AU/ACSC/O'MALLEY/2009

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

FREE TO FLOW:
A PARADIGM SHIFT FOR
MULTI-LEVEL SECURITY DATA EXCHANGE

by

Scott A. O'Malley, Maj, USAF

Advisors: Mr. Michael Ivanovsky, Lt Col Robert Bement

Maxwell Air Force Base, Alabama

April 2009

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **APR 2009**	2. REPORT TYPE **N/A**	3. DATES COVERED **-**

4. TITLE AND SUBTITLE

Free To Flow: A Paradigm Shift For Multi-Level Security Data Exchange

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Air Command And Staff College Air University Maxwell Air Force Base, Alabama

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

The original document contains color images.

14. ABSTRACT

As information systems evolved within the Department of Defense (DoD), safeguards were developed to protect the information being stored and processed. The levels of protection put in place are commensurate with the potential consequences of inappropriate disclosure, following the US governments policy of information sharing based on need to know. The militarys homeland defense mission and the intelligence and law enforcement communities homeland security mission require greater collaboration. This shift for collaboration necessitates a process for evaluating information exchanges for improved information synchronization between DoD and non-DoD operations. Multi-level security information systems are an approach to solving this challenge. There are a number of technology solutions that facilitate multilevel security information sharing. These solutions involve data replication through trusted interfaces, information passing through controlled protocols, and sophisticated, single systems that allow multiple interfaces at various security levels. Since agencies already have huge investments in their information technology infrastructure, it is necessary to identify solutions that capitalize on existing investments. This research explains the current state of the art in multi-level security technologies, identifies technology gaps, but most importantly, defines an approach to evaluate collaboration solutions against threats to information assurance.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**SAR**	**39**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Page

Illustrations

Tables

Acknowledgements

The endeavor of compiling thoughts into a cohesive work is not a simple task. It begins with an idea and inspiration. The excitement brought to the classroom by Mr. Michael Ivanovsky and Lieutenant Colonel Robert Bement motivated the contribution this work makes to a challenge the Department of Defense has been investigating for decades.

I would also like to acknowledge the support I received from my family over the last seven months. Without their support, I would find passion in no topic.

Abstract

As information systems evolved within the Department of Defense (DoD), safeguards were developed to protect the information being stored and processed. The levels of protection put in place are commensurate with the potential consequences of inappropriate disclosure, following the US government's policy of information sharing based on "need to know." The military's homeland defense mission and the intelligence and law enforcement communities' homeland security mission require greater collaboration. This shift for collaboration necessitates a process for evaluating information exchanges for improved information synchronization between DoD and non-DoD operations. Multi-level security information systems are an approach to solving this challenge.

There are a number of technology solutions that facilitate multilevel security information sharing. These solutions involve data replication through trusted interfaces, information passing through controlled protocols, and sophisticated, single systems that allow multiple interfaces at various security levels. Since agencies already have huge investments in their information technology infrastructure, it is necessary to identify solutions that capitalize on existing investments.

This research explains the current state of the art in multi-level security technologies, identifies technology gaps, but most importantly, defines an approach to evaluate collaboration solutions against threats to information assurance.

FREE TO FLOW: A PARADIGM SHIFT FOR MULTI-LEVEL SECURITY DATA EXCHANGE

At times, in the name of national security, secrecy
has put that very security in harm’s way.

—DANIEL PATRICK MOYNIHAN

1. Introduction

As information systems evolved within the Department of Defense (DoD), safeguards were developed to protect the information being stored and processed. The levels of protection put in place are commensurate with the potential consequences of inappropriate disclosure, following the United States (US) government’s policy of information sharing based on “need to know.” The military’s homeland defense mission and the intelligence and law enforcement communities’ homeland security mission require greater collaboration. This shift for collaboration necessitates a process for evaluating information exchanges for improved information synchronization between DoD and non-DoD operations. Multi-level security information systems are an approach to solving this challenge.

This research explains the current state of the art in multi-level security technologies, identifies technology gaps, but most importantly, defines an approach to evaluate collaboration solutions against threats to information assurance.

Problem Background and Significance

The US has a history of information protection going back to “secret” and “confidential” messages passed by General George Washington to his field commanders during the Revolutionary War.[1] Systems for protecting information have continued to evolve throughout the United States military history to include strategies on information technology systems. These schemes had been focused on limiting information disclosure to protect sensitive information, sources and methods of collection. As information sensitivity increased, a greater level of security was applied. This strategy is commonly referred to as "need to know."

In the analysis of the terrorist attacks of September 11, the 9/11 Commission identified the need for a new unity of effort in information sharing.[2] The challenge of sharing is compounded by the fact that domestic intelligence collected by law enforcement and foreign intelligence collected by the military and national agencies rarely overlapped.[3] In response to the 9/11 attacks, the Bush administration defined the following needs in the National Strategy for Information Sharing: 1) rapid identification of immediate and long-term threats, 2) identification of people associated with terror-related activities, and 3) implementation of "information-driven and risk-based detection, prevention, deterrence, response, protection and emergency management efforts."[4] The National Strategy focuses on improving information sharing at the federal level, with state, local and tribal officials, with private sector, and foreign partners while protecting individual privacy.[5]

The Office of the Director of National Intelligence (ODNI) acknowledged the "dynamic tension" that existed in the pre-9/11 intelligence community (IC).[6] The challenge of changing the culture is managing the risk, which is balancing mission effectiveness with information protection. In its 500-day plan for information sharing, the ODNI identified two impacts of an improved information sharing environment to be "deeper knowledge" and "more timely intelligence to the nation's leaders and defenders of the homeland."[7] To achieve this, ODNI established a program called the Information Sharing Environment (ISE) initiative.[8] The ODNI, recognizing the limitations of the existing system, is making deliberate effort to change the culture from "need to know" to "responsibility to provide."[9]

The IC is not the only community in the government that can make use of new solutions for information sharing. A couple of examples are: 1) the coalition environment in combined joint task forces, and 2) interagency coordination for homeland defense and security. The challenge of sharing information is the same for all these cases, but there are some nuanced differences.

A common issue is the protection of the shared information infrastructure. Responsibility for government networks falls to different organizations. This should not change based on interconnections. There are risks assumed by allowing network access to organizations outside of the owner's span of control. It is also necessary to consider what technology is authorized for release. For example, US export laws restrict the release of encryption technology to foreign countries which could impact a multi-national coalition scenario.

There are a number of technology solutions that facilitate multi-level security information sharing. These solutions involve data replication through trusted interfaces, information passing through controlled protocols, and sophisticated, single systems that allow multiple interfaces at various security levels. Since agencies already have huge investments in their information technology infrastructure, it is necessary to identify solutions that capitalize on existing investments.

With whatever technology solution is most appropriate, the biggest challenge will be how the systems are managed. Issues like reduced control of infrastructure, interagency cooperation, and information segregation need to be dealt with.

Paper Structure

The US government and military relies more and more on technology to facilitate the sharing of information, with the expectation the system is reliable and protects the information stored on it. Since the technology aspect makes this problem intimidating, section 2 provides a background on multi-level security, threats to information assurance and a review of some pertinent government policies used for this analysis. Next, section 3 describes three possible solutions to the information sharing problems faced by homeland security and defense organizations and the methodologies being used to analyze them. Section 4 documents the evaluation of the analysis process on the three possible solutions. To wrap up, section 5 provides the conclusions of the analysis and the road ahead.

2. Background

Defining a Common Lexicon

To be able to discuss the challenges of the multiple security domain interconnection issue, a well defined and understood vocabulary is necessary. Unfortunately, industry and government both use a number of closely related terms with significantly different meanings. This section provides an illustrative dictionary of technical terms that are easily confused for one another.

