Implications of Interoperating with Non-Hierarchical Security Domains

Dr. Tony Valle
Cobham Analytic Solutions
Colorado Springs, Colorado
Tony.Valle@cobham.com

Kelly Djahandari
Northrop Grumman Information Systems
Orlando, Florida
Kelly.Djahandari@ngc.com

ABSTRACT

To date, Cross Domain Solutions (CDS) systems have usually been employed to protect information in a "high" security domain from being accessed by systems or individuals in a "low" security domain. This common situation is a case of hierarchical domains in that from a security policy perspective, the high side can have unrestricted access to all the information on the low side. As a result, the CDS usually employs a "pass all" rule set that permits all the low side information to flow freely while restricting the high side information that passes to the low side.

This paper considers the case of non-hierarchical domains in which there is no unambiguous high side or low side, but rather two domains, each of which contains information that must be restricted from the other, but both also have common information that must be shared to allow for interoperability. The policy implications are numerous: is a single CDS device sufficient, or are two required? Can a rule set be constructed that can physically reside in one or both domains or is a third location required to comply with security policy? How can the common domain be defined in general? How can Operation Security (OPSEC) rules be defined in such a way to allow participants in each domain to be properly briefed? If battlespace content restrictions are to be imposed, how can the "master" site be defined to enforce them and how can scenario development be done by the domain participants without revealing inference to one another? We discuss each of these implications by showing how they fall into general cases, provide guidance on identifying the appropriate case for any specific instance, and describe what solutions are available to accommodate them.

ABOUT THE AUTHORS

Dr. Tony Valle is a Chief Scientist for Cobham Analytic Solutions residing in Colorado Springs, Colorado. He is currently supporting the USAF Distributed Mission Training Operations and Integration contractor in Orlando, Florida. He has more than 20 years experience in Modeling and Simulation architectures and has supported large scale simulation integration activities for the Army, Air Force, and Missile Defense Agency. He has a PhD in Physics from the Georgia Institute of Technology.

Kelly Djahandari, CISSP, is a Security Software Engineer at Northrop Grumman Information Systems and is leading a Cross Domain Solution Research and Development task order under the Distributed Mission Training program. Her information assurance experience includes more than 16 years of software engineering in network security research and cross domain solutions. She has co-authored conference papers on work in cross domain solutions and automated intrusion response approaches. She received a bachelor's degree from George Mason University and a master's degree from the University of Virginia.

Implications of Interoperating with Non-Hierarchical Security Domains

Dr. Tony Valle
Cobham Analytic Solutions
Colorado Springs, Colorado
Tony.Valle@cobham.com

Kelly Djahandari
Northrop Grumman Information Systems
Orlando, Florida
Kelly.Djahandari@ngc.com

PROBLEM STATEMENT

The description of the basic technical problem depends on several definitions which we provide here and which the reader should refer back to as needed.

A security domain is a collection of protected information with classification described by a Security Classification Guide (SCG). The SCG itself is assumed to be classified at the highest level contained within it. Throughout this paper we will use two basic domains, Alpha and Bravo that are assumed to be distinct, non-hierarchical, and overlapping. That is the Alpha domain contains some protected information in common with the Bravo domain, and both Alpha and Bravo contain information not contained in the other domain.

We define two new domains based on information content (see Figure 1). The Union domain is the collection of all information protected within the Alpha and Bravo domains, while the Intersection domain is the set of protected information in common to both. Both of these new domains are *artificial* in the sense that there may not be an SCG associated with either, but rather the classification of the protected data items is inferred from the Alpha and Bravo SCGs independently.

