Wiemer-Murray[1] Domain Security Policy Model for International Interoperability

Douglas J. M. Wiemer, BEng, MEng

douglas.j.wiemer@cpmx.saic.com

SAIC Canada
50 O'Conner Street, suite 1615
Ottawa, ON
Canada
K1P 6L2

Abstract: In recent years, a considerable amount of effort has been spent identifying areas where technology may be used to improve business practices. This is particularly true of the concentrated review of the Department of National Defence/Canadian Forces (DND/CF) Information Technology Infrastructure (ITI), under the direction of the Management Command and Control Re-engineering Team (MCCRT). This review has identified considerable areas where consolidation of infrastructure is required to reduce expenditures and achieve economies of scale. The main themes of the DND/CF ITI is information centralization, information access and interoperability. However, the DND/CF places considerable priority on information sharing and interoperability with its allied partners. As a result, the existing infrastructure consists of several systems, which from an internal point of view, are isolated systems that create enclaves. Therefore, a security policy model is required that will allow multiple enclaves of caveat information to share systems and information while guaranteeing the separation of information and users as necessary. In addition, the policy must maintain the ability for information sharing and interoperability with allies. This paper describes the Wiemer-Murray Domain Security Policy Model for International Interoperability that meets these requirements.

Keywords: Information Technology Security (ITSEC), Security, Policy, Model, National, International, Interoperability, Information Domain, Separation, Access Control, Information Sharing, Information Exchange.

Wiemer-Murray[1] Domain Security Policy Model for International Interoperability

Douglas J. M. Wiemer, BEng, MEng

1 Introduction

In recent years, a considerable amount of effort has been spent identifying areas where technology may be used to improve business practices. This is particularly true of the concentrated review of the Department of National Defence/Canadian Forces (DND/CF) Information Technology Infrastructure (ITI), under the direction of the Management Command and Control Re-engineering Team (MCCRT). This review has identified considerable areas where consolidation of infrastructure is required to reduce expenditures and achieve economies of scale. The main themes of the DND/CF ITI is information centralization, information access and interoperability. This trend is not isolated to the DND/CF. The Department of Defense (DoD) Technical Architecture Framework for Information Management (TAFIM)[2] identifies that consideration of information centralization, information access and interoperability eliminates the consideration of isolated or stand-alone implementations as a means of providing security.

The DND/CF places considerable priority on information sharing and interoperability with its allied partners. As a result, the existing infrastructure consists of several systems, which from an internal point of view, are isolated systems and create enclaves. The view from the external systems perspective is quite the opposite. The prevailing design has been one of sacrifice of internal interoperability, in favor of allied interoperability. These systems operate in system high security mode of operation based on an operational caveat (CANUS, AUSCANNZUKUS, NATO, etc). Systems operating in different caveat domains are completely isolated from each other. This isolation results in a collection of separate systems to support each enclave. This is the very architecture that the TAFIM identifies that organizations can no longer afford to build.

Therefore, a security policy model is required that will allow multiple enclaves of caveat information to share systems and information while guaranteeing the separation of information and users as necessary. In addition, the policy must maintain the ability for information sharing and interoperability with allies. The following paper describes the Wiemer-Murray Domain Security Policy Model for International Interoperability. Section 2 describes some Security Policy Model Background, including the Bell-Lapadula Model[3] and the Security Concepts proposed in the TAFIM. Finally, Section 3 describes in general terms, the Wiemer-Murray Domain Security Policy Model, including a brief description of how it meets the requirements for the TAFIM. While the TAFIM is not a document recognized by DND, it serves as supporting guidance to promote acceptance of this model in international or allied forum.