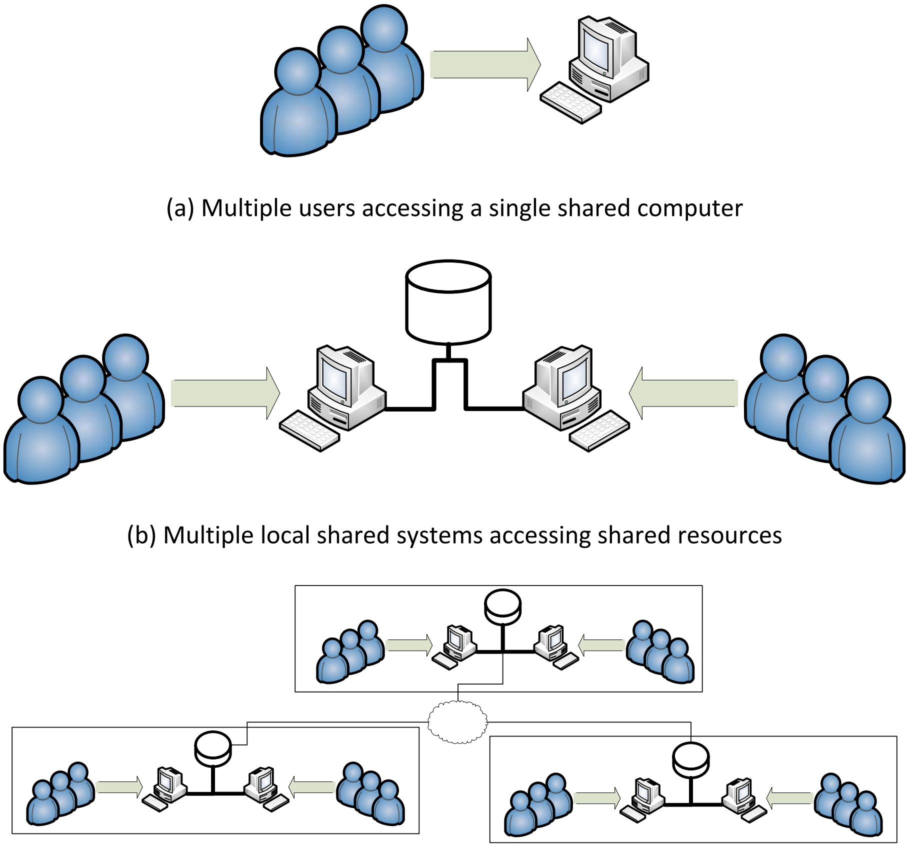
To begin, it is necessary to understand the classification process. The government uses a dual classification process to protect information. First, *Classification Level* refers to sensitivity level of the information. Second, *Clearance Level* identifies the trust level given to an individual or information storage area (e.g. facility, vault, safe, computer system).[10] Both processes use *Security Levels*—Unclassified, Confidential, Secret, Top Secret—to describe the assigned classification and clearance level.[11]

The multi-level security challenge deals with clearance levels assigned to information systems. The issue, however, is not merely a technical issue. It involves computers and networks of computers, but other key artifacts that make up the system are the human users and policies that govern computers and users. It is important to understand the key characteristics of each to understand the foundation of the problem.

Next, a foundation of technology terms is needed. The *personal computer* (PC) has become the information technology commodity used by the majority of computer users today. The PC is characterized by a central processing unit with attached storage, operating system and application software, and interfaces for input and output devices (e.g. keyboard, mouse, monitor display, printer, and network interface card). The life-cycle of the PC is about 3-5 years, and the cost has remained relatively constant over the last decade, though the features have increased and improved over time. In contrast to the PC, *client-server architectures* have begun resurging in specialized markets. This architecture is, generally, defined by a central server that performs the processing for the entire set of attached client systems. The user interfaces with the system through a thin-client appliance (typically a small device that input and output devices connect). Regardless of the system, the computing environment in which the user is affected is the operating system and software. Today, most PCs run Microsoft operating systems and applications, and though terminal server versions of Microsoft exist, the majority of client server systems use specialized operating systems.

Regardless of the type of hardware the user has, it is typically connected to a network in a single clearance level, or *security domain*. Like the government’s security level system, industry has analogous security domains that may be based on the separation of proprietary information (software engineering companies, for example, typically have production and development networks for testing). The intent is to protect information from being disclosed to unauthorized users.

Users with authorized access to different classification levels work, to some degree, in a *multiple-security level* environment. In the simplest example, the only aspect of the system that is shared is the user. The computers accessed by users and the computer communication networks are discreet from one another, as shown in figure 1.



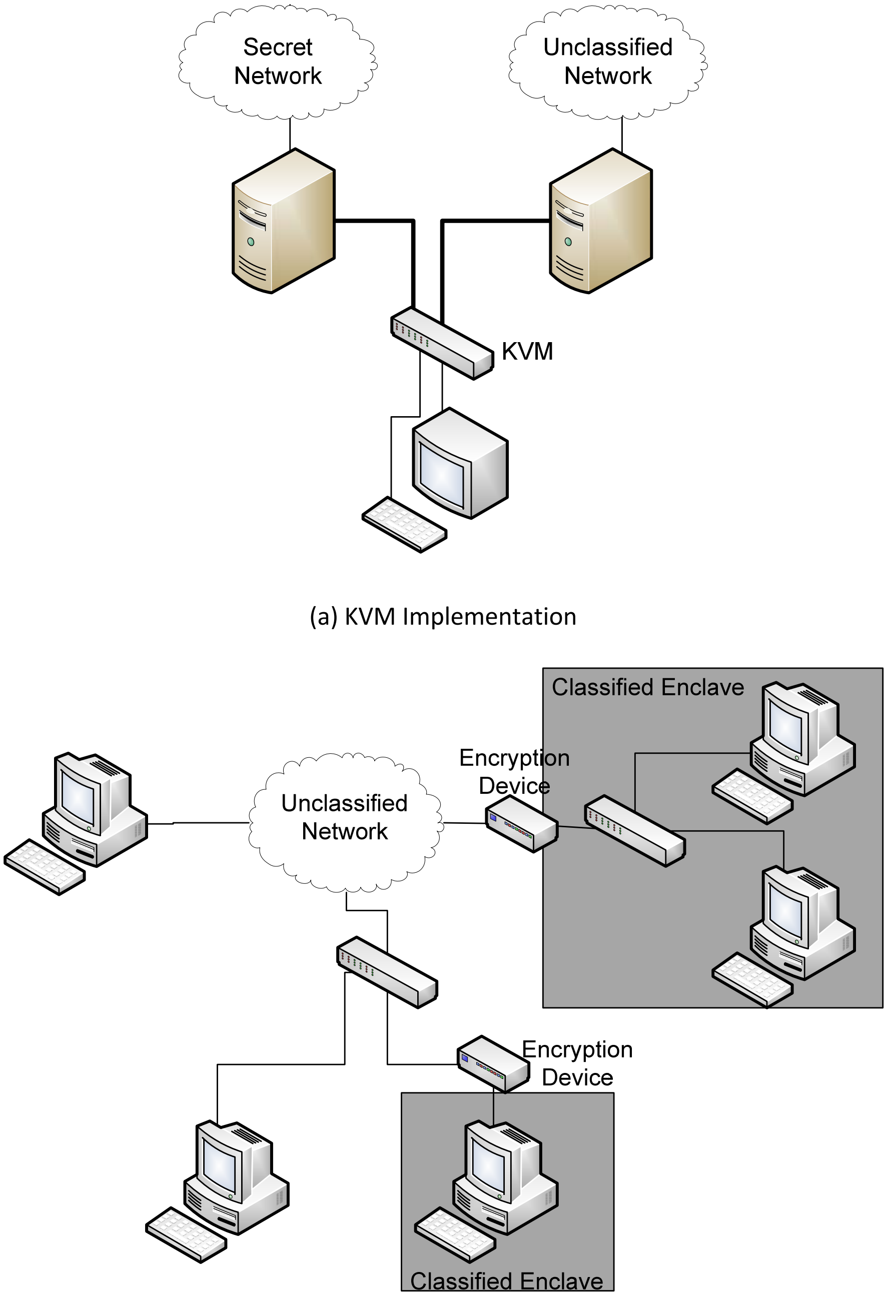
(a) Multiple users accessing a single shared computer

(b) Multiple local shared systems accessing shared resources

(c) Multiple local networks interconnected

Figure 1. Shared Computer Environments

There are technologies in use today that allow for parts of the system infrastructure to be shared. For example, the DoD has approved the use of Keyboard Video Mouse (KVM) switches, like Avocent's Switchview SC-100 and -200, to reduce the number of peripheral devices a user would need.[12] The use of encryption devices, like General Dynamics' Taclane (KG-175), allows the reuse of network infrastructure by encoding classified information for transmittal on networks with lower classification levels.[13] Figure 2 shows examples of shared infrastructure.