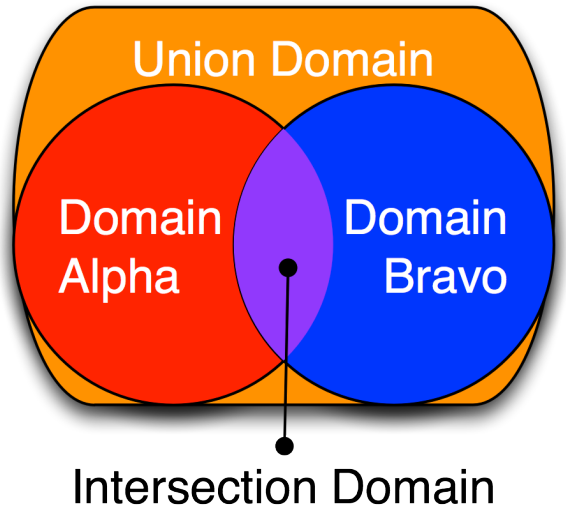

Figure 1. Security Domain Definitions

Within the Combat Air Force (CAF) Distributed Mission Operation (DMO) environment, aircraft simulators and support equipment are organized into Mission Training Centers (MTCs), each of which normally operates with a preferred security domain. Thus, we assume that one or more MTCs can operate in the Alpha domain while another subset of DMO MTCs can operate at the Bravo domain. We do not assume in general that any MTC would normally operate at the Union or Intersection domains.

With these definitions in place, the basic problem is this: how can two MTCs, MtcA and MtcB, operate in the Alpha and Bravo domains, respectively, and share a common battlespace providing adequate interteam training? Because the security domains are distinct, a cross domain solution (CDS) must be provided, and we consider the alternative solution architectures here.

Analogies Used

Discussion of generic security domains and their associated rule sets can be hard to follow without some examples, but real world examples are difficult to use in an unclassified environment. To better illustrate some of the key points, we will use examples based on science fiction sensors, weapons, and systems that do not have a real world counterpart. For instance, we can assume for purposes of illustration that the Alpha domain describes the capabilities of the USS Enterprise and the Bravo domain the capabilities of a Klingon Bird of Prey and that we desire to build a CDS to allow the simulators for these vessels to operate together against simulated Borg attackers. Our sensors include "scanners" and "probes"; our weapons, "phasers", "disruptors", and "photon torpedoes"; and our systems, "cloaking devices" and "warp engines". In this way, we can make the discussion more concrete in a safe and hopefully enjoyable way without being frivolous.

Classes of Protected Data

The classes of information protected in the Alpha and Bravo domains can usually be organized into three types that govern the nature of the solution implementation. *Operational* information is that which

governs the function or behavior of a subsystem. A good example would be the "cloaking device": a device that renders the Klingon vessel less detectable to Federation sensors. *Technical* information is that which governs the performance or limitations of a system. A good example would be the range, yield, speed, and available count of "photon torpedoes" on the Enterprise. Finally, *Representational* information is that which governs the way a system is modeled or presented in the simulated environment. An example might be the "disruptor", whose existence and nature must be protected, being represented as a "phaser" with equivalent operating characteristics.

Technical and Operational Rules

To isolate the Alpha and Bravo domains, we use a combination of Technical rules that are implemented in a Controlled Interface and Operational rules that govern the behavior of the participants in a distributed exercise. Technical rules filter the Distributed Interactive Simulation (DIS) Protocol Data Units (PDUs) to either block, guise, or pass unmodified the PDUs from one security domain to the other. Using the above examples, the "disrupter" would be guised as "phaser" representational information, or the "photon torpedo" technical information such as speed would be limited by the rule set.

Both technical and operational rules are required, in general, because a solution based solely on technical rules can be unfeasible. The simplest example is the presence of simulated voice traffic between MtcA and MtcB. Interoperability requires that the radios function across the DMO environment, so the Controlled Interface would not disrupt DIS Signal PDUs from voice radios. But the content of the PDUs is not feasible to examine, so participants could reveal protected information verbally over the radio channel. The only means to protect the information, therefore, is to instruct participants not to say things on the radio that would reveal protected information.