2 Security Policy Background

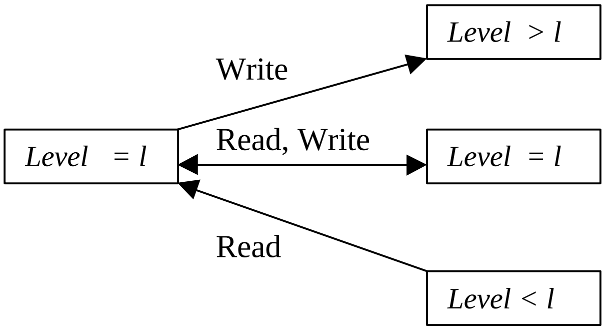
Significant literature and study exists concerning acceptable security policies to define access to information from different security information domains. For example, the Bell-Lapadula model has made considerable contribution to the information security community. Certainly, in Defence and other Government applications, it has received widespread acceptance. The Bell-Lapadula model defines access rights to information based on a hierarchy of security levels. In contrast, the TAFIM describes an information domain as a set of users, their information objects and a security policy. It further states that these information domains are not hierarchically related. The following section will briefly describe these security models. Later the model proposed in this paper will be described in accordance with these models to substantiate its claims.

2.1 Bell-Lapadula Security Policy Model

The Bell-Lapadula model is designed to facilitate information sharing in a secure manner across information domains. Within the model a hierarchy of levels is used to determine appropriate access rights. For example, using conventional DND document labeling standards, SECRET is treated above CONFIDENTIAL. The Bell-Lapadula model uses axioms of “read-down” and “write-up”. Therefore, assuming appropriate need-to-know, an individual in a SECRET domain is authorized to “read-down” into the CONFIDENTIAL domain since personnel with sufficient clearance for SECRET are also cleared for CONFIDENTIAL. However, the user in the SECRET domain may never be authorized to “write-down”. This occurs because the clearance in the CONFIDENTIAL domain is not sufficient to handle the SECRET information.

Similarly, an individual in a SECRET domain is not authorized to “read-up” from a TOP SECRET domain. This happens because the SECRET domain does not include a sufficient clearance. However, an individual in the SECRET domain may be authorized to “write-up” to the TOP SECRET domain. This happens as a result of the inherent ability for all personnel in the TOP SECRET domain to have sufficient clearance to read the lower domain information.

Figure 1: Bell-Lapadula Model for Access Rights



Unfortunately, implementations of this model often find mechanisms to bypass these restrictions. For example, in a system high SECRET domain all information is to be treated as SECRET, regardless of whether or not it is. A rigid application of this, coupled with the use of the Bell-Lapadula model, result in no transfer of information from the SECRET domain to a lower domain.

However, it is widely recognized that the information, though contained in a SECRET domain may only be CONFIDENTIAL or UNCLAS. In this situation, a “release authority” may be granted the access rights to bypass the Bell-Lapadula model, thus allowing a transfer of information from the SECRET domain to a lower domain.

Likewise, this model does not apply well in an environment where the security levels are not hierarchically rated. For example, from a Canadian perspective, CANUS and CANUK are not hierarchically rated to each other. The Bell-Lapadula model does not account for transfer of information between these domains, even if it is determined that the information is actually, CANUKUS.

2.2 TAFIM

By contrast, Volume 6, Section 3, of the TAFIM provides some fundamental security concepts to be applied while using this framework. The TAFIM framework clearly states that information domains are not hierarchically related. The following passage from the TAFIM details this position:

> *"Note that the apparent hierarchy among U.S. national security policy classifications is actually a property of user privileges, in the form of clearances, rather than a relationship imposed on information of different classifications. Information that is classified Secret is* not *a subset of information that is classified Top Secret."*

In the context of the TAFIM, these statements make logical sense. The TAFIM defines an information domain as a set of users, their information objects, and a security policy. An information domain security policy is the statement of the criteria for membership in an information domain and the required protection of the information objects. Information domains are not hierarchically related, nor may they implicitly or explicitly infer sensitivity relative to multiple categories of sensitivity.

From the perspective of caveat separation and interoperability, two key points must be understood. First, information objects can be transferred between domains only in accordance with established rules, conditions, and procedures expressed in the security policy of each domain. Secondly, the transfer can be accomplished only by a user who is a member of both the sending and receiving information domains and, if required by the information domain policies, has been granted the appropriate privileges (e.g., "release authority").

