Multilevel Security Assessment for the Distributed Mission Operations Network (DMON)[1]

Bonnie Danner, CISSP
Northrop Grumman
Orlando, Florida
bonnie.danner@ngc.com

Tony Valle, Ph.D.
Sparta
Orlando, Florida
tony.valle@trwdmt.com

ABSTRACT

This paper presents the technical and policy issues, architectural considerations, ongoing assessment results, and plans for Distributed Mission Operations Network (DMON) multi-level security (MLS) implementation. In this paper, the Combat Air Force (CAF) Distributed Mission Operations (DMO) Operations and Integration (O&I) team builds on previous Combat Air Force Distributed Mission Operations Multi-Level Security feasibility research and recommendations. Combat Air Force Distributed Mission Operations involves simulations built from components provided by independent vendors for different training communities. The Combat Air Force Distributed Mission Operations MLS problem comes when not all participants have the appropriate clearances for all information. There is a need for aircrews with different capabilities at different security levels, need-to-know, and categories to train together. MLS for simulation is a very challenging problem, not yet solved globally, yet critical to accurate representation of war fighting to distributed audiences at different security levels.

Findings in this paper are based on a Combat Air Force Distributed Mission Operations O&I research and development (R&D) task order focusing on the integration of a MLS Guard into the Combat Air Force Distributed Mission Operations Network. The research involves analyzing and documenting technical architectures for incorporating a MLS Guard into the evolving Combat Air Force Distributed Mission Operations system. The research also will include assessment of the MLS Guard integrated with the Combat Air Force Distributed Mission Operations Portal Kit in a test environment and on the Distributed Mission Operations Network. In addition, the research addresses training feasibility and associated limitations of the guard security rule sets.

ABOUT THE AUTHORS

Bonnie Danner, CISSP, is the Northrop Grumman task order manager for the MLS Guard R&D effort and contractor Security Engineering Lead for the Combat Air Force Distributed Mission Operations O&I Program. She has more than 20 years of information technology experience in systems engineering, software development, and information assurance. Her technical and project management experience includes Department of Defense and civil federal programs for Defense Advanced Research Projects Agency (DARPA), Navy, Federal Aviation Administration (FAA), National Aeronautics and Space Agency (NASA), Air Force R&D, and TRW Internal Research and Development (IRAD) projects. Ms. Danner's technical specialty is high assurance systems. Ms. Danner received a B.S. Degree from Virginia Tech University and a M.S. Degree from Virginia Commonwealth University.

Tony Valle is both a military and commercial simulation designer. He is currently the lead for the CAF DMO Common Models Standard, and the developer of the Master Conceptual Model. He served as the Chief Architect of both the Joint Simulation System (JSIMS) and Advanced Distributed Simulation Technology (ADST) programs and worked for LORAL and Lockheed Martin before taking on the job of Division Manager for the Orlando, FL office of SPARTA, Inc. Dr. Valle's work on commercial air combat modeling includes contributions to a variety of flight and air combat simulations. He received a B.S, M.S, and PhD from Georgia Tech University.

[1] 22 CFR 125.4(b)(13) applicable, Log #5003

Multilevel Security Assessment for the Distributed Mission Operations Network (DMON)[i]

Bonnie Danner
Northrop Grumman
Orlando, Florida
bonnie.danner@ngc.com

Tony Valle
Sparta
Orlando, Florida
tony.valle@trwdmt.com

INTRODUCTION

This paper provides an initial assessment of an ongoing investigation of the issues associated with integrating the Multi-Level Secure (MLS) Distributed Network Training Guard (DTNG)[2] into the existing United States Air Force (USAF) contractor-operated Distributed Mission Operations Network (DMON). It presents current considerations for guard deployment, lessons learned, and recommended next steps. These interim results are based on Operations and Integration (O&I)[3] contractor support to the MLS test bed and Security Working Group at the Distributed Mission Operations Center (DMOC) along with independent engineering analyses.

BACKGROUND

A Distributed Mission Training MLS Feasibility study in late 2001 was the precursor to current Combat Air Force Distributed Mission Operations (CAF DMO) MLS Guard research. This study determined the feasibility of potential MLS or compartment solutions for Combat Air Force Distributed Mission Operations training. To meet the Combat Air Force Distributed Mission Operations roadmap, geographically distributed federate sites and/or Mission Training Centers (MTCs) must be able to participate together in the same training event at different security classification levels or compartments. Today Combat Air Force Distributed Mission Operations distributed training events are held at a single security level with the same compartments[4].

The early study defined technical approaches to achieving a MLS solution, identified limitations and risks, and considered time frames for possible implementation. At its conclusion the feasibility study determined that although there were available MLS technologies that might be applied to the Combat Air Force Distributed Mission Operations MLS problem, there were no current policies or off-the-shelf technologies that could alone solve the Combat Air Force Distributed Mission Operations MLS challenge. Detailed descriptions of the MLS modeling and simulation problem and the suggested approaches were described in *MLS Feasibility in the Modeling and Simulation Environment*, paper number 167, published at the 2002 I/ITSEC Conference.