(a) KVM Implementation

(b) Layered Security with Encryption Devices

Figure 2. Examples of Shared Infrastructure

Though the tools available to reduce the infrastructure are helpful, they do not change the fact that the user is working within multiple, discreet classification levels. The DoD defines the *multi-security level* environment as one that "data of multiple security levels are processed and transferred by the system, which also separates the different security levels and controls access to the data."[14]

The DoD recognizes four distinct operating modes for information systems that contain various classification levels of information: dedicated, system high, partitioned, and multi-level. In a *dedicated* system, all users of the system are authorized access to any of the information that resides on the system. Essentially, the only protection required of the system is access, which can be provided by physical perimeter security. For access to a *system high* system, all of the users are required to have the same clearance level. The user may not have the need to know all the information stored on the system, so mechanisms are in place to prevent information from being disclosed to unauthorized users. Security permissions in today's multiuser operating systems are sufficient for protection. The responsibility of ensuring the permissions are correctly defined lies with the information owner. The *partitioned* system is a special class, as it is similar to system high in that all users have the same clearance level, but at the Top Secret security level, information is also partitioned into special access programs, or *compartmentalized*. Additional protection requirements are required for this operating mode. The *multi-level* system is the unique case, however, because the requirement that all users be cleared to the same clearance level is not enforced. This operating mode has been demonstrated to accrediting authorities that an authorized user can access information cleared for release at his clearance level and below. Likewise, users are unable to access information on the system that is classified at a higher security level.[15]

Techniques for Creating Information Interchanges

Achieving true multi-level security remains an elusive objective today. Partial solutions exist that provide a level of information exchange between networks. The following technologies are defined (in order of complexity) in detail: hosts, guards, workstations, networks, database management systems, and systems.

Host. The host is the basic building block of a multi-level secure system. It is the combination of trusted operating systems and hardware that allows trusted applications (e.g. file servers, e-mail servers, database servers, and print servers) to run while preventing information of higher classification levels to seep into processes running at lower clearance levels. An example of a multi-level secure host currently in development is the Navy Postgraduate School's MYSEA project which utilizes a DigitalNet XTS-400 server and DigitalNet's STOP operating system.[16]

Guard. High assurance guards pass information either uni- or bi-directionally between two networks. Uni-directional guards guarantee that information only goes in one direction, but limits the effectiveness of today's computer protocols which require two-way communication for passing acknowledgement messages. Bi-directional guards allow information to be passed back to the originating system. Typically, both types of guards are implemented for low-to-high transmission of information. One of the first implementations of a mail guard was Honeywell's Secure Communications Processor, or SCOMP, in 1983.[17] Its development became a model for the US governments Trusted Computer Systems Evaluation Criteria, or *Orange Book*.[18] The Defense Messaging System, for example, uses the High Assurance Guard to enforce transmission security rules.[19] In August of 2007, Trusted Computer Solutions announced significant improvements in their bi-direction secure gateway with the addition of a secure version of Red Hat Linux.[20]

Workstation. A multi-level secure workstation is a terminal device used for processing information at different classification levels. A system cleared at the secret level may contain information at the confidential or unclassified levels, but that is not sufficient to be multilevel secure. The workstation must provide mechanisms for labeling and data segregation. Multi-level secure workstations can be connected to a multi-level secure network or, as Trusted Computer Solutions' Trusted Workstation does, connect to multiple single level networks.[21]

Network. At the physical level, the network is only concerned with passing electrical or optical signals from one system to the next—data is being moved, not information. The multi-level secure network is concerned with how the data is reconstructed and protected. If network devices allow routing of classified information to devices that are not cleared without protecting the information with encryption, then it is possible for that information to be routed anywhere. When a multi-level secure network is constructed, engineers must consider design issues such as protected distribution systems to house cabling, infrastructure for tamper prevention, and detection appropriate for the highest security level on the network.

Database Management System (DBMS). The multi-level secure DBMS provides the most powerful application for system users. The DBMS provides "the management, storage, and retrieval of multiple levels of related data, allowing users of different security levels to have access to a shared set of data according to their individual authorizations."[22] This environment provides users the ability to search through information in a standard method while eliminating the possibility of inconsistent data sets. A user would only see data at the appropriate clearance level, but changes made to that data by a user at a higher level would be instantly available to all users cleared to access it. Databases have traditionally allowed designers to mask attributes, or columns of data in a table, from different groups of users.

Using a fictional intelligence database as an example, consider a table that provides for the storage of records made up of the following attributes: date acquired, imagery data, longitude, latitude, analyst's narrative description and source tag. If the "source tag" is classified top secret, but the other data fields are classified secret, attribute masking would allow users at the top secret level to view all the fields and the user at the secret level to view only the secret fields. Further, the secret user would only be aware of the secret columns of data; nothing in the system would allow the user to have knowledge of the classified attribute. This would apply to the entire set of data in the table, however, so the database engineer has made the decision *a priori* the classification level of the data that is being stored. With the release of Oracle 10, the DBMS became capable of natively masking rows of data based on label security.[23]

This is a significant improvement for DBMSs, because the function of restricting records, or a row of data, used to be a function of the database engineer's query design. Traditionally, a query filters out the data that the requestor needs to see and creates a record set. The query runs against the entire set of data. If the user is able to manipulate the query command, there are no other protections to restrict the record set. Oracle 10 made the security labeling native to the DBMS. The baseline table that a user will be able to query will be filtered to only the information at the appropriate security level without requiring the query command to be constructed with that particular filter. Referring back to the fictional intelligence database example, the analyst inputting the data would determine the classification of each attribute and overall classification for the record. A secret user would only have access to data classified secret and below. If the analyst has created a record initially classified top secret but is later reclassified at a lower level, the record becomes available to lower level users.

Threats to Information Protection

Whether information resides on a traditional or multilevel security computer network, protection of the information is critical. Joint Publication 3-13, *Information Operations*, describes information assurance as the "measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation."[24] Three common threats to these five pillars of information assurance are denial of service, data disclosure, and corruption of data.

Denial of Service. Preventing the availability of information is the objective of a denial of service attack. This is a threat that can occur from internal or external sources, and, because of the complexity of information systems, a computer network is a target rich environment. Figure 3 illustrates a simple computer network with potential vulnerabilities.