This approach lends itself to the legitimate transfer of information from a SECRET domain to a CONFIDENTIAL domain. A release authority may make a verification of the content of the information and determine that the protective mechanisms in the CONFIDENTIAL domain are appropriate. Assuming that the release authority is a member of both domains, he/she may then transfer the information in accordance with established rules, conditions, and procedures expressed in the security policy of each domain.

2.3 DND Environmental Conditions

The DND/CF has a requirement to exchange information between systems operating at different caveat classifications. The main systems in consideration can be grouped as Canadian Eyes Only (CEO), CANUS, AUSCANUKUS, AUSCANNZUKUS, and NATO. A security policy is required which will meet the following conditions:

- ensure separation of information where the caveats or classifications are incompatible
- facilitate exchange of information if the caveats or classifications are compatible
- ensure the security of the Canadian Operational domain (i.e., ensure sovereignty)
- facilitate exchange of information with allies
- support a generalization that may be applied for any national perspective

3 Wiemer-Murray Domain Security Policy Model

The Wiemer-Murray Domain Security Policy Model is defined to control the initiation of access to a particular information domain. As such, the model is based around a concept of "connection dominance". It is a policy model for inter-domain access control verification based on user access rights associated with the initiating information domain. The authentication mechanism to verify the user's identity and the security of the information in transit are outside the scope of this policy model. The following section will describe in general terms the fundamentals of the Wiemer-Murray Model. This description will begin with some basic assumptions about the environment, then proceed into the model itself, including example applications. Finally, the model will be compared to both the Bell-Lapadula model and the TAFIM.

3.1 Environmental Assumptions

An information domain framework is required in order to understand the context of this policy model. This framework describes the attributes associated with the information in a domain. This framework leads to some basic assumptions about the nature of the domains and the transfer of information among them. This framework and assumptions are provided below:

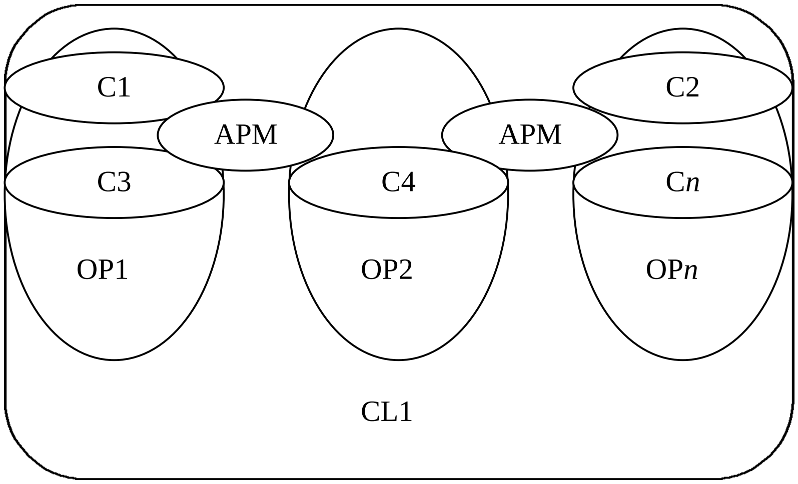


Figure 2: Model Framework

- An information domain will be characterized by three security attributes (classification label (CL*n*), caveat label (C*n*) and operational label (OP*n*)).
- The security attribute labels may be implicit (based on the physical attributes of the connection) or explicit (based on binding of a logical label).
- An Access Policy Mechanism (APM) is available to mediate the initiation of access between information domains.
- A Transfer Policy (TP) is available to mediate the transfer of information between information domains.

3.2 General Policy Model

In order to meet the DND Environmental conditions, specified in section 2.3, the conditions for user membership in a domain, rules for connection initiation and the rules for transfer between domains must be defined. The Wiemer-Murray Model applies specifically to the initiation of connections and the transfer policy.

To be a member of a domain the user must satisfy three policy statements, namely, the Clearance policy, the Need-to-Know policy and the Formal Access Approval policy. These policies are defined as follows:

- ***Clearance policy*** – The user must have the requisite personnel security clearance for access to the classification of the domain, as defined by the classification label.
- ***Need-to-Know policy*** – The user must have a recognized requirement to have access to the information.