MLS for simulation is a very challenging problem, not yet solved globally, yet critical to accurate representation of war fighting to distributed audiences at different security levels. The current MLS Guard research objective is to further investigate supporting MLS, multiple security levels (MSL), and/or compartmented security for events on the Distributed Mission Operations Network by exploring a guard product suitable for the modeling and simulation environment.

This paper reflects the best O&I contractor knowledge of guard applicability to the Distributed Mission Operations Network to date. The assessment has identified nothing at this point in time that would preclude the use of the DTNG in the Combat Air Force Distributed Mission Operations environment. At the same time there are considerations that indicate a current immaturity of the guard with respect to its overall viability for the DMON. This guard assessment relies largely on information obtained from DMOC and Independent Verification &Validation (IV&V) team participants

DMON

The Distributed Mission Operations Network (DMON) provides the communications infrastructure for the conduct of events between Combat Air Force Distributed Mission Operations Federate Systems at

[2] The DTNG system consists of both a trusted guard and a separately hosted security rule set support tool developed by Trusted Computer Solutions (TCS) for the Air Force Research Laboratory Human Effectiveness Agency (AFRL HEA) in Mesa, Arizona.
[3] O&I Contractor MLS Guard research is sponsored by USAF ASC/ACSSW/SMSG/DM.
[4] Differing compartmentation, or compartments would mean that at least two kinds of information require different formal access approvals.

distributed locations. Additionally, the Distributed Mission Operations Network provides a distributed test network for Combat Air Force Distributed Mission Operations Federate System software development, integration, and test. At present, the USAF conducts Combat Air Force Distributed Mission Operations training and test events at either dedicated or system high security operations for various combinations of participant sites. The Distributed Mission Operations Network supports simultaneous training and/or test events at different security compartments; however, each event is conducted independently at a single level and compartment.

Future requirements for the Distributed Mission Operations Network involve additional sites representing different security domains. To enable events that cross security domains, the Distributed Mission Operations Network will incorporate a trusted guard solution. The current Distributed Mission Operations Network MLS Guard R&D activities are designed to lay the groundwork for compartmented and MLS Distributed Mission Operations Network events.

Today the Distributed Mission Operations Network provides Combat Air Force Distributed Mission Operations Federate Systems with secure data services in support of distributed team training. The system concept mirrors Internet Service Providers (ISP) and the services they provide. Each Combat Air Force Distributed Mission Operations Federate System is a subscriber to Distributed Mission Operations Network. As part of the overall system, each subscriber has a unique address space assigned. The O&I contractor, is responsible for the maintenance and the operation of the Distributed Mission Operations Network including provision of a Combat Air Force Distributed Mission Operations Portal Kit consisting of portal devices, NSA Type 1 encryptor devices, routers, and switches at each participating site.

The Distributed Mission Operations Network and its associated portals operate in an environment of mutual trust designed to meet the Director of Central Intelligence Directive (DCID) 6/3, Protection Level 2 (PL-2) requirements for Dedicated and System High Security operations. The Distributed Mission Operations Network requires a trusted controlled interface (guard) to conduct events between different security domains. The Distributed Mission Operations Center (DMOC) Security Working Group is steering the effort to provide a cross domain solution that can be certified and accredited by the Air Force and in the future, by the Intelligence Community (IC). The Security Working Group is performing the necessary management, technical, and policy tasks for DTNG MLS planning, documentation, integration with the Combat Air Force Distributed Mission Operations Portal, security rule set development, Distributed Mission Operations Network MSL system implementation, Certification and Accreditation, and overall assessment.

ASSUMPTIONS

Some assumptions for the current MLS guard assessment research are listed below.

1. The analysis discussions in this paper refer only to the initial testing of the guard to date and are too premature to reflect a complete assessment of a full-up implementation.

2. The term “security level” in the context of this paper may not necessarily mean hierarchical level. The term “compartment” is used to distinguish different airframe communities with additional separation needs at a single level.

3. Currently, a Combat Air Force Distributed Mission Operations Mission Training Center (MTC) participates in an event with a single compartment at a time. In this context, training events include briefing, execution, and debriefing. MTCs may be grouped into single compartment enclaves.

4. A Director of Central Intelligence Directive (DCID) 6/3 Protection Level 3 (PL-3) or higher controlled interface is required to connect Combat Air Force Distributed Mission Operations enclaves of different compartments. A trusted guard solution will be required to screen, filter, and guise data. For multiple security levels (MSL), a PL-4 controlled interface will be required.

5. If there are cases where the security compartment differences do not justify a PL-4 guard separation, then a lower assurance separation approach (PL-3/PL-2 controlled interface) may be a possible solution.

6. Combat Air Force Distributed Mission Operations Network performance (near real time) is a key consideration for sharing simulations using a trusted guard/controlled interface.

7. DMON participant systems with compartmented operation requirements will be accredited according

to USAF regulations, as directed by the USAF designated approval authorities.

8. The DMON Wide Area Network data is always encrypted during transmission over public service providers using Type 1 Encryption.