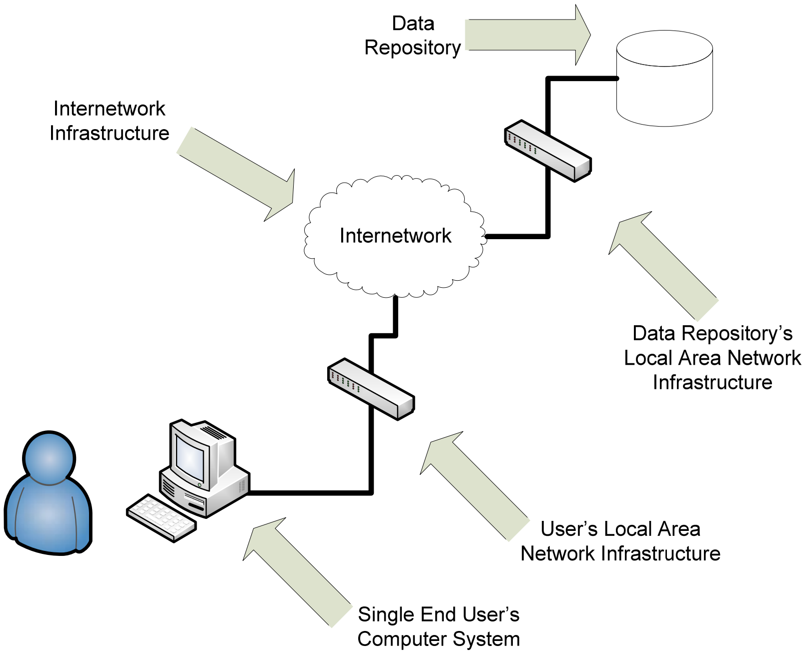

Data Repository
Internetwork Infrastructure
Internetwork
Data Repository's Local Area Network Infrastructure
User's Local Area Network Infrastructure
Single End User's Computer System

Figure 3. Vulnerabilities to Denial of Service

The vulnerabilities annotated in figure 3 are each a point of failure and susceptible to a variety of denial of service attacks. For a single user (as depicted), an attack on any point denies the user access to the data repository. Considering a system with many users, the impact of an attack increases when the vulnerability exploited is closer to the data repository.

System designers allow for redundancy and recovery in their designs to ensure availability. Redundancy eliminates single points of failure within the system, while consideration of recovery deals with the time it takes to repair or replace a component. It may not be practical to have a 100% redundant system as designers must balance cost and the users' tolerance to system outage.

Potential attacks can be significantly varied. There are two types of insider threats. The nefarious attacker intentionally introduces sabotage into the system. On the other hand, unintentional acts by a reckless or an inexperienced user opens the system to all manners of disaster. For example, poor system administration leaves known security vulnerabilities unresolved and even the least sophisticated hacker can find scripts to attack those vulnerabilities. Additionally, poorly trained system administrators can make mistakes during preventative maintenance (or fail to conduct preventative maintenance) that negatively impact the networks performance.

Data Disclosure. The prevention of data disclosure to unauthorized people is the objective of confidentiality. Confidentiality is not focused on any particular security level and the techniques for protecting information at the unclassified level are the same as for top secret (though the tools used are different).

Encryption is the primary method for ensuring confidentiality. DoD networks utilize bulk encryption of all network traffic transmitted outside of an installation's metropolitan area network. Additionally, user-to-user communications, like e-mail, can be protected with Public Key Infrastructure encryption. Mechanisms also exist for encrypting file systems on storage media, like hard drives, flash drives and discs. If properly applied, these tools significantly reduce the likelihood of inappropriate data disclosure. Many times, however, system users fail to use encryption and the information is unintentionally left unprotected.

Confidentiality can also be defeated by nefarious users. The inside threat is generally a difficult problem to solve. The military attempts to prevent this threat by screening employees prior to approving security clearances. Additionally, physical security measures are in-place to prevent material from being taken out of approved areas; however, no process can guarantee confidentiality.

Another data disclosure problem facing information assurance specialists is steganography. A technique for hiding messages within messages used for centuries, steganography is the practice of hiding data within other data files without making an observable change.[25] The phenomenon is usually seen in multimedia files such as pictures, audio and video files. Since data encoding techniques are designed with future enhancements in mind, parts of a data stream can be identified to be used to carry a payload. As an example, today's computer displays easily support a 16 million color palette which means that each pixel of a picture is composed of three 256-bit values representing the red, blue and green (RBG) components of color. The basic alphabet can be encoded with eight bits. By using eight bits out of each RBG component, 512 colors are eliminated from the 16 million color palette, but three letters of a message can be encoded in each pixel. A one inch by two inch digital color photo contains approximately 31,000 pixels. Based on this steganography scheme, a 90,000 character message could be embedded in the photo without significantly altering the look of the photo or changing the size of the digital file. Software tools are specifically designed for steganography, but other software can do this unintentionally as well.

The latest version of Microsoft Word can allow for data disclosure by way of its Track Changes feature. Take for example, the situation of a user trying to prepare a document to go from a high system to a low system. The user is very contentious about redacting any classified information, but because the system maintains previous versions of the document the classified information is still in the data file. Trusted Computer Solutions has developed a tool to scan hidden data that is included as part of its multidirectional gateway, but it will only be able to find what the designers program it to discover.[26] New software and revisions of trusted software immediately introduce new vulnerabilities to data transfer and confidentiality.

Corruption of Data. Users of information systems expect the data they store and process will not be changed inappropriately. In an information system, data can be corrupted at three different places in the process (see figure 4). The remaining three pillars—integrity, authentication, and nonrepudiation—applied in concert with one another protect information systems from being corrupted.

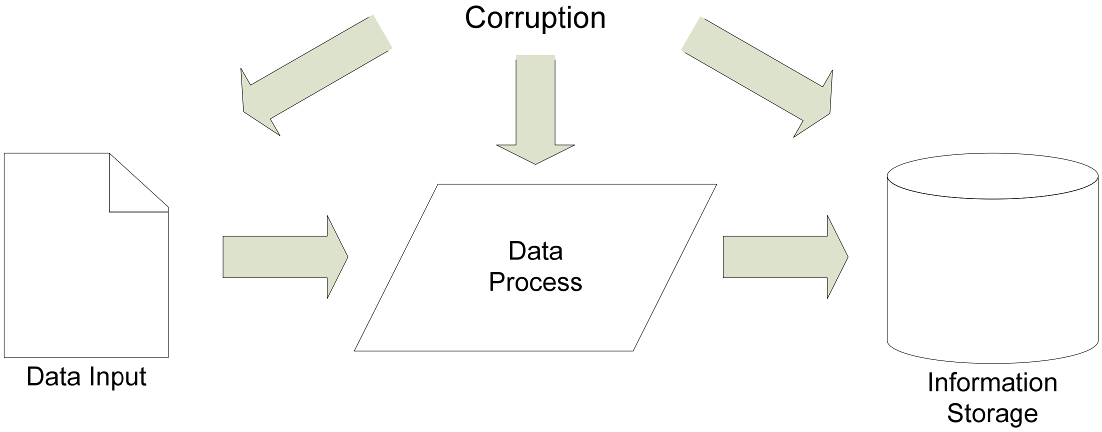


Figure 4. Vulnerabilities to Data Corruption

Tools to implement authentication and non-repudiation are used to protect information on either end of the data processing cycle. Authentication is the process of restricting access to systems to only authorized users (human or machine). Methods of authentication tests users for something they know (username and password or personal identification numbers), something they are (biometrics), or something they have (smart cards). Non-repudiation is the process of guarantying the originator of the data. A common application of non-repudiation is the use of a digital signature. Digital signatures make use of an infrastructure that provides for public and private key issuance (which may be loaded onto smart cards for a higher degree of protection), and third-party validation of the originator's identity. These tools help ensure the data provided to the system or returned from the system is valid.

To protect the data within the process, systems are designed and tested to ensure that when data is processed it is modified in a defined and expected process. As an elementary example, a calculator that performs the addition function on two numbers, such as 3+3, results in the expected answer (i.e. 6). The system assumes the data provided will be correct and provides the result based on its programming.

3. Applying the Technology to the Information Interchange Challenge

Proposed Solutions

In the post-9/11 environment, the ability to quickly identify, analyze, share, synchronize and act on information can mean the difference between life and death. Take as an example the following scenario from the Director of National Intelligence:

> In the spring of 2005, the CIA and the military's Northern Command received information about two passengers aboard a plane flying from the Middle East to Mexico that would shortly cross U.S. airspace. Because the flight was not operated by a U.S. carrier and was not scheduled to land in the United States, there was no requirement for the passenger list to be reviewed prior to takeoff. Although the airline's ticket agent thought the two passengers appeared suspicious, the flight departed before their names could be checked. The airline passed on the names and the flight information to U.S. authorities, however, and this information was funneled to the National Counterterrorism Center, the U.S.

