, certify, accredit and implement a cloud based system. PM TRADE would then select the cloud service provider that most closely meets their requirements. The PM TRADE TaaS model has a number of cloud requirements that will need to be completed prior to Initial Operating Capability (IOC). The requirements include the above categories in Table 1 as well as specific security functions to limit the risk exposure of moving a DoD system to the cloud include continuous monitoring, strict configuration management and change control, and direct reporting of incidences to United States Cyber Command (DISA, 2013). NIST's Cloud Computing Security

Reference Architecture document outlines a process for aligning the FedRAMP's Assessment & Authorization process with the NIST Risk Management Framework (RMF) (NIST, 2013). (NIST Cloud Computing Security Reference Architecture, 2013). NIST's RMF is scheduled to replace DoD's current C&A process, DIACAP.

FUTURE WORK

Future work will continue to document the process used for Certification and Accreditation (C&A) as PM TRADE implements a cloud computing components within its Live Training Transformation (LT2) Product Line. The process from a DoD standpoint will become more transparent and accessible for DoD PM's to quickly and efficiently stand up cloud implementations much in the same way the commercial sector has already done. The cost, schedule, and performance impacts are much too great to pass up for the DoD to not facilitate this opportunity.

REFERENCES

Badger, L., Grance, T., Patt-Corner, R., & Voas, J. (2012) *National Institute of Standards and Technology Special Publication 800-146 Cloud Computing Synopsis and Recommendations*. Retrieved October 24, 2013, from http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf

Bamiah, M., Brohi, S., Chuprat, S., & Brohi, M. N. (2012, December). Cloud implementation security challenges. In Cloud Computing Technologies, Applications and Management (ICCCTAM), 2012 International Conference on (pp. 174-178). IEEE.

Bernsmed, K., Jaatun, M. G., Meland, P. H., & Undheim, A. (2011, August). Security SLAs for Federated Cloud Services. In Availability, Reliability and Security (ARES), 2011 Sixth International Conference on (pp. 202-209). IEEE.

Chief Information Officers Council & Chief Acquisition Officers Council. (2012). *Creating Effective Cloud Computing Contracts for the Federal Government.* Retrieved on October 25, 2013, from http://www.gsa.gov/portal/mediaId/164011/fileName/cloudbestpractices

Claycomb, W. & Nicoll, A. (2012). *Insider Threats to Cloud Computing: Directions for New Research Challenges.* Retrieved October 24, 2013, from http://www.cert.org/archive/pdf/CERT_cloud_insiders.pdf

Cloud Security Alliance. (2011). Security guidance for critical areas of focus in cloud computing v3. 0. *Cloud Security Alliance*.

Defense Information Systems Agency. (2013) *DoD Enterprise Cloud Service Broker Cloud Security Model.* Retrieved October 25, 2013, from http://iase.disa.mil/cloud_security/downloads/CloudSecurityModel_v1-1.pdf

Defense Information Systems Agency. (2013). *Security Technical Implementation Guides (STIG).* Retrieved on October 31, 2013, from http://iase.disa.mil/stigs/

Jansen, W. & Grance, T. (2011) *National Institute of Standards and Technology Special Publication 800-144 Guidelines on Security and Privacy in Public Cloud Computing.* Retrieved October 24, 2013, from http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909494

Jasti, A., Shah, P., Nagaraj, R., & Pendse, R. (2010, October). Security in multi-tenancy cloud. In Security Technology (ICCST), 2010 IEEE International Carnahan Conference on (pp. 35-41). IEEE.

Kundra, Vivek. (2011). *Federal Cloud Computing Strategy.* Retrieved October 5, 2013, from http://www.dhs.gov/sites/default/files/publications/digital-strategy/federal-cloud-computing-strategy.pdf

PM TRADE LT2Portal. (2013). *Training as a Service Fact Sheet.* Retrieved October 5, 2103, from https://www.lt2portal.org/FileGatekeeper.aspx?file=LT2_L0/TechnologyCompass/Fact%20Sheet%20for%20TaaS.pdf

National Institute of Standards and Technology (NIST). (2013). *Cloud Computing Security Reference Architecture Special Publication 500-299.*

National Institute of Standards and Technology (NIST). (2013). Security *and Privacy Controls for Federal Information Systems and Organizations Special Publication 800-53.* Retrieved on October 25, 2013, from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Mircea, Marinela. (2012). *Addressing Data Security in the Cloud.* Retrieved October 23, 2013, from http://www.waset.org/journals/waset/v66/v66-99.pdf

Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. (2009) *Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds.* Retrieved October 23, 2013, from

http://www.cs.cornell.edu/courses/cs6460/2011sp/papers/cloudsec-ccs09.pdf

Srinivasamurthy, S., & Liu, D. Q. (2010, November). Survey on Cloud Computing Security. In *Proc. Conf. on Cloud Computing, CloudCom* (Vol. 10).

Subashini, S., & Kavitha, V. (2011). A Survey on Security Issues in Service Delivery Models of Cloud Computing. *Journal of Network and Computer Applications.*

Takai, Teresa, (2012). Department of Defense Chief Information Officer Cloud Computing Strategy. Retrieved October 4, 2013, from http://www.defense.gov/news/dodcloudcomputingstrategy.pdf

Tenable.com. (2013). Tenable Delivers Best-of-Breed Configuration Compliance and Vulnerability Management for U.S. Department of Defense. Retrived on October 29, 2013, from: http://www.tenable.com/sites/drupal.dmz.tenablesecurity.com/files/uploads/documents/whitepapers/ACAS_CS_(EN)_v1_web.pdf

United States Army. (2009). *Army Regulation 25-2 Information Assurance.* Retrieved on October 31, 2013, from http://www.apd.army.mil/pdffiles/r25_2.pdf