9. The lowest security level for a DMON site participant is SECRET/NOFORN.

10. Each DMON guard location must have its own pair of portal kits including encryptors, one for the high side and one for the low side.

11. The Combat Air Force Distributed Mission Operations vision includes other services and coalition partners. This is assumed to be a long-term integration effort and may require additional guards for security separation.

DTNG IN THE DMON ENVIRONMENT

The MLS test bed at the DMOC was the initial location chosen by the USAF to prototype the DTNG for future use in Distributed Mission Operations Network (DMON) compartmented and MSL events. The test bed provided a classified environment for testing the guard using the first DMON-developed rules within a system high environment. The guard implementation effort at the test bed was defined within a Spiral 1 process with 5 phases. Spiral 1 phases 1, 2, 3, and 4 offered a simulated low side and a high side, both contained in the test bed at a single system high level.

Significant challenges evolved during the test bed activities including system programmatic issues, guard installation considerations, and interoperability with gateways and other systems at each phase. A subset of the Security Working Group with additional subject matter experts (SME)s developed a rule set for conduct of an event between an identified high participant site (or enclave of high sites) and an identified low site or enclave. Test events were conducted at system high (PL-2) with an identified participant site on the Distributed Mission Operations Network.

Early efforts with guard set up and initialization at the DMOC test bed required a basic understanding of the environment-specific security policy and its implementation. The initial install of Trusted Solaris and its associated configuration modeled the more generic MLS DoD labeling schemes, rather than the compartmented needs for the DMO test environment. To better model the DMO environment, there was a need to configure the trusted operating system with appropriate label encoding and policy structure. The foundational security policy had to be in place and well understood to correctly install the guard for DMO implementation.

The DTNG is a high level architecture (HLA) device in the DMOC test bed environment and requires translation devices to interoperate with the distributed interactive simulation (DIS) systems. Use of HLA gateways for translation created additional complexity within the test bed environment. The translation gateways performed unpredictably during DMOC MLS test bed guard engineering tests conducted in late 2004 and experienced performance limits in tests this year. Gateway problems are still being resolved.

Two different engineering tests were conducted using the HLA portal device, and then using the DIS portal with two HLA gateways. Currently, the MLS test bed must use DIS portals and two gateways for HLA guard implementation. Using both of the gateways for guard translations adds the potential for instability, additional latencies, and performance problems. For future participant sites with HLA simulators and HLA portals, use of the gateways would not be necessary for HLA guard implementation.

RULE SET DEVELOPMENT

The use of a guard in the Combat Air Force Distributed Mission Operations environment requires identification of the protection needs between the high and low participant site domains and the development of the associated information flow rule set(s) for the guard. The process followed to develop the rules during this effort was necessarily flexible and shaped by events because of the novelty of the task. The Rules Working Group (RWG) analyzed security requirements, consulted domain experts, developed strawman rules sets, and iterated these steps as the technical and operational realities became clearer and as the capabilities of the guard and the implementation of the rules development tool were better understood.

At the beginning of the effort, the Rules Working Group consisted primarily of security professionals knowledgeable in the system classification guides and the requirements for protecting the sensitive data. Their approach focused on minimizing the exposure risk of the protected information. Lessons learned from this initial effort point to several other constituencies that must also be represented.

The first set of rules proposed by the working group contained some examples that were easy to explain verbally, but almost impossible to implement in a distributed simulation. In addition, the implementation may have created an inconsistent and unrealistic battle space that would have affected training, and could even have caused internal database consistency issues for participating simulations. The key lesson is the need for distributed simulation domain experts participation in the rules development process. They possess the engineering knowledge required to identify the rules approaches that could lead to inconsistent representations or that could prove extremely challenging to implement.

After several iterations through the security requirements, it became clear that some security protections nearly impossible to solve technically were easily handled through operational rules. These operational rules might govern the configuration of the system, or the behavior of the participants, or the content of the scenarios. Like their technical counterparts, operational rules can induce training limitations that have to be documented and accepted. This led to the conclusion that Subject Matter Experts on the systems being simulated are also required. They possess the expertise necessary to determine reasonable approaches and are able to contribute insight on real world system employment as it would apply to the distributed simulation.

Also, in implementing the rules properly, the Rules Working Group must understand the detailed protocol elements used by the simulation components. The Rules Working Group cannot freely assume that the simulated and real world systems operate identically. Nor is it true that the operations used in the field are necessarily emulated in the simulation environment. Therefore, it is essential that the Rules Working Group has access to engineers who are intimately familiar with the simulation implementations and can definitively address questions about the protocol, system configurations, and operational limitations that are unique to the simulated environment.

The ease or difficulty of implementing a rule in the guard is a function of its construction and limitations. On one key occasion during the rules implementation on this task, the Rules Working Group discovered that the technical capabilities of the guard itself had to be augmented to prevent exposure of critical information. The capability in question was a complex function of the nature of the data, the behavior of the HLA simulation protocol, and the specific rules being proposed. Early participation by the guard vendor might have exposed this issue sooner and permitted more time to implement the solution in code, as was eventually done. An additional constituent of any rules working group should be a senior engineer from the guard vendor who has an in-depth understanding of the simulation protocol and the details of the internal guard architecture and processing.