> government's hub for all counterterrorism intelligence, where analysts can access more than 30 separate government computer networks carrying more than 80 unique data sources. Within hours, the NCTC found information indicating that the two passengers had been placed on a "no-fly list" immediately after 9/11 because they had lived in the United States in the 1990s, had connections to two of the 9/11 hijackers, and possessed pilot's licenses. Based on this information, the plane was denied entry into U.S. airspace, and the pilot decided to return to Europe. The intelligence community's real-time coordination and rapid-response capabilities were essential.[27]

The ability to reduce time lags in the processing and exploitation phases of the intelligence collection timeline enhances national leadership's ability to make timely decisions.[28] With the basic concepts of multilevel security, a number of ways exist that the government can implement multilevel security techniques to achieve improved information fusion. For the purpose of discussion, the following assumptions are made regarding the requirements of the system:

- the intelligence community and military's primary information system resources reside on the classified high side,
- the state, local and tribal entity's primary information system resources reside on the Controlled Unclassified Information (formerly Sensitive But Unclassified) level, and
- information will flow in both directions.[29]

With these assumptions made, consider three possible implementations of multilevel secure information systems.

<u>Multidomain Mail Service</u> – The first possible implementation is a multidomain mail service. For this option, the mail server is the only interconnection of the various networks. Benefits of this implementation include a low entry cost for all organizations as the mail service suite is the only equipment needed and a single controlled interface for management. A major drawback to this approach is unintentional disclosure. An approach to mitigate this risk involves

a *validator* (either software or a human) for reviewing messages prior to release. A conceptual diagram is available at figure 5.

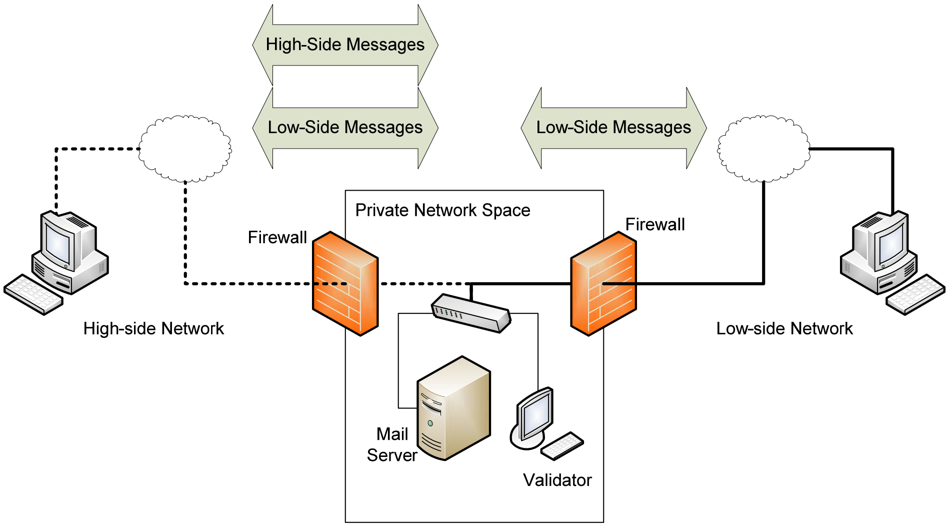


Figure 5. Multidomain Mail Server

Analysts Workstation – The second approach is a multilevel security workstation for the analysts. For this implementation, organizations requiring collaboration need access to specialized workstations that interconnect to multiple networks. Additionally, encryption devices are needed to protect the data travelling through the network. Not all organizations will need access to these workstations. Figure 6 illustrates a conceptual design for this implementation.

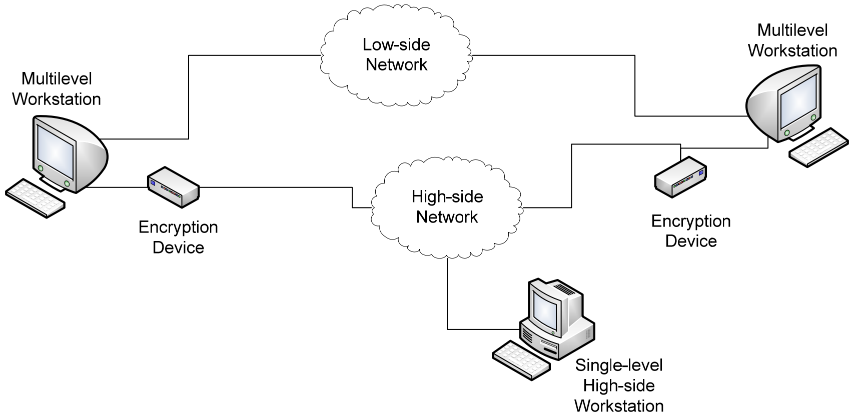


Figure 6. Multilevel Analyst Workstation

Collaboration Environment – The last approach to consider is a more robust implementation that includes tools such as chat, audio and video conferencing, mail and file sharing. Like the Multidomain Mail Server implementation, this is done by attaching single-level networks to a secure enclave. These additional tools, however, open the network to vulnerabilities. For example, adding audio and video conferencing limits the ability to monitor and validate multicasting data streams. See figure 7 for this implementation.

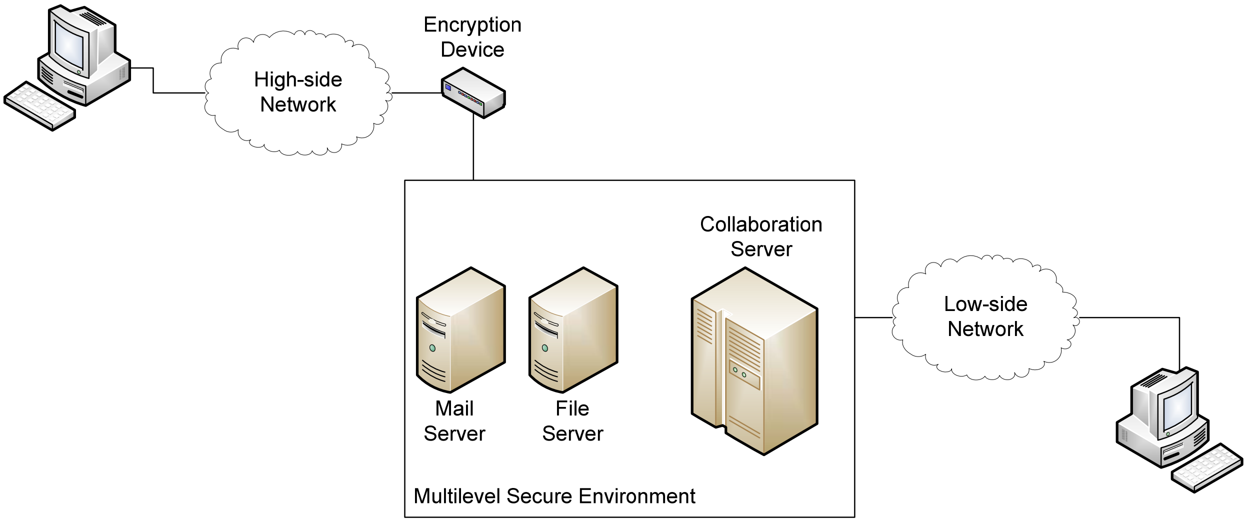


Figure 7. Collaboration Environment

Evaluation Criteria

The three proposed solutions each offer an enhanced collaborative capability for users of multiple security level environments. In order to compare the solutions, an operational risk management (ORM) process is applied. Though operational risk management is typically associated with "preserving assets and safeguarding health and welfare," another goal of ORM is to improve "warfighting effectiveness on the battlefield and in the operational aerospace environment, helping to ensure decisive victory in any future conflict at the least possible cost."[30]

The evaluation follows the six step ORM process: 1) identify the hazard, 2) assess the risk, 3) analyze risk control measures, 4) make control decisions, 5) implement risk controls, and 6) supervise and review.[31] The particular hazards considered in step 1 are: denial of service, data disclosure, and corruption.

