

# MULTILEVEL SECURITY FEASIBILITY IN THE M&S TRAINING ENVIRONMENT

|                      |                        |                    |                         |                                 |                         |
|----------------------|------------------------|--------------------|-------------------------|---------------------------------|-------------------------|
| <b>Bonnie Danner</b> | <b>Carl Muckenhirn</b> | <b>Tony Valle</b>  | <b>Charles McElveen</b> | <b>Joanne Bragdon-Handfield</b> | <b>Andrea Colegrove</b> |
| <b>TRW</b>           | <b>SPARTA</b>          | <b>SPARTA</b>      | <b>SPARTA</b>           | <b>TRW</b>                      | <b>SPARTA</b>           |
| <b>Orlando, FL</b>   | <b>Columbia, MD</b>    | <b>Orlando, FL</b> | <b>Huntsville, AL</b>   | <b>Reston, VA</b>               | <b>Columbia, MD</b>     |

**Abstract.** This paper describes the results of a Distributed Mission Training (DMT) Operations and Integration (O&I) Research and Development (R&D) Task, DMT Multilevel Security (MLS) Feasibility Assessment, performed for the USAF. The focus of the study is the feasibility of employing MLS capabilities within a virtual training environment. MLS continues to be a significant challenge for military communications networks with unique issues arising in the modeling and simulation (M&S) context. The fundamental MLS issue in a simulation environment is how to construct a consistent, useful battlespace at each participating classification, while not revealing, through inference or direct disclosure, information for which participants are not cleared. The common battlespace consists of all observations and interactions possible among all participating Simulation Objects (e.g., Federates). Approaches that obscure aspects of the system that have observable effects impact the fidelity of the simulation event and may impact the training value of the event. Defining the common battlespace and obtaining agreement among the participating communities can then be difficult to accomplish. The achievement of M&S MLS solutions will require a clearly identified strategy defining security risk and identifying the policy and technology changes needed to move from isolated, system high, to distributed, MLS, training. Current MLS solutions only partially address the information sharing needs between simulated airframe, joint, and coalition communities. Based on technology and policy assessments, this paper provides a description of the core issues via scenarios for MLS in M&S and describes technical approaches using existing technology to solve these issues. This paper addresses policy considerations with an eye toward the potential changes needed for a fully functional MLS training system to be constructed.

**Bonnie Page Danner**, CISSP, has more than 20 years of information technology experience in systems engineering, software development, and information assurance. She has technical and project management experience on Department of Defense and civil federal programs including research leadership of DARPA, Navy, FAA, NASA, Air Force R&D, and TRW IRAD projects. Ms. Danner's technical specialty is high assurance systems. Her technical experience includes MLS, formal methods, certification & accreditation, COMSEC, software safety, and IV&V. Her modeling and simulation program experience includes JSIMS Security Lead and currently, TRW Security Engineering Lead for the Distributed Mission Training (DMT) Program. Ms. Danner was manager for the DMT MLS Feasibility Study R&D Task Order and manages the DMT Briefing/Debriefing Functional Requirements Study R&D Task Order. Ms. Danner has published a variety of articles in journals and conference proceedings on information assurance, software engineering, and field theory. She received a BS degree from Virginia Tech University and a MS degree in Mathematical Sciences from Virginia Commonwealth University. She was awarded the professional designation of Certified Information Systems Security Professional (CISSP).

**Carl Muckenhirn** has 20 years of experience in Information Security disciplines. He currently leads SPARTA's Security Engineering Division. He serves as the Accreditor's representative for the Joint Simulation System where he provides evaluation of the technical security products slated for deployment. He has performed technical research in communications and computer security application to networked systems and is a co-author of several papers and Internet standards related to key management of multicast/group communications structures. Mr. Muckenhirn was a key contributor to the Air Force sponsored work reported here. He received a BS EE degree from the University of Notre Dame.

**Dr. TonyValle** is both a military and commercial simulation designer. He is currently the lead for the Distributed Mission Training (DMT) Threat Representation and Computer Generated Forces Standard, as well as 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. His work on commercial air combat modeling includes contributions to a variety of flight and air combat simulations.

**Charles McElveen** has over twenty years of professional computer systems design, development, and implementation experience. Of those twenty years of experience, fifteen have been dedicated to the protection of the nations information systems via various information security disciplines including COMSEC, COMPUSEC, Personnel Security, Physical Security, and Organizational Security. The focus of Mr. McElveen's experience has been in the field of COMPUSEC/information security. Mr. McElveen was one of the original designers and developers for the AT&T Unix Multi-Level (MLS) operating system. Since that time, Mr. McElveen has worked on a number of MLS projects including -Service/Agency Automated Message Processing Exchange (I-S/A AMPE), Joint Simulation System (JSIMS), and Distributed Mission Training (DMT) System. Mr. McElveen has a graduate degree in management information systems from Florida TEC and an undergraduate degree in computer science from the University of Southern Mississippi.

**Joanne Bragdon-Handfield** has more than nineteen years of information security experience including security policy guidance and participation on security engineering review boards in support of the Intelligence Community. She was a technical lead for the JANUS program, a B1 intelligence system. She provided highly technical, specialized guidance in the management, design, development, implementation, and integration of a MLS intelligence system. She was a security engineer for the analysis and implementation of requirements as they applied to a security database guard. Ms. Bragdon-Handfield was a security verification analyst in the early development and design of the Restricted Access Processor (RAP), a formally verified, MLS guard processor developed for NASA to intercept, screen, and route satellite messages.