Another issue that can arise is the aggregate risk that results from accumulating large volumes of performance data over multiple scenario executions. A single "phaser" shot does not reveal the maximum range of the weapon, nor do a few dozen shots over the course of a day's training events. If, however, the log files for hundreds of events can be collected and analyzed, the performance envelope of the "phaser" would be fairly easily estimated. A technical rule cannot operate in a statistical fashion: it must be crafted either to let the shot be passed, or to block or guise it every time. The only protection against the accumulation of statistical data, therefore, is the use of an operational rule that requires log files to be purged or prohibits the use of those files for analysis purposes.

SOLUTION ARCHITECTURAL CONSIDERATIONS

Non-hierarchical cross domain solution architectural considerations include the intended training federation, location of the Controlled Interface and rule set, and rule set implementation including rules development, certification pre-requisites, and testing.

Training Federations Definition

If we are going to invest in the development and implementation of a CDS, we should do so with a vision in mind of the intended training federation. Specifically, there may be no training partners for the MtcA and MtcB systems that operate at the level of Intersection domain. It may well be that a common *Floor* domain is the only effective "low side" that can be employed. If that is the case, then the solution must consist of a pair of distinct CDS devices that permit separate interoperability between the Alpha and Floor, and between the Bravo and Floor domains. The possibility of building CDS to the Intersection and then an additional CDS to the Floor is prohibited by the restriction that we do not generally allow a "cascade" configuration of CDS devices to exist.

Because this problem is simply an iteration of two hierarchical "ordinary" CDS systems, we believe the issues are well-known and don't consider it any further here. Similarly, if there is a system that operates at the Union (or a higher level) domain, we can build independent CDS devices that isolate that domain from Alpha and Bravo, respectively. The interesting case is one where no MTC operates at the Union, Intersection or Floor domains, and the problem involves isolating the two non-hierarchical domains from one another directly.

Controlled Interface and Rule Set Location

Because the content of the SCG is usually classified at the same level as the domain it describes, the rules themselves are generally classified at that same level. That implies that the most general set of rules that govern the isolation of the Alpha and Bravo domains is itself classified at the Union level. Because neither MtcA nor MtcB operates at the Union level, the Controlled Interface device could not reside at either MTC, but would have to be placed at a third location (see Figure 2). This has architectural implications in

that the network will have to be configured to pass all simulation traffic to the third location and then back out to the MTCs, potentially resulting in higher latency and increased bandwidth requirements. An architecture that employs a single CDS that operates on the simulation data in both directions will be called a "union" configuration and the rules a "union" rule set.

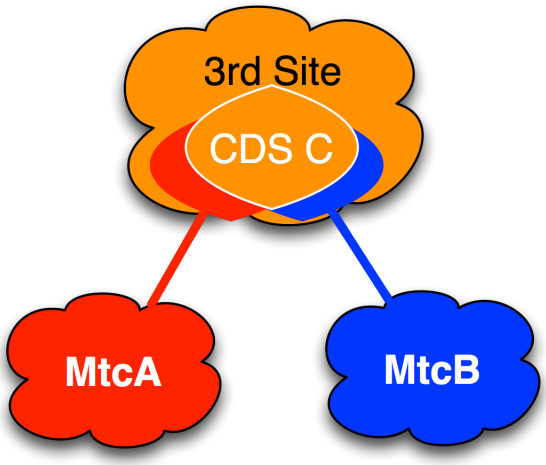

Figure 2. Union CDS Architecture

A second approach is to build separate CDS devices that isolate each domain from the Intersection domain. This "intersection" configuration involves a CDS at each MTC with the output sent to the other site and both operating with a "pass all" rule going from the local "low" to local "high" side. There are now two "intersection" rule sets: Alpha-to-Intersection and Bravo-to-Intersection that are separately implemented, tested, and maintained (see Figure 3).