RULES DEVELOPMENT PROCESS

A properly-constituted rules working group should begin by analyzing the security requirements and classification guides. With a solid understanding of the nature of the information to be protected, they should use the subject matter experts to gain a working knowledge of the operational uses of the system and identify the battlespace content (entities and interactions) that require protection and produce a set of recommendations for providing that protection through operational and technical means.

A series of discussions of the implications of the protection approaches and their likely impact on simulation consistency and training value should be conducted. By iterating over the implications with all constituents, the group is better able to anticipate implementation issues and identify more promising alternatives. This activity concludes with a set of abstract rules, described in the language of the simulation protocol, but still not suitable for direct implementation on the guard.

The abstract rules become the basis for developing a test plan suitable for accreditation of the guard screening component of the system. The technical and operational rules are labeled for organizational convenience and collected into related groups. Each rule becomes the source for generating detailed test cases that can be used to verify that the rule provides the protection claimed. The test plan should show the trace between specific classification guide items, the corresponding rules, and specific test cases that will be used to demonstrate proper function of the guard. The test plan is best maintained in a document that also contains the necessary simulation implementation background, as well as the reasoning that led from the operational and technical discussions to the abstract rules set. These form essential context for an accreditor, who is unlikely to have an in-depth understanding of distributed simulation implementations.

SYSTEM EXPANSION

As the number of sites on the Distributed Mission Operations Network grows and additional security protections become necessary, the challenge of building a consistent, useful battlespace for all participants grows. There are relatively few technical techniques at the abstract level that can be used effectively, and they were discussed in the previous MLS Guard feasibility study. All of these techniques: blocking, guising, and substitution, are being employed in one way or another in the current prototype.

It is impossible to predict in detail the protections required by new platforms on the current federate system projection, in large part because the analysis of candidate rules requires appropriate clearances for the rules working group participants. But some protection challenges could require fundamental changes to the operation of the current Distributed Mission Operations simulation protocols. This would be the case, for instance, if sensor adjudication of radar or infrared detection were deemed unacceptable because of the restrictions on cross-section revelation. Such systems may require long lead times to allow for adjustment of the protocol, testing of the new approaches, and deployment to multiple sites. Establishment of a standing rules working group with the proper expertise and clearances as far in advance of the addition of a new platform to the Distributed Mission Operations Network as possible will be needed. This is especially true for the platforms with the most stringent security requirements.

DTNG EXPERIENCE AND TEST RESULTS

Guard testing during Spiral 1 included integration, engineering, operators in the loop (OITL), war fighters in the loop (WITL), and Beta testing. In addition, the government tasked an independent contractor to conduct security testing of the guard. The security independent verification and validation (IV&V) activity was designed to assess how well the guard meets DCID 6/3 PL-3 and PL-4 requirements.

Initial testing at the MLS testbed focused on integration of the guard, gateways, Combat Air Force Distributed Mission Operations Portal Kit and simulation systems in the classified environment. These integration tests were conducted during early phases of Spiral 1. At the same time, systems security and communications security (COMSEC) activities were conducted to allow the MLS testbed to participate on the Distributed Mission Operations Network as a high side site. Lessons learned in the early phases included the need to recognize that significant time was required for equipment ordering and contractual resolution for technical support. Also, there was a need to prepare in advance for the complexity and time involved in setting up of the guard in a specific operational environment.

Engineering Tests

The guard engineering tests conducted at the MLS testbed provided initial visibility into the implementation of the guard device and the high side to low side rule set. The DTNG automated rule set support tool was used for rules creation.

The DTNG tests demonstrated the proof of concept of a cross domain solution for the Distributed Mission Operations Network, initially with a pass all rule set, then using the rule set developed for compartmented operations. The guard successfully employed the rule sets, but the guard proof of concept does not yet extend well outside of the HLA environment.

Lessons learned include the need to plan and schedule extensive system integration testing of the guard well in advance to address known and unknown interoperability problems. For all Spiral 1 phases, the tests need to be repeatable to ensure a stable foundation.

Beta Tests

The guard developer conducted an unclassified Beta 1 test for Air Force and Defense Intelligence Agency (DIA) certification officials at their development site in 2004. This test provided initial security assurance to the certifiers that the guard was properly configured and installed on the Trusted Solaris (TSOL) operating system in accordance with DCID 6/3 PL-3 and PL-4 requirements. From a stand-alone perspective, the Beta 1 test provided the groundwork for additional Beta testing of the guard in the classified DMOC MLS testbed environment. Beta 2 testing followed the engineering tests using the Rules Working Group-developed rule set in the guard. At the conclusion of Beta 2 tests, certification and accreditation officials gave interim approval to operate (IATO) the guard at the MLS testbed. The approval was granted with the understanding that any documented concerns would be addressed. There still remains a requirement to obtain formal accreditor approval for the guard rule set prior to allowing actual compartmented (PL-3) operations. This rule set approval is being addressed by the Air Force.