**Andrea Colegrove** has been working in the field of Information Assurance for fourteen years. Her experiences have included systems security evaluation, secure protocol design and analysis, research in the field of group security, and key management architectures. Ms. Colegrove was a key contributor to the technology assessment portion of the MLS study presented in this article and to the DMT MLS Feasibility Assessment Final Report. She earned a BS in Mathematical Sciences from the University of Washington and an MS in Computer Science from Johns-Hopkins.

# MULTILEVEL SECURITY FEASIBILITY IN THE M&S TRAINING ENVIRONMENT

|                      |                        |                    |                         |                                 |                         |
|----------------------|------------------------|--------------------|-------------------------|---------------------------------|-------------------------|
| <b>Bonnie Danner</b> | <b>Carl Muckenhirn</b> | <b>Tony Valle</b>  | <b>Charles McElveen</b> | <b>Joanne Bragdon-Handfield</b> | <b>Andrea Colegrove</b> |
| <b>TRW</b>           | <b>SPARTA</b>          | <b>SPARTA</b>      | <b>SPARTA</b>           | <b>TRW</b>                      | <b>SPARTA</b>           |
| <b>Orlando, FL</b>   | <b>Columbia, MD</b>    | <b>Orlando, FL</b> | <b>Huntsville, AL</b>   | <b>Reston, VA</b>               | <b>Columbia, MD</b>     |

## INTRODUCTION

At the Distributed Mission Training (DMT) First Federation milestone anticipated in 2003, DMT simulation aircraft communities will include F-15C, F-16 Block 50, and E-3 (Airborne Warning and Control System). As DMT expands to the Objective System, many additional types of aircraft will be included such as RC-135 (Rivet Joint), E-8C (Joint Surveillance and Target Attack Radar System), Predator, A-10, Joint Strike Fighter, B-1, B-2, F-15E, F-117, F-22, and cargo and tanker aircraft. The DMT vision over the next 10 years will include the potential for integrating other services and coalition forces aircraft. Multi-level Security (MLS) capabilities will be needed to achieve the vision of allowing pilots to train as they fight (see Figure 1).

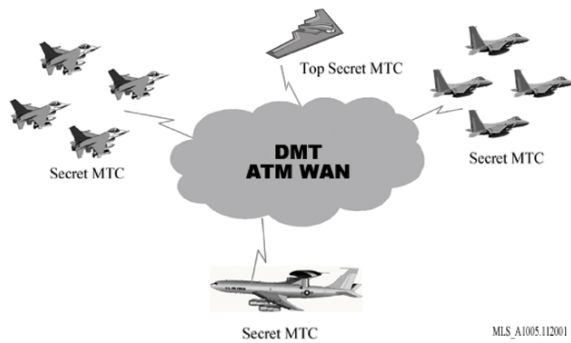


Figure 1 DMT MLS Federation

The Operations and Integration (O&I) DMT MLS Feasibility Research and Development (R&D) task focus was to define the problem and to address what would be needed to advance DMT effectiveness through MLS capabilities.

The principal goal of DMT MLS is to enhance training by allowing Mission Training Centers (MTCs)/Federates operating at different classification levels to interoperate.

The DMT MLS Feasibility study examined a number of options for providing multi-level capabilities ranging from development of new multi-level, DMT simulators to development of “multi-level confederations” that provide MLS features at the federation boundary. One abiding constraint considered throughout was the need

for DMT to continue to accommodate dedicated and/or system high security legacy systems.

## PROBLEM OVERVIEW

In defining the problem the DMT O&I team considered observable, operational issues along with traditional MLS issues. Operational challenges include observability and physical and operational performance. Traditional MLS technical challenges include data separation, security labeling, process separation, and mandatory access controls.

### Common Battlespace

In a simulation system, the data can be broadly categorized into two areas, parametric information that drives models and state information that describes the evolving dynamic battlespace. In general, parametric information is not passed during the simulation execution, although it may be transmitted over a network as part of the configuration of MTC assets prior to an event.

How to create a Common Battlespace without inadvertently disclosing classified information to participants who are not cleared for that information is a fundamental issue. The Common Battlespace consists of all observations and interactions possible among all participating Federates. The conceptual view is illustrated below (see Figure 2).

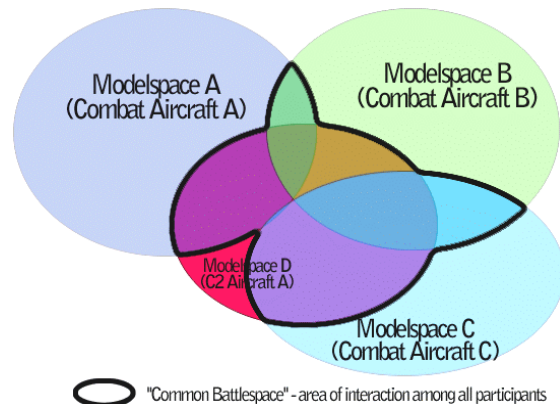


Figure 2 Common Battlespace

Determining the simulation information that can be shared and reaching sharing agreements among the airframe communities are difficult problems. Ways to

attack the problems all have issues associated with them.