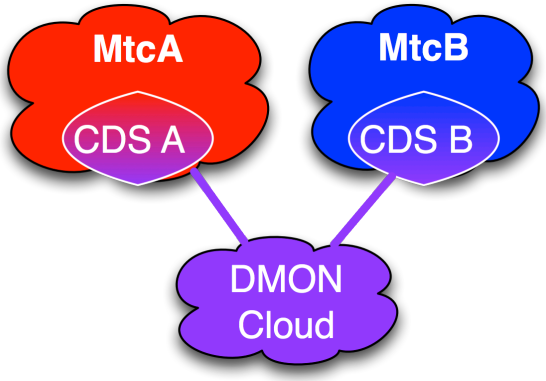

Figure 3. Intersection Domain Architecture

Rule Set Implementation

Implementation of a technical rule set is a complex process involving rule set working group meetings, documentation of all aspects of the rule set to support certification of the rule set and cross domain solution, rule set coding, and rule set testing. Many aspects of hierarchical rule set implementations can be carried over to non-hierarchical rule set implementations. This section describes hierarchical rule set implementation and the areas where there are implications with implementing a non-hierarchical domain rule set.

Rules Development

Development of a rule set involves rule set working group meetings with subject matter experts including pilots, simulator builders, cross domain solution developers, and aeronautical simulation experts. Working groups include members from both security domains of the cross domain solution to discuss and agree upon what and how the sensitive data is protected by the cross domain solution rule set, yet still provide effective training. The SCG provides guidance about the data to protect for a security domain and is referenced when developing the English Language Rules for the rule set. All members of the working group must be cleared to the Union security domain. This is no different than for hierarchical rule set working groups. The working group documents the rule set in an English Language Rules Plan, referencing the Security Classification Guide.

For a "union" rule set, the working group determines bi-directional rules, i.e., Alpha domain to Bravo domain rules as well as Bravo to Alpha rules. In hierarchical rule sets, low to high rules are frequently not used. For a union non-hierarchical rule set, the rule set would be classified at the Union domain and the cross domain solution would reside in a third party location that is cleared to the Union domain. The English Language Rules Plan would reference the Security Classification Guides from both security domains.

For an "intersection" rule set, the rule set working group determines two separate rule sets. One rule set would be from Alpha security domain to the Intersection domain (Alpha∩Bravo), which would be a lower domain. This would be a traditional hierarchical high to low rule set. There would be no low to high rules. The second rule set would be from Bravo security domain to the Intersection and again, no low to high rules. An intersection rule set would be classified at the "high" side (Alpha or Bravo) and the cross domain solution would reside at the corresponding MTC (MtcA and MtcB, respectively). The low side Intersection may be a new security domain and no MTCs need

participate at this security domain. Two English Language Rules Plan would be developed, each referencing the Security Classification Guide applicable for the "high" side security domain. Note that this approach does not require any participants in the Rules Working Groups to be cleared to the Union domain to perform this function. However, conducting testing may require personnel cleared to the Union domain in the event of a test failure or to assess the risk of the operating configuration.

Certification Pre-requisites

In order for the cross domain solution with the implemented rule set to be used operationally, it must go through Certification and Accreditation (C&A). Certification is a process to technically evaluate the system to certify the components comply with established security requirements. Accreditation is the formal acceptance by a Designated Approving Authority. The Designated Approving Authority reviews the Certification Package to determine if he/she wants to formally accept the risk and approve the cross domain solution with the rule set to test or operate at a site. An Interim Approval to Test must be received from the Designated Approving Authority before cross domain testing with the sites. An Approval to Operate must be received before the cross domain solution can be used for operational cross domain team training events.

A Certification Package consists of several documents including rule set-specific documents such as the English Language Rules Plan, English Language Rules Implementation Report, Certification Test Plans (configuration and functional), test results, and Residual Risk Report. These rule set-specific documents become more complex or numerous with a non-hierarchical rule set. The documents that are not specific to a rule set such as the Security Requirements, System Security Plan, Privileged User's Guide/Standard Operating Procedures, and Configuration Management Plan would not be different from a hierarchical rule set Certification Package.