- ***Formal Access Approval policy*** – The user's nationality must coincide with caveat of the domain, as defined by the caveat label. Also, where the user is to be a "release authority", the user must formally agree to abide by the Transfer Policy.

The Wiemer-Murray Model is used to determine whether or not one information domain is allowed to initiate a connection to another information domain. This connection is based on a concept of "connection dominance". A connection may be initiated provided that:

- **The initiation of a connection is unidirectional and must be initiated from a *more restrictive* to an *equivalent* or *less restrictive* domain (note that once the connection is established, communications may be bi-directional based on the transfer policy below).**

Where the following definitions apply:

- ***More restrictive*** domain is defined as an information domain in which the protective mechanisms associated with the characteristic labels imply greater protective mechanisms and the domains are not *mutually exclusive*;
- ***Less restrictive*** domain is defined as a formal access domain in which the protective mechanisms associated with the characteristic labels imply lesser protective mechanisms, and the domains are not *mutually exclusive*;
- ***Equivalent*** domains are defined as two information domains which share exactly the same set characteristic labels; and
- ***Mutually exclusive*** domains are defined as two information domains which are neither *equivalent*, *more* restrictive, or *less* restrictive (i.e. NATO and AUSCANNZUKUS are mutually exclusive information domains).

3.2.1 The Wiemer-Murray Transfer Policy

For the purposes of the Wiemer-Murray Model, the Transfer Policy is used to determine if the receiving domain has the appropriate protective mechanisms for the information to be transferred.

A user, having met the policy requirements to be a member of both information domains and having been granted rights of release authority, may transfer information between domains provided that:

- **Users in the receiving domain meet the membership policies (Clearance, Need-to-know, and Formal Access Approval).**
- **The information is verified as releasable.**
- **The transfer of information is controlled from a *more restrictive* or an *equivalent* domain. Users in a *less restrictive domain* may never gain control of information transfer.**
- **The release authority is responsible to ensure information does not have any eyes-only caveat that is not suitable for the receiving domain and the information are of a suitable classification for the receiving domain.**

3.3 Example Applications

Applications of the Wiemer-Murray Model must ensure that all three characteristic labels (caveat, classification, operational labels) are verified and that in all cases the labels are considered *more restrictive*. For example the protective mechanisms generally required of UNCLASS information domains are *less restrictive* than a CONFIDENTIAL domain, therefore a connection may never be initiated from the UNCLASS domain. However, CONFIDENTIAL is *more restrictive* than UNCLASS, therefore a connection may be initiated from the CONFIDENTIAL domain (provided that the other characteristic labels are also *more restrictive*).

From the Caveat label perspective, the protective mechanism required of an information domain is *more restrictive* if the formal access approval policy reduces the number personnel allowed access. For example, CEO is considered *more restrictive* than CANUS because only Canadians may have access. Likewise, the caveat label US is *more restrictive* than CANUS because only US nationals may have access. However, the labels CEO and US are considered *mutually exclusive*.

3.4 Case Study – JWID'97

During the Joint Warrior Interoperability Demonstration 1997 (JWID'97) a DND SECRET AUSCANNZUKUS/NATO system was connected to a variety of Foreign SECRET systems via an Allied SECRET AUSCANNZUKUS/NATO Coalition Wide Area Network (CWAN). During the preparations for the demonstration, which would test and evaluate security functionality, it was decided that the Canadian system would be treated as a notional CEO system. In the notional CEO environment the information was formally considered SECRET AUSCANNZUKUS/NATO, however, it was treated as CEO. This use of a notional CEO domain provided a secure environment for testing the Wiemer-Murray model, while preventing any possibility of a security infraction. For each domain, confirmation of the Classification, Caveat and Operational domain suitability was established prior to initiating a connection. The confirmation for the DND system follows:

- Classification domain – The DND system lies in a SECRET domain, as does the CWAN (*equivalent domains)*. Therefore, the DND system is authorized to initiate a connection to the CWAN, provided Caveat and Operational tests pass as well.
- Caveat domain - The DND system is being treated as a CEO caveat. The caveat domain is a member of the CWAN domain and is *more restrictive* than the AUSCANNZUKUS/NATO CWAN. Therefore, from a caveat perspective the DND system may initiate a connection to the CWAN.
- Operational domain - The DND system lies in the Canadian Operational domain. The Operational domain is a member of the CWAN and is *more restrictive* than the AUSCANNZUKUS/NATO CWAN. Therefore, from an operational perspective the DND system may initiate a connection to the CWAN.