### **Observability Problem**

Observers of a simulation exercise are able to draw conclusions from the performance of systems in the simulation, even without access to the underlying parametric data or dynamic state information. This is possible because the simulation is supposed to mimic real world behavior. The observer is able to draw on his real world knowledge for analogies and to extract conclusions from the simulation evolution. It is this ability to infer from real world knowledge that challenges the definition of MLS policy for a feasible DMT solution. Restrictions on access to the computer data may not protect the underlying classified information from compromise in the presence of knowledgeable observers. This presents a compelling argument for establishing a rule of thumb that the minimum level of classification of an exercise is the observable state of the simulation entities. Observable performance can be broadly categorized as physical information and operational information.

**Physical** Physical performance consists of all the directly observable behavior of manned and unmanned platforms and those quantities that can be derived from logs of the simulation traffic. Examples of instantaneous (or single observation) values include speeds, turn rates and radii, climb rates, accelerations, lethal radii, and ranges for acquisition or tracking. Values that can be derived after repeated observation include hit and kill probabilities, maximum speeds, turn rates, or climb rates; fuel consumption rates; cruise ranges; loadout limitations (weight, type, and count); and vulnerabilities. Some of these values are classified differently than others, so an important issue for designing an MLS solution in the DMT context is access control to logs and replay data both during and after exercise execution. It may be possible to conduct a single exercise at one level, while the aggregate information from repeated runs of that exercise is classified at a different level. This would imply that casual observers may need to hold a different clearance level than long-term participants and will affect MLS policy considerations.

**Operational** Operational performance issues consist of the doctrine and tactics as practiced by the exercise participants. Tactics must be predicated on weapon system capabilities. When the nature of those capabilities must be protected, observation of the tactics may result in compromise. Solutions to this problem cannot be derived by technical means. Policy must dictate the need to classify certain operations at a given level, and restrictions on allowed tactics may be required. Restrictions on tactics can have a profound

effect on the value of the training, so it must be considered with careful deliberation as part of the MLS policy-making process.

### **MLS Technical Problem**

The technical MLS challenge arises with the need to provide systems that can protect classified information, implement mechanisms that share different levels of the information, and simultaneously meet DMT training needs. On a small scale, traditional MLS problems are solvable near term; but when the scope of the effort expands, the task becomes more complex. For example, on a trusted operating platform, files can be easily labeled; however, if a custom application is developed to parse individual items within the file, the process becomes much more complicated. This new application must be trusted to parse the information correctly and ensure that each piece of information is correctly labeled. For this process to work correctly both the new application and the trusted platform must be integrated to perform the tasks. In the case of DMT, the traditional MLS problem is much more complicated than the previous example. The various simulators and the DMT network were developed independently without consideration for MLS or high assurance.

**HLA** High Level Architecture (HLA) compliance creates a problem for DMT similar to the custom application described above. The heart of HLA is the Run Time Infrastructure (RTI), which must run on each participating platform in the simulation. The RTI defines and controls who has access to what information. The process for obtaining access to information is called expressing an interest. Once an entity expresses interest in certain information, the RTI sends this information to that entity when available.

By definition, implementation of an MLS operating environment means that system high security features (identification and authentication, access control, audit) must also be enhanced. The majority of these enhancements will be achieved in the area of increased security assurance. For example, rather than using only a username and password for authentication, certificates may be required.

**Platforms** Currently, there are only a few commercially certified and accredited MLS platforms due to corporate economic decisions. Some agencies and Designated Approval Authorities (DAA)s recognize that some products not labeled as trusted can still provide a high level of assurance. Two of the most widely used products are the Solaris operating system and the Oracle database management system. The O&I team technology assessment included a detailed analysis of potential MLS platforms. Development of MLS systems and the required assurance for these systems are time consuming and costly. In general,

most programs do not attempt to develop these types of systems using their own resources. However, in-house development or modification of an MLS platform could be an option for DMT.

Even with their limitations/issues, MLS platforms can provide excellent functionality at a reasonable cost when they are integrated into an overall architecture that includes both trusted and non-trusted systems. Each component of a trusted architecture does not have to be trusted.

**Guard Technologies** In general, guard technologies fall into two broad categories, Two-Way-Guards and One-Way-Guards or Data Pumps. The primary purpose of a One-Way-Guard is to ensure that a system operating at a lower classification is not contaminated by a system operating at a higher classification level. The primary purpose of a Two-Way-Guard is to ensure that information at a higher classification level is not released to a system operating at a lower classification. Two-Way-Guards normally function as both a Two-Way and One-Way Guard ensuring that only authorized information is released and that a lower enclave is not contaminated by a higher enclave. The primary issues for Guards include network performance impacts, security certification, the need for well-defined information format, high assurance costs, and limited availability of guard candidates.

**Cryptography** The primary issue with cryptography is not security (assuming the encryptor employed is a NSA Type I approved device) but operational requirements. Operational issues include the network performance, key distribution limitations, network compatibilities, and multiple encryption key support.

### **MLS and Inference Policy Problem**

The most significant DMT MLS policy problem arises from the inference associated with the transmission or availability of state information from a higher level MTC to a lower level MTC. Even though the state information itself may not be classified, the results stemming from the implementation of state data can produce classified results via inference. For example, if a given weapon destroys a target that is outside of the published capabilities, then one would be able to infer that the weapons system had more than the published capabilities. In this case, unpublished capabilities are classified, and not all users are cleared or have a need to know for this information. Solving the inference problem is not purely a technical or policy issue, but will require a combination of the two.