The amount of documentation in the Certification Package would depend on the type of non-hierarchical rule set being implemented. Since an "intersection" rule set is essentially two separate rule sets, two sets of documentation would need to be prepared, each classified at the high-side security domain. In addition to the additional documentation, the Designated Approving Authority would need to supply an Interim Approval to Test for each rule set. To run the cross domain solution in an operational environment, two separate Approvals to Operate would need to be received.

The Certification Package for a "union" rule set would be classified at the Union security domain. The "union" rule set documentation would consist of the same number of documents as a hierarchical rule set, but the contents would include security protection methods and tests for both security domains.

Conduct of Testing

To obtain an approval to operate, extensive testing of the cross domain solution and rule set is required to achieve the approval authorities' confidence that the cross domain solution protects sensitive data and performs according to assurance requirements. For non-hierarchical rule sets, testing becomes more complicated than with hierarchical rule sets.

For hierarchical rule sets, four phases of testing are performed on the DMO Network CDS. Phase 1 is unclassified and confirms the proper configuration, integration, and functioning of the hardware and software being deployed to the MTC site. Phase 2 tests the classified rule set functions according to the English Language Rules Plan in a classified laboratory environment operating at the "high" side security domain. Phase 3, single level testing, uses the cross domain solution equipment at the MTC site with the classified rule set with the "high" side MTCs at the "high" side security domain and a "fake" low side MTC operating at the "high" side security domain during a live event over the DMO Network. Phase 3 tests the rule set in the real environment but removes the possibility of a data spill since it is run at a single security level. Phase 4, cross domain testing, is a true cross domain event with a true "high" side and "low" side. Phase 3 and Phase 4 tests run scenarios that exercise all the rules in the rule set. The software versions of all "high" side devices must be constant for Phase 3 and Phase 4.

Non-hierarchical rules change how these testing phases must be conducted. For a "union" rule set, Phase 1 testing could be conducted, but the hardware could not be deployed to the MTC. The equipment must deploy to a third party location. Phase 2 testing could be conducted at the Union security domain. Phase 3 testing as previously defined would not be possible without the sites operating at the Union security domain, which may be prohibited by operational considerations. As an alternative to live single level testing, a separate live scenario test of each security domain with the other side being the third party location operating at the "other" side security domain could occur. In other words a test would be set up using MtcA operating at the Alpha domain through the CDS to a third party site operating at the Bravo level but without MtcB connected. A

second test would operate between MtcB and the third party site at the Alpha level. The tests would be recorded for later analysis. Each MTC would run a test scenario that exercises all the rules. If a data spill occurs, this limits the cleanup to the third party location hard drives. Phase 4 tests would involve each site operating at their respective security domain running a scenario to test all rules in the bi-directional rule set. Note that this still requires the CDS site to be operated at the Union level since that is the presumed level of the "union" rule set itself.

For an "intersection" rule set, most of the testing is similar to hierarchical rule set testing, but with two separate (hierarchical) rule sets. Phase 1 testing is conducted on two distinct cross domain solution sets of equipment before being deployed to each MTC. Phase 2 testing is conducted separately on each of the separate rule sets. Phase 3 testing consists of testing each site's cross domain solution and rule set separately with a "fake" low side site. The "fake" low site could actually be running at the high side security domain. Both cross domain solutions at each MTC running their respective rule set in a single cross domain event would be used for Phase 4 testing.

SOLUTION EXECUTION CONSIDERATIONS

Operational considerations with a non-hierarchical cross domain solution include operational security, battlespace content control, and residual risk.

Operational Security

As discussed previously, a complete cross domain solution requires both technical and operational rules, these latter governing the limitations on the training audience and instructors, the content of the shared battlespace, and procedures that must be in place to support a cross domain event. In the traditional hierarchical case, the unambiguous "high side" contains all the "low side" content as well, so personnel operating in the high MTC are able to oversee the operation of the CDS and control the scenario with perfect knowledge of the items to be protected.

In the case of non-hierarchical domains, both MTCs are at least partially ignorant of the capabilities and protected content in the other domain. This introduces additional complexity in the development of operational rules and especially the content of the OPSEC briefings that are provided to the MTCs. In the case where the Alpha or Bravo domains are protecting representational information (such as the existence or basic function of a capability or subsystem) the OPSEC briefings have to be carefully constructed to prevent inference being gathered from their content.