WITL Test

At the time of this paper, successful operators-in-the-loop (OITL) and warfighters-in the loop (WITL) tests are required as part of phase 4 of the MLS Testbed Spiral 1. The system high tests involve the high side MLS testbed where the guard resides, and two Distributed Mission Operations Network participant sites, one as the high side site and one acting as a low side site (simulated low). Results from a successful WITL test should provide insight into the initial viability of the guard for DMO training events. Achieving favorable war fighter input will be an important step toward moving to the final Spiral 1 phase 5. Assuming a successful WITL test is achieved with the guard, consideration can then be given toward trial implementation of a guard to advance the proof of concept for compartmented Distributed Mission Operations Network day-to-day team training.

IV&V

While the DCID 6/3 requires independent verification and validation (IV&V) only for PL-4 and higher assurance devices, the Combat Air Force Distributed Mission Operations vision for the future extends beyond the PL-3 needs of today. The Air Force certification officials expressed that performing IV&V testing on the guard now will provide current insight into the guard. The IV&V effort will also lay the groundwork for a future PL-4 IV&V activity and approval to operate (ATO) when the need arises for additional Combat Air Force Distributed Mission Operations platforms. The Air Force contracted an IV&V team to assess the ability of the DTNG to meet PL-3 and PL-4 security requirements. The IV&V effort was conducted at an unclassified site in the Washington DC area

PHYSICAL ARCHITECTURES

There are three possible Combat Air Force Distributed Mission Operations guard architectures each having advantages and disadvantages. These architectures are presented as the Basic Use Case, Multiple High and Single Low Mission Training Center (MTC) Use Case, and High MTCs with Low Virtual Flag MTC Use Case.

The independent use cases illustrate the operation of the Combat Air Force Distributed Mission Operations Portal, the various simulation protocols in use, and the logical and physical connectivity among the network components. In the physical architecture diagrams, a shape and color code is used to illustrate the protocol type and level of classification of the data, respectively. The HLA protocol is shown using open-head arrows. The DIS protocol is shown using filled-head arrows. Portalese traffic is shown using dotted line where Portalese is the private protocol used in portal communications. In all cases, the classification of the underlying simulation content is illustrated using a line color. The boundary between a MTC participant site and the Distributed Mission Operations Network (DMON) includes passing the traffic through a Type 1 encryptor to allow it to be sent over commercial wide-area network lines. Because this step is common to all MTCs and does not affect the protocol translations or DTNG function, it is not represented in the diagrams. The key is depicted below in Figure 1.

Figure 1. Simulation Protocol Diagram Key

Basic Use Case

The basic use case involves two MTCs operating at two different levels and is shown in Figure 2. This case is representative of current DMO operations. It shows a BLUE (high site) MTC, using the DIS protocol, interacting with a RED (low site) MTC that also uses DIS.

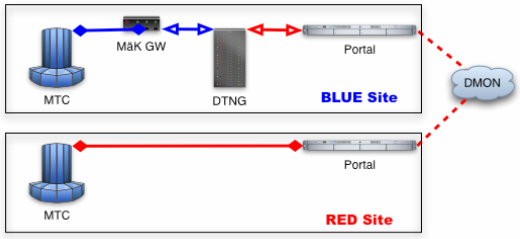

Figure 2. Two-Level Operational Exercise

The fact that the DTNG only operates with HLA simulation traffic requires that some device translate the local DIS data to HLA before sending it through the guard for sanitization. For illustrative purposes, Figure 2 shows a MäK gateway performing this function. This configuration also requires the Portal at the BLUE MTC to operate as an HLA Portal rather than a DIS Portal as would normally be the case for a distributed exercise involving that MTC. Finally, as can be seen from the diagram, the Portal itself and the

Distributed Mission Operations Network operate at the RED classification level during this exercise. Current procedures are not designed to accommodate the situation of a BLUE MTC with a BLUE load operating over a RED network connection, so additional procedures will have to be devised and agreed upon to permit the network to be brought up as shown below in Figure 3.

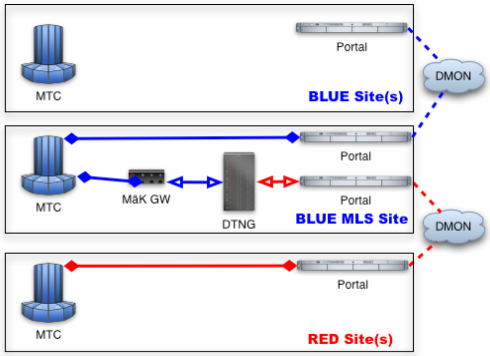

Figure 3. Multiple High, Single Low Configuration

Careful coordination and connection sequencing is essential to ensure that no contamination can occur. Debugging simulation issues may be hampered by the presence of the DTNG, which prevents visibility into the MTC from the Portal kit test computer. In addition, the physical location, ownership, and configuration responsibility of the gateway and DTNG must be addressed for this architecture.