### **Simulation Security Challenges**

When considering DMT MLS, the O&I Team recognized that techniques are needed to address scenario challenges involving information that cannot

be fully shared during a simulation. For example, a weapon system needing to employ highly classified enhancements presents a challenge for scenario development. The techniques that might enable simulation information sharing in such a constrained environment include external secondary modeling, filtration, suppression, and obscuration.

### **Techniques**

**External Secondary Modeling** External modeling consists of importing state information about battlespace entities into a higher enclave and using that data to perform additional computations. In a distributed simulation, this must be *secondary* because the primary models (observable quantities) must remain in the lower enclave due to guard restrictions. The most common system having these characteristics is a sensor that needs to collect battlespace state, but which has no direct observable effect by itself.

**Battlespace Suppression** One approach is simply to change the things being simulated so that the capability to be protected isn't being used, or is being used in a way that doesn't reveal the capability. We refer to this as "suppression" of the simulated capability. This approach does not require any additional technological or policy decisions because it changes the simulation to eliminate the classification issue. The downside to this approach is that it is likely to have a severe adverse effect on the quality of the training. If we are expecting to "train as we fight", we are certainly expecting to use the actual capabilities of the sensors and weapons system that we would fight with. This is also the hardest to implement in an existing system, because battlespace rules are determined early in the design and architecture phase. Fundamental battlespace changes will usually have a significant impact on the implementation and will require a large effort to code into the simulation.

**State Change Controls** Another approach is the use of guard technology to filter out state changes and restrict them to subsets of the network. This is feasible only if the battlespace can be partitioned in a way that filtering out the state changes will not lead to inconsistencies in the simulations behind the filter. Typically, this implies that the state information in question has to be associated with the modeling of capabilities that do not produce observable battlespace interactions. That is, the filtered state cannot be an observable quantity (like location, velocity, or existence), and it cannot lead to observable changes in others (such as damage or destruction).

**Obscuration** This approach consists of running two models in parallel, one that operates using the protected model, and the other running a model that doesn't reveal the system capability. In other words, a "cheat"

is set up whereby the capability is protected by masking the protected model as some other system or combination of systems that produce the intended effect. This is an exceedingly difficult approach and will likely be feasible only in very limited cases. Logically, if the real capability and the masked capability operated identically, there would be no need to protect the capability at all. So there must be instances in operation where the protected capability operates differently in some way. In these instances, masking the capability involves inventing self-consistent battlespace state that keeps both the protected and lower-level battlespaces synchronized. This is a difficult engineering problem and not well suited to most cases.

**Issues** To perform external secondary modeling, it should be possible to safely import dynamic state information in real time into an enclave of a higher level. In addition, the higher classified model cannot have any direct effect on the observable battlespace behaviors since this would raise the security level of the overall exercise.

Filtration may require partitioning of state data to achieve high assurance and comprehensibility. Simulation protocols are not developed with partitioning in mind, so the result may be that a new protocol will need to be developed, an expensive proposition with the legacy world of DMT.

Suppression may involve not modeling a particular system or disabling a system that has been modeled. Turning off a system model in a legacy simulation can have unintended consequences for the rest of the models. Technical solutions do not yet exist that would allow dynamic blocking of key phrases or code words from certain tactics or procedures that ensure no operational compromise. How to implement suppression solutions becomes more of a MLS policy and risk management problem.

There are few examples of obscurations being used in practice. If this technique is attempted, there could be significant implications to the consistency of the battlespace.

## Scenarios

The O&I Security Team identified five possible simulation scenarios for discussion. These scenarios are: Mode of Operation, Sensor, Multisource Fusion, Undetectable Emissions, and Performance.

**Mode of Operation** Consider a gun system that uses a new barrel design that greatly increases the effective range of the weapon. Suppose we wish to train pilots of aircraft that use the new gun system, while protecting its capability from other participants in the distributed

simulation. The question is: What can be done in each of the three categories outlined previously?

Suppression involves not using the gun at all, or only using it within conventional effective range. This leads to potential training limitations since the pilots are not able to execute proper long-range firing tactics that use the advanced capability.

State change controls will be problematic in this instance, because if the gun is fired outside conventional range and scores a target hit, filtering this interaction will result in an inconsistency between the protected and exterior battlespace.

Obscuration might take the form of representing the gun effects in the exterior battlespace as a short ranged missile. This latter approach will work, so long as the missile dynamics (speed, range, homing ability) are plausible and do not differ too much from the gun characteristics.

**Sensor** Consider a novel sensor system that uses a detection mechanism that must be protected. For example, assume that the sensor detects ultraviolet band emissions from the target. This fact must be protected from participants on platforms that do not use the sensor.

Suppression in this instance involves not using the information from the sensor. This may arise if the simulation as built does not advertise UV signatures, and asking implementers to provide such a signature would itself represent a compromise.

State change controls will work well in protecting the function of the sensor if the network can be partitioned into sensor users and non-users. This would permit sensor coordination, for example, to be done through distributed protocols while still protecting the sensor function.