Also, in the hierarchical case the high side participants are typically aware of the technical rule set content so they know how the battlespace seen by the low side has been shaped by the CDS. In the case of a "union" rule set, neither the Alpha nor the Bravo domain can in general be aware of the rule set content. This means that some anomalies or deviations from normal (non-cross domain) events may arise that can be confused with malfunctions or simulation errors, but may be normal for the cross domain event. As a result, problem reports that emerge from cross domain events may have to be handled by technical experts cleared to the Union domain to assess whether they are "bugs or features" and route them accordingly, properly sanitized.

A key feature of operational security is simulation implementation certifications. The technical rules firing in the CDS are dependent on preconditions in the simulation data stream to isolate those PDUs to be blocked or altered. Simulation vendors must be willing to assert with high assurance that the data stream produced by the simulators and support applications will satisfy the critical preconditions. Verification of these certifications is part of the testing and development of the C&A package.

Battlespace Content Control

One likely operational restriction is on the allowed content of the shared battlespace. Using our science fiction examples, let's propose that the Enterprise's "probe" is capable of detecting the signatures of Romulan engines at long distances, but this is protected information. If the Enterprise simulation is accurate, we may be unable to prevent the crew from reacting to a Romulan in the scenario thus revealing the ability of the Enterprise to track it. This may result in a restriction on the scenario content along the lines of "don't use Romulan ships in cross domain scenarios". Obviously this restriction is one that can't be shared with the lower domain since the very restriction is itself revelatory. For a hierarchical domain, this isn't an issue since control over the scenario content can be freely given to the high side since they know what's protected and what's possible for the low side simulations.

In the case of non-hierarchical domains, this becomes an issue. If in addition to the issue above, the Klingons' "disruptor" is capable of penetrating certain classes of "shields" and this is a protected capability, we face a conundrum. We cannot inform the Klingons not to place Romulans in the scenario, or the Enterprise not to use certain shield types without revealing protected

information outside its proper domain. In this case, a "white cell" or neutral scenario developer with knowledge of both domains is required to ensure that the scenario content is valid for both. Each player will have to communicate general scenario requirements to the white cell (they can't be too specific or the changes themselves might allow inference) and then allow the full scenario to be developed externally. This is a somewhat different paradigm than one would normally see in a distributed training environment.

Residual Risk

As with any security solution, risk of compromise is managed rather than entirely eliminated. Even with a guard that functions perfectly, risk remains from the possibility of observational inference, communications errors, scenario content errors, and certification errors. In general these operational risks are far more probable than a technical malfunction or compromise of the CDS device, especially in a controlled environment such as the DMO network.

In addition to direct violations, there is residual inference risk associated with the log files, generally associated with observation of system performance or behavior. Past history with CDS devices suggests that anomalies that could lead to inference occur in many event executions, but that the risk of observation in real time by personnel without insight into the protected data is very low. The risk increases if detailed analysis can be performed however, so managing this risk will often lead to a restriction on the use of log files ("may not be used for analysis") or the amount of data that can be accumulated ("delete log files after an aging period").

Of course for the hierarchical domain case, the high side log files can be maintained and used for any purpose subsequent to the event, and this allows for troubleshooting and forensic analysis. In the non-hierarchical case with a "union" rule set, the "ageing" restriction will almost certainly apply to both domains (this may be the case even for the "intersection" rule set). The operational policy may interfere with the ability to maintain audit records or troubleshoot problems after the ageing period has passed and has to be considered part of the training limitations that is incurred in cross domain events.

OTHER CONSIDERATIONS

Other considerations for a non-hierarchical cross domain solution and rule set are configuration management and generic rule sets.