Multiple high and single low MTC Use Case

The case of multiple BLUE MTCs operating with a single RED MTC is shown in Figure 3. Here, the Distributed Mission Operations Network operates as it would for simultaneous BLUE and RED events, with separate cryptographic networks for each color.

This configuration illustrates that the site containing the DTNG has to have two independent connections to the Distributed Mission Operations Network with separate Portal kits for a successful two-color event. One Portal uses the native local simulation protocol (DIS in this case), while the second is an HLA Portal so that it can communicate with the DTNG. As for the two MTC case, a MäK gateway is assumed to provide the translation from DIS to HLA before passing the simulation traffic to the Guard.

This configuration requires new procedures to be developed to accommodate the simultaneous two-color operation at the single MTC where the DTNG is located. The site must be equipped with both BLUE and RED crypto keys. Careful configuration and sequencing are again required to ensure no contamination takes places on the RED network. As before, there are issues that must be addressed in physical location, ownership, and configuration responsibility for the gateway and DTNG.

This configuration allows access to all the MTCs for the purpose of debugging simulation traffic, but different MTCs must be accessed through different colored Distributed Mission Operations Network sub-networks. This represents a deviation from current network operations and requires additional procedures and safeguards.

High MTCs with Low Virtual Flag MTC Use Case

Another case arises when BLUE MTC assets are used in support of a Virtual Flag exercise. In the configuration shown in Figure 4, the current MLS Testbed houses the DTNG and connects to the Distributed Mission Operations Network as a BLUE MTC would, using an HLA Portal. Sanitized RED simulation traffic is then sent through a MäK gateway to the DMOC main floor, which is also connected to the Distributed Mission Operations Network as a RED MTC.

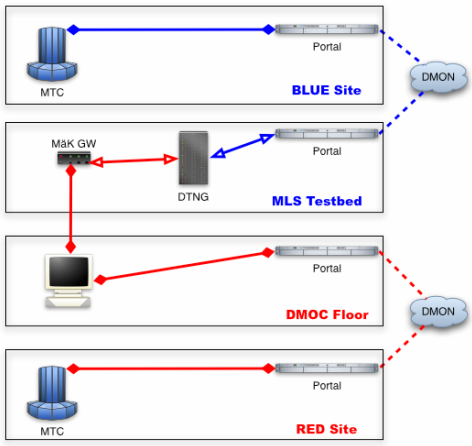

Figure 4. Virtual Flag Configuration

This case greatly simplifies the procedural consequences of a two-color exercise in that the Distributed Mission Operations Network is configured as it would be for two simultaneous and independent RED and BLUE events. In addition, all of the Portal kits operate as they do today with no change in simulation protocol or security classification required. No additional equipment is required at the operational MTCs to function in this configuration.

The disadvantage of this configuration is that only one two-color exercise can be conducted at a time.

Furthermore, the DMOC assets must be used; so setting up this configuration for a normal training mission would involve additional coordination and planning to ensure that the DMOC was properly configured and available.

The same questions arise in the area of physical ownership and management responsibility for this case. Additional procedural safeguards may need to be instituted to ensure that only appropriate sites are connected to the DMOC Floor during the two-color event. This is especially true because the O&I contractor does not have visibility or control of the Distributed Mission Operations Center (DMOC) network connectivity.

PLACEMENT, OWNERSHIP AND RESPONSIBILITIES

In all of the cases described above, questions arise regarding the physical placement, ownership, configuration management, and maintenance responsibilities for the DTNG and any auxiliary items (such as MäK gateways) required to support its function. Decisions in this area will affect the content of security policies and procedures, event control and configuration, availability calculations, and Combat Air Force Distributed Mission Operations Standards content. As above, there are several cases to consider.

The simplest case involves O&I ownership of all the required DTNG assets. The DTNG and gateway would be physically associated with the Portal kits (two are required for the site that houses the guard function) at the MTC. Because the path through the second Portal kit is used only when a two-color exercise is in progress, it would be necessary for the O&I Networking team to be able to control the traffic flow to and from the MTC LAN, probably through a switch located at the boundary between the MTC LAN and the Portal kits.

Because both the gateway and the DTNG rule set are sensitive to the content of the local battlespace at the MTC, local configuration changes that are transparent to the Portal might still require engineering changes to the Guard components to maintain training effectiveness. If the DTNG and gateway are owned and operated by the O&I, it is essential that configuration management of the software, Federated Object Models (FOMs), RTI Integrated Description (RID) and Federated (FED) files, and the rule set can be performed remotely. It also is essential that health and status diagnostics will be available over the Distributed Mission Operations Network. This may require software changes to the current DTNG implementation.

A second case is if the gateway and DTNG could be owned and operated by the local site, either through the local support contractor or through the USAF personnel at that location. Making the MTC responsible for the guard function would shift the responsibility for configuration management, maintenance, and health and status monitoring to local personnel, and remove the need for remote configuration control. It could, however, lead to a multiplicity of disparate guard configurations. This would complicate the event control process because of the increased coordination required between the guard-using MTC and the DMON Networking team.