Obscuration in this case is likely to take the form of external secondary modeling. In this instance, the sensor models are built so that they take publicly available state data (such as engine setting, thrust level, current speed) and use that to generate a "best guess" value for the UV signature that then feeds the sensor model. In this case, the enhanced detection ability of the protected platform can be attributed to better conventional sensors, or to superior tactics, doctrine, or training.

**Multisource Fusion** Consider a data link or similar function that allows a flight of aircraft to share detailed target information that arises from any sensor in the flight. Suppose that this capability must be protected from the other participants in a distributed training exercise.

Suppression involves turning off the data link. Given the value of situational awareness in modern air combat, this constitutes a severe training limitation.

State change control can ensure that the coordination messages among sensors within a flight are restricted to that flight. This is therefore a very effective technique in this instance.

Obscuration in this case is similar to that involving the long ranged gun, but more severe. Presumably, the ability to share the sensor information provides a significant increase in situational awareness and perhaps in the ability to engage targets with various weapons. This means that conventional sensor systems would not be able to achieve those capabilities. Mimicking them will therefore prove difficult, and may lead either to compromise through observation, or to disbelief in the realism of the simulation.

**Undetectable Emissions** Consider the case of a new active sensor system that produces emissions that are undetectable by current ESM suites. For example, assume that the radar uses ultra-wideband waveforms that spread the emissions across such a range of frequencies that Radar Warning Receivers (RWR) do not pick up the signal. This ability to track targets without alerting them must be protected.

Suppression in this case involves not using the protected radar. Traditional radars, though, will produce RWR indications that will allow targets to take defensive actions when tracking begins. This will substantially alter the element of surprise in most situations and result in severe training limitations for pilots using the protected radar.

State change control will work if the simulation protocol does not depend on the sensor to explicitly pass detection information or pulse characteristics. If the sensor models are implicit, the capability can be easily protected. If the sensor models are explicit, however, the state change control will “break” the protocol and lead to problems in the distributed simulation execution.

Finally, obscuration is very difficult to achieve in this instance because representing the radar as a conventional system gives up the significant advantage of non-reacting targets. It is possible that frequency bounds or some similar limitation of the RWR can be used to obscure the true radar capabilities, but this in fact leads to a non-detectable emission, just one of a different kind. Whether this constitutes a compromise is a matter for policy decision makers to determine.

**Performance** Consider the case of a new air superiority aircraft that has performance characteristics so far in advance of conventional aircraft that they must be protected. As a specific example, assume that the maximum climb rate and maximum sustained turn rate of the aircraft must not be revealed to other participants.

Suppression in this case involves flying the aircraft at less than its full performance value. Pilots must endeavor not to use their best performance, but to keep the aircraft within conventional limits. Alternatively, it may be possible to alter simulation parameters to achieve the same effect. This will almost certainly lead to training limitations since limiting the aircraft’s performance will be very detrimental to its success in most turning combat actions.

State change control is of no value at all. The protocols for any distributed simulation demand that entity position and velocity be passed to other participants. It is hard to envision how a distributed simulation could, even in principle, avoid this requirement. As a result, climb rates and turn rates can be derived directly from observation of the event. Some protection may arise from blocking access to saved state, but in most cases any educated observer of the simulation would be able to see performance outside the conventional range when it occurs.

Obscuration isn’t applicable to this case since it is logically equivalent to suppression for observable performance characteristics.

**Synergistic Effects** Finally, advanced systems often have more than one of the above capabilities that function in cooperation. The result is a much more effective weapon system than any conventional system can be. When multiple effects come together, even separate protection for each of the individual capabilities may result in an overall effectiveness that isn’t consistent with the obscured behavior.

## TECHNOLOGY AND POLICY ASSESSMENTS

The O&I team examined the applicability of potential MLS technology approaches and assessed security policy issues for DMT. The team spoke with Air Force, other defense, government and industry points of contact engaged in MLS research, policy, and implementation. Reports summarizing the results of nineteen major contacts may be referenced in Appendix C of the final report.

### Technology

The O&I team grouped the MLS technology assessment results by Trusted Platforms, Guards/Data Labelers, and Cryptography.

**Trusted Platforms** To address the DMT MLS Problem, security applications/functions will need to be built on trusted host platforms that offer a foundation for assurance and accreditation.

Platform security covers a myriad of properties on which an application relies to execute securely. Some of these features may include data separation, data and process labeling, higher assurance levels, identification

and authentication, access controls, enhanced auditing features, encryption, and basic firewall capabilities. In years past there were a number of trusted platforms from which to choose. More recently, vendors are moving away from this market for profitability reasons. However, many of the so-called *untrusted* platforms have features that at one time were only available on trusted platforms. Assessment results detailed in the final report include a description of the security functions of each final candidate platform and an assessment of each candidate's strengths and weaknesses. The primary candidates included Trusted Solaris [TM] 8.0, Security Enhanced (SE) Linux (including SE Linux with NetTop), and Getronics STS300.

Of the available trusted platforms today, Trusted Solaris is the most widely used and provides the most security capabilities. For future considerations, SE Linux offers promise as a trusted operating system. The Trusted Solaris 8 upgrade was undergoing evaluation during the DMT MLS assessment. SE Linux demonstrates the principles of flexible security policies and type enforcement compatible with the well-known operating system, Unix.