In order to review the data, a decision support matrix will be used. A template of the decision support matrix is available at table 1. The following section proceeds through each of the ORM six steps, building the matrix. When the risk assessment is complete, the proposals can be compared for suitability.

Table 1. Decision Support Matrix[32]

Risk No.	**IA Cat** (note 1)	**Hazard**	**Severity** (note 2)	**Prob of Occur** (note 3)	**Risk Level**	**Mitigation Strategy**
Notes: 1. Information Assurance Category (IA Cat): Denial of Service (DS), Unauthorized Disclosure (UD), Corruption (C) 2. Severity: I – Catastrophic, II – Critical, III – Moderate, IV - Negligible 3. Probability of Occurrence (Prob of Occur): A – Frequent, B – Likely, C – Occasional, D – Seldom, E – Unlikely						

4. Evaluation of Solutions

Comparison of Proposed Solutions

The three proposed solutions provide for improved information collaboration. Using the six step ORM methodology, the solutions can be evaluated for suitability. The first step of the process is to identify the hazard. For this problem set, the hazards are based on threats to information assurance—denial of service, unauthorized disclosure, and data corruption. The hazards can be seen in table 2.

Table 2. Decision Support Matrix – Hazards

(a) Multidomain Mail Server

Risk No.	IA Cat (note 1)	Hazard
1	DS	Distributed Denial of Service (DDoS) attack on Low-Side Network Firewall
2	DS	DDoS attack on High-Side Network Firewall
3	DS	DDoS attack on Mail Server
4	DS	Virus on Mail Server
5	DS	Virus on Client System
6	UD	Inappropriately Marked Classified Message
7	UD	Classified Message Sent to Unclassified Account
Note: 1. Information Assurance Category (IA Cat): Denial of Service (DS), Unauthorized Disclosure (UD), Corruption (C)		

(b) Multilevel Analyst Workstation

Risk No.	IA Cat (note 1)	Hazard
1	DS	DDoS attack on Workstation
2	DS	Virus on Workstation
3	DS	Virus on High-Side Network
4	UD	Inappropriately Marked Classified File
5	UD	Classified Information Sent to Unclassified Account
6	UD	Classified Data/Information Stored on Workstation Accessible to Unauthorized Users
7	C	Encryption Device Not Properly Keyed
Note: 1. Information Assurance Category (IA Cat): Denial of Service (DS), Unauthorized Disclosure (UD), Corruption (C)		

(c) Collaboration Environment

Risk No.	IA Cat (note 1)	Hazard
1	DS	DDoS attack on Workstation
2	DS	Virus on Workstation
3	DS	Virus on High-Side Network
4	UD	Inappropriately Marked Classified Message
5	UD	Classified Message Sent to Unclassified Account
6	UD	Classified Data/Information Accessible to Unauthorized Users
7	C	Encryption Device Not Properly Keyed
8	C	File System Corruption
Note: 1. Information Assurance Category (IA Cat): Denial of Service (DS), Unauthorized Disclosure (UD), Corruption (C)		

The next step in the risk management process is to assess the risk for probability of occurrence (Frequent, Likely, Occasional, Seldom or Unlikely) and severity of the impact (Catastrophic, Critical, Moderate, or Negligible). This combination is the risk level involved with the hazard (see figure 8).

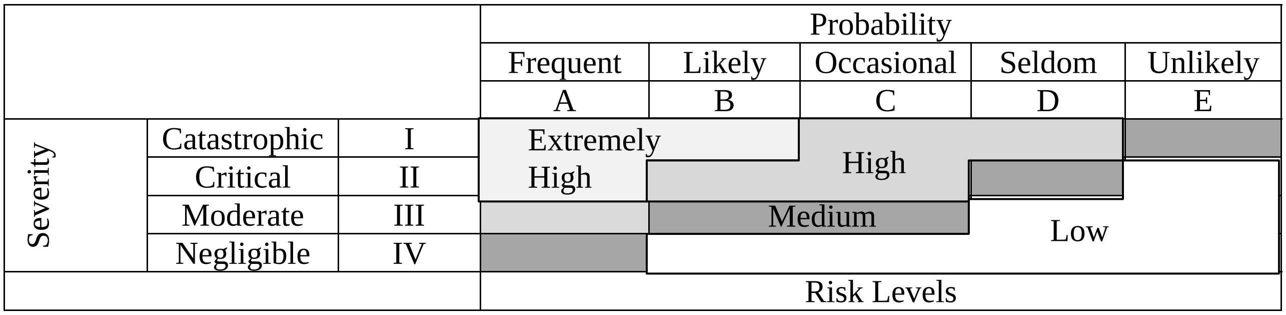


Figure 8. Risk Assessment Matrix[33]

Rating severity and probability for hazards has both an objective and subjective element. One approach to measuring the severity of information assurance hazards considers the number of users impacted by an incident. As the number of potential users increase, the severity rating increases. Measuring the probability of a hazard occurring can be accomplished by comparing statistical data for similar situations. In both cases, however, the assignment of the quantities to the categories is dependent on the system being evaluated.

To determine whether or not the risk is acceptable, one must acknowledge the following points: some level of risk is a reality, this process involves tradeoffs, identifying the risk is not sufficient for safety, and the determination of risk is subjective.[34] The assessment of risk levels of hazards are shown in table 3.

Table 3. Decision Support Matrix – Risk Assessment

(a) Multidomain Mail Server

Risk No.	**IA Cat** (note 1)	**Hazard**	**Severity** (note 2)	**Prob of Occur** (note 3)	**Risk Level**
1	DS	DDoS attack on Low-Side Network Firewall	III	D	Low
2	DS	DDoS attack on High-Side Network Firewall	III	E	Low
3	DS	DDoS attack on Mail Server	II	E	Low
4	DS	Virus on Mail Server	II	C	High
5	DS	Virus on Client System	III	C	Medium
6	UD	Inappropriately Marked Classified Message	II	C	High
7	UD	Classified Message Sent to Unclassified Account	II	D	Medium

Notes:

1. Information Assurance Category (IA Cat): Denial of Service (DS), Unauthorized Disclosure (UD), Corruption (C)
2. Severity: I – Catastrophic, II – Critical, III – Moderate, IV - Negligible
3. Probability of Occurrence (Prob of Occur): A – Frequent, B – Likely, C – Occasional, D – Seldom, E – Unlikely

(b) Multilevel Analyst Workstation

Risk No.	**IA Cat** (note 1)	**Hazard**	**Severity** (note 2)	**Prob of Occur** (note 3)	**Risk Level**
1	DS	DDoS attack on Workstation	III	C	Medium
2	DS	Virus on Workstation	III	C	Medium
3	DS	Virus on High-Side Network	II	D	Medium
4	UD	Inappropriately Marked Classified File	II	C	High
5	UD	Classified Information Sent to Unclassified Account	II	D	Medium
6	UD	Classified Data/Information Stored on Workstation Accessible to Unauthorized Users	II	C	High
7	C	Encryption Device Not Properly Keyed	III	D	Low
Notes: 1. Information Assurance Category (IA Cat): Denial of Service (DS), Unauthorized Disclosure (UD), Corruption (C) 2. Severity: I – Catastrophic, II – Critical, III – Moderate, IV - Negligible 3. Probability of Occurrence (Prob of Occur): A – Frequent, B – Likely, C – Occasional, D – Seldom, E – Unlikely					

(c) Collaboration Environment

Risk No.	**IA Cat** (note 1)	**Hazard**	**Severity** (note 2)	**Prob of Occur** (note 3)	**Risk Level**
1	DS	DDoS attack on Workstation	III	C	Medium
2	DS	Virus on Workstation	III	C	Medium
3	DS	Virus on High-Side Network	II	D	Medium
4	UD	Inappropriately Marked Classified Message	II	C	High
5	UD	Classified Message Sent to Unclassified Account	II	D	Medium
6	UD	Classified Data/Information Accessible to Unauthorized Users	II	C	High
7	C	Encryption Device Not Properly Keyed	III	D	Low
8	C	File System Corruption	II	C	High
Notes: 1. Information Assurance Category (IA Cat): Denial of Service (DS), Unauthorized Disclosure (UD), Corruption (C) 2. Severity: I – Catastrophic, II – Critical, III – Moderate, IV - Negligible 3. Probability of Occurrence (Prob of Occur): A – Frequent, B – Likely, C – Occasional, D – Seldom, E – Unlikely					

The next two steps are analyzing risk control measures and making control decisions. Hazards need to be prioritized to determine which hazards must be mitigated to reach an acceptable level. For the purpose of this analysis, all of the hazards will have a control measure identified. The mitigation strategy for each hazard is shown in table 4.