Having established that all policy domain checks had been met, it was confirmed that the DND system was in a position of "connection dominance". Therefore, the DND system was allowed to initiate connections to the CWAN.

A similar confirmation process was used to determine if systems on the CWAN might initiate interactive sessions to the DND System:

- Classification domain – The CWAN lies in a SECRET domain, as does the DND system (*equivalent domains*). Therefore, CWAN systems are authorized to initiate a connection to the DND systems, provided Caveat and Operational tests pass as well.
- Caveat domain - The systems on the CWAN lie in the Coalition (AUSCANNZUKUS/NATO) caveat. The caveat domain for this system is *less restrictive* than the CEO caveat domain of the DND systems. Therefore, from a caveat perspective, systems on the CWAN are restricted from initiating a connection to DND systems.

- Operational domain - The systems on the CWAN lie in the Coalition (AUSCANNZUKUS/NATO) Operational domain. The operational domain for this system is *less restrictive* than the operational domain for the DND systems (Canadian only). Therefore, from an operational perspective, systems on the CWAN are restricted from initiating a connection to DND systems.

While the classification domain criteria were met, the caveat and operational domain criteria were not. Since both the caveat and operational domain criteria were not met, the systems on the CWAN were not in a position of "connection dominance". Therefore systems on the CWAN were restricted from initiating interactive sessions to DND Systems.

A similar set of tests could have been performed for all National systems. Based on the operational domain policy, the confirmation of "connection dominance" would all identify that connections were allowed from the National system to the CWAN, but not from the CWAN to the National systems. Intuitively, this makes sense. The National Sovereignty of each respective National system was preserved, while allowing interoperability among partners across the CWAN.

3.5 Special Considerations

Protocol Violations - The above restriction places some interesting limitations on the architecture of the systems. For example, in an X.400 Mail system, the originating Message Transfer Agent (MTA) must initiate a connection to the receiving MTA. This results in a Wiemer-Murray Model violation if the originating MTA lies outside the DND Operational domain. Similarly, in order to identify the recipient, the originator must have access to the X.500 Directory Service Agent. Unfortunately, from an originator outside the DND Operational domain, access to the DND X.500 DSA would be an attempted violation of the Wiemer-Murray Model.

How then is it possible to maintain the policy while ensuring that joint or allied systems outside the National Operational domains may send messages to the National systems? Rather than allow a violation of the policy for either X.400 or directory protocols, it is recommended that a Message Store (MS) and X.500 directory be maintained external to the APM. This solution will apply to other interactive services for supporting protocols to prevent policy violations.

For example, a simplified X.400 architecture is provided in Figure 3. A user in National 2 system originates a message for a user in National 1. To find the appropriate recipient address, the DSA is available in an allied area. The originating user initiates a connection to the DSA and retrieves the address. The originator then sends the message via the local MTA. This MTA checks the address and initiates a connection to the MTA in the allied area. This MTA then forwards the message to the MS, in the allied domain. When the recipient logs in, within the National 1 system, the UA initiates a connection to the MS to retrieve the X.400 message. In this way, an X.400 message (or SMTP, etc) may be securely retrieved and read in the National domains, without violation of the Wiemer-Murray Model.