Configuration Management

Configuration Management is vital for an operational CDS. Software and hardware baselines of the CDS device must be carefully controlled. In addition, any change to the interfacing systems that may affect the rule set must be approved before use. For hierarchical CDS rule sets, this means any change to a "high" security side system must be reported and approved before the change can be used in a cross domain event; "low" security side devices are not required to report changes. For non-hierarchical rule sets, changes to either security domain device would require approval before use in a cross domain event, greatly increasing the number of potential change requests and corresponding approvals for one rule set.

A reported change to a "high" side system may require testing before the change is approved for use in a cross domain event. The configuration review board determines the testing required to approve a change. Tests using MTCs on the DMO Network, similar to previously mentioned Phase 3 and Phase 4, may be needed; or tests using previously recorded playfiles in a classified test environment may be sufficient. For a non-hierarchical "union" rule set, testing may be required due to a change to either security domain. For an "intersection" rule set, each rule set (Alpha to the "intersection" domain and Bravo to the "intersection" domain) could be treated independently and changes to systems interfacing the Alpha security domain would only affect the Alpha to the "intersection" domain rule set, so any approval tests would only be required of that rule set.

The Configuration Manager must retain the classified baselines, such as the rule set, at the security domain level of the "high" side. For a non-hierarchical "union" rule set, this would require a "union" security domain configuration control. For "intersection" rule sets, each rule set would be controlled separately in their own "high" security domain.

Generic Rule Sets

Development of multiple rule sets has led to a few recurring "patterns" that seem to arise naturally in distributed simulation and many technical rules seem to arise out of these patterns. While it is not certain that such patterns will apply to the non-hierarchical "union" rule sets, they should apply to "intersection" rule sets, which are still of the general "high-to-low" type, but coupled and correlated. Because "union" rule sets operate on the data stream in both directions, logic suggests that there are multiple ways to factor their

behavior, possibly leading to new patterns that work more effectively.

CONCLUSION

CDS systems have traditionally been implemented to protect information in a "high" security domain from being accessed by systems in a "low" security domain since the security domains are hierarchical. When security domains on either side of the CDS system are non-hierarchical, the complexities of the CDS and its operation increase dramatically. As more MTCs are added and combined in varying team training combinations, the capability to allow participants of different non-hierarchical security domains to conduct team training and mission rehearsals on the CAF DMO Network will be needed. This paper discussed several implications of a non-hierarchical cross domain solution including architectural considerations and operational considerations.

REFERENCES

Danner, B., Muckenhirm, C., Valle, T., McElveen, C., Bragdon-Handfield, J., & Colegrove, A. (2002). Multilevel Security Feasibility in the M&S Training Environment. *Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) 2002*, Paper 167.

Danner, B., & Valle, T. (2005). Multilevel Security Assessment for the Distributed Mission Operations Network (DMON). *Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) 2005*, Paper 2165.

Danner, B., Valle, T., & McGregor, B. (2006). A DMON Cross Domain Solution (CDS) for Recurring Team Training. *Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) 2006*, Paper 2775.

Danner, B., & Djahandari, K. (2008). Cross Domain Solution Policy, Management, and Technical Challenges. *Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) 2008*, Paper 8343.

Danner, B. (2009). Cross Domain Solution (CDS) Certification and Accreditation for Persistent, Simulation Training. *Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) 2009*, Paper 9142.

Djahandari, K., Archer, J., & Danner, B. (2009). Cross Domain Solution Challenges Transitioning From Concept to Operations. *Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) 2009*, Paper 9133.

DMT O&I Contractor (2010). Combat Air Force Distributed Mission Operations (CAF DMO) Network Users Guide, Version 2.0. Retrieved May 26, 2010, from https://secure.dmodmt.com/document.cfm?id=2248 .

DoD (2004). Joint Air Force, Army, Navy (JAFAN) 6/3 Manual (FOUO).

Harris, Shon (2008). *All in One CISSP Exam Guide* (4th ed). New York, NY: McGraw-Hill.

Johnson, W. (2008) Combat Air Force Distributed Mission Operations: Immersion Into Daily Training. *Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) 2008*, Paper 8008.