**Guards and Data Labelers** Trusted guards and data labelers allow network enclaves and devices operating at different system-high security levels to communicate within the confines of a carefully constructed security policy implemented by a well-defined rule set that defines the flow of information across enclave boundaries. The candidate guards that were assessed include the AFRL HLA Guard research effort (more recently called the Distributed Training Network Guard), Radiant Mercury, particularly the latest Version 4.0, scheduled for DIA certification near term. The certification is for employment in the Joint Simulation System as a one-way guard to pass HLA objects from a SECRET Federation to a TOP SECRET/SCI federation. Other guards addressed include the Navy Java Guard and the Cryptek Diamond TEK product. The assessment results in the O&I team final report document the strengths and weaknesses of each guard. For potential DMT MLS experimentation, the AFRL HLA guard and Radiant Mercury Version 4.0 appear to be the most viable candidates. Additional engineering studies will be needed to verify their viability.

**Cryptography** Several issues associated with the potential cryptographic approaches, the High Assurance Internet Protocol (IP) Encryptors (HAIPE), may influence the evolution of the DMT architecture. Currently DMT employs a HAIPE device, the TACLANE (KG-175), in the DMT network. Today HAIPE are not interoperable with commercial IPsec. They are evaluated with a system high security mode of

operation assumption. Additionally, the current HAIPE are not capable of dynamic multicast (group) key management.

The implication of HAIPE devices not being interoperable with IPsec is that a mixture of NSA approved Type 1 devices and commercial devices need to be constructed in a carefully nested manner.

The fact that HAIPE devices are evaluated to run at system high or one security level at a time impacts the number of encryptors needed at each DMT site. While multi-level operation is theoretically possible, no one has yet attempted to have their device evaluated for Type 1 MLS.

Initial releases of HAIPE devices do not support dynamic, or even automated, multicast key management. Such a capability would facilitate DMT key management, particularly in the future as new systems are added and key management becomes more complex. The complexity of key management rapidly increases for MLS solutions.

### **Policy**

The O&I team assessed the state of current security policy issues that may exist for DMT MLS. The major policy issues identified were: information sharing agreements, information classification for DMT Federates, accreditation process, and evolving security guidance.

**Information Sharing Agreements** The information sharing security requirements and risks for MTC/Federate simulation training are not well understood or known by all policy makers. This makes sharing agreements difficult to address. Security risk management including the identification of risks compared to training benefits is essential for enabling the sharing of information for DMT. At present, there are local policy and requirements-driven constraints and there is reluctance to share protected information between different communities. Senior government agreements on policy to mandate (and enforce) the sharing of information between Federates based on effective risk management will be needed to achieve MLS for DMT. Achieving such policy changes as a trade for more effective training is a significant challenge.

**Information Classification for DMT** A key issue in implementing a capability that permits training between single level enclaves of different classification levels is the challenge of developing a rigorous description of exactly what information can be shared and what information must be protected in a manner that can be implemented by a high assurance guard processor (GP). There are two approaches to addressing this issue. First, the GP can simply block

certain data elements from leaving a Federate System or, second, the Federate System or its GP can obfuscate the information leaving the Federate System to protect the data.

Data aggregation is a substantially more complex problem. For example, reviewing SECRET weapon system data over a period of time can reveal limitations that are TOP SECRET. The existence of a weapon system limitation may not be apparent until after the training is complete resulting in the requirement to purge SECRET Federates of TOP SECRET data. It will not be possible to address all aspects of data aggregation. Data aggregation continues to be a challenging area of information security research.

Another complex problem is protecting some attribute of a weapon system. Suppose a Federate has a special system whose products are relevant to another Federate; however, its existence must be protected from all the Federates. Alternatively, suppose some aspect of a weapon system is TOP SECRET, for example, its maximum range where activities below a certain range are unclassified.

Developing Rule Sets addressing these issues with sufficient assurance that the data owner will accept the risk of connecting his Federate system to the DMT is one of the most difficult technical and policy security challenges to be solved.

**Accreditation** As the DMT mission evolves, TOP SECRET (TS) Federate Systems requiring Intelligence Community (IC) Accreditation will join the network. Federate Systems requiring military Designated Approving Authority (DAA) Accreditation at foreign locations that may require State Department involvement are anticipated later. This evolution to multiple Federate Systems at different classification levels, with different accreditation processes, and different DAAs will add complexity and new challenges to the certification and accreditation process.

The multiplicity of DAAs and accreditation requirements will make accrediting the DMT network a complex problem. Initially, the USAF will accredit the DMT; however, as the DMT adds TOP SECRET, Intelligence Community (IC) and foreign Federate (coalition) systems, the USAF DMT DAA will be responsible for coordinating the top level accreditation with the IC and the State Department as required.

**Evolving Security Guidance** Many security guidance and requirements documents within the government are undergoing changes. Certification and accreditation, particularly for high assurance, MLS systems will require that DMT solutions be designed to meet the changing requirements evolving within these different

communities including DIA, TSABI, NSA, DoD, and the Air Force.

## SUMMARY FINDINGS

MLS solutions for DMT will not be achievable without many changes. An important action will be to ensure Program Managers, policy makers, and security decision-makers are well informed and willing to take the necessary risks to go forward with DMT MLS approaches.