Table 4. Decision Support Matrix – Mitigation Strategies

(a) Multidomain Mail Server

Risk No.	**IA Cat** (note 1)	**Hazard**	**Severity** (note 2)	**Prob of Occur** (note 3)	**Risk Level**	**Mitigation Strategy**
1	DS	DDoS attack on Low-Side Network Firewall	III	D	Low	- Utilize a Virtual Private Network to restrict network access to authorized systems
2	DS	DDoS attack on High-Side Network Firewall	III	E	Low	- Existing infrastructure should minimize risk to external DDoS attacks - Ensure virus detection software is installed on network devices to minimize risk of DDoS agent being installed on infrastructure
3	DS	DDoS attack on Mail Server	II	E	Low	- Utilize a Virtual Private Network to restrict network access to authorized systems - Ensure virus detection software is installed on network devices to minimize risk of DDoS agent
4	DS	Virus on Mail Server	II	C	High	- Ensure virus detection software is installed on network devices to minimize risk of virus
5	DS	Virus on Client System	III	C	Medium	- Ensure virus detection software is installed on network devices to minimize risk of virus
6	UD	Inappropriately Marked Classified Message	II	C	High	- Utilize a classification marking tool in conjunction with e-mail software - Establish message release procedures to include message review - Ensure message logging and auditing is available
7	UD	Classified Message Sent to Unclassified Account	II	D	Medium	- Utilize a classification marking tool in conjunction with e-mail software - Establish message release procedures to include message review - Ensure message logging and auditing is available - Utilize a message validator to review messages prior to release to lower classified network - Establish system scrubbing procedures for rapid recovery from spillage

Notes:

1. Information Assurance Category (IA Cat): Denial of Service (DS), Unauthorized Disclosure (UD), Corruption (C)
2. Severity: I – Catastrophic, II – Critical, III – Moderate, IV - Negligible
3. Probability of Occurrence (Prob of Occur): A – Frequent, B – Likely, C – Occasional, D – Seldom, E – Unlikely

(b) Multilevel Analyst Workstation

Risk No.	**IA Cat** (note 1)	**Hazard**	**Severity** (note 2)	**Prob of Occur** (note 3)	**Risk Level**	**Mitigation Strategy**
1	DS	DDoS attack on Workstation	III	C	Medium	- Existing infrastructure should minimize risk to external DDoS attacks - Ensure virus detection software is installed on network devices to minimize risk of DDoS agent being installed on infrastructure
2	DS	Virus on Workstation	III	C	Medium	- Ensure virus detection software is installed on network devices to minimize risk of virus
3	DS	Virus on High-Side Network	II	D	Medium	- Ensure virus detection software is installed on network devices to minimize risk of virus
4	UD	Inappropriately Marked Classified File	II	C	High	- Utilize a classification marking tool in conjunction with e-mail software - Establish message release procedures to include message review - Ensure message logging and auditing is available
5	UD	Classified Information Sent to Unclassified Account	II	D	Medium	- Utilize a classification marking tool in conjunction with e-mail software - Establish release procedures to include review - Ensure logging and auditing is available - Establish system scrubbing procedures for rapid recovery from spillage
6	UD	Classified Data/Information Stored on Workstation Accessible to Unauthorized Users	II	C	High	- Ensure access control permissions are set correctly - Ensure logging and auditing file access is available - Establish scrubbing procedures for rapid recovery from spillage
7	C	Encryption Device Not Properly Keyed	III	D	Low	- Establish procedures for synchronizing and validating encryption keys

Notes:

1. Information Assurance Category (IA Cat): Denial of Service (DS), Unauthorized Disclosure (UD), Corruption (C)
2. Severity: I – Catastrophic, II – Critical, III – Moderate, IV - Negligible
3. Probability of Occurrence (Prob of Occur): A – Frequent, B – Likely, C – Occasional, D – Seldom, E – Unlikely

(c) Collaboration Environment

Risk No.	**IA Cat** (note 1)	**Hazard**	**Severity** (note 2)	**Prob of Occur** (note 3)	**Risk Level**	**Mitigation Strategy**
1	DS	DDoS attack on Workstation	III	C	Medium	- Existing infrastructure should minimize risk to external DDoS attacks - Ensure virus detection software is installed on network devices to minimize risk of DDoS agent being installed on infrastructure
2	DS	Virus on Workstation	III	C	Medium	- Ensure virus detection software is installed on network devices to minimize risk of virus
3	DS	Virus on High-Side Network	II	D	Medium	- Ensure virus detection software is installed on network devices to minimize risk of virus
4	UD	Inappropriately Marked Classified Message	II	C	High	- Utilize a classification marking tool in conjunction with e-mail software - Establish release procedures to include review - Ensure logging and auditing is available
5	UD	Classified Message Sent to Unclassified Account	II	D	Medium	- Utilize a classification marking tool in conjunction with e-mail software - Establish release procedures to include review - Ensure logging and auditing is available - Utilize a message validator to review messages prior to release to lower classified network - Establish system scrubbing procedures for rapid recovery from spillage
6	UD	Classified Data/Information Accessible to Unauthorized Users	II	C	High	- Ensure access control permissions are set correctly - Ensure logging and auditing file access is available - Establish scrubbing procedures for rapid recovery from spillage
7	C	Encryption Device Not Properly Keyed	III	D	Low	- Establish procedures for synchronizing and validating encryption keys
8	C	File System Corruption	II	C	High	- Ensure virus detection software is installed on network devices to minimize risk of virus or Trojan horse infection

Notes:

1. Information Assurance Category (IA Cat): Denial of Service (DS), Unauthorized Disclosure (UD), Corruption (C)
2. Severity: I – Catastrophic, II – Critical, III – Moderate, IV - Negligible
3. Probability of Occurrence (Prob of Occur): A – Frequent, B – Likely, C – Occasional, D – Seldom, E – Unlikely

The last two steps of the ORM process are outside of the scope of this research as they are applied during the actual implementation of the system. The "Implement Risk Controls" step requires that mitigation plans identified above are incorporated into the system. Finally, during the "Supervise and Review" step, system administrators must continue to ensure the control measures and mitigation plans.

Identified Weaknesses

The Decision Support Matrix identifies the risk involved with possible solutions for using multi-level security to improve information sharing. This process allows designers to deliberately think about the challenges the systems must overcome. One of the most difficult problems across all the solutions is the defense against nefarious insider threats. These threats exist during any information systems implementation.

Based on the analysis above, denial of service and unauthorized disclosure are the predominant hazards identified. By creating interfaces between low-side and high-side networks, there is an inherent risk that hazards will occur. Since guaranteeing information will be protected from all threats to information assurance is unrealistic, it is more important to put measures in-place to identify when the hazards occur in order to recover. This is as true for multi-level secure networks as it is for single level networks.

5. Conclusion

Improving the information sharing culture following the terrorist attacks of September 11, 2001, became a major emphasis of the Bush administration. Tasked to the ODNI, the ISE initiative set out to define common architectures for sharing information between foreign and domestic intelligence collection agencies. One technology that offers the government improved information sharing is multi-level security. Though research into multi-level security goes back to 1973 with the Air Force's quest to find a formal security policy, the implementations of multi-level secure systems have been few.[35]

The holy grail of multi-level security solutions still remains elusive, but the last four decades of research has significantly contributed to the field of information assurance. A number of solutions exist that meet many of the requirements to improve multi-domain collaboration, but there are still potential risks. ODNI recognizes that to change the culture from "need to know" to "responsibility to provide" means those risks need to be accepted and mitigated.