Finally, the guard function could be placed and maintained at a single site common to any two-color exercise. This would allow centralized management of the guard components, and reduce the burden of additional coordination procedures being imposed upon the MTCs. This approach does raise some performance issues, however, which are addressed in the sections below.

There are numerous ownership issues that remain to be settled. It is assumed that the DTNG will require product licenses for its core software and be subject to maintenance and software upgrades just as any commercial product. The rule sets used by the DTNG are intellectual property, both in the form of human-readable descriptions, and in the form of encoded rules that are extracted from the automated rule set support tool. Audit and other logs that are generated on the DTNG or the gateway are also owned items, and are important because of their potential impact on debugging and availability calculations.

The complexity of the current DTNG configuration is substantial. The majority of Combat Air Force Distributed Mission Operation sites use the DIS simulation protocol, so conversion to HLA suitable for use by the DTNG greatly complicates debugging and configuration control for the Distributed Mission Operations Network system. As a consequence, there is considerable work that remains to be done to introduce the guard function tested at the DMOC into the Distributed Mission Operations Network as an operationally-useful capability. The considerations and alternative deployment approaches are discussed in the section below.

ARCHITECTURE CONSIDERATIONS

The discussion of possible use cases of the current DTNG for Distributed Mission Operations events illustrates that there are practical considerations for DTNG placement that have a profound effect on the total system cost and flexibility. For example, the greatest flexibility for setting up two-color exercises is to have a DTNG and gateway, as well as a second Portal kit, available at each BLUE MTC. But this adds considerable cost and complexity to the operation of an MTC, and has security implications even when the site is being used for single color exercises.

An alternative is to place the required guard and support equipment in some subset of the BLUE MTCs. This reduces the total cost, but still requires multiple Portal kits at those MTCs. This alternative still imposes the burden of additional security and event control procedures. A single DTNG and gateway can be deployed at the DMOC to service all sites, but that requires DMOC availability for any two-color exercise, introduces a non-O&I element into the event control process, and requires that the latency and bandwidth necessary to support the entire high-to-low simulation traffic twice (once on the BLUE side, once on the RED side) be available at the DMOC.

As additional simulation capabilities become available, and as the DTNG matures and acquires additional rules sets, Distributed Mission Operations Network events will eventually be faced with three-color configurations such as the one illustrated in Figure 5.

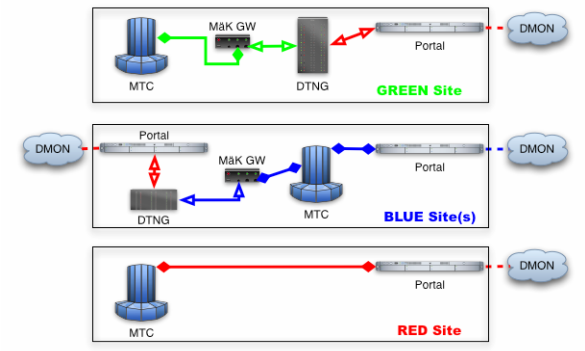

Figure 5. Three-Color Exercise

This configuration represents a new platform MTC, operating internally at GREEN classification and participating in a RED lower-level distributed network, while simultaneously a set of BLUE sites share data and participate in the RED network through the DTNG.

As can be seen from the diagram, the Distributed Mission Operations Network is partitioned as before into two cryptographically separated subnets, at BLUE and RED levels. A DTNG configured with a rule set suitable to downgrade from GREEN to RED is located at the new platform MTC. Combined with a MäK gateway to translate from the native DIS to the Guard's HLA protocol, and an HLA Portal, the MTC is able to participate with the RED MTC network. The assumption is that this is the only GREEN MTC in the event, so there is no GREEN DMON subnetwork.

As discussed in the previous section, the BLUE MTC requires a gateway and DTNG, as well as two DMON connections and two Portal kits, to participate in the three-color event. The assumption is that there are multiple BLUE sites participating, requiring a BLUE DMON subnetwork.

This configuration implies additional procedure definitions to deal with the complexity of the three security levels (or compartments), to help ensure no contamination is possible among the different color enclaves.

PERFORMANCE CONSIDERATIONS

Each of the network architectures described so far has a common characteristic: all the BLUE simulation traffic has to pass through a single gateway and a single DTNG. At present it has not been feasible to rigorously test the performance limitations of the guard or gateway, and there is no certainty that they are able to support typical multi-MTC DMO missions.

Should the performance of the DTNG or gateway be an issue, it may be possible in the future to build a network architecture as shown in Figure 6 using multiple DTNGs (and/or other guards) in parallel to accommodate the required simulation bandwidth.

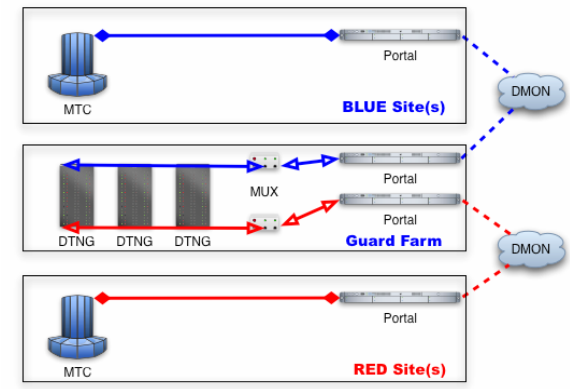

Figure 6. Guard Farm Architecture

The MUX illustrated in Figure 6 would be a new device that partitions and combines simulation traffic in some reasonable fashion so that the set of guards operates only on a subset rather than the full stream. The MUX would not be performing any security-related function, but would merely be making a logical, engineering-driven battlespace separation and recombination.