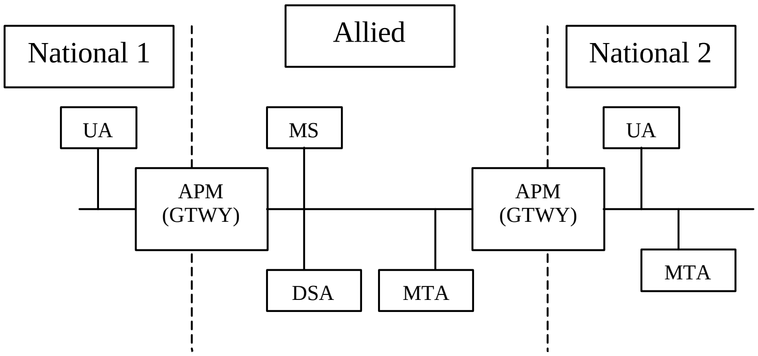


Figure 3: Example X.400 Mail Architecture Supporting the Wiemer-Murray Model through a Gateway

Policy Deadlock - Figure 4 is used to identify a situation in which additional supporting infrastructure is required to prevent policy violations that could result in "Deadlock". Consider that users in the National 1 Operational domain wish to supply information to a user in the National 2 Operational domain, using FTP. From the Wiemer-Murray Model the user in the National 1 domain would violate the operational domain criteria to access the server in the National 2 domain to initiate the FTP. Likewise, a user in the National 2 operational domain might attempt to initiate an FTP session to the National 1 domain in order to retrieve the same file. Assuming that, both national systems apply the same policy of restricted access, the National 2 user would also be prevented from establishing the connection and retrieving the file. A Deadlock situation has occurred.

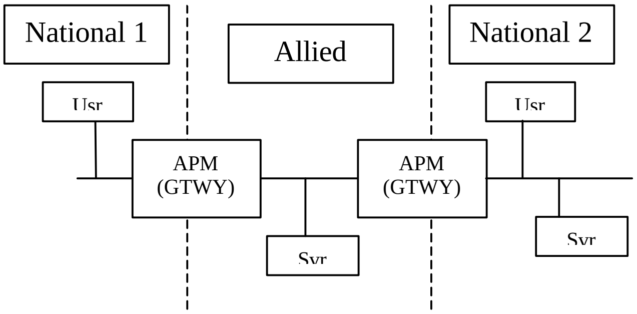


Figure 4: Example Architecture Supporting Policy Deadlock Resolution

Policy Deadlock Resolution - Each system, National 1 or National 2 is allowed to initiate a connection out of their respective domains, but not into the desired domain. Deadlock can be resolved through the addition of a server in the allied operational domain (between each APM Gateway). The National 1 user can now initiate a connection to the server in the allied domain, without violation of the policy, to upload the file to the server. Similarly, the user in the National 2 operational domain can initiate a connection to the allied systems area server, without violation of the policy, to download the file to the National 2 operational area.

3.6 TAFIM Verification

Presentation of the Wiemer-Murray Model in terms of the TAFIM Security Concepts must explicitly define rules to support the relationship imposed by the *Clearance* policy. In addition, it must be demonstrated that the non-hierarchical relationship of caveat and operational domains may be expressed as rules concerning connection initiation and information transfer. Furthermore, the policy must include rules to establish membership and the rights of a release authority.

The Wiemer-Murray Model includes membership criteria. For the membership policy the following applies:

- **The policy rules concerning membership in a domain are applied unchanged in the TAFIM context.**

To impose the TAFIM Security Concepts on the Wiemer-Murray Model in terms of "connection dominance", the rules must be explicitly defined. The following rules are provided:

- **Classification label rules:**
    - Top Secret systems may initiate to Top Secret, Secret, Confidential, Designated (Sensitive But Unclassified (SBU)), Unclassified and Public systems.
    - Secret systems may initiate to Secret, Confidential, Designated (SBU) Unclassified and Public systems.
    - Confidential systems may initiate to Confidential, Designated (SBU) Unclassified and Public systems.
    - Designated (Sensitive But Unclassified) systems may initiate to Designated, Unclassified and Public systems.
    - Unclassified systems may initiate to Unclassified and Public systems.
    - Public systems may only initiate to other Public systems.
- **Caveat label rules:**
    - Control for connection initiation must rest with the caveat domain that has *more restrictive* access criteria. This implies the fewest number of acceptable national labels. For example, CANUS has fewer national labels than CANUKUS and is therefore *more restrictive*.
    - All national labels characterizing the initiating system must be included in the labels characterizing the system to be connected to. That is to say the domains are not *mutually exclusive*. For example, the CANUS label is included in a CANUKUS label. Therefore, a connection may be initiated. However, the CANUKUS label is not included in a CANUS label. Therefore, a connection may not be initiated.
    - Optionally, a system-specific policy may be required to explicitly state the rules for connection initiation. This policy will be dependent on the national perspective of the policy authority. For example, a Canadian policy may specifically state that CEO may connect to CANUS, CANUK, AUSCAN, CANNZ, NATO, CANUKUS, etc. The advantage of this approach is that specific connections to national systems that are specifically prohibited based on national policy may be denied by excluding them from the explicit policy.

- **Operational label rules:**
  - Control for connection initiation must rest with the operational domain that has *more restrictive* access criteria, as described in the caveat label rules above.
  - All national labels characterizing the initiating system must be included in the labels characterizing the system to be connected to, as described in the caveat label rules above.
  - Optionally, a system specific policy may be required to explicitly state the rules for connection initiation. This will be dependent on the national perspective of the policy authority, as described in the caveat label rules above.

The above description defines the Wiemer-Murray Model for connection initiation in terms of the TAFIM. However, the TAFIM also identifies that a Transfer Policy must exist to allow an exchange of information. This policy must include rules to define both the authorities to transfer information and the rules surrounding the transfer.

From the Wiemer-Murray Transfer Policy in Section 3.2.1:

- **A user, having met the policy requirements to be a member of both information domains…**

This directly supports the TAFIM, which identifies that a user, who is a member of both domains, must maintain control of the transfer of information.

- **…having been granted rights of release authority, may transfer information between domains.**

This also directly supports the TAFIM which identifies that where required transfer must be controlled by a member with rights of release authority.

Having established the authority to transfer information, the rules must be established to control the transfer of information. The TAFIM imposes little restriction on this process, as long as the policy is well defined. Therefore, in respect to the Wiemer-Murray Security model:

- **The policy rules concerning transfer between domains are applied unchanged in the TAFIM context.**

This section has demonstrated that the Wiemer-Murray Model contains the essential elements required by the TAFIM Security Concepts and that all aspects of the model may be expressed in terms of these concepts.

4 Conclusion

This paper has presented the Wiemer-Murray Domain Security Policy Model for International Interoperability. The model provides a specification for verification to ensure that connections may only be initiated from a *more restrictive* domain to an *equivalent* or *less restrictive* domain. This property has been termed “connection dominance”. The model was presented with in a manner that is supported by the US DoD TAFIM, which should aid in acceptance of the model in international forum. Furthermore, the model meets the stated requirements of:

- ensuring separation of information where the caveats or classifications are incompatible
- facilitating exchange of information if the caveats or classifications are compatible
- ensuring the security of the Canadian Operational domain (i.e., ensure sovereignty)

- facilitating exchange of information with allies
- supporting a generalization that may be applied for any national perspective

Work is continuing with the Wiemer-Murray Model to add supporting formal specifications of the policy statements. Use of a formal specification will provide additional verification of its validity. A formal specification will also ensure that implementations of the model may be verified to high levels of assurance.

[1] Original model development by Capt Doug Wiemer (ret'd Canadian Forces), and Capt Mike Murray (ret'd Canadian Forces) in support of Mission Critical Information System Security Policy (Department of National Defence, Canadian Forces), March 1997.

[2] Defense Information Systems Agency (DISA), Center for Standards, *DoD Technical Architecture Framework for Information Management, Volume 6: DoD Goal Security Architecture*, version 3.0, 30 April 1996.

[3] Bell, D.E. and Lapadula, L.J. *Secure Computer Systems: Unified Exposition and Multics Interpretation*, MTR-2997 Rev. 1, MITRE Corp., Bedford Mass., March 1976.