There is no off-the-shelf policy and technology DMT MLS solution. However, there are approaches and technologies that are available to attack the problem. There are specific solution steps to address the problem. At DMT First Federation, all information between the Federate systems will be shared at the same security level with all Federate systems operating in a system high security mode. MLS was not considered during the development of current DMT simulators. These systems are designed to operate in a closed environment at a single security level.

The need for MLS exists today. Sharing information at the highest level for security operation is not the most desirable or efficient way to operate distributed training for Federate systems. Once DMT sites evolve to include Federate systems of higher security levels and additional compartments, some degree of MLS in the overall implementation will be required for distributed training. More specific technology and policy findings resulted from team analysis of discussions with the MLS contacts. These findings are listed in the final report.

## TECHNICAL APPROACHES

The O&I team defined time phased technical approaches to address the DMT MLS problem. Technical approaches are based on evolving DMT architecture considerations and the technology assessments for MLS feasibility and partial MLS solutions over time.

### Guard-based Multilevel DMT Confederation

The Guard-based Multilevel DMT confederation approach involves use of existing Guard technology, as applied to other M&S programs, to provide filtering and very limited data masking of information flowing out of MTCs at one security level to other MTCs at a different security level. Therefore, the guard provides a means to interface at least two MTCs operating at different security levels. The sophistication of the multi-level communication is constrained by the difficulty of developing the filtering rules, implementing the guard, achieving adequate performance, and getting the overall system accredited.

This first technical approach is illustrated conceptually (see Figure 3).

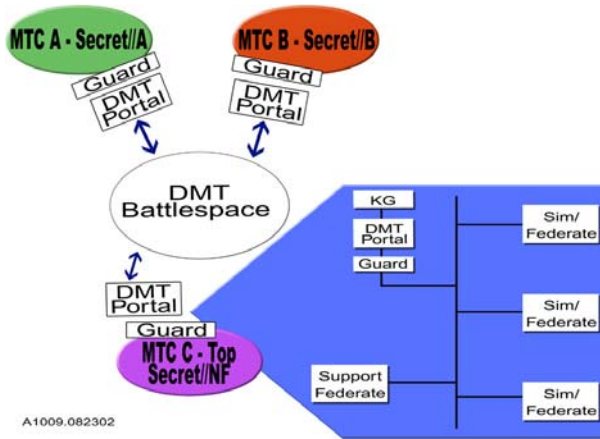


Figure 3 Guard-Based Multilevel Approach

### MLS Component Insertion

To improve throughput and add the ability to make “stateful” changes to the behavior of MTC “models,” the next option is to embed MLS technology into critical portions of an MTC. This option is best for implementation where MTCs have distinct simulation/simulator elements that deal with the sensitive system capabilities and can make appropriate changes to the simulation Reference Federation Object Model (RFOM) representations to allow the sensitive capability to be represented in a declassified manner. This second technical approach is illustrated conceptually (see Figure 4).

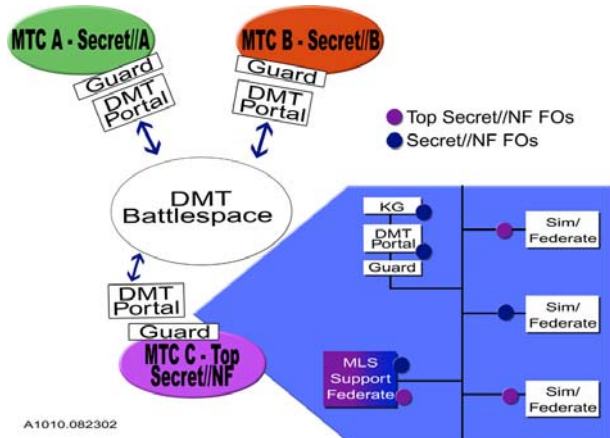


Figure 4 MLS Component Approach

This option is conducive to protecting activities within high (security level) MTCs that have known and observable characteristics in the Battlespace, or activities that have a tight binding with low objects.

### MLS DMT Federation (MLS MTCs)

The final target/approach calls for full implementation of MLS throughout the DMT federation. All MTCs (that have data they wish to restrict) operate as MLS entities providing full MLS services (mandatory and discretionary access controls (MAC and DAC), labeling, reference monitor, etc.). Each MTC is capable of deciding, with high assurance, which data within the MTC can be released (both from a classification level (MAC) and need-to-know (DAC) constraint) to the remainder of the DMT federation. In principle, this approach allows for each MTC to interact differently with every other MTC.

This approach requires that there be a trusted platform/network infrastructure to support the high assurance MTC MLS applications. This technical approach represents a long-term goal for DMT MLS. To aspire to MLS MTC/Federates, plans must be defined and steps taken near term. The government must lay the groundwork for MLS MTC development including identifying and sponsoring early tasking. Early tasking includes domain expertise and security engineering for a full understanding of the security classification of simulation data, the incorporation of security into the RFOM, the prototyping of trusted platforms for MLS simulators, the exploration of impacts to training, and an understanding of the potential benefits. This third technical approach is illustrated conceptually (see Figure 5).