This multiple-guard (Guard Farm) configuration offers several advantages. Each of the MTCs continues to operate at a single level using their current Portal configuration and classification. The only site requiring multiple DMON connections and Portal kits is the specialty Guard Farm site, which can be located as desired to take advantage of low latency and high WAN accessibility. The Guard Farm site can be designed with as many Portal kits and guards as required to support multiple simultaneous two-color events, and would be the only site required to operate at multiple colors. The new procedures required to safely conduct such exercises would affect only the Guard Farm, and so no coordination or additional responsibilities would be required of the current MTCs.

NEXT STEPS

MLS and compartmented security research remains an ongoing effort required to achieve the Combat Air Force Distributed Mission Operations Roadmap for future platforms. Near term steps are essential. Some of the MLS Guard results anticipated for incorporation into the current research effort were delayed due to the complex work and amount of time required to integrate and test MLS testbed components and to obtain IATO for the PL-3 DTNG and its associated rule set.

Recommended next steps include completion of the MLS Spiral 1 activities with a successful Distributed Mission Operations Network compartmented event. Assuming success, an experimental deployment of a DTNG for Combat Air Force Distributed Mission Operations training events could follow. A DTNG installation would lay the groundwork for establishing a fielded guard and its associated integration, operations, maintenance, and security procedures. This installation would allow for additional performance testing enabling compartmented Distributed Mission Operations Network team training events between a high MTC and a low MTC.

Another next step would be to create a MLS or compartmented security implementation plan for Combat Air Force Distributed Mission Operations. Results of early discussions with platform communities needing guard technology to connect to the Distributed Mission Operations Network (DMON) will be necessary for plan development. The ability to develop a plan with real specificity depends on getting access to all the necessary data.

Additional next steps would be to support expanding/improving the Distributed Mission Operations Network guard(s) rule set development and maintenance process to facilitate rapid security approvals and provide technical support for certification and accreditation. This involves work with new platform communities and new MLS/Security Working Groups to support the development of new rule sets and security issues including certification and accreditation of the guard and rule set.

ACKNOWLEDGEMENTS

The authors wish to thank the following USAF SMSG/TO technical advisors for their guidance and support: LtCol Janet Kasmer, CAF DMO O&I PM; Mr. Robert Lillie; Mr. Don Poe, Mr. Mike Mills, Mr. Pat Imlay, and Mr. Jim Evans. The authors also wish to express gratitude to the O&I contractor contributors to CAF DMO MLS Guard research including Mr. Bruce McGregor, O&I Contractor PM, Ms. Joan Archer, Northrop Grumman security engineer, Ms. Danie Patton, Northrop Grumman systems engineer, and Ms. Kimberlee Hoover, CISSP, SPARTA security engineer.

REFERENCES

AFI 33-202 (2001), *Computer Security*.

AFMAN 33-229 (1997), *Controlled Access Protection.*

CAF DMO O&I Contractor, (2004). *Draft DMON MLS Guard O&I Contractor Workshop Report.*

Director of Central Intelligence (DCI) (1999). *DCI Directive (DCID) 6/3 for Protecting Sensitive, Compartmented Information within Information Systems Manual.*

DMT O&I Contractor (2005). *Draft Multi-Level Security Guard Final Report.*

DMT O&I Contractor (2002). Multi-Level Security Feasibility in the M&S Environment, *I/ITSEC 2002, Paper 167.*

DMT O&I Contractor (2001). *Multi-Level Security Feasibility Assessment Research and Development (R&D) Final Report, Version 1.0 and Appendix C, Assessment Contact Reports.*

DMT O&I Contractor (2001). *DMO Integration Standards* and *DMO Common Definitions* from https://web2.trwdmt.com/dmt/sdwg/index.cfm

DoD (2000). Memo for Department of Defense Chief Information Officer Guidance and Policy Memorandum No. 6-8510, *Department of Defense Global Information Grid Assurance*.

DoDI 5200.40 (1997). *Department of Defense Information Technology Security Certification and Accreditation Process DITSCAP*.

NSA (2003). *Guard Certification Test and Evaluation (CT&E) Handbook Version 2 .0.*

NSTISSAM (1999). *Common Criteria for Information Technology Security Evaluation.*

NSTISSAM COMPUSEC (1999). *Advisory Memorandum on the Transition from the Trusted Computer System Evaluation Criteria to the International Common Criteria for Information Technology Security Evaluation.*

NSTISSP 11 (2000*). National Information Assurance Acquisition Policy*

[i] **22 CFR 125.4(b)(13) applicable, Log #5003**