This research demonstrates that by following the ORM process, with particular attention to the principles of information assurance, systems can be adequately evaluated for suitability. Since ORM considers the system over its entire lifecycle, system designers can put non-technical and procedural mitigation steps into place. With well-defined controls in place, systems can be developed to meet operational requirements.

Notes

[1] Relyea, "Security Classified and Controlled Information," 4.

[2] 9/11 Commission, "The 9/11 Commission Report," 416-417.

[3] Randol, "Homeland Security Intelligence," 1.

[4] Bush, *National Strategy for Information-Sharing*, 2.

[5] Ibid., 3-4.

[6] McConnell, *United States Intelligence Community Information Sharing Strategy*, 8.

[7] McConnell, *United States Intelligence Community 500 Day Plan for Integration and Collaboration*, 6.

[8] ISE, "ISE Architecture Program."

[9] McConnell, *United States Intelligence Community Information Sharing Strategy*, 8.

[10] Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 140.

[11] Smith, "Introduction to Multilevel Security."

[12] Avocent, "SwitchView SC100 & SC200 KVM Switches Enhance Security at the Desktop," 1.

[13] General Dynamics, "Taclane Encryptor (KG-175)," 1.

Notes

[14] DoD Multilevel Security Program, "Multilevel Security in the DoD."

[15] Ibid.

[16] Irvine, et al., "Overview of a High Assurance Architecture, 39.

[17] Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 146.

[18] Ibid., 147.

[19] CNSS Instruction 4009, *National Information Assurance Glossary*, 30.

[20] "Trusted Computer Solutions Releases New Trusted Gateway."

[21] TCS, "Secure Trusted Workstation."

[22] DoD Multilevel Security Program, "Multilevel Security in the DoD."

[23] Oracle Corporation, "Oracle 10g Release 2 Defense-in-Depth Security," 5-6.

[24] JP 3-13, *Information Operations*, II-5.

[25] Westphal, "Steganography Revealed."

[26] "Trusted Computer Solutions Releases New Trusted Gateway."

[27] McConnell, "Overhauling Intelligence."

[28] JP 2-01, *Joint and National Intelligence Support to Military Operations*, III-28.

[29] Bain, "Sensitive but Unclassified Category Simplified."

[30] AFI 90-901, *Operational Risk Management,* 1-2.

[31] Ibid., 3.

[32] Based on the ORM Risk Matrix developed by MITRE, for more information on the MITRE's implementation can be found at MITRE, *Risk Matrix User's Guide*, 15.

[33] AFPAM 90-902, *Operational Research Management (ORM) Guidelines and Tools*, 19.

[34] Ibid., 9.

[35] Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 139.

Bibliography

9/11 Commission. "The 9/11 Commission Report." 9/11 Commission. http://www.9-11commission.gov/report/911Report.pdf (accessed 10 November 2008).

Air Force Instruction (AFI) 90-901. *Operational Risk Management*, 1 April 2000.

Air Force Pamphlet (AFPAM) 90-902. *Operational Risk Management (ORM) Guidelines and Tools*, 14 December 2000.

Anderson, Ross J. *Security Engineering: A Guide to Building Dependable Distributed Systems.* Second Edition, Wiley, NY, 2008. http://www.cl.cam.ac.uk/~rja14/Papers/SE-07.pdf (accessed 5 November 2008).

Avocent. "SwitchView SC100 & SC200 KVM Switches Enhance Security at the Desktop," Avocent. http://www.avocent.com/uploadedFiles/Avocent_Resources/Data_Sheets/1007-SVSECURE-DS.PDF (accessed 25 January 2009).

Bain, Ben. "Sensitive but Unclassified Category Simplified, " *Federal Computer Week*; 12 May 2008. http://fcw.com/Articles/2008/05/12/Sensitive-but-unclassified-category-simplified.aspx (accessed 9 February 2009).

Bush, George W. *National Strategy for Information Sharing*. Washington, White House, October 2007.

Committee on National Security Systems (CNSS) Instruction 4009. *National Information Assurance Glossary*, June 2006.

DoD Multilevel Security Program. "Multilevel Security in the Department of Defense: The Basics," National Security Institute. http://nsi.org/Library/Compsec/sec0.html (accessed 5 November 2008).

General Dynamics. "Taclane Encryptor (KG-175): Worldwide Deployment and Support," General Dynamics C4 Systems. http://www.gdc4s.com/documents/TACLANE_PIB1.pdf (accessed 25 January 2009).

Information Sharing Environment (ISE). "ISE Architecture Program." Office of the Director of National Intelligence. http://www.ise.gov/pages/eaf.html (accessed 15 November 2008).

Irvine, Cynthia, Timothy Levin, Thuy Nguyen, David Shifflett, Jean Khosalim, Paul Clark, Albert Wong, Francis Afinidad, David Bibighaus, and Joseph Sears. "Overview of a High Assurance Architecture for Distributed Multilevel Security." *Proceedingd of the 5th IEEE Systems, Man and Cybernetics Information Assurance Workshop*, United States Military Academy, West Point, NY (10-11 June 2004): pp 38-45.

Joint Publication (JP) 2-01, *Joint and National Intelligence Support to Military Operations.* 7 October 2004.

JP 3-13, *Information Operations*. 13 February 2006.

McConnell, Mike. "Overhauling Intelligence." *Foreign Affairs*, July/August 2007. http://www.foreignaffairs.org/20070701faessay86404/mike-mcconnell/overhauling-intelligence.html (accessed 4 February 2009).

———. *United States Intelligence Community 500 Day Plan for Integration and Collaboration*. Washington, DC: Office of the Director of National Intelligence. http://www.odni.gov/500-day-plan.htm (accessed 9 November 2008).

———. *United States Intelligence Community, Information Sharing Strategy*. Washington, DC: Office of the Director of National Intelligence, February 22, 2008.

MITRE, *Risk Matrix User's Guide Version 2.2*. Bedford, MA: MITRE Corporation. http://www.mitre.org/work/sepo/toolkits/risk/ToolsTechniques/files/UserGuide220.pdf (accessed 3 February 2009).

Oracle Corporation. "Oracle 10g Release 2 Defense-in-Depth Security," Oracle Corporation. http://www.oracle.com/database/docs/bwp_security_db_database_10gR2_0508.pdf (accessed 3 February 2009).

Randol, Mark A. *Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches*. CRS Report 7-5700. Washington, DC: Congressional Research Service, 2009.

Relyea, Harold C. "Security Classified and Controlled Information: History, Status, and Emerging Management Issues." Congressional Research Service, 11 February 2008. http://assets.opencrs.com/rpts/RL33494_20080211.pdf (accessed 4 November 2008).

Smith, Rick. "Introduction to Multilevel Security." University of St. Thomas Computer and Information Sciences. http://www.cs.stthomas.edu/faculty/resmith/r/mls/index.html (accessed 5 November 2008).

Trusted Computer Solutions. "Secure Trusted Workstation," Trusted Computer Solutions. http://www.tcs-sec.com/documents/SOTrustedWorkstationSolFS.pdf (accessed 29 January 2009).

"Trusted Computer Solutions Releases New Trusted Gateway," *M2 Wireless News*. 29 Aug 2007.

United States Joint Forces Command (USJFCOM). "Multinational Information Sharing and the Cross-Domain Collaborative Information Environment," United States Joint Forces Command. http://www.jfcom.mil/about/fact_cdcie.html (accessed 8 February 2009).

Westphal, Kelly. "Stegonography Revealed," *Security Focus*. 9 April 2003. http://www.securityfocus.com/infocus/1684 (accessed 8 February 2009).