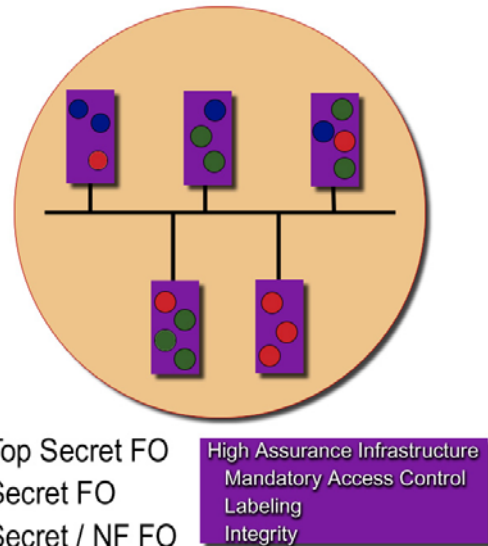


Figure 5 MLS DMT Federation

### RECOMMENDATIONS/CONCLUSIONS

Government initiatives and actions will be required to change the way DMT acquisition and implementation

are done today to pave the way for MLS solutions. To implement potential solutions derived from the options presented here, government must plan in advance for long-term and mid-term DMT MLS solutions. Even “baby steps” toward MLS will require government and industry cooperation to employ the significant domain, security, and system engineering expertise needed to identify information to be shared and how it can be shared. Information classification and sharing rules must be defined to classify and identify what can be passed between MTCs/Federates at acceptable risk as the DMT sites move forward to allow interoperability between Federates at different levels or categories.

Based on the approaches discussed above, the O&I team determined a set of recommendations to address the DMT MLS problem. These recommendations provide actions for near term results and lay the groundwork for longer-term solutions to the MLS DMT Problem. Options for addressing the DMT Multi-level training problem can be viewed in terms of an implementation timeline, operational effectiveness, and technical risk.

#### **High Assurance Guard Pilot**

Research to implement a pilot DMT MLS guard application offers the potential for very near term results that will provide an electronic interface between two DMT Federates at two different security levels or categories. The task assessment results indicated there are candidate MLS research products and commercial guard products in use in systems accredited to operate in a MLS mode. Some guards may be directly applicable to the HLA Federations planned for DMT at First Federation and beyond.

#### **MLS Intelligence, Surveillance, and Reconnaissance Prototype**

The MLS Intelligence, Surveillance, and Reconnaissance (ISR) Prototype would target, potentially, the Rivet Joint simulation for future DMT application. The Rivet Joint simulator, planned to be a DMT participant, is a multi-level Federate operating with two different levels of security. The prototype will initiate steps for a Federated model MLS implementation within the Federate system. This step expands MLS functionality beyond a guard interface and moves the MLS implementation into the Federate system itself.

#### **MLS ISR Model Integration and Test**

This recommended action integrates the MLS ISR Prototype Model into the Rivet Joint Federate (mission training) system or another appropriate mission training center. This would carry the proof of concept a step further to implement and accredit an actual MLS

Federate system. The MLS Federate system would interface other Federate systems through the trusted guard that supports the trusted exchange of federated objects.

#### **MLS Battlespace Object**

This recommendation is to conduct research on the viability of developing a true MLS battlespace object based (initially) on a single airframe/weapon simulation. The research would explore the potential for eliminating and obfuscating airframe protected (e.g., weapon systems, speed, etc.) information while achieving a common battlespace object that would be able to achieve effective training.

#### **MLS Federation**

This recommendation is to perform the foundational steps for a long-term solution that would offer a MLS capability for DMT Federations. Working toward a long-term MLS solution as technology advances, research actions must be taken near term to determine the MLS rules for each Federate system and provide a high assurance infrastructure that supports full interoperability and consistent execution control for multi-level and system high Federates.

#### **ACKNOWLEDGEMENTS**

The authors wish to thank the following ASC/YWI technical advisors for their valuable guidance, input and support: Mr. Dale Luebking; LtCol Jeffrey Nicholson, DMT O&I PM; Mr. Robert Lillie; Mr. Jim Evans; Mr. Arthur Daum; Mr. Ron Hannan; Mr. Duane Thorpe, and Mr. Terrence Mahoney. The authors also wish to express gratitude to the many contributors of information to the technical and policy assessments. These contributors are described in Appendix C, Contact Reports, of the *MLS Feasibility Assessment R&D Final Report*. Finally, the authors wish to express appreciation for the contributions from additional O&I team participants: Mr. Warren Pearce, TRW; Ms. Irene Nunley, SPARTA; Mr. Dick Losee, TRW; and Mr. Chris Gray, TRW; and for technical guidance from Dr. Michael Papay, TRW O&I PM and Mr. Bruce McGregor, TRW O&I DPM.

#### **REFERENCES**

AFI 33-202 (2001), *Computer Security*. AFMAN 33-229 (1997), *Controlled Access Protection (CAP)*. DMT O&I Contractor (2001), *MLS Feasibility Assessment Research and Development (R&D) Final Report, Version 1.0 and Appendix C, Assessment Contact Reports*.

DMT O&I Contractor (2001), DMT Integration Standards and DMT Common Definitions at <https://web2.trwdmt.com/dmt/sdwg/index.cfm>

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

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

MITRE/AFIWC (2001), *Survey of Trusted Automation Capabilities for Cross-Domain Data Exchange Volumes 1, 2, and 3*.

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*.

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

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

NIAP (2001) Validated Products List at <http://niap.nist.gov/cc-scheme/ValidatedProducts.html>

TCS/AFRL/HEA (2001), *The High Level Architecture Multi-Level Guard Project Report*.